Alexander-
I am responding to "FYI" FDIC RIN 3064-ZA18.
I will answer - partially - Question's 5; 8; 9; 10; 11; 13-25 (inclusive).

I am trying to get this to you by end-of-day today (as this is your "close" deadline).

The two documents are being sent to you in support of our answers:
1) OCC Response Document JEC FINAL.pdf
2) ACPR FINAL.pdf*
*[under separate email cover].

In short, our interest in the "FYI" FDIC RIN 3064-ZA18 is due to the fact it dovetails with much which we have already shared with the OCC and ACPR already. Advanced Systems Management Group (ASMG) have a twenty plus + year service record in standards ratification efforts. We are the authors of the Object Management Group (OMG) standards-body certified Information Exchange Framework (IEF) Reference Architecture (RA) for data -centric security (DCS). Our solution applies to big data contexts, FinTechs, your community [insured depository institutions/IDEs and community banks] for starters.

The OCC Digital Asserts Review drew very widely from financial sector disruptors, which is why we are sending your our Report for the OCC. As well, we responded to the Banque du France (ACPR) comments exercise as well. That report is also enclosed.

You may also wish to speak with Mark Montoya, at your organization (FDIC), who was in touch with us as an OMG standards body member Company earlier this summer.

Since I am pressed for time, only having seen your "FYI call-up" at 10:00 am this morning eastern standard time, I am answering in an abbreviated fashion.

The following Question's will receive brief responses:

Q5. 'challenges for insured depository institutions (IDEs)/community banks' a.k.a. [point 3]: 'information sharing and data protection'.
Advanced Systems Management Group (ASMG) possess the definitive solution to this challenge. The Information Exchange Framework (IEF) Reference Architecture (RA) is a standardized solution to this very topic. The OCC and ACPR Submissions address this issue in detail. This solution is available to be Demo'ed now. Please be advised, the defense sector are in advanced testing stages, and the financial supervisory authority (such as yourselves at the FDIC) would be in a prime 'sweet-spot' to benefit from the twenty years worth of ratification effort, already completed. The solution is in 5th Generation of capability today, and is in excellent standing to evaluate.

Q8. 'does voluntary (standards) certification -- undermine innovation?
restrict selection?'
This questions is redundant. The Information Exchange Framework (IEF) Reference Architecture - on which the data-centric security (DCS) solution is standards-body based, has been available for commercial adoption for an extensive period of time. The only way to ensure this does not happen is to go to a quasi-permanent, quasi -mandatory enforcement exercise. ASMG's opinion is that standards certification should be quasi -mandatory enforcement, in general.

Q9. 'Alternative Approach'. ASMG feel you at the FDIC 'insured depository institutions (IDEs)/community banks' - with which you identified your opportunity in the RFI - should be specifying a "quasi-permanent, quasi -mandatory enforcement exercise" for standards to achieve your goals. You should be the enforcer and auditing authority, not a standards-setting organization (SSO). If you allow an SSO to be the judge and jury, ASMG feel you are setting yourselves up for the same disappointment we have endured, as we have witnessed the public and private sector dragging their feet on adopting the DCS paradigm solution.

Q10. 'Other regulatory options'. An excellent template is provided by the Principality of Luxembourg for their defining of Virtual Asset Service Providers (VSAPs) See: OCC Submission Page 256 / Foot Note # 516. See
also: the derivatives regulatory effort in the EC - European Market Infrastructures (EMIR) See: OCC Submission Page 228 / Foot Note # 449.
Both of these supervisory efforts have much to be commended, the VASP (Luxembourg) for its inclusivity of parties to be examined; the derivatives regulation (EMIR) for the 'push' efforts to make data salient and regulatory enforcement actions coherent and effective. Other examples are widely cited throughout the OCC Submission (ASMG).

Q11. 'modeling examples' [a.k.a. to be standardized]. All examples should be addressed, no exemptions allowed (in ASMG's opinion).

Q12. 'which technology and operational aspects are appropriate to be standardized'. ASMG feel wherever their is an existing data store, data asset, a data-centric security (DCS) solution needs to be applied. Without exception.

Q13. 'Challenges / benefits to models [AI & ML] by data processing / big data processing'.
ASMG believe the DCS solution needs to be implemented as an anchor framework. See: ACPR Report Submission by ASMG; plus, answer to Q. 7-OCC Submission (ASMG).

Q14. 'How can FDIC identify / track / monitor Third Party players'.
Simple: determine where data is housed, what is its providence, and all measures regarding a Third Party Player are known. From the DCS, the 3rd Party's - financial condition; cyber security preparedness and operational resilience 'all fall under the FDIC's lens'.

Q15. 'Partnering with an SSO'. Not advised. The FDIC should remain the omnipotent authority with regards to this supervisory activity, an SSO could be in a secondary, non decision-making capacity.

Q16. 'Rapid deployment (several fronts)'. Neutral. The standards approach will not ensure rapid deployment. Trust ASMG - our DCS solution is proof-of-this.

Q17. 'What draft industry standard as a framework.' Data-centric Security (DCS) / OMG Solution. Why? This secures the data asset, and from there all your work is significantly enhanced, and made much easier to accomplish.

Q18. 'Will Third parties cooperate.' NO. They will protect proprietary interests, always. The DCS solution is a non-proprietary solution, requiring a mandatory adoption (and roll-out / implementation). See: ACPR Report Submission by ASMG; plus, Appendix A [and full Report] - OCC Submission (ASMG).

Q19. 'Structure for SSO.' Object Management Group's Special Domain Model (which berthed the DCS solution) is as good a template as any to consult.

Q20. 'governmental levels to be involved'. All levels - with FDIC as the decision-support authority and "Lead" voice only.

Q21. 'Cert org's - benefit?' Answer: negligible.

Q22. 'Cert org's - effective?' Answer: Not really. Some Cert org's are exemplary, but we will not comment further (in this public a manner).
Certification organizations will serve their 'internal clock', and funding source. But if FDIC funds them, be prepared for issues to arise which will seem to swallow up resources, and diffuse your organization's effectiveness. (ASMG's opinion).

Q23. 'model validation by Cert org's - 1) testing - NIST would advise on this; 2) protect intellectual property (Really? Dept. of Commerce may advise, if you absolutely need a 2nd opinion); 3) sensitive business data
- Install DCS solution, and you are fully covered on this point.

Q24. 'Malfeasance'. The FDIC should protect yourselves at all costs. 1) applied rights - under FDIC mandate; 2) how to notify - under FDIC mandate; 3) information sharing agreements - Implement DCS solution, maintained by FDIC.

Q 25. 'Maintain oversight authority within the FDIC.' It is not advised to second this right to an SSO.

I am now sending you our two reports.
Bon Chance!

Jim Carter
ASMG - Toronto (Canada)
carterj@asmg-ltd.com

9/11/2020

OCC Response Document

Title: National Bank and Federal Savings Association Digital Activities
12 CFR Parts 7 & 155 [Docket ID OCC-2019-00288] RIN 155-AE74

Table of Contents

Overview 2

OCC Response Document Questions 14
Q1. – recent technological advances 14
Q2. – Hurdles to tech advance and innovation 23
Q3. – What digital issues not addressed 37
Q4. – Crypto assets / crypto currencies 45
Q5. – Distributed ledger technology (DLT) for banking 53
Q6. – Payment technologies a.k.a. 'getting interoperability right' 101
Q7. – AI / ML security / governance and regulatory complexity 146
7.2 Anti-Money Laundering (AML) / Fraud 157
7.3 Customer ID / Due Diligence 160
7.4 Trading / Hedging 162
7.5 Forecasting / Marketing 164
7.2.1 A Short Diversion: The ACPR AI / ML Report 166
Q8. – RegTech and the OCC: Governance embedded in technology 169
8.1 Trade surveillance 194
8.2 Client onboarding 197
8.3 Investment case management (Investigative case management) 200
8.4 Transaction monitoring 206
Q9. – Considering small institutions and research departments 216
Q10. – What other changes need OCC address 230
Q11. – Changes to banking (post Covid-19) 235
11-1 Cyberthreats 235
11.1.1 Broken access controls 240
11.1.2 XML external entity (failures) 241
11.1.3 Sensitive data exposure 243
11.1.4 Broken architecture 244
11.1.5 Injection (with untrusted communications / data / authorizations) 248
11-2 Apps - Dapps not secure (IoT/mobile) and 'What DLT Data Center?' 253

Appendix A 1
The Solution - 1
Data-Centric Security (DCS) – a.k.a. – ASMG and the IEF 1
The Information Exchange Framework (IEF) Use-Case 1
Operational Analysis for Semantic Interoperability 5
Key elements in the Information Sharing Policy Life-Cycle 8
Overall effect of IEF and IEPPV adoption 9
IEPPV Architecture – 10
Overall ISS Solution 13
Applicability to a Banking Context 18
In Summary 19
What can ASMG Offer? 21

Appendix B 1

Overview

Advanced Systems Management Group (ASMG) are an entity which operates with information security as our primary objective and mission. We have chosen to respond to your invitation for submissions to the OCC Digital Activities Review. The OCC Response Document, titled "National Bank and Federal Savings Association Digital Activities - 12 CFR Parts 7 & 155" sets an ambitious agenda to seek principle-based (not prescriptive), technology-neutral *advance-notice* of *proposed-rulemaking* (ANPR) comments, covering electronic activities of banking (12 CFR part 7, subpart E) and the use of electronic means and facilities (12 CFR part 155) to prepare for regulatory and governance realities you face.

The best we at ASMG[1] can offer *herein*, is to point out benchmarks which would apply, specifically, in the case where the implementation of security (solutions) are required – and (we feel) lacking at present – in the approach we see the international financial community, and international regulatory supervisory authorities and regulatory agencies, are tasked and mandated to pursue.

Our goal in this Submission will be to address all eleven (11) Questions you have raised. Should information be repeated in one section to the next, this repetition may be defended along the lines that every effort has been made to offer thorough and comprehensive answers to each of the questions raised. Where such an occurrence takes place – *a.k.a.* repetition of facts presented – all repetitive materials will be traced, according to foot notes, back to the source citations, for ease-of-reference and evaluation.

The OCC Digital Activities Review Team have succinctly enunciated the challenges you face. Prime among these, in Advanced Systems Management Group's (ASMG's) view, is the issue of consumer privacy and protection. This is one of the bulwark issues underpinning the security agenda, and is built on institutional trust, and one-version-of-the-truth.

On Page 6 of your Preamble – Introduction the OCC states "AI and machine learning (ML) play an increasing role, for example, in fraud identification, transaction monitoring, and loan underwriting and monitoring." ASMG strongly agree. The Autorité de Contrôle Prudentiel et de

[1] ASMG-Ltd is a Canadian technology company based in Ottawa, Canada. The company delivers policy based data centric security (DCS) solutions for information sharing and safeguarding. ASMG software can be integrated into client environments, compliant to the Object Management Group (OMG) Information Exchange Framework (IEF) Reference Architecture (RA) which our firms' principals authored. The Information Exchange Framework (IEF) Reference Architecture (RA) is fully supported by published standards, directives, policy vocabularies, data models and data ontologies, according to the solution strategy it specifies. ASMG provide policy based software services addressing the challenges of information access and protection (security, confidentiality and privacy). The software can be integrated into existing environments as a standards compliant data access service, gateway, or application programming (product) interface (API). We support secure structured data and other files, videos, and sensor data, through commercially available networks including web, virtual private networks (VPNs) or other network interfaces. Encryption and attribution tagging is supported based on information sensitivity analysis based on policies defined by the organization.

Résolution (ACPR/Banque de France) – OCC's counterpart organization in France – has addressed AI and machine learning (ML) modeling issues, in their AI / ML systems consultation review process,[2] leading up to the publication of a definitive study on the matter. The Autorité de Contrôle Prudentiel et de Résolution (ACPR/Banque de France) skipped a critical discussion of canonical models, but came close in their section titled – Workshop on the topic Probability of Default (section 8.4).[3] This raises very important issues regarding the dependency (interdependency) of risk spread between AI solution providers. In one specific case, the risk is controlled insofar as the provider enables the customer to review all stages leading to the delivered machine learning (ML) model.[4] Advanced Systems Management Group (ASMG) will return to this issue, in answer to Q7. 'AI – ML security / governance and regulatory complexity,' appearing later in this Submission.

At the outset, Advanced Systems Management Group (ASMG) observes that the OCC Digital Activities Review document *implies* a future role for central bank digital currency (CBDC). Our submission will refer to central bank digital currency (CBDC), only in situations where it is unavoidable, or awkward, not to do so. Should ASMG indirectly, and without prejudice, touch upon any prospective OCC-supported central bank digital currency (CBDC), our opinions will be cloaked in a non-prescriptive, and technologically neutral stance. We feel this addresses the clear articulation the OCC has requested of all Submission Respondents in your *advanced-notice* of *proposed-rulemaking* (ANPR) call-up, requesting all Submitters remain non-prescriptive and technology-neutral, in the answers they provide. This we feel we achieve, in all respects, responding to the OCC's ANPR call-up document.

Advanced Systems Management Group (ASMG) are the authors of a standards-body ratified reference architecture, addressing a comprehensive information sharing and information safeguarding solution. This is the core of our enterprise. Our firm's participation and leadership at this Open Standards ratification organization, solidifies our *bona fides,* that we meet the letter-of-the-Participants' mandatory requirement *request* by the OCC's *advanced-notice* of *proposed-rulemaking* (ANPR) call-up documentation: e.g. [Submitters are to} present *non-prescriptive* and technology *neutral* information – in answer to any/all questions in the

[2] Source: ACPR (Banque de France) Discussion document titled "Governance of Artificial Intelligence in Finance (Dated June 2020)" by authors Dupont, Fliche and Yang. See *also*: "ACPR – Submission by Advanced Systems Management Group," dated July 2, 2020 - ASMG Submission document *available upon request*.
[3] Source: "ACPR (Banque de France) Discussion document – "Governance of Artificial Intelligence in Finance (Dated: June 2020)." See: Page 30 – '(*a.k.a.*) Third Party AI suppliers/providers outside regulatory perimeter;' Page 33 – '(*a.k.a.*) challenger models'. Discussion: [*at their* ACPR Discussion document - Foot Note # 17; Page 33] ACPR state: "To put it in perspective, the effort required for building an *alternative* (*i.e.* challenger) AI / machine learning (ML) algorithmic model – *e.g.* implementing a credit model for a banking institution – typically involves tens of employees, over a timespan of several years, even though its scope is limited to the organization's own data."
[4] Source: "ACPR (Banque de France) Discussion document – "Governance of Artificial Intelligence in Finance (Dated: June 2020)." See: I*bid*., [Foot Note # *2*] '(ACPR-Banque de France) Customer-Provider Risk: Customer to review all stages – *a.k.a.* machine learning (ML) testing, evaluation and acceptance –*before* contractual obligations are ratified (between Client and Vendor -3rd Party Supplier)'.

Submission documents presented. Advanced Systems Management Group (ASMG) conform to this request – each step of the way – in our enclosed Submission.

Advanced Systems Management Group (ASMG), by answering all Eleven (11) Questions the OCC has posted, are fully respectful of the goals you have set. Foremost to our approach, however, is a singular mindset to address security issues definitively, and in depth. ASMG site one missing link we see in the OCC's *advanced-notice* of *proposed-rulemaking* (ANPR) call-up, which we feel is mission critical. This is addressed via a critical need, in your corner, for a data-centric security (DCS) solution strategy *paradigm-shift*, vis-à-vis adopting specific data-centric security (DCS) solutions, which we will itemize as they are identified, by the use-case scenarios we encounter throughout our Submission. In addition, we will add two appendices to address Advanced Systems Management Group's (ASMG's) *specific* data-centric security (DCS) solution – via a deep-drill examination of the Information Exchange Framework (IEF) Reference Architecture's (RA's) ratified provisions – included at this Submission's conclusion.

To accept that a deficiency in approach – which we allege may even exist in the first place – is not an accusation we make lightly. Advanced Systems Management Group's (ASMG's) duty is to report what we know: our observation that the financial services sector, and their regulatory agencies, are missing a critical evaluation paradigm – to aid in assisting your organizations' reach your goals and objectives – better be an observation which is water-tight! We believe the OCC will be indelibly assisted in shifting your organization's carriage, by listening to our views. We will go one better. We will include a full explanation of the data-centric security (DCS) paradigm shift, and the DCS solution strategy, wherever the business use case in this Submission presents an opening for this solution strategy, when it arises, and requires the application of this solution strategy to fix deficiencies we identify. This will be framed, wherever possible, by direct linkages to the specific regulatory compliance context you are seeking to have addressed.

There is a lot of material presented in this Submission. Accordingly, here is a high-level synopsis of the Advanced Systems Management Group (ASMG) responses to the Eleven (11) Questions.

Question 1)
'Recent technological advances' addresses our premise that data is not fully characterized or properly understood. Financial service information is scattered across the cloud, at the edge or even widely disbursed to Internet-of-Things (IoT) mobile devices. Real-time processing of data is at a heightened state of activity, and the financial services industry are introducing a wide range of what we call *data appliances*. To our knowledge, this is not a term used frequently, if at all, in the popular literature pertaining to our sector. For our methodological purposes, a *data appliance* is a 'data warehouse appliance' which may have a software or a hardware connotation of some kind, usually (but not always) supported by one vendor.[5] That is a *so-so*

[5] Source: "Big Data Appliances," By R. Sathyanarayana [online], Slide # 6 of 12. Dated: July 23, 2020. See: cdn.ttgtmedia.com. See *also*: Ibid., [Foot Note # *15*].

definition of the term. Add in the phrase 'supported by vendors (plural)' and 'proscribed by open standards,' and we are much more comfortable with this definitional approach.

Reference(s) – such as the OCC's *responsible innovation framework* – when they are not specifically included in the questions we have been asked to examine, will accordingly be exempted from our answers. Advanced Systems Management Group (ASMG) reviewed the agile computing, microservices service-oriented architecture (SOA) advances in mainstream banking, with a Canadian Big Five Bank we are familiar with as the exemplar of this innovation, and included this example prominently in our answers to Q. 1. and Q2. This example portrays how this bank has embedded regulatory compliance into their Lines-of-Business (L-o-B) Data Domains. Advanced Systems Management Group (ASMG) found this Big Five Canadian Bank – which hosts much of their data centre away from the edge or the cloud – to have offered a particularly striking level of innovation, equal to the innovation spread across the financial industry (FI) vertical, in total. The traditional centralized banking infrastructure, and the decentralized finance (DeFi) financial services sector as well, are moving at a monumentally break-neck speed towards introducing Internet-of-Things (IoT) mobility devices-supported services, a trend that has only accelerated as of late. All of this by way of noting the datasphere is changing. Advanced Systems Management Group (ASMG) have examined security shortcomings and vulnerabilities in traditional, centralized banking, and have mapped these failings to the datasphere methodology at every available opportunity. The Bank for International Settlements (BIS-2020) have assisted us with our knowledge of the decentralized finance (DeFi) *space*, where our experience has been less formal. The Bank for International Settlements (BIS-2020) have reported that conventional and distributed ledger technology-based (DLT-based) infrastructures often store data multiple times, and in physically separate locations, which may be the source for future data tracking and data monitoring vulnerabilities. As data management specialists, this is a topic which presents a grave concern to our Company, and is something we address extensively throughout our Submission.

In our answer to Q1 – and subsequent questions – Advanced Systems Management Group (ASMG) offer a special perspective acquired from our long-standing membership-in-good-standing participation in, and authoring of, open standards. These open standards are ratified by our peer group from the international security community. We will augment this record of accomplishment with additional research searches from the literature, as required, and by presenting and summarizing our firm's principals' first-hand knowledge. Advanced Systems Management Group (ASMG) will not hesitate, whenever possible, to point out areas in need of further reflection and study.

Question 2)
'Hurdles to tech advance and innovation' closely follows the topics identified in the question's title. We start with a reflective stance on the advent of FinTechs, the encroaching advance of Big Data and the data lake, touch briefly on Open Banking a.k.a. *platformication*, examine one Canadian Big Five bank's DevOps, microservices-laden service-oriented architecture (SOA) agile computing smart core advance, in much greater detail than was presented in Q1. We slip

through a summary of the decentralized finance (DeFi) segment of financial sector activities, briefly visit cloud, edge and endpoint synergy issues with a linkage of these topics to decentralized finance (DeFi), which – all told – can best be described as a somewhat fast gallop around the block!

Question 3)
'What digital issues not addressed' brought our analysis to bear down hard on highlighting the intelligent Web, Intelligent Cloud combo. BigTech, Web 3.0 and neural networks are advancing at a dizzying pace, particularly within the institutional side of things amongst the BigTech behemoths. In the old Web (Web 1.0 and Web 2.0) powerful Integrated Development Environments (IEDs) were introduced to make sense of more and more data. But these Integrated Development Environments (IEDs) pale in comparison to the new, more complicated, or intricate, code writing exercises which lie in store with the Web 3.0 revolution's automated code-writing capabilities which lies ahead of us. Financial Institutions (FIs) are wrestling with the forward onslaught of technological advance, and technological progress, but are oftentimes left in the shadows of the BigTech behemoths. Without tipping our hat too soon to reveal all we have found out prematurely, we will state that we are concerned that *data security* is simply not being addressed robustly enough, by any of the parties or Stakeholder groups we examined, under these set of technological conditions we uncovered.

Advanced Systems Management Group (ASMG) had found a few very brief reference points to insert a mention (or two) about the data-centric security (DCS) paradigm, and DCS solution strategy, in Q1 and Q2. Since the data-centric security (DCS) solution strategy is not equated with something the OCC specifically raised – in the Eleven Questions – we will be very strategic in introducing this topic. Should seminal (foundational) digital issues arise, and require data-centricity to be addressed, our patience in finding these openings will be rewarded, and we will not be shy in raising our voice to address these issues aggressively.

Question 4)
'Crypto assets / crypto currencies' are pushing into the realm of demanding more specific supervisory and regulatory attention. This attention must now be focused on critical issues which, undoubtedly, can no longer be ignored or swept aside. We began our answer to this question by citing the requirement for i) consumer / investor protections ii) money laundering provisions and iii) terrorism financing as three (3) critically important issues we wished to see addressed. This is an introductory or exploratory set of issues for Advanced Systems Management Group (ASMG) to raise. Why? For one, we are not subject-matter-experts (SMEs) on these topics. Secondly, we have not found a consensus among the blockchain Stakeholders concerning what type of regulatory provisions they are comfortable complying with or even accepting.

Advanced Systems Management Group (ASMG) proceeded first by conducting a self-educational review of the terrain. We reviewed the top ten (or top twenty) crypto currency or

crypto asset entities, as much to educate ourselves as anything else, then proceeded to review two entities in greater analytical depth.

This is one of our briefer answers. The reason for this is that the entire formal discipline, and unifying vision – which *crypto* assets or *crypto* currencies wish to present to the world – is simply not there. Advanced Systems Management Group (ASMG) adopted a conceptual approach in our answer, to fill the void we see the *crypto* assets or *crypto* currencies community failing to address. After Advanced Systems Management Group (ASMG) gave a conceptual anchor to this segment of the economy, we were then able to answer Q4 with something approximating an empirical answer. By creating a conceptual approach – possibly overly simplified – to capture some of the philosophical and service proclivities or shortcomings (inconsistencies?) which the blockchain has spawned, we then uncovered way too many issues which blockchain Stakeholders are simply side-stepping, and leaving unaddressed. This was the right course of investigation for Advanced Systems Management Group (ASMG) to adopt. Our technological 'bent' was *locked and loaded*, however, for the next question – Q5 'Distributed ledger technology (DLT) for banking' – where we set to work to address this growing set of challenges and regulatory policy issues which need to be addressed.

Question 5)
'Distributed ledger technology (DLT) for banking' comes alive for Advanced Systems Management Group's (ASMG's) technologically-driven agenda. ASMG are sticklers for definitions, and methodological consistency. We feel that before the business use-cases may be derived, identified, and technological solutions brought to the table, we must address issues comprehensively – but with an accurate methodological focus – before the issues themselves can be accurately understood. A lot of very interesting ideas came out of the questions the OCC raised in Q5.

One interesting observation Advanced Systems Management Group (ASMG) arrived at and embraced while working on our answer to this question was that the blockchain – and the distributed ledger technologies (DLTs) surviving Stakeholders in the decentralized finance (DeFi) community – are single-mindedly disrupting the functioning of their opposite party, the centralized financial services segment of the global economy. Advanced Systems Management Group (ASMG) have reached this conclusion with some trepidation. Neither party in this contest seems willing to cede any territory to the other party in what seems to be shaping up as a 'winner-take-all' struggle for dominance and survival. The mainstream (centralized) financial economic services delivery model and the decentralized finance (DeFi) economic services delivery model need – Advanced Systems Management Group (ASMG) believes strongly – to find an accommodation, the one with the other. This should happen via a standardized approach, through standards-ratifying organizations, which yields the best results.

There is a great deal of information contained in ASMG's answer to Q5. We believe that technology *is* an *enabler.* And, acting as an enabler, technology will directly impact the work of regulatory compliance initiatives which seek to bring a balance to the financial datasphere. We

believe the OCC will appreciate the important role technology must play, in assisting you with the mission you are setting for yourselves. A heightened respect and appreciation for technological advances accompanies, or goes hand-in-hand, with the goal-setting exercise the OCC are expected to pursue.

Advanced Systems Management Group (ASMG) ask the OCC to pay attention to technology in this light. We have much we wish to discuss with the OCC regarding this question's perplexing, intersecting, and multifocal (at times) relationships and interdependencies, which are moving the financial markets in all kinds of directions at once.

Question 6)
'Payment technologies a.k.a. 'getting interoperability right' and yes, we weren't kidding! Advanced Systems Management Group (ASMG) stated at the beginning of this question that: all the analysis, particularly of web-cloud-edge innovations etc., are obstacles on the road which must be cleared out of the way, first. With those obstacles cleared, their messages understood, and the implications of what they stand for certified and accepted in advance, leads us to arrive at the position we are now finding ourselves 'in', which is to comprehend and *clearly* understand 'how-to-do' payments.

BigTech platforms – as we discovered in our answer to Q3 – casts a huge shadow over the financial services industry. This is a very diverse, and complicated, technological landscape to map out. Advanced Systems Management Group (ASMG) arrived at our conclusion that we had to approach the real-time payments (RTPs) infrastructure's myriad developments with an iron-clad eye focused on understanding *all* the technology inputs that make it work. We came up with a taxonomy for an '*integration*' components / service advance topic and an '*infrastructure*' – *nee* physical networks (and transport functions) service and components capability topic – which we have used to drive and organize our analysis and referential viewpoint.

Here is the challenge: these technological inputs live and are harbored inside BigTech (behemoth) companies, and jealously and fiercely guarded, at that! This has just made Advanced Systems Management Group's (ASMG's) resolve even more fortified to get to the core of the issue! The convergence of *integration*' components / service advances and *infrastructure*' *nee* physical networks (and transport functions) components / service advances – are replicated by software, middleware and hardware (and communications componentry). These software, middleware and hardware (and communications componentry) *inputs* (Tools? Toolkits? Appliances?) work to: present and capture real-time data, ingest and enrich (real-time) data, and provide data storage (redaction, etc.) of *real-time data* all in the service of the Internet-of-Things (IoT) edge. This section is not an easy read by any means! It exposes: i) data propagation / data debugging challenges ii) data safeguarding lapses iii) data recording or data life-cycle mishaps and iv) analytical processing anomalies or analytic misbehaviors / inconsistencies.

To capture Q6. accurately, Advanced Systems Management Group (ASMG) introduced an in-depth analysis of: i) Adobe Kafka (Kafka SQL and Kafka Streams), ii) Cato Networks – a secure access service edge (SASE) services entity, and; iii) Elasticsearch – a data indexing operational capability or functionality. This set of technologies and technological platforms makes up a smorgasbord, or cross-word puzzle-styled, set of component interactions and systems integrations.

Question 6. 'Payment technologies a.k.a. 'getting interoperability right' did *not* directly address interoperability. Why? Advanced Systems Management Group (ASMG) decided that this topic – interoperability – was better left to (and deferred to) our answer provided in Q8. ''RegTech and the OCC: Governance embedded in technology.' Q8. provided a superior foothold to address *data management issues* in a panoply of different ways. For now, *data interoperability* can be achieved through knowing data's provenance. A basic concept, but one which very few parties in the datasphere have yet embraced! To achieve this? Advanced Systems Management Group's (ASMG's) data-centric security (DCS) solution was brought forward and presented. With respect to information interoperability specifically, as it applies to mobility devices – the centre piece of the payments infrastructure today – Advanced Systems Management Group (ASMG) kicked the ball a little further down the field. We felt compelled to add a separate section to address this topic. This latter topic we propose to address in answer to Q11. 'Changes to banking (post Covid-19)' in the second part of our answer titled: 'Apps - Dapps not secure (IoT/mobile) and What DLT Data Center?'

Oh, and one more thing – along the way – we had a few things to say about '*payments*'.

Question 7)
'AI – ML security / governance and regulatory complexity' is a scene-setter, or scene-stealer, however one wishes to approach it. Every part of every economic activity commonly pursued around the globe today, is affected by regulatory compliance. What do we need to know about AI and machine learning (ML) entering the equation, and participating in what regulatory supervision is asked or tasked to do?

For starters, we introduced this question by summarizing where AI and machine learning (ML) topics have already been addressed in Q1 – Q5. This may be one of the most difficult questions you, at the OCC, posed to the Stakeholder community to answer. Why? Quite simply, it may apply itself to a wide range of issues, which we selected as follows: credit underwriting / credit monitoring; anti-money laundering and fraud; customer ID and due diligence; trading / hedging; and forecasting and marketing.

Issues which the OCC sought answers to have also, quite recently, been asked by your sister regulatory (supervisory) agency in France. The French organization, the Autorité de Contrôle Prudentiel et de Résolution (ACPR / Banque de France) raised a few issues which Advanced Systems Management Group (ASMG) fell obligated to share with the OCC in our answer to Q7). They include: fraud identification, transaction monitoring, credit approvals and investment

management services, to cite a few examples from the ACPR's consultative review and report-writing exercise.

Advanced Systems Management Group (ASMG) believe that technology, in the advanced technological category of the AI and machine learning (ML) *modeling* segment specifically, drives competitive advantage. But maybe to an extreme end of the continuum! At the extreme end of the financial services continuum – if you will – are many monopolistic economic organizations, with their own set of behaviours and ideologies. This will challenge regulatory efforts, and the OCC should navigate these waters carefully. ASMG hope our answer will provide some interesting terms of reference, to assist the OCC reach your regulatory compliance goals and objectives. If not, you have an interesting technology report card to file for future reference.

Question 8)
'RegTech and the OCC: Governance embedded in technology' is a question which, for Advanced Systems Management Group (ASMG), picks up where our answer to AI and machine leqrning (ML) left off. We jump right in with an analysis of crypto assets and decentralized finance's (DeFi's) smart contracts. Smart contracts are governance embedded in code, simply put. This is a whole new area for regulatory agencies and supervisory authorities to put under their 'lens'. Where we have deep misgivings on all of this is that Advanced Systems Management Group (ASMG) believe enterprises, whether they are centralized mainstream financial institutions (FIs) or the new breed of decentralized distributed ledger entities', don't have the time or resources to introspect data. What do we mean by introspecting data? To ASMG, when an organization knows the data life-cycle it has introspected data.

We continue our answer by taking, inevitably, a deep-drill examination of the networks – both centralized and decentralized. Advanced Systems Management Group (ASMG) applaud the work of mainstream banking as they deal with Current Expected Credit Loss (CECL) regulations and Allowance for Loan and Lease Losses (ALLL) requirements, both of which require an enormous amount of intellectual rigor and technological mastery to address. Against this backdrop, ASMG have culled a wide grouping of software, middleware and hardware (and communications componentry) entities which all lay claim to protecting or defending data resilience in some means or fashion. This group consists of data management entities proclaiming their: i) data productivity tools ii) data quality tools and toolkits and iii) data connectors. Many of these separate methodological categories are subsumed under one corporate umbrella, as in the Googles, Amazons, Microsofts (or even Facebooks) of the world.

We zig-zagged forwards through this technological maze, and ended up with Talend Open Source – a file management and data flow orchestration capability – which offers DevOps and programming professionals a building block of code, to use to weave together 'businesses, customers, suppliers and employees'. As we mentioned in our answer, Advanced Systems Management Group (ASMG) gave these sundry of stakeholders and players ample opportunity to make the case for data-centric security (DCS) solutions. We are somewhat guilty of delaying

the job of addressing 'getting interoperability right' – deferred from Q6 to be resituated here in Q8. – many of our confreres in this wide segment of technological activity all claim to have data management frameworks, or data management strategies, etc. etc. But they do not agree or subscribe to Advanced Systems Management Group's (ASMG's) views on this topic. We have been quite generous, and allowed our allied stakeholder consulting partners – participating in this vertical (as data-centric management and data-centric frameworks or security solutions providers) – to 'go first'. Their views and solutions, we must be honest, have come up short.

From here we digressed even further, and visited a list of topics: trade surveillance; client onboarding; investment case management / investigative case management; transaction monitoring, and finally we reviewed the Bank for International Settlements (BIS-2019) call for compliance placed into the tokenized (distributed ledger technology/DLT) market segment. Advanced Systems Management Group (ASMG) feel strongly the Bank for International Settlements (BIS-2019) have failed to make a convincing case for their proposition. ASMG feel that by knowing data's life-cycle, you know data's provenance, which is the only tried and true way to secure data, not by a tokenized decentralized approach. We ended Q8. by examining, in a very cursory manner, small business lending by FinTech's, although much more analysis of this sector's activities remains to be uncovered and addressed.

Question 9)
'Considering small institutions and research departments' is a question we have an admiration for, and an affinity and sympathy for the second party or stakeholder group mentioned in this question, research groups. It would seem to us, at times, that our company are destined to remain in our *research mode* indefinitely. To our benefit, Advanced Systems Management Group (ASMG) see this situation turning around, very soon.

We addressed the first half of the question possibly in an erroneous way. We may have defined the question regarding 'smaller institutions' too narrowly. Advanced Systems Management Group (ASMG) defined and determined *small institutions* to be small banking, or community banking entities, a dwindling sub-vertical in the US banking vertical. This was an interesting topic, nonetheless, to investigate. It somewhat falls outside our national reference point, as these types of financial institutions are largely absent in Canada. An interesting stakeholder group worth examining, all the same.

In terms of the second portion of the Q9. question 'research departments' there are many issues which came up that surprised us. But first, we addressed regulatory agency and supervisory authority issues by a back-door examination of MiFID II, the EMIR supervisory regime and a somewhat abbreviated mention of the EU's General Data Protection Regulation (GDPR). The latter we have left as a topic of our second appendix. Next, we must admit, we have a deep respect for this second topic, research institutions. These specialists toil in their subject-matter-expertise (SME) areas of concentration across the economy, and are not just affecting the financial proclivity of their supporting investment management service organizations, or their banking bosses, per se. They are having a much more progressive and

influential effect, on the economy as-a-whole. Hopefully, we have reported a few things which will be helpful here, for regulatory compliance specialist organizations such as the OCC, to examine further.

Question 10)
'What other changes need OCC address' was a question which gave us the chance to exercise our *creative license*. As many small businesses, like our firm, struggle to find our footing in this Covid-19 pandemic environment, we worry about the economic reset we must face, or better put, we all must face. The global economy is undergoing a *reset* of almost biblical proportions. Advanced Systems Management Group (ASMG) have taken umbrage with this issue, in not knowing what is coming next. We have turned this into a positive issue, on our internal clock, by looking at bail-out funding mechanisms, and the way they have kept national, and international economies afloat.

ASMG placed the hedge fund industry 'under-the-lens', and we were required to scour far and wide – to uncover and present a very unrestricted and intensive analytic answer – which paints a fascinating portrait of this unique segment of the financial services economy. The economic reset? All we can say is it will be particularly dramatic, when looking at the US – or even Canada's – economy, to find the right solutions for what ails us, as we move our economies back to some semblance of normality. Hopefully, this is not too far afield from where the OCC sits, although we have no certainty in our minds if this falls under the OCC's jurisdictional wheel-house of issues, for regulatory compliance management, or not. Possibly, the OCC's sister regulatory agencies will have this at the top, or near the top, of their regulatory *to do* lists to address.

Question 11)
'Changes to banking (post Covid-19)' … cyberthreats! Coming straight out of the gate, what could be more unnerving to a financial services sector regulatory agency to contemplate than this issue? Here is the topic, and the reasons we have for defending our security solutions expertise, which attracted Advanced Systems Management Group (ASMG) to view ourselves ideally suited to be responding to this OCC *advance-notice* of *proposed-rulemaking* (ANPR) Digital Activities Review Submission request, in the first place. As an organization, throughout our history, we have been hyper-focused on cyberthreats, as a defining issue. Cyberthreat actors affect all digital infrastructure, which we all hold as a foundational pillar of society in the free-world.

Advanced Systems Management Group (ASMG) are troubled by dark web actors in the decentralized finance (DeFi) vertical, just as much as we are worried about the situational awareness context of the command and control (C&C) community in defense circles. In our answer, we cite Google having brought progressive web apps (PWAs) to the world's attention. This has certainly led to modern web browsers growing in their market prominence. But security? Pretty much ignored! The Open Web Application Security Project (OWASP) foundation are playing 'clean-up' here to fix things. ASMG jumped in to assess five of the vulnerabilities

that the Open Web Application Security Project (OWASP) foundation have identified, which has made our concern that data life-cycle issues are not being taken seriously today elevated to an even more prominent position of concern!

This brought us to part two of our answer to Q11. The second part of this question addressed – Apps - Dapps not secure (IoT/mobile) and 'What DLT Data Center? – a carry-over topic from Q6. Payment technologies a.k.a. 'getting interoperability right.' Time and time again, Advanced Systems Management Group (ASMG) have stated that Apps - Dapps *are* not secure (IoT/mobile), while the topic 'What DLT Data Center?' is a puzzler! Advanced Systems Management Group (ASMG) have side-stepped that fact that society e has a colossal security problem with mobility devices, left unprotected, which inflicts untold damage on our modern-day economy, and its security apparatus. We carefully explore, in this second section of Q11., all facets of this issue. Even though the Internet-of-Things (IoT) security-thwarting proposition is self-sustaining – caused by the inertia of so many actors unwitting behavior and lack of concern to address this strategic issue – we trust we will not remain alone in raising the alarm. We all need to pitch in and find a comprehensive solution to fix the security breach which exists today with mobility devices globally. This led us, indirectly (we admit) to believing that a distributed ledger technology (DLT)) – monolithic and oligopolistic infrastructure is beginning to create itself – before our eyes. Can't be stopped! This fascinating development has run as a sub-theme throughout our Submission. Since mobility and Internet-of-Things (IoT) advances move along at their rapid pace, unchecked, we have come up with our own brain-storming idea, an idea Advanced Systems Management Group (ASMG) formulate in the form of a question: 'What about DLT Data Centers?'

The final section of this Submission – attached as "Appendix A: ASMG and the IEF - *a.k.a.*- Data-Centric Security (DCS)" – is a review of Advanced Systems Management Group's (ASMG's) interoperability vehicle, embracing the data-centric paradigm, and envisioning a data-centric security gateway / interfacing solution – as currently undergoing its advanced-stage testing in the defense sector – which we hope to seed (and spread) into the financial services sector vertical. Although the financial sector may have adopted a mandate and strategies for governance and accountability [of data] – deliverable via high level policies – the implementation of this mandate is lagging. Advanced Systems Management Group (ASMG) believes the robust solution for data governance and data assurance – *a.k.a.* data accountability (and data accessibility) – lies with pre-defining domain-based policies regarding that data. Once those policies, rules, ontologies and vocabularies governing how 'all data' is specified and enforced, ASMG's data-centric security (DCS) solution comes to the foreground. The data-centric security (DCS) solution provides: i) a set of software-defined services, ii) programming language-clarified directives applied to the minimally necessary data attributes required for an information sharing / information safeguarding solution to be adopted, and iii) exchange messaging capability, *all* ready to be implemented.

A second Appendix – attached as "Appendix B: EU GDPR / Privacy-Enhancing Technology (PET) data-centric security (DCS) Solution Proposal" – is *self-explanatory*. The terms and conditions

identified in the Advanced Systems Management Group's (ASMG's) PET pilot proposal remain unaddressed to date. The EU Parliament's 'Horizon 2020 Funding Programme (for GDPR solutions)' – and the response crafted by ASMG and dated April 2017 – would have offered a solution to *data security* and *breach notification* issues, specifically. Without a major EU-based corporate champion to join us in this pursuit – a mandatory requirement which we couldn't meet – ASMG's innovative PET pilot proposal was subsequently *disqualified* and died on the shelf. It is more than an historical artifact. The terms and conditions of our solution delivery identified by ASMG's Privacy-Enhancing Technology (PET) pilot are as necessary today, as they were when submitted in April 2017. ASMG believes strongly that data-centric security (DCS) solutions are required in the world today, and more so since if we protect the data, we become virtually unassailable.

We welcome the OCC reviewing this Submission. We look forward to interacting with you, and your colleagues in the regulatory compliance field. Bon chance, Good luck. Let's reconvene our dialogue in short order.

OCC Response Document Questions

Q1. – recent technological advances

Technology is racing forward from the internet and the personal computer, to the mobile device and the newest of the *new* – the Internet of Things (IoT). The growth of data is at all time explosive levels. Advanced Systems Management Group (ASMG) have worked on data, and data specifically, as the world has moved from pedestrian personal computers (PCs) to the ubiquitousness of the global web.

As more and more applications proliferate, to search, stream and order our data, and assist us in communicating and moving (and analyzing) data and metadata, ASMG has been there. ASMG's mission and purpose has been, and steadfastly remains, to figure out the *how* to make sense of these comprehensive and potentially divisive advances, applying a data-centric lens to these developments.

Legacy infrastructure has not helped. Organizations' pre-existing *legacy* infrastructures and systems, often force data to be silo'ed in dead-end repositories, knowingly misplaced and unmapped, and therefore lost to their users' appraisal.

Startup organizations – and this includes the organizational form of the *neo* cryptocurrency and crypto asset managed portion of the expanding financial services industry – have neither fixed nor benefitted from mapping their data stores. They really haven't progressed with their handling of data, through data sharing and data safeguarding means, any better than their peers in the traditional, centralized financial service industry's *traditional* legacy system and legacy infrastructure *space*. This allows the OCC and the US Treasury Department a unique

opportunity to address unmet challenges. Principal among these challenges is the undefended status of so much of the data we depend upon daily. Regulatory regimes, particularly with our nascent crypto economy emerging from its genesis, can be designed to specify how data is to be secured, at its source, which is the route Advanced Systems Management Group (ASMG) heartily recommends.

ASMG has witnessed the critical demeaning of the value of data with alarm. Whether they be the *status-quo* -derived banking legacy infrastructures, or these more fleet-of-foot mobility-enhanced FinTech and decentralized finance (DeFi) crypto currency *neo* startups – the latter offering distributed ledger *crypto* systems and practices – the result is always the same: both camp's data-centric security failings remain unaddressed.

Here is another important opportunity for the OCC to consider. All financial institutions (FIs) seem to be focusing on their enterprise's data lake.

The enterprise data lake receives and stores data, but this raw data has no firm assumptions attached to it, with respect to its ontologies, or whether it has the correct schema attached to it to organize and manage (itself) effectively. Raw data is, relatively speaking, left for the consumer of the data *themselves* to contextually interpret, analyze, and decide how they should proceed to make sense of it. By its inherent nature, the enterprise data lake acts as a continuous reservoir, receiving data feeds, from all sorts of application programming (product) interfaces (APIs), and distributed applications (Dapps[6] – in the mobility setting), and a multiplicity of heterogeneous systems feeding the data lake with even more unwieldly, and often disparate, sources of information.

Let's examine heterogeneous systems for a minute.

[6] The difference between a dapp and an app: '*Dapp'* stands for decentralized application, and uses an entire peer-to-peer (P2P) network to run their back-end code, called backend modules. Dapps have the capability of storing value, and handing it out to users after contract conditions have been fulfilled. This means dapps eliminate the need for a third party (intermediary) since they allow value to be stored directly inside the app. Dapps may or may not run on blockchain – e.g. BiTorrent and BitMessage don't run on blockchain. The majority do run on blockchain. allowing them to integrate easier with one another, and be inter-compatible. A dapp changes code (and functions) automatically. Since a *dapp* has its back-end code running on a decentralized peer-to-peer (P2P) network, and has a public backend, any suspicious activity needs rigorous monitoring. To build dapps, developers use smart contract programming languages, or traditional app development scripts (Java, C#, C++, JavaScript, SQL, Golang). Since dapps' open-source 'backend' code resides on P2P nodes - in distributed networks, as opposed to apps which run on centralized servers - users must acquire more understanding about the elements of the blockchain ecosystem such as wallets, tokens etc. Decentralized applications may run on top of other cryptographic systems such as Ethereum. Dapps mostly differ from apps in where dapps get (and save) their data. An '*app*' relies on a standalone computer or a cloud server. Traditional apps use a trusted third party to secure financial transactions. Apps require an intermediate to connect the user with an application. It is also controlled by its design through developers, whom are responsible for changes in codes and functionalities. Source: "How Dapps are Different from Regular Mobile Apps?' By Tanya (Editor-in-Chief) Mobile App Daily [online]. Dated: January 10, 2020. See: https://www.mobileappdaily.com/difference-between-dapps-and-regular-apps.

Data Age 2025,[7] a collaboration between Seagate and the Information and Data Community (IDC) organization, studied the growth of the global datasphere. The IDC Report (2018) has defined three primary locations where digitization is happening, and where digital content is created: the *core* (traditional and cloud datacenters[8]), the *edge*[9] (enterprise-hardened infrastructure like cell towers and branch offices), and the *endpoints* (PCs, smart phones, and Internet-of-Things/IoT devices[10]). The summation of all this is as follows: data, wherever it is created, captured, or replicated, is called the Global Datasphere.[11]

The *core* of the global datasphere – for many entities and organizations – is the Cloud.

In the defense sector, where Advanced Systems Management Group (ASMG) practice our art, the advanced state of data codification, ontological pinpointing of the accuracy and verifiability of data (and metadata), defining data's shared meaning and communicated context, etc. is captured by the comprehensive term *situational awareness*. Situational awareness does not take kindly to the public Cloud. Defense sector principals' treat data governance and data accountability with the highest, most rigorous discipline. Advanced Systems Management Group (ASMG) believes that understanding and controlling data, via its *metadata*, is of prime importance. Once the policies, rules, ontologies and vocabularies governing *all* data are

[7] Source: "The Digitization of the World: From Edge to Core," By David Reinsel, John Gantz and John Rydning, IDC White Paper [online]. Dated: November 2018. See: https://www.seagate.com/files/www-content/ouar-story/trends/files/idc-seagate-dataage-whitepaper.pdf. See *also*: *Ibid*., [Foot Note # *11, 25, 27, 371*].

[8] The Cloud, to most people, refers to software and service(s) that run on the Internet, instead of locally on your computer. If your business driver is agility, then the fear of a 'vendor dictated lock-in' will not produce the desired results. *Agility* is achieved in the Cloud when you leverage higher level services, such as AWS's RDS, a Database-as-a-Service feature, or Google's Big Query, a petabyte scale Data-Warehouse as a Service, or Microsoft Azure's Cortana Intelligence Suite, which provides Machine-Learning-as-a-Service capabilities. With all three of these examples, there is no need to stand up infrastructure. All these capabilities are accessible via APIs. The cloud provider handles all the infrastructure, middleware and auto scaling, while developers can quickly build high value business applications on top of these services.

[9] The *edge* is a distributed computing paradigm, bringing compute, storage, and applications closer to where users, facilities, and connected things generate, consume, and/or leverage data. Edge computing is already used in ample applications, mainly in combination with the Internet of Things (IoT). See: *Ibid.,* [*footnote # 248*] "SASE-The Optimal Architecture to Secure and Connect the New Enterprise perimeters," by Cato Networks [corporate website], Dated: July 2020. See: go.catanetworks.com. See *also*: *Ibid*., [Foot Note # *240*] "What is SASE and Why Should You Care," By Info Systems Architects, staff [online – isacybersecurity.com] Dated: February 7, 2020. See *also*: *Ibid*., [Foot Note # 241] "Say Hello to SASE (secure access service edge)," By Andrew Lerner, Gartner [online – gartner.com]. Dated: December 23, 2019.

[10] With regards to *device management*, many Internet-of-Things (IoT) devices currently do not support implementation of strong security controls, and maintaining a security baseline will only get harder as IoT devices proliferate. The pervasiveness of Internet-of-Things (IoT) data collection, coupled with advanced analytic capabilities applied to IoT data collection efforts, could potentially result in more rampant consumer privacy violations. These hackers will continue to attack datacenter surfaces with seeming impunity. This is a result of ineffective perimeter security defences in the cloud, as well as, ineffective protections applied to the *traditional* (internal or on-site) datacenter.

[11] Source: "The Digitization of the World: From Edge to Core," By David Reinsel, John Gantz and John Rydning, IDC White Paper [online]. Dated: November 2018. See: [abbreviated excerpt] *a.k.a*. https://www.i-scoop.eu/big-data-action-value-context/data-age-2025-datasphere/. See *also*: *Ibid*., [Foot Note # *7, 25, 27, 371*].

specified and enforced, ASMG's data-centric security (DCS) solution can then be acted upon as: i) a set of software-defined services, ii) programming language-clarified directives, and iii) rules and policies applied to the minimally necessary data attributes required to provide an end-to-end information sharing – information safeguarding exchange data *security* and data *messaging process* of the highest order.[12]

ASMG are jumping ahead here, for a specific reason. The financial services sector approach the issue of 'securing (and safeguarding) data' as a *business intelligence* issue. Business intelligence conducts the search, exploration, analysis, visualization and collaboration initiatives for a line-of-business (L-o-B) as specific to the information *discovery stage*, more often (than not). This differs, in the traditional datacenters' case, since by performing line-of-business (L-o-B) information discovery at the *edge* or the *endpoint* stage – applying the Data Age 2025's definition of the global datasphere – data security is essentially left unaddressed.
This is a very important observation. By moving the information discovery stage away from the *core* (Data Age 2025's definition of the *core* situates the data 'core' within the *traditional* and cloud datacenters), Data Age 2025's disciplinary rigor, instead, locates the information discovery stage '*in*' either the *edge* (enterprise-hardened infrastructure like cell towers and branch offices) and/or at *endpoints* (PCs, smart phones, and IoT devices) which changes the *securing of data* equation markedly.

How do you secure the data in (or at) the perimeter or *edge* (of the Cloud)? How do you secure the data at the *endpoints* – the PCs, smart phones, and IoT devices?[13]

Why we have jumped ahead, to re-arrange the Data Age 2025 taxonomy, and make *traditional* datacenter treatment of information discovery so vastly opposite to its occurrence at the *edge* or *endpoint* data discovery processing points? Or even, why are we asking it to be treated in a fundamentally different manner to how we treat data and information discovery – performed as a Cloud computing datacenter function? The *traditional* financial services sector *datacenter* – not hosted in the Cloud – is very simply, fundamentally different. Here is how we see this issue.

[12] For the *traditional* datacenter - located internally within the bank (i.e. *on-premise*) – this is their definitional exigency of what they term the 'core'. Sure, slightly different connotation, but bear with us! The *traditional* datacenter's core is where: Solution examples, UI components, Data grid components, Configuration files, Data sets, and Methodology and *Tools* manage, and codify and interpret data. Data sets are managed *here* [vis-à-vis]: i) outward-facing presentations a.k.a. cloud-protruding *Production instance(s)*, containing encrypted client data (facing the User/Client) and; ii) cloud-protruding *Authoring instance(s)* presentations are deployed, which mask client data (facing the Solution team / bank Employee). Plus, any applicable or suitable security controls are made manifest at the *Authoring instance(s)* presentation layer. We (at ASMG) defer in our agreement to the validity of this last point. ASMG's approach to data (/metadata) security, which we will address comprehensively *later,* adopts the premise that data (/metadata) needs be secured, first and foremost. See *also*: 'Appendix A: ASMG and the IEF - *a.k.a.*- Data-Centric Security (DCS)' solution, at the end of this Submission.

[13] Moving information and data discovery towards endpoints, possibly relying upon the general adoption of user interface components, means data security, at best, is dependent on network-centric (or application-centric) security protections. This is, quite simply, something which is not working well today.

The Bank of Montreal (BMO), one of Canada's Big Five banks with whom ASMG are intimately familiar, regard the *core* – a.k.a. their traditional datacenter *not* hosted in the cloud – as something BMO attributes to the naming convention they term their information delivery platform (IDP) / (BMO) Smart Core. This information delivery platform (IDP) / (BMO) Smart Core produces high-value (account) asset (HVA) reports, covering the bank's 'Frequency of Reporting' (bimonthly / monthly) regulatory and internal executive-briefing documentation, and administrative and fiscal updates. Frequency of Reporting (bimonthly / monthly) high-value (account) asset (HVA) updates are shared with: Audit Committee Members, Executive Committee Members, Board Members etc. These upper level management employees regularly receive: i) Evidential reporting; ii) Acting-on-recommendations reporting) and; iii) Lessons-learned reporting. These comprehensive data reporting actions make up a *basket* of crucial Governance and Compliance (G&C) reporting responsibilities, performed by BMO, or by any other Big Five (5) bank in Canada, or by all US-based *too-big-to-fail* Financial Institutions (FIs).

Drilling down into this definitional context even deeper – the Bank of Montreal (BMO) Smart Core / information delivery platform (IDP) – embeds regulatory compliance and data governance together, into core banking processes. Semantics aside, this is a very important point. This ensures that data stewards, data holders, data owners and data custodians *all* treat data as a departmental Line-of-Business (L-o-B) responsibility, and not as a *side group effort* undertaken by a compliance team, divorced from the day-to-day operational activity of the bank. The (BMO) Smart Core / information delivery platform (IDP) model shows the impact of everything across the enterprise,[14] from regulatory compliance to merger and acquisition activities, to sales (customer) analytics, to understanding profit and loss (P&L), etc. Where the (BMO) Smart Core / information delivery platform (IDP) is going next (post 2018), is to take the initial implementation – based on data appliances[15] – and overlay it, with analytics, to create a whole new set of opportunities and solutions via cognitive learning.

The next location which the Information and Data Community (IDC) organization studied – in their Data Age 2025 Report – is the global datasphere layer they call the *edge*. The edge

[14] Hadoop distributions make available several components to achieve information advantage, as do Tibco, the later Company's tools and toolkits deployed by the Big Five Canadian bank, the Bank of Montreal (BMO). Other vendors providing similar information advantage capability include (but are not limited to): Databricks, Cloudera, Google Big Query, Hortonworks, Snowflake, Apache Spark, and more. NB: Compiling an accurate cross-reference of these products and services, in a *comparability* sense, is a chore beyond this Report's interest - or motivation or desire - to complete.

[15] Data appliances include - e.g. presenting only a partial listing of tools or toolkit items deployed at BMO - Tibco EBX and Tibco Spotfire. Tibco EBX is a master data management enterprise class software module. Tibco Spotfire is an analytics and business intelligence platform. By using a whole number of 'Spotfires' on top of the bank's Smart Core / information delivery platform (IDP), this allows BMO to bring to light the power of the information ingrained within all banking sector business use cases. These banking sector business use cases are assembled and codified (and analyzed), whether for: regulatory compliance, risk management, finance, customer analytics, or just understanding profit and loss (P&L) functions. This is brought together holistically - as *one-version-of-the-truth* - recognizable by any/all employees trained to decode this version of the *truth* across the bank. See also: Ibid., [Foot Note # 15] *a.k.a.* "Big Data Appliances," By R. Sathyanarayana [online], Slide # 6 of 12. Dated: July 23, 2020. See: cdn.ttgtmedia.com.

contains enterprise-hardened infrastructures, such as cell towers and branch offices. In datasphere terms, *edge computing* refers to an extensive foundational, or infrastructure enabling layer, which will allow mobile and Internet-of-Things (IoT) technologies and communications devices, and other data appliances and software tools and toolkits etc. – such as sensors, cameras, 3D printers etc. – to take advantage of faster connectivity to data, and compute resources. This faster connectivity, oftentimes reaching single-digit-millisecond network latency performance measures, reveals the powerful processing advances reached via the Cloud computing footprint.

Before we applaud the remarkable performance we just cited – rendered via Cloud-enhanced *edge computing* – we should remember that appliance-based communications, in traditional systems, sends information in a single direction, on a single path. Getting beyond communications in this singular, one-directional manner, may be a challenge which decentralized, distributed ledger data processing tasks must soon come to terms with. More robust *built-out* networks may be required to deal with multi-focal delivery via cloud (and edge) applications and services, etc., to accommodate a crowded field of issues, listed as follows:
i) SD-WAN device connects (to any mix of fiber, cable, xDSL, or 4G-LTE connections); or
ii) global private backbones (basically ERP-styled delivery and reporting systems 'with *eyes*'); or
iii) Firewall-as-a-Service / F-a-a-S (*e.g.* virtual firewalls weaved into a mesh); or
iv) Service Web Gateways (*e.g.* AWS Direct Connect and/or Microsoft Azure Express Route options); with everything packaged together as the Secure Access Service Edge (SASE) – requiring each end, at the *sending* and *receiving* terminus, having their own assigned point-of-presence (P-o-P) hosting – or information exchange *endpoints* – installed.[16]

All in the service of reaching that elusive goal – information interoperability.

Advanced Systems Management Group (ASMG) would suggest that the Information Exchange Framework (IEF) Reference Architecture (RA) – providing the Policy-based Packaging Service (PPS) component – is the better route. We believe it is the only route – demonstrably proven – to address information interoperability conclusively. The Information Exchange Framework's (IEF's) Policy-based Packaging Service (PPS) component serves as part of the ontology and data modeling underpinning, which the data-centric security's (DCS's) *rules-based* secure information exchange solution offers. The Policy-based Packaging Service (PPS) 'knocks on your door', and asks: "Do you want this? Here is your access format authorization to receive this secure message, with tagging, labeling, cryptography and/or an identity access management (IAM) service applied!" If you – the Client in the Community-of-Interest (C-o-I) –have a Policy-based Packaging Service (PPS) component installed on your *receiving side*, the message is delivered *instantly*. If you – the Client in the Community-of-Interest (C-o-I) – have *no* Policy-based Packaging Service (PPS) component installed, as specified by the data-centric security (DCS) protocols for information sharing and safeguarding, the Information Exchange

[16] Source: "SASE – The Optimal Architecture to Secure and Connect the New Enterprise Perimeters, by Cato Networks [online website infomercial]. Dated: July 2020. See: go.catonetworks.com. See also. See *also*: *Ibid*., [Foot Note # *248*].

Framework's (IEF's) Policy-based Packaging Service (PPS) component will communicate with your (receiving party) API,[17] and the message is received. Secure. End-to-end. And noted by an audit trail "re: all data sent / received" – captured by a virtual [real-time] data life-cycle mapping – any time data is *-redacted*, data is *-transported* [and/or] data is *-placed-in-storage* (via the storage means [and/or] storage device, of *whatever* configuration 'hardware / middleware or software' – without exception.[18]

The benefits of edge computing, and where it can be applied – in the financial services sector's use-case determination – may involve conventional (or traditional) centralized infrastructure, or distributed ledger technology (DLT) infrastructure. Conventional and distributed ledger technology-based (DLT-based) infrastructures often store data multiple times, and in physically separate locations. The main difference between them lies in how that data is updated.

In conventional databases, resilience is typically achieved by storing data over multiple physical nodes, which are controlled by one authoritative entity – the top node of a hierarchy. By contrast, in many distributed ledger technology-based (DLT-based) systems, the *ledger* is jointly managed by different entities, in a decentralized manner, and without the action of a top node. Consequently, each update of the *ledger* in many distributed ledger technology-based (DLT-based) systems needs to be harmonized between the nodes of all entities (often using algorithms known as "consensus mechanisms"). This typically involves broadcasting and awaiting replies on multiple messages, before a transaction can be added to the *ledger,* with finality.[19]

The Bank of International Settlements (BIS-2020) authors whom provided us with the node analysis we have just referred to, continue their analysis by pointing out that the vulnerabilities of data supplied by conventional (or traditional) centralized infrastructure, or distributed ledger

[17] The Policy Enforcement Point (PEP) – in data-centric security (DCS) parlance – is the component of the Information Exchange Framework's (IEF's) Policy-based Packaging Service (PPS) which taps the communications formatting interface to the receiving party's API, or communicates directly to a Policy-based Packaging Service (PPS) component installed on your receiving side. Source: Information Exchange Framework (IEF) Final Revised Submission (FRS), See: OMG Document Number: MARS/2017-02-21; pp. 31, 294, 298. Discussion: The Information Exchange Framework (IEF) Security Service Gateway (ISSG) provides a single point for users (vendors and integrators) to integrate IEF components with the users' own security services (e.g., Identity, credential, access-control, and key management) and infrastructure. The ISSG-Request (User-Identification), for example, may have a message metadata instruction containing a special message indicator (special caveat), in which case the PEP packages an ISSG-Request to gather the recipient's authorizations. The Policy Decision Point (PDP) would next adjudicate the request using current user policies, and packages the response as a PDP-AuthorizationResponse message and issues this response to the PEP to be enforced.

[18] This, and the previous foot note, are the *first* of several introductions to the Information Exchange Framework (IEF) data-centric security (DCS) solution. More references and explanations are coming, woven into the fabric ASMG's – OCC Digital Activities Review – Submission. See *also*: 'Appendix A: ASMG and the IEF - *a.k.a.*- Data-Centric Security (DCS)' solution, at the end of this Submission.

[19] Source: "The technology of retail central bank digital currency," by Raphael Auer, Rainer Böhme. Bank of International Settlement (BIS), Dated: March 1, 2020. See: https://www.bis.org/publ/qtrpdf/r_qt2003j.pdf; *and/or* https://www.bis.org/publ/qtrpdf/r_qt2003j.htm. See: *Ibid*., [Foot Note # *57, 156, 185, 420*].

technology (DLT) infrastructure, are different. The key vulnerability of a conventional architecture is the failure of the top node, for example via a targeted hacking attack. The key vulnerability observed with distributed ledger technology (DLT) architectures is the consensus mechanism, which may be put under pressure, for example, by a denial-of-service (D-o-S) type of attack.

The Bank of International Settlements (BIS-2020) claim, quite rightly, that digital innovation knows no borders. Responding to this challenge, the Bank for International Settlements (BIS-2020) set up "Innovation Hubs" in multiple locations, in partnership with central banks. The first three (3) BIS Hub Centres were launched in late 2019 in the Hong Kong *special autonomous region* (SAR), one in Singapore and one closer to their home-base in Switzerland. The BIS Hubs aim to catalyze collaborative efforts among central banks, and co-operate – when appropriate – with academia, financial service providers and the broader private sector.[20]

The importance of the *edge*, with all the software, hardware, infrastructure and *new* services that have been popping up in recent years, suggests even more advanced technology capabilities are finding their way into commercial avenues of acceptance, in such fields as: i) *self-service* data ingest, ii) data preparation, iii) data profiling, iv) data classification, v) data governance, vi) data lineage, vii) metadata management, viii) global search, and ix) *security* service offerings. In terms of the new *edge* services, the list is long, and includes: a) Internet-of-Things (IoT) platforms for the IoT edge – *edge* gateways*, edge* servers*, micro data* centers[21] – and the whole *fog computing*[22] environment.

Business models – and the location of data management in the datasphere – may be changing, but the technical requirements and challenges remain. Data must be archived and stored in ways that provide appropriate levels of performance, enables analytical processing and

[20] ASMG would respond positively to the Bank of International Settlements (BIS) *via* a proposal for a joint (*prospective* solution pilot) effort – *a.k.a.* utilizing and deploying ASMG's / (OMG's) internationally-sanctioned open standards –based data-centric security (DCS) solution. We would participate in this technology demonstrator project (TDP) at any one of BIS's several Technology Hub's, if so welcomed.

[21] Source: "What are Micro Data Centers?" By Stackpath staff, [online]. Dated: 2020. See: https://www.stackpath.com/edge-academy/micro-data-centers/. Discussion: In recent years, applications including IoT (Internet of Things), content delivery, and 5G have created a large demand for low-latency access to data processing and data storage. Traditional centralized data centers, such as those used by AWS (Amazon Web Services) and Microsoft Azure, weren't designed with those use cases in mind. A micro data center (MDC) is a small-scale modular data center that includes all the compute, storage, networking, power, cooling and other infrastructure required for a given workload. (Cooling?). See *also*: "Q+A: Stackpath Takes Users Closer to the *Edge*," By David Kirkpatrick, 0online]. Dated: February 12, 2019. Discussion: '(Stackpath-2019) Edge Computing Containers and Virtual Machines spun up at any of forty-five locations – at Stackpath's micro-data-centers (MDCs), a type of data center design – with repositories like GitHub or Gitlab, your choice (as their Client/Customer).'

[22] Fog computing is a model which provides an intermediary between data, processing and applications concentrated in IoT devices and the cloud computing infrastructure. Extra computing power closer to the data creation site, in a fog computing configuration, gets located at a fog node. The fog node is found in a smart router or gateway device, allowing for data to be processed on this smart device, so that only the necessary data gets further transmitted to the cloud, and decreases the bandwidth used. A smart electricity grid is one example. See: https://www.techradar.com/news/what-is-fog-computing.

intelligence gathering (to *apply always*), and data handling and data management must be accomplished cost-effectively and securely. This is not necessarily an easy task, given that as companies create hybrid systems, combining – data lakes, enterprise data warehouses, data repositories *on-premise*, or data repositories *in-the-cloud* – the following questions must be answered: - Is the data secure? - Is access controlled? - Are all compliance regulations taken care of? - Is activity tracking enforced with an audit trail? - Is data controlled (and managed) through its complete data life-cycle? Many industries have too much data resident in data silos, which defeats the opportunity to introduce cross-border information interoperability and/or to introduce information sharing via secure information exchange advances. Advanced Systems Management Group (ASMG) say "we know!" Our expertise in this realm can prove this fact conclusively.

Institutions *can* use big data analytics to monitor for covert threats. This helps enterprises and institutions to identify evolving external and internal security risks, and react much more quickly. And the 'miniaturization of technology' that has driven smartphone growth, has also made biometric security more practical. For example, some banks allow customers to access their accounts using thumbprints, or even voice and facial recognition – an approach that is more convenient for consumers and improves security.

Making data actionable is, however, something which the heavy proliferation, and preponderance of, mobility device-generated Internet-of-Things (IoT) advances cannot keep up with. In our increasingly complex – and growing – data landscape, the steepening growth of structured data,[23] unstructured data,[24] and the requirement to derive meaning and insights from information, by leveraging it at the *right time* and *right moment* for the *right reasons*, are all pressing disruptive actions which concern many Stakeholders in the financial services marketplace today.[25] This topic – taken one step further – in some circles is termed *fast data*. Fast data[26] solves a problem, or creates business value. The goal of *fast data* is to quickly gather

[23] Structured data, in Big Data environments, may be Computer- or Machine-generated. Machine-generated data generally refers to data that is created by a machine without human intervention. Human-generated: This is data that humans, in interaction with computers, supply. Some examples are 'touch point' data (in financial transactions), 'click-bait' data (in advertising/malware attacks) and game related data (understanding how end users move through a gaming portfolio).

[24] Unstructured data is the largest piece of the data equation, and the use cases for unstructured data are rapidly expanding. On the text side alone, text analytics can be used to analyze unstructured text and to extract relevant data and transform that data into structured information that can be used in various ways. For example, a popular big data use case is social media analytics for use with high-volume customer conversations. In addition, unstructured data from call center notes, e-mails, written comments in a survey, and other documents is analyzed to understand customer behavior. This can be combined with social media from tens of millions of sources to understand the customer experience. If twenty (20) percent of the data available to enterprises is structured data, the other eighty (80) percent is unstructured.

[25] Source: "The Digitization of the World: From Edge to Core," By David Reinsel, John Gantz and John Rydning, IDC White Paper [online]. Dated: November 2018. See: https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf. See *also*: *Ibid*., [Foot Note # *7, 11, 27*, *371*].

[26] Source: whatis.techtarget.com/definition/fast-data; - 'Definition of *Fast data* a.k.a. a technology disruptor deployed to gather and mine structured and unstructured data.'

and mine structured and unstructured data, so that action can be taken. Fast data applies more robust data analytic processes to the task of analyzing and using big data, in a trading environment handling securities (for example), by accessing, analyzing and moving that data into many more manageable, smaller data sets – or data bytes – in near- or -virtual *real time*.

In datasphere terms, edge and (device) *endpoint* synergy should lead to an extensive – e.g. expansive – increase in *real-time* processing and analysis efforts, coupled with some form of assurance that 'everything-is-secure'. In this last regard, as the global datasphere conducts business in either the traditional datacenter model – e.g. the Bank of Montreal (BMO) Smart Core / information delivery platform (IDP) platform services model – or via *edge* or *endpoint* computing platforms and devices, possibly situated within the cloud datacenter infrastructure, both sets of Cloud and *traditional* datacenter footprints are *very* far from secure!

Let's end this section with the following point, from the Information and Data Community (IDC) Organization's Data Age 2025 Report. The IDC and Seagate (2018) Report proclaims: "Data Age 2025 forecasts that more than 150B devices will be connected across the globe by 2025, most of which will be creating data in real-time. These estimates indicate that by 2025, every connected person in the world, on average, will have a digital data engagement – over 4,900 times per day – which is approximately 1 digital interaction every 18 seconds.[27]" Stunning!

Q2. – Hurdles to tech advance and innovation

The too-big-to fail financial institutions (FIs) and their Big Five (5) Canadian counterparts are all increasing their reach-out – via better connectedness *tracking* their customers' experience – to achieve more seamless, efficient and pro-active emphasis on *smart* processing of data. But that movement toward *smart* data – whether with machine learning (ML) tools, with or without AI, plus featuring advanced automation – must adhere to two fundamental principles: make data's *meaning* and data's *context* irrevocably assured and easily represented.[28]

[27] Source: "The Digitization of the World: From Edge to Core," By David Reinsel, John Gantz and John Rydning, IDC White Paper [online]. Dated: November 2018. See: https://www.seagate.com/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf. See *also*: *Ibid*., [Foot Note # *7, 11, 25*, *371*].

[28] Source: Peter Winstanley, Director – Semantechs Consulting Ltd., – signatory # 556 of 837 on the data-centric manifesto. Discussion: (*Quoting* Peter Winstanley: For automation instances, data is centralized, and it's *meaning* and/or *context* must be known. That *context* is self-described, by the data itself. The data-centric approach is particularly essential when it comes to automation. Data without context is meaningless. Data that is inaccessible creates lost opportunity, and an economic hardship." See: http://www.datacentricmanifesto.org/signatories/. See *also*: *Ibid*- [Foot Note # *530*] '(Abramson-ASMG) signatory # 763 of 837 on the data-centric manifesto. Discussion: Michael Abramson – and colleagues at ASMG – have made a career of creating the Data- Centric Security (DCS) Paradigm. Data-centric security (DCS) provides a comprehensive security-enforced data policy – that is independent of the infrastructure and application – used to share and process data. This has resulted in the publication of the Information Exchange Framework (IEF) Reference Architecture (RA), and all supporting data ontologies, data models and data vocabularies, etc. at the Object Management Group (OMG). A policy-driven data-centric solution to information sharing and safeguarding, fashioned as an open standard, provides a 'unified and integrated vision' for securing data at its source.

In the answer to the previous Q1. 'recent technological advances,' we touched upon the interoperable data lake. The interoperable data lake is at the *crux* of data centricity. Data centricity has a permanent primary core, data itself. Data centricity is the opposite of application centricity. Application centricity is oriented towards a specific use case in which each application has its own data lake, and is responsible for collecting and storing the data it needs. Data centricity is equated with a single data model, or more explicitly, is a unified and integrated *vision* of the data. This means that you can model your data for a specific use case, but always in a centralized way. When data is governed by rules, access protocols and security measures, data becomes an asset with enriched accuracy, integrity and timeliness.

The implementation characteristics of a data lake, namely inexpensive (data) storage and (data) schema flexibility, make it ideal for insightful information discovery and data analysis. However, these traits do not necessarily translate into a high-performance, production-quality, analytical platform. Making new insights available to the broadest possible audience requires *data optimization*, which is providing greater maturity of *analytical* models and their *semantic consistency*.[29] These three points – data optimization, the maturity of analytical models, and insightful appreciation of data through semantic consistency – when combined as one, achieve the insightful appreciation of data.[30] Let's examine data optimization first.

As new insights are discovered, the work of *optimizing data* passes from the data science team to the data engineering team. Data engineers take the *new* questions and optimize the data to provide new insights and answers. The Team of data engineers refine and optimize the raw data, then re-run analytical models. Existing data integration processes can be used, or new

[29] Source: https://tdan.com/the-data-centric-revolution-implementing-a-data-centric-architecture/24116. Discussion: For every type of data governance, metadata is critically important for the success of big data projects. Semantic concepts, as applied to a data warehouse, require that many parts of the application ecosystem should be model-driven. A model-driven API layer, e.g. Public APIs, will be defined in the model. For instance, we can have model-driven user interfaces (UIs) for data optimization, analytics and new process builds. Many implementations of the model-driven API layer – Public APIs – are based on a shared model. A shared model features all parts of the architecture understanding and implementing data consistently. It includes, for example, such concepts as processing a stored query, or a constraint, or the managing of classes that make up the basis for a model driven UI.

[30] See: Source: https://martinfowler.com/bliki/DataLake.html. The *insightful* appreciation of data identifies three Enterprise Application Layers:

- Presentation layer – Components that handle HTTP requests and implement either a (REST) API or an HTML-based web UI. In an application that has a sophisticated user interface, the presentation tier is often a substantial body of code.
- Business logic layer – Components that are the core of the application and implement the business rules.
- Data-access layer – Components that access infrastructure components such as databases and message brokers.

See *also*: https://martinfowler.com/bliki/MultipleCanonicalModels.html – 'discussion of the special case – canonical models'. Source: "Domain-Driven Design – What it is and how to use if?" By Andrew Powell-Morse, [online]. Dated: April 21, 2017. See: https://airbrake.io/blog/software-design/domain-driven-design. Discussion: This reference explains the subtleties and complexities of Domain-Driven Design (DDD).

processes can be built.[31] The maturity of analytical models' process steps we can touch upon next. Mature analytical models – found in multiple deployment modes across most modern data warehouses – may have complimentary data storage, and data analytical solution capabilities. They may occur in cloud, and/or cloud-hybrid designs, and may constitute a virtual data warehouse (or several data warehouses) grouped together. These data warehouse repositories or data resources, deliver – through the aid of mature analytical models – the means to display or view data via data virtualization.[32] The insightful appreciation of data is extremely important, particularly with respect to this third point's vital characteristic, achieving semantic consistency.

The ordering of the layers which compromise a modern or logical data warehouse[33] – from the bottom up – are:

User Access / reporting tools
Metadata / views into the data storage
Storage / data persistence
Software / database management system (DBMS)
Foundational systems / servers, network

The metadata layer of a logical data warehouse would situate the *data visualization abstraction* component of a mature *modern* logical data warehouse within the Metadata layer, the second layer from the top. In the logical data warehouse example, a metadata model should be put in place to facilitate search, understanding and reuse of data across departments. Without proper

[31] Source: "Data Lakes: The biggest big data challenges: Why data lakes are an important piece of the overall big data strategy," by Prashant Tyagi, Director Analytics-GE Software and Haluk Demirkan, Professor - Business Analytics, University of Washington-Tacoma / Milgard School of Business. Table 2: 'Data warehouses vs. data lakes' & Table 3: 'Four components of data lakes.' Dated: 2018. See: http://analytics-magazine.org/data-lakes-biggest-big-data-challenges/. See *also*: DesigningAModernDWandDataLake_MelissaCoates.pdf (Slide 7 of 73). Both *citations* (Tyagi / Demirkan & Coates) provide an exhaustive treatment of data lake / data warehouse design and implementation issues. Recommended.

[32] Source: "Designing A Modern Data Warehouse and Data Lake," By MelissaCoates.pdf (Slide 7 of 73). See *also*: *Ibid* – [*footnote # 31, 33*]

[33] Source: "Designing A Modern Data Warehouse and Data Lake," By MelissaCoates.pdf (Slide 7 of 73). See: http://analytics-magazine.org/data-lakes-biggest-big-data-challenges/. See *also*: *Ibid* – [*footnote # 31, 32*]; Quoting Philip Russom, TDWI - *a.k.a.* 'Melissa Coates' Slide deck, (Slide 42 of 73).

metadata management[34] in place, business users will simply be lost in the 'abyss' of information.

For today's data security platform to thrive, it must be connected all the way from the mobile device through the connected infrastructure: eCommerce, *mobile*, batch, 3rd party ingress, *web services* and peer-to-peer (P2P) and all accompanying encryption elements selected, etc. Data governance – in banking and the regulatory technology domain – overlaps. It enables customers, and company-wide data citizens and/or banking service representatives —plus IT staff — to access and use reliable data, to create actionable insights, in a *self-service* approach. That is the goal. This is also referred to as the *platform strategy* for banking, or sometimes shortened to the term 'platformication.' This platform strategy in banking also includes Third Party Players (TPPs) *plus* the 3rd party applications which a Customer has installed, on their electronic device or smart phone.

Organizations that fail to provide good data governance – the cornerstone to RegTech – will lose and lose big.[35] Financial establishments, as they wrestle with regulatory compliance issues, experience threats from a variety of sources. Most prominently, mobile applications and web portal proliferation, are adding additional compromising footprints which expand the vectors of attack *surface* in all directions, placing mobile applications and web portal access under increasing threat attack, and threat detection duress. Cyber criminals may steal or manipulate

[34] Many industries have worked hard over the last decade to define shared meta-models specific to their industry, and it is these models that now form the basis for contractual information sharing across organizations and across geographic borders. A typical usage scenario of the [Sparx] Schema Composer is in the creation of message definitions (/schema) to exchange information between organizations, ensuring that such messages comply with the underlying meta-model that has been adopted by the involved parties. When information is shared between organizations, it is frequently the case that only a subset of the full meta-model is required, but it is essential that what is shared conforms precisely to the agreed meta-model. This converts a UML class model to a W3C XML Schema (XSD), This [Sparx – Schema Composer] toolkit also allows Data Modellers to start working at a conceptual level in UML. Source: "Sparx Systems Enterprise Architect User Guide Series – Schema Model 6 Version: 1.0," [online], Page 4-6. Dated: June 3, 2017. Discussion: All interesting stuff, but slightly beyond the scope of this Report.

[35] Source: "CIO: 3 Questions to Ask about your Enterprise Data Lake," By Ciaran Dynes [online – talend]. Dated: August 8, 2016. See: https://www.talend.com/blog/2016/08/08/cio-3-questions-to-ask-about-your-enterprise-data-lake/. See *also*: *Ibid*., [Foot Note # *344, 365*]. Discussion: Since the Global Finance Crisis (GFS), financial institutions are under far greater government scrutiny. As a result, the bar has been raised in terms of the IT and data governance measures required to meet these regulations. For example, a US bank recently settled a multi-million-dollar penalty with the SEC, due to its failure to enforce policies and procedures to prevent and detect false securities transactions (involving the misuse of material and non-public information). See *also*: "Build a True Data Lake with a Cloud Data Warehouse," By Talend staffers [online]. Dated: not given *a.k.a*. [Foot Note # *366*]. See *also*: "Creating a company culture where the respect of personal data is top priority," By Maud Bailly, [online – talend]. Dated: 2020 *a.k.a*. [Foot Note # *367*].

valuable user data and or "clone" banking apps, and use them for nefarious purposes.[36]

Framed against all of this, how have the financial institutions (FIs) fared? Here is a look at their progress. First, before continuing with this analysis and turning our attention to examine how new era decentralized, distributed ledger technologies (DLTs) are faring, let's sum up the situation with financial services offered from the *starting point* adopted by the traditional, centralized service delivery model associated with mainstream banking.

The most discernable advance traditional banking introduced was called *agile* banking. Agile banking emphasized the *corridors-of-change* insights and impacts associated with *microservices* service-oriented architecture (SOA) DevOps-inspired 'webs' of microservices applications. Microservices, or more accurately a web of DevOps-inspired microservices applications,[37] use distinct modules to run applications, with a backbone application programming (product) interface (API) communicating between them. For example, each microservice runs a single job, in the manner of a User Interface (UI) to – for example: i) take payments; or ii) share an identity document with, in the latter case, a passport issuing office. Microservices are *stateless,* so they themselves, do not store Personal Identity (PII) information.

The banks have pursued a microservices architecture services implementation model to leverage the ideology of developing a single application – as a suite of small, narrowly focused independently deployable services. Each microservice runs its own process, and communicates with a lightweight mechanism, often an HTTP resource application programming (product) interface (API). Those services which the microservice has encapsulated addresses specific business capabilities, and are deployed independently, using a fully automated mechanism. REST (Representation State Transfer) application programming (product) interfaces (APIs) are key to microservices architecture. A RESTful application programming (product) interface (API) breaks down a transaction, to create a series of small modules, each of which addresses an underlying part of the transaction. This modularity provides developers – DevOps professionals

[36] In the security services report by third party player TokenEx, they state: "As many as 20 million card details potentially revealed in breach". Source: Email dated Friday, April 3, 2002 at 9:45 am. [to: J. Carter, ASMG]. Discussion: Global fintech firm, London-based Finastra, takes multiple servers offline after suffering breach. A ransomware attack on Finastra has resulted in a disruption to the services it provides North American customers, including two U.S. financial institutions. Details of the breach, which customers were affected, and what records were exposed have not yet been made available. See *also*: *Ibid*., [Foot Note # *469*, *470*] '(Finextra publication-2020) Finastra cyber security breach undermines Company's global networking operations.'

[37] *Microservices,* in the banking sector's service-oriented architecture (SOA) implementation model, feature services which are: i) independently deployable (from one another); ii) scalable, and; iii) tailored to fit business implementations by operating on the business process itself. This builds a matrix of multiple service sets. Microservices implementations adapt differing programs, language and database management (e.g. storage technology) solutions. The Customer-centric focus practiced by all of today's modern banks, deploying this service-oriented architecture (SOA) / microservices' implementation model, adds domains of knowledge, directed from the core outwards (concentrically and concurrently), specifically demands that the bank must hold *all* data stewards, data holders, data owners, and data custodians – and their upper Business Line executives – accountable to *owning* the information they use.

– with a lot of flexibility for developing lightweight application programming (product) interfaces (APIs), which are more suitable for browser powered applications. With their creation of DevOps microservices[38] application *pockets*, threaded together into a service-oriented architecture (SOA) mesh, *agile* computing has arrived.

The big financial institutions (FIs) we have been analyzing so far are achieving four (4) things, we may usefully describe as 'system' *service item* components / solutions:

1) A solution Library
2) User interface components
3) Data grid components
4) A rapid implementation methodology and authoring tools.

1) The *solution Library* – eradicates unnecessary boundaries between information and data analysis components, consisting of:
Use cases – combining information, logic and analysis from two or more domains required to solve a problem;
Domains – information and analysis reflective of an area of expertise;
Elements – standard data structures used to assemble domains.

The *solution Library* provides: i) all the detailed information for rapid assembly, ii) all the elements which define data, be they: Views, Measures; Dimensions; Catalogs; Transactions; Relationships; Unstructured data; navigation data, and; a (data) Glossary. This stage in the bank's data management system handles data 'Domains of knowledge' *a.k.a.* the subject matter / area expertise, for all activities conducted by the bank. They may include: Technology; Cybersecurity; Processes; Suppliers; Facilities; Operations; Initiatives; M&A; Audit & regulatory; Financial crimes, and; Objectives (enterprise, performance, and performance vs. objectives).

2) *User interface components* – conduct the search, exploration, analysis, visualization and collaboration initiatives of the *information discovery* stage. This means pulling from Solution examples, UI components, Data grid components, Configuration files, Data sets, and Methodology and tools vis-à-vis presenting outward-facing, cloud-protruding *Production instance(s)* containing encrypted client data (facing the User/Client) and; the cloud-protruding *Authoring instance(s)* which mask client data (facing the Solution team and/or bank Employee).

[38] Microservices must run in a redundant configuration: using a container management system or 'orchestration tool' such as Kubernetes, which allows you to use policies to dictate container placement. Kubernetes (or Docker Swarm or DC/OS) act as *service proxies* responsible for communication with other service instances, and can support capabilities such as: service (instance) discovery, load balancing, authentication and authorization, secure communications, and *others*. Containers run a standardized frame for all services by abstracting the core OS code from the underlying hardware. Security may become an issue, as we are accustomed to applications with a well-defined endpoint. Microservices, however, break endpoints up into a hundred smaller endpoints, each requiring specific security controls to ward against exploits and attacks. There's a lot of surface area to cover. This topic covers an extensive vista, and may be addressed via 'securing microservices endpoints with API façades.' Source: https://www.networkcomputing.com/cloud-infrastructure/microservices-management-securing-endpoints.
See *also*: https://www.mulesoft.com/resources/api/what-are-microservices.

3) *Data grid components* – contain *all* data model components utilized to organize information. Data grids play a role to standardize the enterprise's data model, and make it understandable for cross-domain comparisons. The Data grid is built on a rigorous standardization effort, empowering the data Experts / data Owners to enter views in Excel, and pull the information they need, when the need it, and share it with collaborative teams to improve enterprise decisions.

4) The rapid *implementation methodology* and *authoring tools*[39] – tie in with the need for greater efficiency and faster development. For rapid application development (RAD) the focus is on minimizing the planning and maximizing prototype development[40] efforts.

In the banking example which Advanced Systems Management Group (ASMG) has the most familiarity with, here is how the *new* era — or new *agile* banking transformation process — approaches things:

a) Connect / integrate services, using an enterprise service bus (ESB). This process enables the banking domain Business Rules (e.g. rules governing a service, delivered by an application) to be put in the banking *core*, as opposed to leaving these business rules as residing in *all* the distributed applications. Secondly, new *era* (i.e. agile) banking:

b) Places Business Rules in the enterprise's *core* (not placed within the apps, or within distributed applications), as this allows the Lines-of-Business (L-o-B) channels to be abstracted, or built with a single code base, making it infinitely easier for the bank to dissipate business rules across all banking channels, at a much faster rate.

This preceding paragraph describes conditions which the US's 'too-big-to-fail' banking majors, and their counterparts – RBC being Canada's 'too-big-to-fail bank,' plus the *other* Canadian Big Five (or big Six, if you include the National Bank of Canada in Montreal, Quebec in the count) – Banks are all chasing: the ubiquitous *virtual* banking organizational model. Some common forms of virtual banking are: i) ATMs, ii) use of magnetic ink character recognition code (MICR), iii) Electronic clearing service scheme(s), iv) Electronic fund transfer(s), v) real-time gross

[39] Authoring Tools help the author [user/programmer] write hyper-text for multimedia applications. It enables the developer to combine text, graphics, audio, video and animation. Or, it allows the creation of simple, static HTML pages with the flash player Plug-in. For a specialized example, Islay – an interactive animation authoring tool, allows an [authoring] program to be used as a control program that processes something periodically, for example an IoT device. Source: "IoT Technologies: State of the Art and a Software Development Framework," By Takahiro Inui and Masaru, [online – Smart Sensors Networks]. Dated: 2017. See: https://www.sciencedirect.com/topics/engineering/authoring-tool.

[40] Rapid application development (RAD) emphasizes the niche format of adopting customizable software development advances, where users test each prototype of the product, then take the prototypes and beta systems and proceed through iterative design phases to the final coding, unit integration and testing phase in DevOps.

settlement (RTGS) systems, vi) computerized settlement of clearing transactions, and vii) centralized fund management schemes, etc.[41]

Let's clear up one point. Virtual banking does not mean *virtualization*. Virtualization is a term which refers to technology which enables a single PC or server to run multiple operating systems or multiple sessions of a single operating system (OS) simultaneously. A machine with virtualization software can host numerous applications, including those that run on different operating systems, on a single platform. The *host* operating system (OS) can support numerous *virtual machines*, each of which has the characteristics of a 'particular OS'. The solution that enables virtualization is a virtual machine monitor (VMM), or hypervisor.[42] There – said it!

Unlike a physical server, this virtual server only sees the resources it has been configured with (i.e. allowed to view), constituting a *select* number of resources, and does *not* view or access all the resources loaded on the physical host itself. Since *virtual machines* (VMs) are already files, copying them produces not only a backup of the data, but also a copy of the entire server, including: the operating system, applications, and the hardware configuration itself. A specialized support to the *hypervisor* is offered by a 'kernel'. What is described here, in effect, is that the 'hypervisor' facilitates the translation and *input/output* (I/O) transmission, from the *virtual machine,* to the physical server device(s), and back again. This allows a self-correcting virtual machine to act in a self-servicing communications loop.

Microsoft states that "The 'virtual machine' is sandboxed from the rest of the system, meaning that the software inside a *virtual machine* can't escape or tamper with the computer itself. This produces an ideal environment for testing other operating systems (OSs') – including beta releases (of those OSs') – accessing virus-infected data, creating operating system backups, and running software or applications on operating systems (OSs) they weren't originally intended for."[43] (*Continuing* here) "For servers, the multiple operating systems (OSs) run side-by-side with a piece of software called a 'hypervisor' to manage them, while desktop computers typically employ one operating system (OS) to run the other operating systems, within its program windows. Each *virtual machine* provides its own virtual hardware, including CPUs, memory, hard drives, network interfaces, and other devices. The virtual hardware is then

[41] Online transaction processing (OLTP) refers to a class of systems that facilitate and manage transaction-oriented applications, typically for data entry and retrieval transaction processing. The "transaction" is not only in the context of computer or database transactions, but also is defined in terms of business or commercial transactions. OLTP has also been used to refer to processing in which the system responds immediately to user requests. An automatic teller machine (ATM) for a bank is an example of a commercial transaction processing application.
[42] The *hypervisor* is of special interest to Advanced Systems Management Group's (ASMG's) middleware product called COIL. COIL (*five* initials - Common Object [Interoperability] Information Layer). COIL is the international standards-body *approved* 'inner core' for protecting data, known also by its more generic term "Data-Centric Security (DCS)". This inner core *layer* protects structured and unstructured data, data encapsulated (wrapped/referenced) by a layer of structured data, and so on. The 'and so on' part relates to highly specific designations for securing data, contained in the OMG's Information Exchange Framework (IEF) Reference Architecture (RA) – see omg.org.
[43] Source: "What is a virtual machine?" By Microsoft staffers [online]. Dated: 2020. See: https://azure.microsoft.com/en-us/overview/what-is-a-virtual-machine/.

mapped to the real hardware on the physical machine, which saves costs by reducing the need for physical hardware systems, along with the associated maintenance costs that go with it, to track everything. Plus, this reduces power and cooling demand." (Cooling demand?).

What is important here (details yet to be worked out between Advanced Systems Management Group/ASMG and interested parties, such as the OCC) is that the 'hypervisor' deployed in a security configuration [ASMG envisions] needs to have select *ports sealed* – for all traffic entering into and departing from [*into* and/or *out-of*] the virtual machines (VMs) – *a.k.a.* this forms a protective layer, which Advanced Systems Management Group/ASMG might define as a VM-[type] secure *wrapper* – to handle information sharing and safeguarding *payloads*.[44] This is a criticality issue which, ASMG believes, so far, nobody but us has wish to see addressed! This is a logical evolutionary extension, for Advanced Systems Management Group's (ASMG's), of our middleware layer called the Common Object [Interoperability] Information Layer (COIL).[45]

The whole purpose of the data processing industry, going back to before we had microcomputers, mobile devices or the Internet, has been premised on one enduring principle. That principle is an enduring belief that by engaging with a financial service provider, or other fiscal services facilitator, our 'focus' is concentrated upon making data a *commodity*, with fully understood *meaning* and *context*. And by its very necessity, that *data* needs to be fully secured. Somehow, we have travelled far away from this guiding or foundational premise or principle.

The ability of the data lake to store and process data at low cost, and to use many different methods for transforming and distilling data, has expanded the data lake's role from its very basic performance of data "extract-transform-load" (ETL) data processing functionality. Extract-transform-load(ETL) is a useful process, to prepare data for analysis in a data warehouse. Data lakes are a natural fit for the ETL data processing functionality of handling Big Data. This sort of "scale-out ETL" – e.g. allowing Big Data to be distilled into a form that is loaded into a data warehouse for wider use – does, nonetheless presents its own set of challenges.

[44] Advanced Systems Management Group (ASMG) have even gone so far as to state that port 4, 5, 6, 7 & 8 - located on the Executive Services configuration/location - would be sealed; while ports 1, 2 & 3 - located on the Information Exchange *Controller* - backwards connected to: - a) Data Processing Service and, - b) Data Packaging Service – may secure data efficiently and effectively, without occupying crucial real estate at the operating system (OS) level. In ASMG's opinion, threat vectors attempting to gain access to the operating system (OS) - and exploit a weakness in the OS - and (subsequently) exploit a direct threat vector channel into the Container, is a situational awareness issue to be avoided, at all costs! If this occurs, it will compromise in-store memory - or during communications events (or instances) – prove to be exceedingly threatening in deployments used *to exploit* core level services. Control the *hypervisor*, and you can plug those risk vectors. NB: ASMG are open to further discussion, with motivated parties, concerning this fundamental threat vector exposure.

[45] Common Object [Interoperability] Information Layer (COIL) applies policies that limit (i.e. proscribe) access to data. COIL sits on a local area network (LAN) as a set of software services, conforming to the Information Exchange Framework (IEF) Reference Architecture (RA). The Common Object [Interoperability] Information Layer (COIL) – or a similar product any other vendor can offer, as adapting the full definitions, directives and rules and policies contained in the Information Exchange Policy-based Packaging Vocabulary (IEPPV – see omg.org) – can reside on a distinct node, or a specified virtual machine (VM). COIL may be provisioned as a subset of services on an Enterprise Service Bus (ESB) or alternatively, may be fashioned as an interface point or a zone access point.

The challenges of managing your data, and succeeding as a data-driven organization, face many roadblocks. As more and more applications proliferate, coupled with an organizations' existing legacy infrastructure and systems becoming more rigid and inflexible, in their operations and data processing and performance metrics, financial institutions (FIs) require a fix. That fix, in small measure, has come from a rapid uptake and expansion of data processing and data management via microservices. The modernization face-lift, e.g. via the transformative introduction of several (or a basket of) microservices, relies on the fact that microservices are an architecture, as well as a mechanism.

Microservices are composed of small, independent processes that communicate with each other, using language-agnostic application programming (product) interfaces (APIs). Alternatively, applications can be written to purely serverless specifications, and use *no* microservices-oriented service provision at all,[46] in which case they appear to more closely approximate the latter description, operating as a mechanism for data processing. It is also very important to note that since microservices are most likely going to be deployed within a 'containerized' environment, it is necessary for developers (DevOps teams) to be made aware of one very crucial issue – to avoid hardcoding secrets – e.g. credentials and keys, in container images or environment variables, as microservices come off the drawing board (design-phase) and become fully implemented (developmental, and then maintenance stages, respectively). While not perfect, most Container orchestration environments provide options for managing secrets securely. It's a good idea – for one – to rotate keys on a regular basis.

Advanced Systems Management Group (ASMG) see an interesting challenge with decentralized finance (DeFi) solutions, with respect to their data management pursuits, which we will touch upon briefly next. ASMG feels that *identity systems* have become the modern perimeter. Here's how this plays out. Identity, whether permissioned or *permissionless* – in terms of its assigned access *authorizations* – in decentralized finance (DeFi) solutions requirements domains, are not just acting as infrastructure alone, but are also protecting data relationships as identities. Our identities need cohesive, end-to-end protection.

Personal identities – or data identities viewed as mapped back to a user/owner – are fragmented data sets which float around on the Internet, and are exchanged between many different Internet-of-Things (IoT) mobility devices. Not only that, but disparate regulatory environments are failing to adequately protect us, nor are they protecting these data identities, and DeFi data management systems are not of great help.

Decentralized identity provides a unique *Use Case* challenge, no doubt. It is situated upon the premise that a prerequisite support system exists to support *identities*, drawing from government standards. Various government standards (and identification –type regulatory half-measures) exist today, to provided data *issuance* and *verification* for digital identities. On top of

[46] Source: "PaaS Vendors, Watch Out! Amazon is all Set to Disrupt the (SAS) Market," by MSV Janakiram. Dated: July 16, 2015. Retrieved July 10, 2016 (this *paragraph*).

that, identity fraud multiplies! Why? Are our identities[47] too rampant? Maybe even too numerous to count, as they are duplicated in so many places – for example – in online submissions, and verifications with third-party providers? Or, after somewhat innocuous visits to social media sites, and so on?

There is nothing particularly earth-shattering about any of the *above* narrative points – mapping out the rapid uptake of new era *agile* computing in the banking sector via *microservices* – nor, in Advanced Systems Management Group's (ASMG's) bold-brush review of the enterprise cloud and cloud computing issues (See: ASMG's answer to Q1) 'Recent technological advances'). Many observers – a World Economic Forum (WEF) representative included in this group – can rhyme off statement after statement about '*blockchain*' having qualities that can 'help build resilience and transparency into supply chains', or 'we need *not* be just tech-focused' – but also 'take a holistic approach to bringing *trusted data* to supply chain ecosystems and into value chains,' or a particular favourite of ours, 'governance protocols need to be stable and predictable enough to foster confidence.'[48] Perhaps the lure of the latest and greatest tech advance has contributed to this state of affairs, in which the cart is put ahead of the horse!

Is the data lake just a dumping ground for data of widely varying quality, better named a data swamp? Sometimes it appears that way.

To deal with the convergence of technology with every other facet of economic activity, in our case our propensity to turn to mobility devices at every turn, the data swamp has yet to fully merge distinct technologies, industries, or *devices* into a unified whole. Maybe that is the prize our World Economic Forum (WEF) representative, and everyone else, is waiting with baited breath to see happen. In the meantime, here is what the Information Technology / Information Management (IT/IM) sector has done to address the data lake, a pillar of support underneath mobile technology.

Any large enterprise needs a model that is either very large, or abstract, or both. And largeness and abstractness both imply comprehension difficulties. Enterprise-wide conceptual modeling addresses multiple applications. Enterprise-wide conceptual modeling may take two forms: 1) a shared database approach to enterprise integration - where integration occurs through applications sharing a single logical enterprise-wide database. Or secondly, 2) a messaging based approach to integration. One of the interesting consequences of a messaging based approach to integration is that there is no longer a need for a single conceptual model to underpin the integration effort.

Messaging-based integration will allow:

[47] Advanced Systems Management Group (ASMG) will return to address the issue of identities in our answer to Q5)- Distributed ledger technology (DLT) for banking [sub-section] '5.2 – Identity projects'.
[48] Source: "World Economic Forum's Nadia Hewett Talks Supply Chains, Covid-19 and Blockchain," by Marie Huillet, [online – Cointelegraph]. Dated: May 5, 2020. See *also*: I*bid*., [Foot Note # *94*].

- several canonical models rather than just one.
- these canonical models may overlap
- overlaps between models need not share the same structure, (e.g. there should be a translation between the parts of models that overlap)

Canonical models need not cover everything that can be represented, they only need to cover everything that needs to be communicated between applications. Multiple models can be built through harvesting, rather than planned up-front. As multiple applications communicate pair-wise, you can introduce a canonical model to replace **n** * **n** translation paths, with ***n*** paths translating to the canonical hub.[49]

Too much detail? Advanced Systems Management Group (ASMG) think not!

The Autorité de Contrôle Prudentiel et de Résolution (ACPR/ Banque de France) – OCC's counterpart organization in France – has addressed what the OCC mentions at Page 6 of your 'preamble – introduction' stating: "AI and machine learning play an increasing role, for example, in fraud identification, transaction monitoring, and loan underwriting and monitoring." ASMG strongly agree this is an important issue.[50] The Autorité de Contrôle Prudentiel et de Résolution (ACPR/Banque de France) did not address modeling, a.k.a. canonical models, in their AI / ML systems review. The closest the ACPR/Banque de France came to discussing canonical models was with their study's hosting of a workshop on the topic 'probability of default (section 8.4)[51] which addressed the issue of the dependency risk towards an AI solution provider (Third Party vendor). In that specific case, the risk is controlled insofar as the provider enables the customer to review all stages leading to the delivered ML model.[52] The banking world are moving to a more immediate, frictionless contact environment with their customers. This is different from what happened in the recent past, when Customer contacts were maintained with meticulous tracking via specific updates added to Customer profiles, via databases. What the 'too-big-to-fail' US financial institutions (FIs) and their Big 5 Canadian banking counterparts are achieving, is the *promise* (down the road?) for data to always be known, always made accessible, and always be shared.

[49] Source: "Data Lake,' by Martin Fowler, [online – MartinFowler.com] Dated: February 5, 2015. See: https://martinfowler.com/bliki/DataLake.html. See *also*: "Multiple Canonical Models," by Martin Fowler, [online – MartinFowler.com] Dated: July 21, 2003. See: https://martinfowler.com/bliki/MultipleCanonicalModels.html.
[50] ASMG will examine AI / machine learning (ML) issues in more depth, in answer to Q.6. 'Payment technologies a.k.a. 'getting interoperability right,' *later* in this Submission.
[51] See: *Ibid*., [Foot Note # *2*] '(ACPR-Banque de France) Page 30 – *a.k.a.* Third Party AI suppliers/providers outside regulatory perimeter.' And, 'Page 33 – *a.k.a.* challenger models'. NB: [at their Foot Note # *17* / Page 33] ACPR state: "To put in perspective the effort required for building an alternative (*i.e.* challenger) model, implementing a credit model for a banking institution, typically involves tens of employees over a timespan of several years, even though its scope is limited to the organization's own data."
[52] See: *Ibid*., [Foot Note # *2*] '(ACPR-Banque de France) Customer review of all provider deliverable(s) *a.k.a*. AI / machine learning (ML) algorithmic model's functioning.'

But if your strategy is to consolidate data centers quickly, a *lift and shift* application – e.g. migration strategy – is likely the best approach. If the strategy is to move to the Cloud for greater scalability and reliability, then application modernization and building new cloud-native applications is possibly the better answer. The key message here is to know your business drivers first, then build the appropriate cloud strategy to support those drivers.

The characteristics of your existing applications will determine the complexity, costs and duration of the effort required to go to the Cloud. Are there mainframe applications? Are there candidates to move to software-as-a service (SaaS)[53] applications? What do the architectures of Cloud ready? Or, will only some applications be considered as migration candidates to the Cloud – maybe even transformed first via modernization face-lifts – e.g. via a transformation into one (or a basket of) microservices? Should some applications be retired?

We will conclude this section of our answer to Q2. 'Hurdles to tech advance and innovation' by examining the topic of Microservices Management - Securing Endpoints.[54] This is the same concept – adapting application programming (product) interfaces (API) façade patterns[55] – which design and DevOps professionals have used repeatedly, and have successfully employed, to scale applications using virtual servers.

The application programming (product) interfaces (API) façade becomes the external official endpoint for the API, and handles communication with the actual microservices. This virtual endpoint offers a strategic and convenient location to scan, scrub, and control requests and responses 'to and from' microservices endpoints. Application programming (product) interface (API) gateways, some ingress controllers, and application delivery controllers, are some options for implementing an API façade.

---

[53] Source: https://www.cloudtp.com/doppler/5-things-every-ceo-know-going-cloud/.
The three most typical Cloud service models are: SaaS, *PaaS* and IaaS. The vendor's (external provider's) *most intensive* delivery offering – asking vendors to manage Applications / the Applications' Stacks & Infrastructure for their Client, is the model called *SaaS* (Software as a Service) - the Client enterprise outsources *all* management and security of the technology to the service provider, and simply owns the administration and account management of IDs. The *middle model*, in which the vendor assumes management responsibility for the Applications' Stacks & Infrastructure layers, is the model called *PaaS* (Platform as a Service) - the cloud service provider moves up the stack and assumes even more responsibility. But the enterprise still owns securing the application itself. Then the third, example, in which the vendor manages Infrastructure *alone* is the model called IaaS (Infrastructure as a Service) - the cloud service provider assumes prime responsibility for managing (and securing) the infrastructure layer *only*. The enterprise still owns, manages and secures 'their' Applications Stack(s), the Application Layer, and the User layer. In all three models, '*security*' is a shared responsibility, but the degree of securing the layers identified is an adjustment in 'shading'.
[54] Source: "Microservices and HTTP/2," By Lori MacVittie, [online - F5 Networks]. Dated: June 8, 2015 See: https://devcentral.f5.com/s/articles/microservices-and-http2. See *also*: "NetOps Primer: What are Microservices?" By Lori MacVittie [online – F5 Networks]. Dated: October 4, 2018. See: https://devcentral.f5.com/s/articles/netops-primer-what-are-microservices-31949.
[55] Source: "Microservices Management: Securing Endpoints," By Lori MacVittie [online – Network Computing]. Dated: May 29, 2018. See: https://www.networkcomputing.com/cloud-infrastructure/microservices-management-securing-endpoints.

Regardless of implementation, by forcing requests to traverse a virtual application programming (product) interface (API), you can better enforce the Security Rule Zero: "Thou shalt not trust user input. Ever." That means, every part of the body of knowledge, called the Hypertext Transfer Protocols (HTTPs) – the set of rules for transferring files, such as: text, graphic images, sound, video, and other multimedia files, on the World Wide Web **–** from the URL to headers, to the payload are assigned 'suspect treatment status' when they arrive at an endpoint. Using an application programming (product) interface (API) facade, you can scan for malicious or malformed content, enforce schemas, and employ additional protections **–** like encryption of sensitive data **–** that may be exchanged in the headers. An application programming (product) interface (API) façade, placed at the ingress, has the added benefit of shielding clients -- whether systems, humans, or things -- from rapidly changing APIs across the microservices' surface. Application programming (product) interface (API) façades are ultimately called upon to process requests.

Using a virtual endpoint also provides a strategic location in the architecture to add additional security measures, to defend against attacks. These may include rate limiting and *bot* detection efforts. Rate limiting at the API façade level prevents microservices from being overwhelmed, and potentially kicking off a series of cascading failures that bring the entire architecture down. '*Bot*' detection can prevent automated scanners from finding and exploiting vulnerabilities in the microservices platforms, and/or vulnerabilities residing in the services (micoservices) themselves.

Microservices possess another weakness, or a key structural vulnerability, we have yet to point out. They require a careful design and implementation of a detailed, well-managed microservices library of functional *families of consistency*, via a centralized logging architecture solution.[56] The *log aggregation library* must reflect accurately the bank's complete e-commerce systemic and operational footprint, and keep it maintained.

What Advanced Systems Management Group (ASMG) have been driving at, in this answer to Q2. 'Hurdles to tech advance and innovation,' is our observation that banking institutions are technology-rich organizations. As such, they are more than adequately prepared to deal with

[56] The *art* of *log collection*(*s*) is as follows: In the most basic sense, you log a message when an action occurs at some point in your code, typically using a logging library like Bunyan for Javascript. The library is configured to send logs to whatever destination you want, like stdout, a local file, or to a log aggregation service like Splunk. Each setup has its pros and cons, and an extensive treatment of each could make this section of the Report way too detailed. To streamline our discussion here, let's review a few logging function best practices uncovered by Jean-Michel Ares' Smart Core technicians. First let's review logging functions. Logs are streams of events continuously flowing. Files are inherently static objects. So, it is a mismatch of abstractions to store logs in files. This mismatch manifests as an additional complexity of parsing log files to generate useful insights and dealing with file size and rotation policies. Secondly, a microservice should not need to know where its logs are going. The execution environment should handle that. That way, you can change the destination of your logs without modifying every single microservice. [Tip: Your microservices should not log to stdout or stderr]. And thirdly, logging should be plug-and-play. A developer should be able to create microservices to whatever language or framework they desire, then drop it into the environment, and have logging working without fiddling with any configurations.

new developments and technology uncertainty, just as the Cloud Players (cloud service providers / CSPs) and large payment processor entities, are equally adept at addressing technological uncertainty.

As strong as their technological prowess may be, they are all focused on network-centric security (and application-centric security) solutions, and not the defense-in-depth security which Advanced Systems Management Group (ASMG) believe is critically absent.

Q3. – What digital issues not addressed

This is a difficult topic to address. The very first activity, bringing 'buyers and sellers' together, causes Advanced Systems Management Group (ASMG) to pause, guardedly, in providing our response. The Bank for International Settlements (BIS-2020)[57] suggest Big Tech firms – Amazon, Apple, Facebook, Google and Microsoft – via their distinctive business models, are extremely well-endowed with: i) network effects (generated by e-commerce platforms, messaging applications, search engines, etc.), and; ii) technology (e.g. artificial intelligence using big data). These business technology-enablers grant them an excessive footprint in their markets, which few other players can match. Due to the predominance of digital advances in every corner of their enterprise, these Big Tech behemoths can exploit their services – provided at almost zero marginal cost – i.e. reducing their rivals to a diminished support role in the marketplace."[58]

Here is an example in the credit underwriting segment of financial service delivery. In the US, Amazon has granted over $1 billion in small business loans to more than 20,000 Amazon customers lenders in the year 2017 alone.[59] Amazon has begun a partnership with the Bank of America (BofA), to greatly expand their small business lending, and is in discussions with the BofA (and soon other banks?) about co-sponsorship of checking account products or services.[60] BigTech firms, such as Amazon, are exploiting their existing networks, and the massive quantities of data generated by those networks, to process and use this data *via* machine learning (ML) models. This is proving that Big Tech "*does*" finance in parallel to serving their non-financial customers. This is troubling, in the sense that by exploiting their 'network effects'

[57] Source: "The technology of retail central bank digital currency," by Raphael Auer, Rainer Böhme. Bank for International Settlements (BIS) Quarterly Review [online], Page 94. Dated: March 1, 2020. See *also*: https://www.bis.org/publ/qtrpdf/r_qt2003j.pdf; *and/or* https://www.bis.org/publ/qtrpdf/r_qt2003j.htm. See *also*: *Ibid*., [Foot Note # *19, 156, 185, 420*].
[58] Source: "BigTech and the changing structure of financial intermediation," By Jon Frost, Leonardo Gambacorta, Yi Huang, Hyun Song Shin and Pablo Zbinden, BIS Working Papers, No. 779, April – 2019, Page 2. See *also*: *Ibid*., [Foot Note # *199, 203, 211*].
[59] Source: Amazon (*unidentified article*). Published by CBInsights (2018).
[60] Source: (2018): "Next Up for Amazon: Checking Accounts," By Glazer, E., L. Hoffman and L. Stevens. Published by Wall Street Journal, March 8, 2018.

and portfolio effects[61] – which BIS claims is both a benefit and a risk (at the same time) – this makes the economic assessment of Big Tech titans – on these issues – a cloudy regulatory matter to deal with.

Software not within scope is a somewhat problematic issue as well.

Here are two examples. You are a computer programmer in a small Company. As a programmer, you are required to, in effect – "write" software within the traditional approach – codifying written instructions in languages such as Python, C++, etc., and then send these (explicit) instructions to the computer, while having to undertake any necessary 'work-arounds." You are experiencing a problem: in your efforts to transfer data to / from a computer application, you have shortcut the task of entering information into a screen, and/or the program misread information from a file. This has compromised your work for the past few weeks. What now?

Or, in a second situation, you have been asked by the small Company you work for, to implement a *chatbot* everyone, particularly that annoying sales department, have been screaming for. To do the required speech recognition tasks required of you, you haven't yet had the discipline (nor motivation) to complete your training module on how to streamline pre-processing tasks, with Gaussian Mixture Models and *hidden* Markov Models of the 'desired state' program?[62] Now what?

Well …what if we change the lens? How about if we really push-the-envelope! If we ask our code writer – you, the employee in question (see the two examples above) – to adopt the *Software 2.0* approach. To do this you will need pursue your (computer) code writing tasks by adopting much more abstract, human *unfriendly* language, such as deciding the weights assigned by a neural network, tasked to apply advanced problem-solving techniques, with no human involvement, in writing the required code base your business use cases require.

Achievable?

---

[61] Source: "Bundling, Tying, and Portfolio Effects: Part 1: Conceptual Issues", By Barry Nalebuff. Published by DTI (economics paper/Paperback), Dated January 1, 2003. NB: "Portfolio effects" can refer to a range of relationships between firms that are not a traditional customer, supplier, or [have a] competitor role.

[62] Source: "The Application of Hidden Markov Models in Speech Recognition," By Mark Gales and Steve Young, [online – NOW publications]. Dated: 2007. See: http://mi.eng.cam.ac.uk/~mjfg/mjfg_NOW.pdf. See *also*: [2nd citation]: http://mi.eng.cam.ac.uk/~mjfg/mjfg_NOW.pdf. Discussion: A Markov process – call it X – with unobservable ("hidden") states – called Hidden Markov Models (HMM;) assumes that there is another process Y whose behavior "depends" on X. The goal is to learn about X by observing Y. In other words, observations are related to the state of the system, but they are typically insufficient to deal with the problem state. Automatic continuous speech recognition (CSR) relies on a set of statistical models representing the various sounds of the language to be recognized. Since speech has temporal structure, and can be encoded as a sequence of spectral vectors spanning the audio frequency range, the Hidden Markov model (HMM) provides a natural framework for constructing such models. Even the best systems are vulnerable to spontaneous speaking styles, non-native or highly accented speech, and high ambient (background) noise. No good alternative to the Hidden Markov model (HMM) has yet been found.

Software 2.0 is a new and emerging programming paradigm. It is based on the premise that it you stop treating neural networks as *only* a pretty good classifier, in the context of slotting it among a class of machine learning (ML) techniques, but instead start treating neural networks as '*the engine*' to produce sets of extrapolations which attempt to solve real-world problems, even though those problem-solving efforts may sometimes fall short of their mark, then we are getting somewhere. This is what the "Google's" and "Tesla's" of the world are pursuing, and many times they are exceeding even beyond their own lofty levels of corporate self-assuredness, and their dramatic belief in their own heightened marketing expectations. Isn't that what all the Big Tech companies do – day-in and day-out?

Andrej Karpathy, Director of AI (Tesla), whom once worked at Google, knows of what he speaks. Karpathy (2018)[63] tells us that Google is currently at the forefront of re-writing large chunks of itself into Software 2.0 code. The "classical stack" of *Software 1.0* is what we're all familiar with. Big tech companies are vying to amass more and more data, and are willing to offer their services for free, in exchange for access to your (User) data. The more classified information they have, the better they'll be able to train their deep learning algorithms. This will, in turn make their services more efficient, than those of their comparable-sized competitors, and bring them more customers. Some of these customers will pay a premium price for Cloud Service Provider (CSP) products and services.[64]

The larger the training data set, the better the performance of the algorithm. Have you heard that observation, in AI and machine learning (ML) circles, mentioned multiple times in the recent past? Big tech companies are vying to amass more and more data, and are willing to offer their services for free, in exchange for access to your (User) data. The more classified information they have, the better they'll be able to train their deep learning algorithms. This will, in turn, make their services more efficient, than those of their comparably-sized competitors, and bring them more customers.

Google are an interesting Company to study. They not only offer a strong cloud service provider (CSP) platform, they also own and operate the franchise of a globally powerful, industry-leading data search engine. The Google Search Engine pushes the statistical strength of the corporation's individual domains, maintaining their marketing dominance. For instance,

[63] Source: "Building the Software 2.0 - Stack by Andrej Karpathy from Tesla," By Andrej Karpathy, [online]. Dated: June 2018. See: https://www.figure-eight.com/building-the-software-2-0-stack-by-andrej-karpathy-from-tesla/. See *also*: See *also*: *Ibid*., [Foot Note # *68, 69*, *73*]. See *also*: https://medium.com/@karpathy/software-2-0-a64152b37c35.

[64] This last point is not always true. Colin Carter's movie software services firm CineSend, and CineSend Stream, is the world's largest repository of film data. CineSend and CineSend stream handle film data in the petrabytes, and are now closing in on Exabyte's of film data transmission. (Exabyte, being 1,000 times *larger than* a *petabyte*. A petabyte being 10^{15} bytes of digital information). IBM Aspera, the world's leading file transfer service [streaming] providers, offer CineSend direct marketing [i.e. sales force] participation to expand CineSend / CineSend Stream reach to prospective industry verticals and Clients. Cloud Service Providers (CSPs) – Amazon Web Serrvice (AWS), and Microsoft Azure at one point, compete to tailor offers to CineSend / CineSend Stream's advantage, to entice them to remain in their services portfolio. Smaller can be better, and may still generate territorial and economic advantage.

Google's internal database structure have evolved so far beyond more traditional systems, that their Artificial Intelligence-enabled platform is transitioning even faster, and has now taken up transformational advances called "The Case for Learned Index Structures."[65] These index structures have replaced core components of more traditionally-oriented data management systems, with a neural network component (or components), clearly outperforming cache-optimized B-Trees by up to seventy (70) per cent in speed, while saving an order-of-magnitude in memory.

Neural network inspired *Software 2.0* advances rarely involve humans in the code writing tasks. There are a lot of weights (typical networks might have millions) and coding, with neural network inspired code writing tasks, is involved '*directly in weights,*' which is *kind- of-hard*. (Mr Karpathy adds: "I tried").

The *Software 2.0* approach specifies some *goal* expected on the behavior of a desirable program (e.g., "satisfy a dataset of input / output [I/O] pairs of examples", or "win a game of Go"). Andrej Karpathy suggests that the next step is to write a rough skeleton of the code (e.g. a neural net architecture), that identifies a subset of the program space to search, and use the computational resources at the neural network's disposal to search this space for a program that works. In the specific case of neural networks, we restrict the search to a continuous subset of the program space where the search process can be made. Not too surprisingly, Karpathy (2018) also suggests that a neural network can be used as a highly adjustable vector function. By this we mean it is possible (and probable) that you will adjust that neural network vector function by changing weights and the biases, but it is hard to change these by hand.

We can let the (neural) network adjust this by itself, by requesting it to train the network under its own command. This can be dome in different ways. It can occur by the formulation of *supervised learning*. Supervised learning is the kind of learning in which we have a data set that has been *labeled* – i.e. we already have the expected output for every input in this data set. This will now act as our 'training data set.' We also need to make sure that we have a labeled data set that we never train the network on. This will be our 'test data set'. The test data set will be used to verify how good the trained network is at classifying *unseen data*.

[65] "The Case for Learned Index Structures" are indexes (e.g. models) adopting B-Tree-Index specification. They model to map a key to the position of a record within a sorted array - a Hash-Index as a model to map a key to a position of a record - within an unsorted array, and a BitMap-Index as a model to indicate if a data record exists or not. The key idea is that a model can learn the sort order or 'structure of lookup keys' and, use this signal to *effectively predict* the position or existence of records. The *Learned Index Structure* will, theoretically, analyze under which conditions learned indexes outperform traditional index structures, and describe the main challenges in designing learned index structure - by using neural nets - we are able to outperform cache-optimized B-Trees by up to seventy (70) per cent in speed, while saving an order-of-magnitude in memory over several real-world data sets. The idea of replacing core components of a data management system through learned models has far reaching implications for future systems design efforts, and this work just provides a glimpse of what might be possible.

When training our neural network, we feed sample by sample from the training data set through the network, and for each of these (occurrences) we inspect the outcome. The reason for this is we need to check how much the outcome differs from what we expected – I.e. the *label.* The difference between what we expected and what we received is called the 'Cost (sometimes referred to as 'Error" or 'Loss'). The *cost* tells us how right (/wrong) our neural network was on this specific sample. This measure – the 'Cost'– can then be used to adjust the network slightly, so that it will be less wrong the next time this sample is fed through the network.[66]

The *Software 2.0* Team (of programmers) will, manually: curate, maintain, massage, clean and label datasets; each labeled as the exemplar (example of) one, or several, literally transcribed programs. The final system will describe *data sets*, with instructions on how they were (/are) compiled, into *Software 2.0* code, via their route of optimization. That is the basic summary of the previous paragraph addressing: *supervised learning,* (neural) network training data, (neural) network testing data, classifying *unseen data*, and measuring the 'Cost (sometimes referred to as 'Error" or 'Loss') of all that the neural, and/or regular network, are feeding a *Software 2.0* Team.

This basic *operational mode* in which neural network *code writing* capabilities or activities might be tackled, via *Software 2.0* advances – possibly even outstripping comparable human agency *code writing* capabilities – is the topic we will turn to next. Here goes the game-changer! It turns out that a large portion of real-world problem-solving network automation advances have the property that '*they may be*' significantly better suited to collect data (or more generally, identify a desirable behavior) than to explicitly write programs.

However, introduce an intelligent *neural network*-guided algorithmic solution – e.g. a detailed programming code-writing *capable Software 2.0*-enabled neural networking solution – and that *Software 2.0*-enabled neural networking algorithmic-based modeling capability may, just may, be able to solve real-world, real-time data analyses problems, by writing actual programming code. A *Software 2.0* Team (of programmers) in their robotized neural network *fully* automated problem-solving mode, may have all the resources required to *automatically* write the *code* that is required to solve the problem*,* then extract the desired result contained in the *data set*, all by themselves.

Software development is an iterative process: a programmer writes a few lines of code, tests it, and then builds upon the results to inform the next few lines of code. Interestingly, these types of processes are exactly what artificial intelligence (AI) systems can automate, taking over the *job of iteration* from software developers, and freeing software developers time to focus on

[66] Source: "Machine Learning: Part 2 – Gradient Descent and Backpropagation," By Tobias Hill [online]. Dated: December 4, 2018. See: https://machinelearning.tobiashill.se/part-2-gradient-descent-and-backpropagation/.

other tasks, and new and innovative solutions[67] that require their attention.

Here are a few new and innovative solutions up close. Andrej Karpathy identifies these examples in 'the world-according-to-Google' mind-frame, and they are things which are truly transformational for our futures, futures which may change, significantly, when low-powered intelligence becomes pervasive around us. Karpathy (2018): "Small, inexpensive chips could come with a pre-trained ConvNet, a speech recognizer, and a WaveNet, a speech synthesis network, all integrated into a small proto-brain. You would attach this proto-brain type device (wrist watch, anyone?) to *stuff*."

Here might be another interesting *Software 2.0* phenomena: If you had a C++ code and someone wanted you to make it twice as fast (at cost-of-performance benchmarking and scaling parameters identified / agreed to, if needed), it would be highly non-trivial to tune the system for the new spec. However, in *Software 2.0* we can take our network, remove half of the channels, retrain everything, and there — it runs exactly at twice the speed (might be it works a bit worse, but only marginally so). Conversely, if you happen to get more data/compute out of your resource you are examining, you can immediately make your program work better, just by adding more channels and retraining everything.[68]

Let's briefly examine a lot of the things Andrej Karpathy has been identifying up to this point. Karpathy (2018) believes strongly that when we give up on trying to address complex problems by writing explicit code, and instead transition the code into the *Software 2.0* stack, then we have left, possibly temporarily, possibly for a significant period of our working day, the space occupied by *Software 1.0*. where if you had C++ code and someone wanted you to make it twice as fast (at a cost of performance if needed, it would be highly non-trivial to tune the system for

[67] Developers spend a great majority of their time reading documentation and debugging code. *Smart programming assistants* can reduce this time by offering just-in-time support and recommendations, such as relevant document, best practices, and code examples. Examples of such assistants include Kitefor Python and Codota for Java. Eyal Katz (Codota) was asked the following questions in an online forum blog: "(What about) the safety of the plug-in? Would the plug-in send a confidential code to some servers?" Eyal Katz (Codota) replied: "Codota does not track individual keystrokes, and does not transmit values of literals (such as the content of Strings). All communication with Codota servers is done over https. Codota only extracts an anonymized summary of the current IDE scope. It does not access other files in your codebase, and does not access other resources on your machine. The anonymized summary sent to Codota is only used for prediction and suggesting code to the user, and is not stored on our servers. Simply put, Codota keeps your code private." Source: "Codota – My First Experience with an AI Assistant in Java," By Eugen Paraschiv [online – Baeldung]. Dated: February 9, 2020. See: https://www.baeldung.com/codota.

[68] Source: "Building the Software 2.0 - Stack by Andrej Karpathy from Tesla," By Andrej Karpathy, [online]. Dated: June 2018. See *also*: *Ibid*., [Foot Note # *63, 69, 73*]. See *also*: https://medium.com/@karpathy/software-2-0-a64152b37c35, '(Karpathy-Tesla director) take our network, remove half of the channels, retrain everything, and there — it runs exactly at twice the speed.'

the new specification.[69]

(Continuing in this vein) Karpathy (2018) states: "Our software is often decomposed into modules that communicate through public functions, APIs, or endpoints. However, if two *Software 2.0* modules that were originally trained separately interact, we can easily back-propagate through the whole. Think about how amazing it could be if your web browser could automatically re-design the low-level system instructions 10 stacks down to achieve a higher efficiency in loading web pages. With *Software 2.0*, this is the default behavior. *It is better than you.* Finally, and most importantly, a neural network is a better piece of code than anything you or I can come up with in a large fraction of valuable verticals, which currently at the very least involve anything to do with images/video and sound/speech.[70]"

Video is an area which is starting to really take off! *Visual Recognition* used to consist of engineered features with a bit of machine learning sprinkled on top at the end (e.g., an SVM – called a support-vector network)[71]. Since then, Andrej Karpathy has discovered much more powerful visual features by obtaining large datasets (e.g. ImageNet)[72] and searching in the space

[69] Source: "Building the Software 2.0 - Stack by Andrej Karpathy from Tesla," By Andrej Karpathy, [online]. Dated: June 2018. See *also*: *Ibid* – [Foot Note # *63, 68, 73*]. See *also*: https://medium.com/@karpathy/software-2-0-a64152b37c35, '(Karpathy-Tesla director) on Software 2.0 *self-writing* its required programming code via AI-enabled neural network solutions capability.'

[70] Hardware and software DevOps people take note. There is no dynamically allocated memory anywhere in the neural network system, so there is next to no possibility of swapping to disk, or experiencing memory leaks, that you must hunt down in your code base. Can Software 2.0 fail? Sure. The Software 2.0 stack can fail in unintuitive and embarrassing ways. Or worse, they can silently fail, by adopting biases in their training data without warning. Or even this can happen: Software 2.0 inputs / outputs (I/O's) may be difficult to properly analyze and examine, when their sizes are in the millions in most cases. We are still discovering some of the peculiar properties of this stack. For instance, the existence of adversarial examples involving cyberthreat actors, and their attacks, highlights the unintuitive nature of this stack. Source: "Attacking Machine Learning with Adversarial Examples," By Ian Goodfellow, Nicolas Papernot *et. al*., [online – openai.com]. Dated: February 24, 2017. See: https://openai.com/blog/adversarial-example-research/.

[71] Source: https://towardsdatascience.com/support-vector-machine-introduction-to-machine-learning-algorithms-934a444fca47. Discussion: SVMs (also termed support-vector networks) act as supervised learning models, with associated learning algorithms, These SVMs will analyze data used for classification and regression analysis, by SVM training algorithms. These algorithms will build a model that assigns new examples to one category or the other, making it a non-probabilistic binary linear classifier (although methods such as Platt scaling exist, and may be useful in SVM, or any other probabilistic classification setting). An SVM model will serve as the representation of the examples 'under examination', and may usefully point to proscribed positions, or geo-locations in space. These points in space will be mapped so that the examples of the separate categories are divided by a clear gap, that will prove to be as wide as possible. New examples are then mapped into that same space, and predicted to belong to a category based on the side of the gap on which they fall.

[72] ImageNet is a publicly available resource, although the actual images are not owned by ImageNet, with over 14 million hand-annotated images using algorithms to identify objects in the datasets images with the lowest error rate. Many see it as the catalyst for the AI boom today. Ms. Fei Li, founder of ImageNet, now chief scientist at Google Cloud, brought this to fruition. Ms. Lei realized an initial brake on the project idea: the best algorithm wouldn't work well if the data it learned from didn't reflect the real world. Solution? Ms Fei Li *built* a better *dataset*. Source: "The data that transformed AI research and possibly the world," By Dave Gershgorn, AI reporter, [online – Quartz]. Dated: July 26, 2017. See: https://qz.com/1034972/the-data-that-changed-the-direction-of-ai-research-and-possibly-the-world/.

of Convolutional Neural Network architectures. Mr. Karpathy recently suggested "we don't even trust ourselves to hand-code the architectures, and we've begun searching over those as well." The *Software 2.0* stack aids in *Speech Recognition* research, which used to involve a lot of preprocessing, with Gaussian Mixture Models and *hidden* Markov Models, but today consists almost entirely of neural net *stuff*. Speech synthesis has historically been approached with various stitching mechanisms, but today the state of the art models are large ConvNets (e.g. WaveNet) that produce raw audio signal outputs.

Regret? I've had a few: (Karpathy) "At the end of the optimization we're left with large networks that work well, but it's very hard to tell how. Across many applications areas, we'll be left with a choice of using a ninety (90) per cent accurate model we understand, or ninety-nine (99) per cent accurate model we don't.

This leaves us with only one further point to make. *Software 1.0* revels in the code we write. For example, we've built up a vast amount of tooling that assists humans in writing *Software 1.0* code,[73] such as powerful Integrated Development Environments (IDEs).[74] In the *Software 2.0* stack, the programming is done by accumulating, massaging and cleaning datasets. For example, when the network fails in some hard or rare cases, we do not fix those predictions by writing code, but by including more labeled examples of those cases. Who is going to develop the first Software 2.0 Integrated Development Environments (IDEs), which help with all the workflows in accumulating, visualizing, cleaning, labeling, and sourcing datasets? Perhaps the Integrated Development Environments (IDEs) *bubble up* images that the network suspects are mislabeled, based on the per-example loss, or assists in labeling by seeding labels with predictions, or suggests useful examples to label based on the uncertainty of the network's predictions.

Better still, data – or metadata more particularly – could tag, label and track *itself* for violations, and send a community-of-interest (C-o-I) the alerting message, based on business data-domain modeling efforts, on data of whatever form it constitutes, and from whatever source or location it is lodged. Worth a look!

[73] Source: "Building the Software 2.0 - Stack by Andrej Karpathy from Tesla," By Andrej Karpathy, [online]. Dated: June 2018. See *also*: *Ibid* – [Foot Note # *63, 68, 69*]. '(Karpathy-Tesla) on Software 2.0 *self-writing* its required programming code via AI-enabled neural network solutions capability.' See *also*: https://medium.com/@karpathy/software-2-0-a64152b37c35.

[74] Integrated Development Environment (IDE) is an application which provides programmers and developers with basic tools to write and test software. An IDE normally consists of at least a source code editor, build automation tools, and a debugger. IDEs may also have features like syntax highlighting, profilers, go-to-def, git integration, and more. Source: "Integrated Development Environment," By Kenneth Leroy Busbee [online – rebus community]. Dated: December 15, 2018. See: https://press.rebus.community/programmingfundamentals/chapter/integrated-development-environment/.

Q4. – Crypto assets / crypto currencies

This question will be answered in a straight forward manner. First, a very succinct introduction to this question's topic is in order. Oasmene Mandeng, Visiting Professor at the London School of Economics (LSE), addressed basic regulatory guidance for addressing crypto assets which we will quote from as our starting point. The regulation of crypto-assets inevitably involves concerns for: i) consumer and investor protection ii) money laundering and iii) terrorism financing. Mandeng (2019) has offered that in the US, some regulatory guidance has ventured from US court rulings to special regulatory regimes (sandboxes), but not much.[75]

The Top Ten (10) Main (largest) crypto coins – a coin being a crypto asset in Mandeng's terminology, and not a currency – represent eighty-five (85) per cent of the total market capitalization in these relatively *new* crypto asset releases. Mandeng's distinction is that crypto-currencies unfittingly conveys the notion of currency, therefore in his paper Mandeng (2019) prefers to use the commonly accepted term *crypto-assets* to cover economic and financial assets. We will go with that distinction. The sector, Mandeng points out, has illustrated considerable innovation with the introduction of distributed ledger technology (DLT), with applications in payments, value chain management, identity, and crowd funding products and services.

The Top ranked crypto asset in Mandeng's Top Twenty Listing is Bitcoin. Bitcoin serves as a convertible medium of exchange, in the limited sense that its value is based on perceived demand, and it does not constitute a counterpart liability or financial claim. A difference decentralized network is Ethereum, with the *ether* token – considered an inside currency or non-convertible medium of exchange. Ether does not have a fixed issuance ceiling and the amount of *ether* being put into circulation is unknown, hence its value is tied to the use of the Ethereum blockchain *only*. Ethereum is ranked number three (3) on Mandeng's Top Ten (10) 'Main crypto-assets List'. Ethereum gets a little tricky, in that its decentralized network substitutes centralized network servers and clouds employing decentralized applications (called Dapps – with a capital 'D' – signifying the decentralized nature of the app). Dapps allow smart

[75] Source: "Basic principles for regulating crypto-assets," By Oasmene J. Manding, London School of Economics (LSE) [online]. Dated: June 20, 2019. See *also*: *Ibid*., [Foot Note # *77*]. See *also*: OJM-Basic-principles-for-regulating-crypto-assets1/pdf. Discussion: Mandeng (2019) identified Chicago-based derivatives exchanges, Cboe and the CME – both launching bitcoin futures markets circa December 2017 – and briefly mentioned that in 2015 the Commodities and Futures Trading Commission (CFTC) classified bitcoin and other crypto instruments as commodities and assumed oversight. Mandeng (2019) also quoted the June 2018 SEC ruling, stating (crypto asset) tokens, such as issued by Ethereum, were securities, and that lack of registration with the SEC violated securities law. Source: "SEC issues investigative report concluding decentralized autonomous organization (DAO) tokens were securities," SEC -Press release. Dated: July 25, 20-17, Page 131.

contracts[76] to execute specific codes which run the programmable Ethereum blockchain. Mandeng's (2019) basic principles paper on crypto-assets[77] mentions stablecoins. Stablecoins are assets backed by other investments or coin / currency values. (Done).

Advanced Systems Management Group (ASMG) take exception with Professor Mandeng's statement *a.k.a.* [Cryptography and Technology / Point 4 – Page 15]: "Regulation should be based strictly on the functions of crypto-assets and not be guided by the underlying technology." Mandeng (2019) seems to rule distributed ledger technology (DLT) has reached a sacrosanct standing. Is Mandeng (2019) suggesting that [the distributed ledger *itself*] giving rise to financial regulation which doesn't touch 'the ledger', is somehow the ideal to be shooting for? If ASMG's Submission to the OCC has one take-home opinion, above all else, it is this: technology and 'the ledger' are so intertwined, that this statement of Mandeng's is a very misconstrued reflection on the ethics and morality of the decentralized ledger, which has – time and time again – betrayed any element of *trust* placed in it by consumer and investor transactors', attempting to benefit from it as an asset class.

Let's get the cards on the table *face-up*!

Binance Coin the crypto token / crypto asset exchange – number fourteen (14) on Mandeng's (2019) Top 20 *globally* ranked Main Crypto-asset Listing – closed their US trading and deposit operations in the US in June 2019. Binance will issue its upcoming new-to-be-launched stablecoin with an unknown partner, named BAM Trading Services. BAM Trading Services will license Binance's crypto assets, including its trading apps.[78]

[76] A smart contract is a computer program or a transaction protocol which is intended to automatically execute, control or document legally relevant events and actions according to terms of an agreement. The US National Institute of Standards and Technology (NIST) describes a smart contract as a "collection of code and data (sometimes referred to as functions and state) that is deployed using cryptographically signed transactions on the blockchain network." Technology, very heavily defined, i.e. this is a technological backbone to a *new* form of asset management.

[77] Source: "Basic principles for regulating crypto-assets," By Oasmene J. Manding, London School of Economics (LSE) [online]. Dated: June 20, 2019. See: OJM-Basic-principles-for-regulating-crypto-assets1/pdf. See *also*: *Ibid*., [Foot Note # *75*].

[78] Why it *matters*: Fifteen (15) per cent of Binance's trading and depositing clientele globally originates (or are domiciled) in the US. Binance's new stablecoin will be pegged to fiat currencies, but will exclude the US dollar in its currency pegging regime. Binance CEO Changpeng Zhao was recently put on the spot to explain why Binance accessed the camera, and recording capability of its Customers' through the Binance app. Mt Zhao had to admit to reviewing the code to remove the audio recording permission (which had been set to automatically record traffic), plus remove other permissions – list not provided. Binance claim not to sell user data, such as KYC data, with blockchain analytics. Binance has been on the hot seat before: Mr. Zhao previously told Cointelegraph that apps with access to the user's clipboards pose the greatest threat, since from the clipboard threat actors can steal a Binance crypto holder's private keys. Mr. Zhao: "[Quoted in Cointelegraph]: Most crypto applications that ask for your key material can simply steal your funds, and you *trust* they don't." See *also*: *Ibid*., [Foot Note # *156*]. See *also*: "As TikTok 'Spyware' Rumor Swirls, Crypto Apps Safety in the Spotlight," By Stephen O'Neal [online – Cointelegraph]. Dated July 24, 2020.

Data collection sits in a gray area, in regulatory parlance today. Plus, when users download a 'crypto asset' app, they offer *approval by default* meaning: Who read the terms and conditions specifying data collection actions and activities? Users just routinely (falsely) assume the only thing the crypto app is accessing is their email address, and maybe their approximate geo-location. Hartej Sawhney - CEO Zokyo suggests "many apps track users even when their mobile app is not in use. Plus, some microphones can be accessed as well."[79]

And for some more sobering news. Alex Heid, Security Scorecard, an information security company, states: "Attackers use malware comprised developer repositories and social engineering to obtain wallet and private keys of vulnerable users, Two examples – a rogue application attack on CoPay wallets via a 'compromised JavaScript library' in 2018, and secondly – the attack on Ethereum, via a node messaging service in 2019. Crypto [user-downloaded] apps require the provision of Know Your Client / anti-money laundering (KYC/AML) compliance, but this does not deter hackers.[80]"

Nym Technologies' Harry Halpin concurs with Alex Heid. Mr. Halpin suggests: "Sending cryptocurrency to a public ledger allows anyone to spy on your transaction. Even developers often build technology that they believe is secure and private, and screw it up!."[81] Harry Halpin concludes by wishing academics or industry, with a good track record behind them, need to fix these security violations and technological vulnerabilities before crypto users' funds – or personal data – gets compromised or stolen.

[79] Source: "As TikTok 'Spyware' Rumor Swirls, Crypto Apps Safety in the Spotlight," By Stephen O'Neal [online – Cointelegraph]. Dated July 24, 2020. See *also*: *Ibid*., [Foot Note # *78, 157*].

[80] Source: "Vendor Profile: Security Scorecard," By Hugh Taylor [online – Journal of Cyber Policy]. Dated: April 23, 2020. See: https://journalofcyberpolicy.com/2020/04/23/vendor-profile-securityscorecard/.
See also: https://securityscorecard.com/product/security-data. 'Security Scorecard's Alex Heid on app vulnerabilities.' Discussion: Alex Heid describes his Company as follows: "SecurityScorecard provides cybersecurity ratings for thousands of companies worldwide. Our technology scans a range of public information, including dark web data, relating to a given company. From this, they derive a cyber risk profile that rates the security of the company's networks, DNS, endpoint security, malware infections, patching and so forth." See *also*: *Ibid*., [Foot Note: # *81*].

[81] Source: "The Next Generation of Privacy Infrastructure," By Harry Halpin [online – nymtech.net]. Dated: 2020. See *also*: *Ibid*., [Foot Note # *80*] '(Nym Technologies-2020) Harry Halpin on app vulnerabilities.' Discussion: Nym Technologies – a Swiss blockchain startup – is building a decentralized and tokenized infrastructure providing holistic privacy from the network layer to the application layer. Nym's network claims to be decentralized, permissionless and incentivized. Nym's Harry Halpin (2020) hopes developers will contribute with their 'builds of applications' that can *anonymize metadata,* both at the level of network traffic, and at the level of applications. Nym is designed to – transmit data without access to, or knowledge of the source, location or content of that data – by the network or its participants. Interesting, but not an approach ASMG would consider supporting. See: https://nymtech.net/nym-litepaper.pdf. [Halpin (2020) optimistically claims: Nym will "ensure the NYM network's *privacy-enhanced network-layer* will resist to even NSA and GCHQ-level adversaries' threat vector penetration capabilities". Since this is all outsourced to third party developers, 'We shall see.'

On Page 8 [12 CFR Part 7, Subpart E] the OCC address ten (10) activities[82] which require a re-cast with crypto issues in mind. *Plus*, on Page 8 [Page 8: 12 CFR part 155] the OCC address two activities with respect to Federal savings associations: (1) Federal savings associations' use of electronic means and facilities generally, and; (2) (requirements for) Federal Savings Associations using electronic means and facilities. These latter two topics have a decidedly technological-leaning connotation.

We will park the other nine (9) issues for now. They are all answered in this Submission, in some manner or other, which will be highlighted as Advanced Systems Management Group (ASMG) proceeds through the narrative we deploy in answering the Questions individually. For the remainder of this section on 'Crypto assets / crypto currencies,' ASMG will assess the launch of a crypto asset manager (a 'crypto' Bank). Secondly, an in-depth examination of a mobile payments provider offering a *permissioned* / moderated blockchain retail distributed application (dapp[83]) will be profiled.

A *new* entry in the crypto asset management theatre has just been announced recently. Partly this is, no doubt, due to the ongoing awareness by Banking institutions that they are faced with the generational challenge of finding younger, more tech-savvy customers. More importantly, this new Banking entrant claims to be a driving force behind regulatory changes in the state of Wyoming. The Avanti Bank and Trust was created through a special purpose depository certificate. Avanti Bank and Trust will be a custodian of crypto assets as well as offering direct access to the Federal Reserve through a master account. This is a novel approach, and introduces a business structure which features financial asset custodians offering a depository (crypto) asset function and a crypto asset exchange service under the same roof.

[82] Source: OCC Response Document – [*title*] National Bank and Federal Savings Association Digital Activities – 12 CFR Parts 7 & 155 *a.k.a.* [Docket ID OCC-2019-00288] RIN 155-AE74. Discussion: OCC - Page 8: 12 CFR part 7, subpart E addresses: (1) electronic activities that are part of or incidental to the business of banking; (2) furnishing of products and services by electronic means and facilities; (3) engaging in an electronic activity that is comprised of several component activities (composite authority); (4) the sale of excess electronic capacity and by-products; (5) acting as digital certification authority; (6) data processing; (7) correspondent services; (8) the location of a national bank conducting electronic activities; (9) the location under 12 U.S.C. 85 of national banks operating exclusively through the Internet; and (10) shared electronic space.

[83] Dapp (or 'dapp,' either/or naming convention works, just fine) – in the case of the Company ASMG have selected to profile their crypto assets / crypto wallet, a Company named Electroneum, *also* referred to as ETN – have built their crypto *product* 'off the Monero codebase,' on a network which has a *decentralised layer*, but is not necessarily decentralized. Electroneum (ETN) CEO Richard Ells states: "The Electroneum (ETN) blockchain is 'open source on GitHub,' which in essence – means, that if we (Electroneum/ETN) shut down for any given reason, all those running a node on our blockchain could instantly re-instate an older copy of our software, and add some simple coding, and begin running a Proof-of-Work system, via ASICS or ASIC resistant." AnyTask is Electroneum's (ETN's) global freelance platform. Electroneum (ETN) is distributed, but its app is best thought of as a *dapp*. Source: "Mobile App Daily: The difference between a dapp and an app," [online]. Dated: Not provided. See *also*: *Ibid*., [Foot Note # 87 – 92 *inclusive*] '(Electroneum/ETN) for a *full description* of the Company, and product offering.'

Avanti Bank and Trust will assume the crypto asset exchanges as deposits into accounts residing inside Avanti. This business model, which combine crypto custodian functions with crypto exchange functions transfers – with both services twinned together – the fiduciary obligation, and the risk, to Avanti Bank and Trust themselves.[84] This creates an interesting confluence between mainstream finance and decentralized finance (DiFi). Ms. Caitlin Long, Avanti CEO and Founder, views the creation of this crypto-friendly institution as the natural evolution in decentralized finance (DeFi). Caitlin Long notes that many [crypto] DeFi banking services providers in the US are served by three relatively small banks – Silvergate, Signature and Metropolitan - with whom Avanti will now join their ranks. Ms. Long mentions that up until now, the JP Morgan's (and Citibank's) of the world-of-finance have refused to compete in this financial vertical. They have had good reason.

Operation Choke Point, a federal Deposit Insurance Corporation (FDIC) program, during the Obama administration starting in 2013, mandated the FDIC to target *not politically favored* (NPF) industries, pay day loan companies, gambling operators, porn and firearms operations, to strong supervision and regulatory interventions and fines. Unfortunately for the crypto currency industry, they were blind-sided and swept into the program, as thought-to-be purveyor of terrorist financial gains, money-laundering proceeds, proceeds from drug trafficking and financial crimes, etc. Obviously, the JP Morgan's and Citibank's, and other depository Financial Institutions (FIs) would be dinged, if they traded in 'crypto' assets – (thereby) deemed too high risk an endeavor – which would trigger their compliance departments having to increase their firm's capital requirements, even more.

When asked what the current major challenge were facing crypto transactor's today, Avanti's Caitlin Long responded that the unregulated nature of nature of their industry was problematic, stifling growth opportunities, and depriving them of employees with prior experience in the regulated financial services industry. Ms. Long (Avanti) feels very strongly that the digital asset ecosystem is encroaching 'sometime soon' upon a safe-landing in attracting a major institutional investor, such as CaIPERS, the CPPIB, or the Ontario Teachers' Pension Plan, over due course. As these major players see the fiduciary and regulatory standards start to take shape, their reluctance to own crypto assets may be re-assessed, and crypto asset stewardship (or ownership) may occur.[85]

---

[84] Source: "National Banks as Digital Asset Custodians," By Chris Kentouris, Editor [online – FinOps Report]. Dated: August 14, 2020. Discussion" How have digital asset custodians prepared for risk obligations? There are four ways: i) cold wallets ii) asset separation iii) multi-signature authentication, and iv) cybersecurity insurance. See *also*: *Ibid*., [Foot Note # *519*] '(Kentouris-2020) technological and risk management fiduciary responsibilities highlighted *vis-a-vis* serving the role of (crypto) Custodian Service Provider.'

[85] Source: "Court Analogizes Coinbase to 'Traditional Bank' for Purposes of Fourth Amendment Privacy Protection," By David Zaslowsky [online – bakermckenzie]. Dated: July 2, 2020. '(Zaslowski-2020) US Fifth Circuit Court rules Coinbase is a virtual currency provider.' The Fifth Circuit Court's ruling found that Bitcoin information is limited, and that transacting through Bitcoin is not "a pervasive [or] insistent part of daily life." The US Fifth Circuit Court further held that the Coinbase records are more akin to a bank's records, than to cell phone data. It said: "Coinbase is a financial institution that provides Bitcoin users with a method for transferring Bitcoin. The main difference between Coinbase and traditional banks, is that Coinbase deals with virtual currency. while traditional

Even traditional asset owners and corporate treasurers', once they see the regulatory landscape solidify – or at least operate on an equal footing to other *mainstream* investment products and services – may push traditional asset owners and corporate treasurers to overcome their reluctance to own, and manage crypto assets. Ms. Long sites the movement by more risk-taking institutions, such as hedge funds and family offices – hopefully now examining crypto assets a little more seriously than in the past – may be a promising sign. As well, these investors – not insignificant in the size of their financial holdings – are beginning to appreciate that decentralized finance (DeFi) may be able to more accurately capture, or portray, counterparty credit-worthiness on the distributed ledger / blockchain. For all these reasons, Avanti Bank and Trust would like to see more *all-encompassing* crypto asset regulations, to assist Avanti prove their credibility and solvency to their Clients.[86]

In short, the lack of banking service fiat *on*- and *off-ramps – currency conversion mechanisms* – to allow crypto asset markets to operate identical to how the traditional banking sector's currency exchange market mechanisms operate, has hurt the crypto industry. This is particularly the case since the big banks stopped crypto exchanges from having fiat on- and off-ramps (or maybe, never even allowed them in the first place?), which has led directly to the 'make-gap' invention of stablecoins. This is the issue, in regulatory governance terms, which Avanti Bank and Trust are attempting to resolve.

Our second topic of examination is a mobile (crypto) payments platform called Electroneum (ETN). Advanced Systems Management Group (ASMG) selected this platform to profile after dismissing the PI Network as a candidate for a business use-case analysis. The PI Network is a pseudo-payments platform, not yet making payments in real-time, which initially caught our

---

banks deal with physical currency. But both are subject to the Bank Secrecy Act (BSA) as regulated financial institutions. Both keep records of customer identities and currency transactions." See *also*: CipherTrace Crypto Advisory 7/13 [2020], John Jefferies, editor/ author. Dated: July 13, 2020. See *also*: *Ibid*., [Foot Note # *136*, *143*]. According to the recent ruling of a three-judge panel from the US Fifth Circuit courts, the American government's Fourth Amendment does not apply to bitcoin transaction data used in a crime, if they stem from virtual currency exchanges. The Fourth Amendment protects, the defendant alleged, his bitcoin transaction history as private / confidential. Judge Haynes, US Fifth Circuit court, explaining why this was struck down, states: "Coinbase is a financial institution, a virtual currency exchange, that provides Bitcoin users with a method for transferring bitcoin." Coinbase, in other words, operates identical to traditional banking's currency exchange mechanisms – which guide and enforce all appropriate measures to prevent the criminal abuse of economic assets – only now these anti-money laundering (AML) and Fraud provisions will now apply equally to *crypto* virtual assets. See *also*: "4th Amendment Does Not Protect Bitcoin Data, US Fifth Circuit Rules," By Jamie Redman [online – Bitcoin.com]. Dated: July 5, 2020. See: https://news.bitcoin.com/4th-amendment-does-not-protect-bitcoin-data-us-fifth-circuit-court-rules/. NB: This issue is summarized, very briefly, at Foot Note # 156 (Auer/Böhme-2019).

[86] Jay Hao, CEO of OKEx, a crypto asset start-up, was even more to the point. Mr. Hao cited Libra (Facebook) as the wrong poster child for the sector. Facebook have problems with unauthorized collection of user data, and data leakage issues, which seriously hurts market confidence in all-things-crypto. Lawmakers' distrust of Facebook even exceeds their reservations about crypto currencies, or of DeFi principles espousing the distributed ledger / blockchain technological base itself. Source: "Sharing Thoughts on Security, OKEx's (CEO) Jay Ho Says Customers Come First," By Vadim Krekotin [Cointelegraph China CEO]. Dated April 23, 2020.
See: https://cointelegraph.com/news/sharing-thoughts-on-security-okexs-jay-hao-says-customers-come-first. See *also*: *Ibid*., [Foot Note # *95*, *354*, *355*].

attention for its [promotion of the Stanford University-originating Stellar Consensus Protocol (SCP) fault tolerance solution. Stellar Consensus Protocol (SCP) fault tolerance solution uses both the Federated Agreement and the Byzantine Agreement for fault tolerance measures. The SCP serves to validate a quorum for a payment transaction by watching other nodes to vouch for their 'truthfulness'. In a blockchain, fault tolerance failures of up to thirty-three (33) per cent of the nodes are acceptable, without negatively impacting the functioning of the blockchain. Stellar Consensus Protocol (SCP) is allegedly calibrated to produce a node 'block' every 3-5 seconds, improving on Bitcoin's lethargic 10-minute transaction processing time delay.

Once we examined PI Network up-close – a competitor to Electroneum (ETN) – PI Network had failed to provide a formal governance mechanics 'blueprint', nor a description of its official mainnet, and we shifted to a mobile (digital permissioned) digital distributed (permissioned / moderated) payments solution provider which would openly publish all its foundational elements, as an appropriate substitute.

Electroneum (ETN) is a permissioned / moderated blockchain[87] payments platform for mobile devices. Electroneum (ETN) allows its distributed app (dapp) to complete payment on-line, from a smartphone to an in-store (on-site) retailer or vendor. Electroneum (ETN) advertises itself as one of the first Know Your Client / anti-money laundering (KYC/AML) crypto-based solutions provider globally.

Electroneum (ETN) is built on the Monero code base[88] using distributed peer-to-peer (P2P) networking consensus. Electroneum (ETN) supports the Ledger Nano S hardware wallet: 1) certified by France's ANSSI cyber security agency; 2) integrates a Secure Element (SE) *chip*, wherein the chip hosts crypto private keys; 3) Electroneum (ETN) owns its own custom operating system (OS/BOLUS) serving to isolate smart phone apps from each other; 4)

[87] The moderated model - or *moderated* blockchain model - works like this: A malicious actor would be required to take control over a minimum of two (2) unique daemon distributions, and the corresponding validator's key. This, were it to happen, may massively disrupt the Electroneum distributed ledger/blockchain. Even if this event were to occur, Electroneum (ETN) administrators' can instantly detect compromised nodes, and resolve their (that mining node's access rights) in seconds, and will broadcast a message to the whole ETN network. This, Electroneum (ETN) states, is provisioned by ETN's *moderated* blockchain model. See *also*: *Ibid*., [Foot Note # *88*] 'Electroneum (ETN) - [*citation*] predictions on Electroneum (ETN) operates 'ring fencing *a.k.a.* payments.' See *also*: *Ibid*., [Foot Note # *89*] 'Electroneum (ETN) - [*citation*] predictions on pricing, and technical deep-drill (as prepared by Competitor Changelly). See *also*: *Ibid*., [Foot Note # *90*] 'Electroneum (ETN) - [*citation*] Use-case on Electroneum (ETN) prepared by 'The Analyst Team at OK.Com.' See *also*: *Ibid*., [Foot Note # *91*] 'Electroneum (ETN) - [*citation*] market statistics, etc.'

[88] Different from Monero, Electroneum (ETN) asks that you register under your identity, but a trusted 3rd party performs the payment transaction through 'ring-fencing'. Ring-fencing involves a confirmation being issued that you have funds in your digital wallet and are not double-spending. This is a form of *escrow* transacting, a process conducted by the 3rd party on ETN's behalf. The fee for the service id dependent on the traffic volume on the network at the time, a calculation with a familiarity to how Uber and Lyft charge for their services. A vendor notification that the transaction has completed is issued to the vendor in approximately one hour from the point-of-sale.

Electroneum (ETN) integrates with Google's Play Store; 5) most mining[89] is conducted by Electroneum's (ETN's) mobile miner running in the background, making it easy to transfer between different users and applications on the smart phone; 6) Electroneum (ETN) is supported by mobile operating systems Android and iOS; 7) Electroneum (ETN) deploys the Ledger product authenticity checker which determines if (and which) 3rd party compromise action(s) may have occurred. Electroneum (ETN) employs HackerOne as a vulnerability assessor and bug bounty platform service. Electroneum (ETN) has a 25-word mnemonic seed, only displayed once (which requires user safeguarding) plus - employs an encrypted 'Pass phase" for sign-on.

Summing up, the Electroneum (ETN) mobile distributed / moderated payment ecommerce solution offers a viable payment service, by 3rd Party escrow (*escrow* - held by Electroneum *a.k.a.* ETN), and performs reasonable anti-volatility benefits for the merchant.[90] Recently, Electroneum (ETN) announced an expansion to 140+ countries for mobile 'top-ups', and identified its customer base as sitting now at four (4) million devices, using 600 mobile network operators (MNOs) globally.

The relevance of the mobile (crypto) payments segment is vast. The Global System for Mobile Communications Association (GSMA) said in their 2019 mobile economy report that at least one mobile top-up takes place every second, a statistic that highlights the demand there is for airtime and data top-ups around the world. By the end of 2018, 5.1 billion people around the world had subscribed to mobile services, accounting for sixty-seven (67) per cent of the global population. The GSMA predicts that by the end of 2025, 5.8 billion people will have subscribed to mobile services, generating US$3.9 trillion of economic value, equivalent to 4.6 per cent of global GDP.[91]

[89] Mining can be conducted according to a github technical (online) notification: ETN prefers to publicize its 'background-running' mining operation, as the preferred route. To pursue a mining operation, by CPU or ASIC – assist, a *github* technical note suggests: Electroneum (ENT) can be mined via the Cryptonight algorithm for mobile devices. The algorithm will mine and assess functions automatically. The ETN Dapp functions as a marketing AirDrop. To perform mining via the CPU: use *xmr-stak-cpu* at the processor stage, which gives the program a *hash* rate more than the Claymore CPU. (NB: Instructions for video card / ASIC-assisted mining, see *citation*). Source: "Electroneum (ENT) Mining Price Prediction for 2020, 2023 and 2030," By Mariia Rousey [online article] Changelly. Dated: January 20020. See: changelly.com.

[90] This Electroneum (ETN) use-case overview has been sourced, as published, at: 'The Analyst Team.' See: OK.Com. See *also*: *Ibid*., [Foot Note # *87 – 91*].

[91] Source: "Electroneum (ETN) expands global mobile top-ups to 140+ countries - earning Electroneum (ETN) on AnyTask is now more appealing," By Surya Maneesh, Malta Blockchain News Summit Economic Newsletter [online]. Dated: February 26, 2020. See: https://www.maltablockchainsummit.com/news/electroneum-expands-global-mobile-top-ups. See *also*: *Ibid*., [Foot Note # *87 – 91*]. Discussion: For ASMG's reservations regarding mobile device data security measures, or lack thereof, see Question 11.

Q5. – Distributed ledger technology (DLT) for banking

Our first thought when we hear the term blockchain is usually our most lasting and enduring impression. Why? For any advance with the hype which blockchain has generated, whether establishing new and novel client-to-institutional trust relationships, disrupting the monolithic data supply chain built up by financial institutions (FIs) over decades, or the rapid advance of inference engines to make sense of the data we encounter in a day – all these occurrences are expending our time and taxing our efforts – dealing with, and benefiting from, distributed ledger technologies (DLTs).

Without even defining what the distributed ledger consists of, we have already set our sights at Advanced Systems Management Group (ASMG) to move the goal posts, and address the technologies at the centre of it all. The challenge is that the effort to address big data[92] requires conscientious "persisting" and "uniting" of disparate data sets, some of which may even be hosted by third party systems – on-site [*theirs*], at the edge or in the cloud. In the middle of these pressing developments, distributed ledger offers the hope for a better way: decentralized, immutable data blocks chained together, with the expressed interest of making everything 'unknown' known again.

Here is an interesting example from another sector's experience. The Mobility Open Blockchain Initiative (MOBI) is a transportation industry standards-setting initiative for smart mobility via blockchain adoption. Examining the Mobility Open Blockchain Initiative's (MOBI's) most recent press release,[93] "MOBI and BMW, Ford, GM, Groupe Renault and Honda (with several more automakers) announced their stakeholder proof-of-Concept for a blockchain-based vehicle identity." Amid all the fanfare, the article cites the pilot program's ability to unlock: 1) mobility payments networks; 2) V2V – V2X transactions; 3) electric vehicle-to-grid integration; 4) usage-based services; 5) fleet operations; 6) congestion pricing 'on roadways,' and; 7) a carbon footprint.

The Mobility Open Blockchain Initiative (MOBI) goes on to state that smart contracts enabling direct, low cost micropayments to (and from) multiple parties will accelerate existing trends toward pay-per-use mobility and mobility-as-a-service. One tricky question remains: This vehicle identifier – is communicated from what road-side sensor? And from that road-side sensor *pinged* to (or from) – the vehicle's on-board sensors, mounted in the dashboard-installed transmitter – to what mobility-guidance systems communications tower? And from that mobility-guidance systems communications tower 'traffic comptroller' to what vendor(s)

[92] Big data – and this is not a definition, but merely a set of observations – employs powerful queries' libraries (often called NoSQL) are changing the dynamics of business. We now think of data volumes in petabytes (or exabytes/EBs), large SQL infrastructures have *sharded* their existing database resources to create more flexible, horizontally scaled environments, to leverage big data tools and capabilities.
[93] Source: "The World's Largest Automakers, Along with MOBI, Announce a Joint Proof of Concept for the First Vehicle Identity on Blockchain," [on-line] MOBI website. Dated: October 14, 2019.

site? To perform what transaction, in what amount of time – including latency period of transmission – and to what incident reporting log (or certificate)? Thought so – no answer!

Global supply chains today are designed for 'silo'ed' centralized systems. The issues we face with supply chains – for example their persistent lack of willingness to share data – are not unique to international value chains. We face a lack of visibility and transparency – difficulties with data integrity, a lack of real-time data, difficulty integrating data from Internet of Things (IoT) devices and technologies – all these challenges exist both for domestic and international supply chains.[94] Few would argue that supply chain processes are based on confirmable trust. The providence of any item is a *shared truth*. For a distributed ledger to work comfortably in this setting, the end-user or supply chain participant can ill afford, nor will they put up with, a loss of confidence in a shared truth.

For example, an individual transacting on a decentralized, crypto asset supply chain (exchange) is expropriated, and forfeits all their hard-earned crypto assets [a.k.a. *digital tokens*]. Why can this happen, or why is it even allowed to happen? Look at the technology platform driving it all, the answer always lies there.

One issue we face with supply chains in general, is the lack of visibility and transparency of the data, data being the crucial ingredient which makes the supply chain work. These data sources – in all their various forms, formats or typologies – whether structured, unstructured, or sourced as *new* and unseen-before data sources – be they passive or active, subject to flat and/or horizontally scalable database structures, or be they data processed by real-time query tools (as opposed to delineated snapshots), and/or other more advanced data analytic processing techniques, *all* data however it manifests itself, serves to enhance our physical, cognitive, and decision-making capabilities. Difficulties with data integrity, a lack of trackable (auditable) real-time data, difficulty integrating data from Internet of Things (IoT) mobility devices on side chains of the distributed ledger – all these challenges exist both for domestic and international supply chains.

One firm's efforts – whether they are replicable in North America, as opposed to their home market in SouthEast Asia, where they are based – have announced they now have agreement for close cooperation with the world's seven largest legal *fiat payment* providers, supporting 30 fiat currencies, including United States dollars and euros. This firm can now accept 17 payment methods including Visa and Mastercard. This is delivered through that firm's OK Chain's fiat gateway project, called OK Chain. OKEx's OK Chain has provided services to more than 20

[94] Source: "World Economic Forum's Nadia Hewett Talks Supply Chains, Covid-19 and Blockchain". By Marie Huillet (dated: May 5, 2020), Cointelegraph [website]. See: https://cointelegraph.com/news/world-economic-forums-nadia-hewitt-talks-supply-chains-covid-19-and-blockchain. See *also*: *Ibid*., [Foot Note # *48*].

million users, in more than 200 countries and regions around the world, and that is still growing.[95]

The point we have been making so far is this. Significant shifts to the decentralized, distributed ledger world are already underway. Southeast Asia's OKex is proof of this fact. This begs us to ask ourselves the next question: what are the technologies supporting these activities? Advanced Systems Management Group (ASMG) have found one list with several key technologies[96] we wish to now address. The elements of innovation and providence, which distributed ledger technologies must protect, are:

5-1) Stablecoin projects and asset tokenization technologies
5-2) Identity projects
5-3) Secure data on chains
5-4) Wallet and other access allocation means
5-5) Decentralized exchange technology
5-6) Fundamental / foundational (security) infrastructure
5-7) A Special Case: Cardano's Distributed Ledger Technology (DLT) Project

5-1. Stablecoin projects and asset tokenization technologies

The first item on the list of seven (7) distributed ledger technologies (DLTs), covers a very wide topic – (crypto) asset allocation. A crypto asset may be: a stablecoin, a token, or a transaction performed by an institutional player, dealing in crypto assets, of whatever service parameter they wish to offer. One interesting example of this is the hybrid crypto banking institution mentioned in Answer to Q. 4: 'Crypto assets / Crypto currencies' – the Wyoming-based financial depository and crypto asset exchange services institution, or *Hybrid Bank*.

Before examining crypto assets such as stablecoins, and tokenization projects specifically, let's first examine how an individual would invest in a crypto asset. This will demonstrate where stablecoins originated, as the process for their origination created their existence as an asset class in the first place. Stablecoins were born out of a process need, due to the systemic failure in crypto transaction valuation processes overall. The big banks resisted the exchange of crypto currency / crypto asset *value* for an exchange to a corresponding amount of monetary 'fiat' currency *value*. With no fiat on- and off-ramps, allowing the means to exchange of the two assets – crypto currency to fiat currency – available, the stablecoin was introduced to fill the breach.

[95] Source: "Sharing Thoughts on Security, OKEx's (CEO) Jay Ho Says Customers Come First," By Vadim Krekotin, [Cointelegraph CEO for China]. Dated: April 22, 2020. See: https://cointelegraph.com/news/sharing-thoughts-on-security-okexs-jay-hao-says-customers-come-first. See *also*: *Ibid*., [Foot Note # *86*, *354*, *355*].
[96] Source: "Peter Vessenes in the Focus of Cointelegraph China," By Cointelegraph (China Focus Talk Show] Dated: March 28, 2020. See: https://cointelegraph.com/news/peter-vessenes-in-the-focus-of-cointelegraph-china. See *also: Ibid*., [Foot Note # *325*]. Discussion: ASMG added Cardano's Distributed ledger technology (DLT) Project, as a seventh entry.

Stablecoins achieve price-stability through different methods, such as a peg against a fiat currency or fiat commodity, through collateralization against other cryptocurrencies, or through algorithmic coin supply management. Stablecoins create connections between the legacy (centralized finance) world and the blockchain (decentralized finance / DeFi) world. Stablecoin users can benefit from the characteristics of blockchain-powered digital currencies, which grant them low-cost, high-speed transactions, alleviated by their acting as a buffer against the high volatility exchange conditions in which many cryptocurrencies are placed. The main way in which stablecoins work is to peg the stablecoin cryptocurrency to fiat money.

Secondly, a crypto-collateralized stablecoin is essentially decentralized, forming a crypto-backed stablecoin that holds value through the use of smart contracts.[97] These stablecoin *smart contracts* act in response to changes in market dynamics. A third form of stablecoin is a non-collateralized stablecoin – known by the moniker 'algorithmic' stablecoin – a digital currency that increases and reduces their coin supply, automatically, using algorithms. Algorithmic stablecoins ensure that their value always remains stable, by these ingenious mathematical programs and calculations. And finally, a less popular but nevertheless available, option is to peg stablecoin to exchange-traded commodities, such as precious metals or industrial metals.

Stable coins are unique, the blog chat Quora tells us. "Since they try to be like fiat money and maintain a certain level of value". But if they are trying to keep the value of their cryptocurrency always at the same price, then how do stablecoins make money[98]? The answer: by receiving dividends from newly issued and pre-existing stablecoins, granted to their owners (/HODLers) for *holding* stablecoin shares.

Stablecoins are three things: shares, coins and bonds. When they fall in price, the issuer / smart bank offers *bonds*. Bonds are a form of promissory note, offering to pay back a denomination of stablecoins value, at some future point.
Another Quora blogger[99] suggested: Stablecoins should not, theoretically, make money. For stablecoins to make money – e.g. Tether, as an example – Tether should store its purchased value in a [financial] off-set held in US dollars, and those US dollars cannot be touched. This

[97] Smart contracts are an addressable blockchain entity that contains a set of storable data representing a logical state and a set of automated instructions used to alter that state. The instructions allow it also to interact through transactions with other addressable entities, and emit events that distributed applications can subscribe to, thereby triggering appropriate behaviours. The state, instructions and transactions are all maintained and secured by the underlying immutable blockchain technology, responding to the requirement to automate interactions among peer-to-peer (P2P) actors consensually. Plus, they typically require a Virtual Machine (VM) interpreter to drive their execution. Source: "Smart Contracts – How to Deliver Automated Interoperability," By Dominic Perini and Michael Jaieola [online – Erlang Solutions]. Dated June 15, 2020. See *also*: *Ibid*., [Foot Note # *158, 159*] '(Perini/ Jaieola-2020) Smart Contracts – How to Deliver Automated Interoperability.'

[98] Source: "How does a 'Stablecoin' make money?" By Almog Atar [blog posted on Quora]. Dated May 21, 2019. See: quora.com.

[99] Source: "How does a 'Stablecoin' make money?" By Almog Atar [online – Quora]. May 21, 2019. See *also*: *Ibid*., [Foot Note # *98*] 'Quora blog by Sylvain Saurel – June 3, 2020'.

ensures that if all users wish to exchange their US dollar 'Tether' for US dollars, all at-the-same-time, they would have these transactions guaranteed.

We sum up here with a third Quora blogger's comments,[100] and leave it at that. Quora blogger Oleg Sergeykin addressed stablecoin valuations by stating: "Stablecoins demonstrate an approximately one-hundred-and-fifty (150) per cent *quarter* on *quarter* growth in loan originations. This demand is driven by investors using cryptocurrency to collateralize loans, as well as 'capture-the-upside' should crypto/stablecoin rates move higher. The Invectus Margin Lending Fund is one investment fund providing investors with exposure to margin lending returns caused by the demand of leveraged trades – which drives higher volatility and higher interest rates – on dollar-based loans. This is due to 24/7 trading, low liquidity (a.k.a. stablecoins *versus* traditional market-held asset valuations) and, the *specialization* [high risk/ high reward profile?] of stablecoin market participants' crypto asset holdings.

Whether stablecoins will be adopted as a popular online payment method, or whether they will be used in fundraising, or will continue to be held primarily by investors as their *temporary store* for funds, during market downturns, remains to be seen[101].

Let's move on to the topic of coin tokenization[102] next. Tokens – created thanks to Ethereum – have different attributes that allow the management of *smart contracts* to establish their financial binding, their security, and offer the means for (their) smart contract *agreements* to enforce the negotiated terms and conditions between parties on which they are based. There are several types of tokens.

Class 1 token – a type of *coin* (these terms are used interchangeably / nebulously, get used to it!) with non-changeability / chargeability [of the transactions themselves]. Class 1 tokens confer rights against a counterparty, but acts as an *assignment* of ownership of the *coin* / a.k.a. *token* itself. Examples: Bitcoin, Bitcoin Cash, Litecoin.

Class 2 token – a token with exercisable rights (against the issuer of the tokens, or possible third parties/intermediaries of exchange or partial ownership). Class 2 tokens act as a 'kind-of-credit', as in 'the holder has the right [to benefit] with presentation of the instrument's title.[103]

---

[100] Source: "How does a 'Stablecoin' make money?" By Almog Atar [online – Quora]. May 21, 2019. See *also*: *Ibid*., [Foot Note # *98*] 'Quora blog by Oleg Sergeykin – October 29, 2019'.

[101] Source: "Stablecoins: What Are They" What is Their Purpose? and How Do They Work?" By staff – [online - Medium] centrumcoin. Dated: March 6, 2019.

[102] Source: "Tokenization: What are Tokens and What Role do they play," By [author *not specified* – at coinidol.com].

[103] Further forms of crypto asset 'monetization or legal ownership or '*title*' – currently managed by Avanti Bank and Trust, Wyoming –include: ten (10) crypto asset smart contract tokens related to (the management of) future payments 2) token(s) as an asset (both material, and intangible) as in 'shares of the issuing legal entity or third party entities – examples managed not specified 3) tokens used for standardized payments 4) tokens specifying a 'right to receive a service (from issuer, or third party). Discussion: Each of these may have regulatory implications, which ASMG will defer to the experts to address. See: https://avantibank.com/.

Examples include: i) smart contract tokens – related to the management of future payments ii) tokens 'as an asset' – right to ownership of a particular asset (both material and intangible) and/or could also represent shares of the issuing legal entity, or third-party entities iii) tokens used for "standardized" payments – e.g. an explicitly defined amount iv) tokens for the management of service performance – in this circumstance, the token holder has the right to receive a certain service or, in the case of an asset, an asset amount (from the issuer or a third party) as per a signed / authorized trade agreement. These may be trade agreements governing access to IT infrastructure, service delivery through 'service performance (of some kind)', and may also have a specific form as a *native* cryptocurrency. Native cryptocurrency is, technically-speaking – NativeCurrency.com – a cryptocurrency built on the Ethereum blockchain**.**

Class 3 token – perform a mixed function e.g. co-ownership [rights], unrelated possibly to a different right, which might be exorcised to the issuer of the security, or to a third party.

The token's advantage is that:
1) It is individually – uniquely labeled, and has associated *descriptive* [contextual] metadata;
2) It is not fractional;
3) Tokens exist in digital form on the blockchain;
4) Tokens can be followed individually in their path – e.g. distributed ledger history – recorded via a 'property chain'.

Tokens can be handled in different ways, depending on the meaning or *value* a token maintains. Tokens have recently migrated to being assigned non-crypto (non-fiat) intrinsic *worth*, and now may be represented in valuation terms, such as: venture capital listing(s), stock purchases (on the *traditional* equities-listed stock market), as proceeds *a.k.a.* 'business angel' financing, and most recently (See: Avanti Bank and Trust, Wyoming) with depository – crypto exchange valuations held by an institutional 'hybrid' *crypto* bank.

Crypto assets are defined by Ernst and Young (UK)[104] Page 4 (their 2018 Report) in these terms: "Crypto assets may commonly be referred to as tokens (but) a hard boundary between a cryptocurrency *coin* and a *token* is difficult to draw." In short, cryptocurrency *is* a crypto asset, which constitutes an alternative to government-issued fiat currency, exchanged on a peer-to-peer (P2P) network, independent of a central bank. The first of its kind was Bitcoin, launched in 2009.

Ethereum – another major crypto player – went live in July 2015. Ethereum was funded by a crowd-sale, hosted by the operating system found on a smart phone. Ethereum supports

[104] Source: "Accounting for Crypto Assets – IFRS (#) Publication," By Jiri (George) Daniel and Amanda Green – authors (Ernst and Young-E&Y EMEIA), and; Hitesh Patel, Associate Partner – E&Y EMEIA (UK) FinTech Team; and Paul Brody, Partner – E&Y Technical Leadership (IFRS & Blockchain) *et. al*. Published by E&Y (UK) Assurance Tax Transactions Advisory Service. Dated: 2018. See: https://www.ey.com/Publication/vwLUAssets/ey-ifrs-accounting-for-crypto-assets-new/$FILE/ey-ifrs-accounting-for-crypto-assets.pdf. See *also*: *Ibid*., [Foot Note # *107*, *108*, *116*, *117*, *141*, *182*].

programming code in its platform, and *runs* smart contracts.[105] The Ethereum crypto asset community experienced a theft of US$50 Million in *stolen* Ether, its version of retained value *a.k.a.* a crypto coin or token, causing the Ethereum community to create an instrument called the distributed autonomous organization (DAO). Distributed autonomous organizations (DAOs) were introduced to return / redeem the stolen crypto assets at a valuation equal to their loss at time of theft. This caught the attention of the US Securities and Exchange Commission (SEC), whom investigated at this point, ruling in July 2017 that distributed autonomous organizations (DAO) *tokens* were securities, and should have been subject to securities laws and regulations.

Ernst and Young (2018) draw the line between a cryptocurrency *coin* and a *token*, by distinguishing a token as providing something *other* than a purely *general-purpose* currency 'value of transfer.' Ether, Ernst and Young (2018) suggest, is a different concept. It acts to incentivize transaction validation in the peer-to-peer (P2P) network, where crypto exchanges are initiated. Secondly, it acts in the capacity which Ernst and Young (2018) describes as a form of crypto-fuel to *run* smart contracts – i.e. acting as an enabler – hosted on decentralized apps (Dapps) built on Ethereum,[106] with their business conducted on mobility devices (smart phones) or computers/workstations.

The ambiguity of Initial coin offering (ICO) issuance – a mainstay of the Ethereum platform – complicates their handling from a regulatory perspective. The SEC's ruling in relation to the distributed autonomous organizations (DAOs), found the Ethereum ICO was in substance an initial public offering (IPO) of shares or debt, i.e. "securities" (*by* its definition). Ernst and Young (2018) state (Page 9): "In most countries, there are strict regulations on not only marketing and issuance but also the subsequent trading if securities and

Initial Coin Offerings (ICOs) may fall within the scope of these regulations.[107] A new development is the Miniature Autocratic Government (MAG) token. MAG tokens call for an Initial Coin Offering (ICO) delivery to occur, via peer-to-peer (P2P) networks, with a developer designing a miniature economy of sorts, in which the *token* – to-be issued e.g. as the [said] medium of exchange – serves as the payment for hard drive-specified storage space. Advanced Systems Management Group (ASMG) believe this form of Initial Coin Offering (ICO) is a technologically-driven development of some sophistication, and will be extremely hard to monitor. ASMG return to this issue of MAG 'tokenization of storage space' in a later sub-section

[105] Source: "Electroneum (ETN) expands global mobile top-ups to 140+ countries - earning Electronium (ETN) on AnyTask is now more appealing," By Surya Maneesh, Malta Blockchain News Summit Economic Newsletter [online]. Dated: February 26, 2020. For an example of something similar "See Electroneum (ETN)," profiled earlier. See: [*several* citations]: *Ibid*., [Foot Note # *87 – 91*].

[106] Ethereum mimics an operating system running on a smart phone. This has led – inevitably – for Ether to be widely used as a means of payment for initial coin offerings (ICOs) via tokens, activity which is clearly a medium of exchange (payment stream). An ICO evokes the concept of an initial public offering (IPO – a security financing tool) such as occurs when companies list on a stock exchange.

[107] The Financial Conduct Authority (UK), Bundesanstalt fur Finanzdienstleistungsanfsicht (Germany) and the SEC (US), in the second half of 2017, issued warnings around ICOs, thus precipitating the (US) ICC's current digital technology assessment review? (Quoted in E&Y – 2018 Report, Page 9).

of this Submission (See: ASMG Answer to sub-section 5-6 'Fundamental / foundational (security) infrastructure')[108].

For a crypto *coin* to qualify as an investment,[109] it should satisfy the following criteria:
- The source code for a crypto *coin* should be readily available;
- a crypto *coin* should not be centralized. A good rule is that if you cannot compile and run your own fully validating node, it is probably too centralized, and not a distributed ledger cryptocurrency;
- a crypto *coin* should have some utility, or *worth*.
At present, the only proven use cases – e.g. *worth* – for cryptocurrencies are holding (HODL)[110] the crypto coin, or paying for something with the crypto coin. The more complicated and/or advanced the transactions undertaken by crypto coin exchanges becomes, the less chance it may acquire legitimacy. Secondly, excessive coin promotion / pumping of a cryptocurrency, makes that crypto coin less credible, and the coin – and the platform on which it is exchanged or trades – may become marginal in the marketplace.

The top three (3) cryptocurrencies are: 1) Bitcoin (BTC – the originator) 2) Ethereum (ETH – specialization project – use case to be determined), and; 3) Litecoin (LTC -lighter version of Bitcoin). There are several coins below these three which suffer blatant disconnects.

The cryptocurrencies suffering the most blatant disconnects are:
-Ripple (XRP – highly centralized, sixty (60) per cent held by owners, no business use case);
-Bcash (BCH or BitCash – altcoin without a use case);
-IOTA (self-crypto, self what?);
-BitConnect (BCC – Ponzi), and;
-Zcash (ZEC – privacy coin, not private-by-default, technology questionable).

The issue here, is that without regulation, no entity serves the role of filtering out, or assigning *market caps* to successfully evaluate how much a *coin offering* is worth. Some coins rank higher in market cap rankings due to: i) very thin order books ii) exchange withdrawal issues iii) they may be held for speculation (Ponzi reasons) only, etc. Bitcoin may be the best coin offering, for the two reasons underlying it's use case: **a**) Bitcoin may act as a payment **b**) Bitcoin may act as a store of value, leading to usage as a payment presently, or in the future.

---

[108] Source: "Accounting for Crypto Assets – IFRS (#) Publication*" By Jiri (George) Daniel, Amanda Green, Hitesh Patel and Paul Brody *et. al*. Published by Ernst and Young (E&Y-UK). Dated: 2018. See: *Ibid*., [Foot Note # *104-original* citation] '(E&Y-UK 2018-*section 2.2.2.2*) *a.k.a.* "Miniature autocratic government" (MAG) tokens*'. See *also*: *Ibid*., [Foot Note # *115 - 117*] '(E&Y-UK 2018-*section 2.2.2.2*) *a.k.a. "*Miniature autocratic government" (MAG) tokens* (Page 9)'. See *also*: *Ibid*., [Foot Note # 141).

[109] Source: "Intelligent Investing in cryptocurrencies," By Brenden Matthews [online] HackerNoon. Dated January 19, 2018. See *also*: *Ibid*., [Foot Note # *112*, *113*].

[110] Essentially the philosophy of HODL is to buy underweighted assets on a continual basis returning to a target allocation reference point as coin values *drift*. The problem being, this has led to virtuous / vicious cycles of always investing / reinvesting.

Matthews (2018) makes the point that if you rank coins by their default view *a.k.a.* via the marketplace monitor "coinmarketcap.com" ranking,[111] each crypto coin can be evaluated according to their *circulating supply*. By this *circulating supply* metric, the top 10 ranked crypto coins are: 1) Bitcoin 2) Ethereum 3) Ripple 4) Bitcoin Cash 5) Cardano 6) Litecoin 7) NSM 8) NEO 9) Stellar and 10) IOTA. Taking a different metric, a ranking measure which "coinmarketcap.com" term as being the crypto coin's *total supply*, the top 10 ranked crypto coins are: 1) Bitcoin 2) Ripple 3) Solar Coin 4) Ethereum 5) ATM Coin 6) Stellar[112] 7) Bitcoin Cash 8) Cardano 9) NEO 10) Bitcoin Atom.

Another factor to watch out for, is the method for using, and/or assessing, circulating supply.[113] One method, which costs a 2.5 per cent fee to have the valuation made (the *valuation* being subject to the value of the coin under consideration, when that [said] crypto currency is being analyzed) on a crypto coin being appraised – for example, using the HODL 10 Index Fund to conduct valuations on crypto coins – is not reliable. The HODL 10 Index Fund methodology is as follows: circulatory supply *plus* the crypto currencies' additional supply – as publicly scheduled for release in the next five years. Matthews (2018) suggests this metric is meaningless.

Matthews (2018) suggests investing anywhere between 1-5 per cent of a crypto coin's value (as a percentage of your total investment portfolio). This is an investment position Matthews (2018) considers as slightly on the *bullish* side. Given their incertitude – and the appearance of useless *worth* coins, such as Ethereum Classic (Ethereum Classic – a crypto coin which nobody uses!) floating around, Matthews (2018) cautions: buyer beware!

Asset allocation – what a colorful topic! After all that sobering advice, especially the analysis offered by our expert (Matthews 2018), we may wish to ask ourselves "if we really want to examine one final remaining topic" – i.e. addressing stablecoins, asset tokenization, or *other* asset allocation options – despite all the experts agreeing to disagree on their *respective*

[111] *Circulating supply* – is equivalent to coins currently available, and; *Total supply* – portrays all coins that will become available (in the future). Circulating supply, from a regulatory perspective, is problematic. By year 2040, Bitcoin may have diluted to around forty-eight (48) per cent of current market value, a difference of twenty (20) per cent from today (January 2018 - date at which Matthews article was posted). Buyer beware!

[112] Stellar Lumens – brought to you by the same originator whom devised/sponsored the discredited Mt. Gox and (sort-of skeptical - from a business sense) Ripple, has no supply limit and inflates forever at a fixed percentage (leaser-unknown or purposefully, the valuation rationale is withheld). What is: Solar Coin? ATM Coin? Bitcoin Atom? Matthews (2018): no one knows, except whoever is pumping them, to dump / cross-invest in Bitcoin? See *also*: *Ibid*., [Foot Note # *109*, *113*].

[113] A true HODL'er keeps their coins off exchanges and online wallets. The reason for this? Rogue employees, involved in coin activities and/or security lapses (simple negligence or planned nefarious activities). See *also*: *Ibid*., [Foot Note # *109*, *112*] *a.k.a*. hodlermanifesto.com [posted by Brenden Matthews – as a project on github – at brndmtthws/hodlermanifesto].

evaluation efforts? Or in short, might cryptocurrency asset allocations devolve[114] even further, with this unstable, yet early maturation form of currency, drifting even further from a state of prolonged, or appreciable, profitability?

As we mentioned previously, the MAG token example introduces a unique form of barter *complexity* to this whole discussion: Is it part security (as a token issue)? Or, is it part 'something else' (hard drive -leased space)? The OCC, and US Department of Treasury have a challenge in wait, to settle scores on this issue. Plus, might there be revenues owed through OCC or Department of the Treasury determinations, that the MAG token is a taxable asset, taxable on the proceeds it generates (from its revenue-generating activities) owed to the Internal Revenue Service (IRS)?

The accounting experts (Ernst and Young 2018; Page 13) weigh in on this issue conclusively: "It is not necessarily clear, at present, (if) digital currencies should not be considered as cash or cash equivalents under IAS 7 Statement of Cash Flows.[115] If entities accept digital currencies, as a means of payment, they should be considered to hold (those digital currencies/assets) for sale, in the ordinary course of business." The above determination doesn't answer the question, so no help there.

The Australian Accounting Standards Board (AASB) in their December 2016 paper "Digital currency – A case for standard setting activity,"[116] couldn't decide if digital currencies constitute cash or cash equivalents, or were [definitively] financial assets (other than cash, intangible assets or inventories). While this is being addressed by experts in fiduciary accounting, another accounting body has attempted to weigh in on this issue.

The International Accounting Standards Board (IASB) – Ernst and Young (2018) report – have picked up the ball where the Australian Accounting Standards Board (AASB / Dec 2016) paper left off. In January 2018, the International Accounting Standards Board (IASB) announced it will address digital currencies,[117] to possibly – include an examination of transactions such as those involving digital currencies – that might form part of a research project within the IASB. The

[114] Devolvement is a process in which if an issue - e.g. initial coin offering (ICO) or initial public [share or security] offering (IPO) - goes under-subscribed, an underwriter is appointed whose job is to subscribe to (i.e. purchase) the remaining issuance of the asset being trade. That asset may be a: crypto coin, crypto token or crypto *barter-in-kind* service, or the traditional stocks and bonds. Being under-subscribed is not a favorable scenario and can lead to bad results for the company involved with the issue.

[115] Source: "The Bitcoin Boom: Asset, Commodity, Currency or Collectible?" YouTube — Aswath Damodaran, https://www.youtube.com/ watch?v=8iNeXCAM_Ik, accessed 24 October 2017. See *also*: "The Ascent of Money: A Financial History of the World," by Niall Ferguson, published by The Penguin Press. Dated: 2008. (Quoted in E&Y – 2018 Report, Page 21).

[116] "Digital currency — A case for standard setting activity. A perspective by the Australian Accounting Standards Board (AASB)," AASB, http://www.aasb.gov.au/admin/file/content102/ c3/AASB_ASAF_DigitalCurrency.pdf, accessed 6 February 2018. (Quoted in E&Y – 2018 Report, Page 18). See *also*: *Ibid*., [Foot Note # *104*, *107*, *108*, *117*, *141, 182*].

[117] Source: "IASB Update January 2018," IFRS, http://www.ifrs.org/newsand-events/updates/iasb-updates/january-2018/, accessed 26 January 2018. (Quoted in E&Y – 2018 Report, Page 18).

conclusion Ernst and Young (2018 at Page 17) accounting auditors arrived at was that "Dealing with crypto-asset accounting, therefore, requires a detailed understanding of both distributed ledger technology, and relevant accounting concepts. In the absence of further action by accounting standard setters, holders of crypto-assets may be *unable* to achieve the accounting treatment they consider most appropriate."

Advanced Systems Management Group (ASMG) were intrigued by several other issues raised by the E&Y (2018) Report. They are:
i) 3.2.1 – forked currencies (short selling), and;
ii) 3.2.2 – token presale (versus ICO issuance actions/activities).

And in the 'Supporting Details' section of the Ernst and Young (2018) Report:
iv) 'Of pseudonymity and privacy' [Page 18] – there is a lack of connection between the [Bitcoin] address and an identifiable legal or natural person;
v) 'transformative forging' [Page 19] – e.g. a bad actor would have to own over ninety (90) per cent of all NXT – a cryptocurrency containing its own blockchain (designed to scale to the level of Visa and Mastercard) to successfully manipulate 'the ledger';
vi) 'ERC-20: crypto-fueling the ICO phenomenon' [Page 20] – e.g. the standardization by Ethereum offering a list of rules for ICO token issuance – regulatory compliance advisable here;
vii) 'Money has no intrinsic value, and yet we consider it an asset' [Page 20] – ASMG views crypto assets as possessing value, no different than fiat (or other investment asset) valuations;
viii) 'IAS 38 cost and revaluation methods' [Page 22] – IAS 38 includes specific guidance as to when the revaluation difference should be recognized, in profit or loss, or other comprehensive income. Advanced Systems Management Group (ASMG) concurs with this viewpoint, and lastly;
ix) 'Payment Service Act (Japan)' [Page 22] – Advanced Systems Management Group (ASMG) concurs with this regulatory approach.

5-2. Identity projects

Digital transactions function as identity claims within an ecosystem. All sectors of the economy are struggling with the issues of Client identity. This struggle involves striking a balance between offering users access to information while, at the same time, maintaining strict and rigorous fiduciary control over that information. Whether on the retail side in banking, or on financial institutions (FIs) investments products and services side of their businesses, banking and investment management advisors need to carefully, and comprehensively, address identity projects.

For the distributed ledger use-case before us, an identity project takes on a very narrow connotation. A decentralized identity (d-ID) is a web-based URL, used in conjunction with public keys, private keys and public keys, or private key pairs. The internet provides us with our IP address, while the application layer of the distributed application/Dapp (on the mobile device or 'wallet') provides our account and password at log-on. Having real-world identities –

defined in this way on the distributed ledger – allows an economic arbitrator to police and/or punish transacting individuals for their fiscal transactions or bartering activities, or at the very least, assign someone their *credentials*.[118]

In the distributed ledger technologies (DLT) context, *identities* are about as easy to define (and consume) as downloading a distributed App (Dapp) or mobile App, on a smart phone, or computing device. Here is one Company's business use case to serve as an example. NuID is product offering a modern – distributed ledger technologies (DLT)-enabled – authentication solution for *identities.* The Company's (NuID's) web site claims there are 5.9 billion passwords breached over the last three-year period, in a large section of Europe and North America. Eighty-one (81) per cent of those breaches were caused by stolen or weak passwords. Solution? Fix the password, or substitute it with something else.

Instead of transmitting passwords from a device to your server – to be verified for registration (and authentication) – NuID uses the device's "sent-off" message to confirm the device is the Users. This offers what the Company NuID terms as protection via a layer of zero knowledge (ZN) cryptography. NuID claim their Clients can *log-in* (to smart phones or other digital devices and/or computers and workstations) – with passwords, biometrics and more – without sharing any sensitive / private data. It happens like this:

The User puts in a username / email address; the LogN client libraries generate the zk (zero knowledge) reference parameter from *secret*; Username / zk parameters are sent to the relying party; which forwards this "stuff' to NuID's service API. ZK parameters are "posted' to ledger; ledger returns a unique txid (of where the parameters are located); username is associated to the txid; registration completed. That's the registration step. The authentication step (more-or-less) mirrors this same procedure. ZK is short for zero knowledge. A ZKP (zero knowledge proof) uses a Schnorr protocol described in the Internet Engineering Task Force RFC 8235 specification.

NuID states: "We use a distributed ledger for this, since everything is non-sensitive, and can be safely shared *publicly*. It is a "bring-your-own-Identity-to-Multiple-Services" principle. It is all meant to be an accessible, yet robust Identity Access Management (IAM) solution. It proposes that customer or employee log-ins, managed on a cloud infrastructure,[119]" (NuID describes) as a key management solution. In somewhat vague terms, the Company claims it is a modern-day *log-in box* – essentially, moving password information from centralized server storage into a distributed ledger technologies (DLT)-type of storage – cloud-hosted, and located on the blockchain.

[118] Source: "We need to get Digital ID Right," (with the) United Nations High Commissioner for Refugees (UNHCR). [online - https://id2020.org/.] '(ID 2020 Alliance) Goal: digital identity using credentials to gain access to services, while preserving privacy, security and maintaining control over (personal-private) information.'
[119] Source: "Decentralized Identity API – Stop Storing Passwords," Product Sales Sheet by NuID [online]. Dated: 2020. See: www.nuid.io. See *also*: *Ibid*., [Foot Note # *120*, *123*].

So, does this make any sense? A review article[120] characterizes several market-leading efforts to create *Consumer-friendly* Identities – such as the NuID *log-in box* type of solution – but did not review NuID's product, or service, specifically. Blockchain technology does not resolve access management issues. These access management issues include: **i**) key management tracking **ii**) recognizing the inherent weakness with server-centric and federated-identity environments or **iii)** Zero Knowledge Proof (ZKP) mechanisms – in which the *prover* demonstrates possession of knowledge, without conveying any information, apart from the fact that the he/she possesses the knowledge – back to the *identified* party. Lim (2018)[121] states: "Emails and passwords are notoriously easy to crack. An on-line provider (NuID in our example) might perform registration and authentication *credentialing*, but distributed ledger technologies (DLTs) act as the *proxy*, at best, for the user."

Using cloud-based key management services does, however, relinquish control over those assets. NuID claim their soon-to-be stabilized application programming (product) interfaces (APIs) – and their supporting Client libraries – will securely store and share user data. Specifically, NuID claim their "*Identity*" so protected, will perform or conform to Know Your Client / anti-money laundering (KYC/AML) regulations and standards, and will attribute (and apply) security controls, and related attestation or authorization and validation tasks, required.

Where are we today? Self-sovereign identity in a globalized world is an elusive goal at present.[122] Should we be able to achieve a qualitative identity assigned as an 'attribute', this would serve as a *qualifier* for an identity-served reference point we all need. Advanced Systems

Management Group (ASMG) feels this is a laudable goal to have.[123] But as with everything else, in the distributed ledger technologies (DLTs) world, digital identities are not something as easy to define, or even to manage, as say the social security number we apply for on our children's behalf when they are born. Perhaps, achieving a self-sovereign identity in a globalized world is an aspirational goal, at best.

---

[120] Source: "Blockchain Technology the Identity Management Service Disruptor: A Survey," By Shu Y. Lim, P T Fotsing, *et. al*., International Journal of Advanced Science Engineering Information Technology, Vol. 8 – No. 4-2. Dated: 2018. See: www.researchgate.net. NB: This academic study provides a canvass of similar products offerings to NuID, although the technology varies widely. See *also*: *Ibid*., [Foot Note # *119*, *123*].

[121] See: *Ibid*., [Foot Note # *120*] '(Lim-2018) DLT acting as a proxy for user identity'. See *also*: "Blockchain for Identity Management: It's Year's Away," By J. Kirk [online]. Dated: 2018. See: https://www.bankinfoseurity.com/blockchain-for-identity-management-its-years-away-a10598/.

[122] Source: "Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion," By Fennie Wang and Primavera DeFilippi [online article] Frontiersin.org. Dated: January 2020.

[123] One identity project Advanced Systems Management Group (ASMG) wished to pursue was our Technology Demonstration Project (TDP) proposal for the EU's European Parliament to address GDPR regulations, which appears in Appendix A of this Submission. This GDPR Submission, had it been funded and the project completed, would have looked at identities from a comprehensive technological examination, *a.k.a.* securing the data (and the data 'audit trail') between Users of data. Not a secure personal Identity project *per se*, but who is to judge that securing personal identities, in the NuID way, is the legit way to go?

5-3. Secure data on chains

This topic will be introduced very simply, and then it will branch out from there. Like everything else in the blockchain world, *simple* is not easy to come by. Here is a crucial challenge that the blockchain must face. Information on a blockchain node must address trust through cryptography and consensus. Bitcoin, the first digital currency, was created without trust agents. Enter Ethereum which devised trusted agents it calls smart contracts. The systemic trust model for smart contracts, however, is missing.[124]

Blockchains restrict computation tasks. In fact, smart contracts, on average, employ a mean of three variables and functions. And one in ten have a security-related issue. Not surprisingly, resolving this while maintaining trust requires verifiable computation. And where does verifiable computation come from? From outside the blockchain, or off-chain. Blockchains are Peer-to-Peer (P2P) systems fundamentally decentralized as their core defining characteristic. Smart contracts on the Ethereum platform are lines of code in one account that execute automatically. Since they are *trustless* they are agreed to by all parties. In permissionless blockchain, the public key of the user – which can be termed a *digital signature* – is often used as the identity of the user.[125]

Enter the *oracle*. Oracles are programs having a smart contract and a regular application part. The smart contract received requests from users, stores them on the blockchain, and issues an event about a new request. The web3 JavaScript API for Ethereum is 'listening' for events. This Ethereum *listening* API collects the query data, and executes it. Smart contracts communicate either through sending transactions or function calls. While smart contracts can have low code complexity – they can be combined – using imports of other contracts and libraries.[126] Getting more deeply into smart contracts requires a more detailed analysis of their functions which we will address next.

Smart contract functions reveal different sets of parameters, and modifiers that they utilize. For example, a modifier could be used to apply certain checks before executing a function, e.g. check to see if the sender of the call or transaction is the owner of the contract. Instead of

---

[124] Source: "Trust and verifiable computation for smart contracts in the *permissionless* blockchain," By Dominik Harz, KIT Royal Institute of Technology, School of Information and Communications Technology, Stockholm, Sweden. [online – diva-portal.org]. Page 1 (Abstract to the Paper). Dated: 2017. See *also*: *Ibid*., [Foot Note # *125*, *126*].

[125] Source: "Trust and verifiable computation for smart contracts in the *permissionless* blockchain," By Dominik Harz, KIT Royal Institute of Technology, School of Information and Communications Technology, Stockholm, Sweden. [online – diva-portal.org]. Page 1. See: *Ibid*., [Foot Note # *124, 126*], Page 16 – 18. '(Harz-2017) Characteristics of blockchain *a.k.a.* smart contract identity issues.'

[126] Source: "Trust and verifiable computation for smart contracts in the *permissionless* blockchain," By Dominik Harz, KIT Royal Institute of Technology, School of Information and Communications Technology, Stockholm, Sweden. [online – diva-portal.org], Page 38. 48, 60, 61 – 62. See *also*: *Ibid*., [Foot Note # *124, 125*] '(Harz-2017) web3 JavaScript API for smart contract queries assembly, and smart contract sending of any/all transactions and function calls, etc.'

defining this piece of code, for every function individually, a modifier could be defined and applied to functions. That's it for simple. Now we get to subtle.

Like everything in the crypto asset universe, transparency – and openness – of intentions is just not on! Case in point: Sergey Nazarov, Founder and Managing Director of QED Capital. QED Capital has been responsible for the launch of ventures which include Crypta Mail, the Secure Asset Exchange (SAE) and most recently ChainLink.[127] ChainLink has launched oracle service which it aims to support smart contracts on the Ethereum platform, Bitcoin blockchain and in support of Hyperledger. ChainLink's goal is to build a system of oracles to, in the words of Founder Sergey Nazarov: "Serve as 'backend middleware' infrastructure, designed in theory never to be noticed by the end user. We make open source software that provides security to an oracle mechanism, and provides the economic framework through which the usage of that oracle mechanism has crypto-economic guarantees."[128]

In short, ChainLink connects to the off-chain data needed to, for example – validate and transmit weather data, economic indicators, or stock prices –to, for example trigger a payment event, or an order transaction of some kind, based on having had access to that external, off-chain data set. Here is another example. Sergey Nazarov was part of the team that built SWIFT's smart bond. The SWIFT wire transfer service smart bond takes the interest rate of five (5) banks, aggregates them into an average rate, and uses this as an 'output' to execute an agreement – e.g. execute payment event – e.g. using this data set to codify 'in' to a SWIFT wire transfer payment *message*.[129]

What the 'stealth' emergence of Nazarov's enterprises are achieving is a cornering of the 'security on chains' marketplace. Don't believe it? On-chain and Off-chain interoperability requires, in the first case (on-chain interoperability) a third blockchain to act as a go-between for two different blockchains. Not viable, from a security point of view. (Nazarov gets this). That leaves off-chain interoperability as the prome real-estate to lay claim to securing the chain, which just happens to be Nazarov's home ground.

Off-chain interoperability employs 'middleware.' This could be a software oracle, relaying online e.g. information from websites, backend APIs or smart contracts, or a hardware oracle. A hardware oracle is an IoT device – Intel's SGX is one example – to track and verify real-world data, before sending it to the smart contract. Nazarov's QED Capital acquired TownCrier, is competitor, which boasts Intel's SGX hardware appliance as part of its package providing hardware oracle services.[130] This is what Advanced Systems Management Group (ASMG) mean

[127] Source: "The mystery of ChainLink's Sergey Nazarov," By Sequence, [online – The Blockchain UX]. Dated: July 6, 2020. See: uxsequence.io.
[128] Source: "The Man in Plaid," By Andrew Leonard [online – coindesk]. Dated: 2019
[129] Source: "The Top 5 Reasons Every Institutional Investor Should Have a Position in ChainLink," By, The Crypto Oracle [online – nouvive.com]. Dated: November 6, 2018.
[130] Source: "ChainLink Acquires Town Crier from the Initiative for Cryptocurrencies and Contracts," By Chainlink staff, [online]. Dated: November 21, 2018. See: https://www.prnewswire.com/news-releases/chainlink-acquires-town-crier-from-the-initiative-for-cryptocurrencies-and-contracts-300741835.html.

by *subtle*. ChainLink, now with TownCrier added, this provides Nazarov the ability to provide: i) a bridge between on-chain and off-chain (sources) ii) a modular oracle-as-a-Service offering and ii) upgradable capabilities. ChainLink can now offer smart contract security solution which have: a) better confidentiality protections b) use of trusted hardware c) infrastructure changes (both hardware and software oracles – together, everything is covered) and d) general oracle programmability.

Adler (2018)[131] spotted this capability and described it as *deterministic verifiability*. To achieve deterministic verifiability a full node, on the blockchain supporting a smart contract, must be able to verify the 'state of the chain'. This, Adler (2018) describes as achievable when: i) clever mechanisms are introduced to store off-chain data, or perform off-chain computation, in a probably correct manner, and; ii) data external to the blockchain – validate and transmit weather data, economic indicators, or stock prices – cannot be deterministically verifiable through cryptographic proofs and must, instead, be made available for on-chain consumption, through other means.

Without an oracle, a (decentralized) smart contract – running on the Ethereum platform, for example – will only be able to perform operations with on-chain data. Oracles will, purportedly, change this. It is important to note one critical issue with respect to security. No decentralized stake-based system impervious to attack! And being able to quantify under what conditions its output can be trusted, this is the essential task or mandate oracle services must deliver.

Do Advanced Systems Management Group (ASMG) view this oracle-service issue as secure? No. Not by a long shot!

According to ChainLink's white paper[132] (the rest of this comments section will be taken from that source) an oracle services' nodes should return replies to data requests and / or data queries made on behalf of a user contract. This Juels *et. al*. (2017) call a *requesting contract*. Three things are required to *action* a requesting contract: i) the oracle-service-provider generates a performance metric which it finalizes, then sends for comparison against the smart contract's 'service-level-agreement' (SLA) parameter, or condition, it is attempting to fulfill. It also feeds an oracle-provider generated *metric* back to the (hosting) *reputation contract.* This is a workflow-type of sequencing, in which the goal is to capture *details* enabling off-chain oracles to execute the agreement, and report back to the on-line oracle, which now takes us to the third step in this process. The third step involves another form of record, called an *aggregating contract* which "tallies' the collective results. Or, to put this more accurately, the aggregating contract calculates a weighted answer.

[131] Source: "The State of Decentralized Oracles," By John Adler [online – Medium article]. Dated: September 28, 2018.
[132] Source: "ChainLink: A Decentralized Oracle Network [*white paper* v.1.0]," By Steve Ellis, Ari Juels and Sergey Nazarov. [online – link.smartcontract.com]. Dated September 4, 2017.

What does the 'weighted answer' do? It detects and rejects outgoing answers, incorrect answers etc. leading to the production of a configurable contact address which is specified by the purchaser. If the purchaser does not have any idea what they need, ChainLink will include a standard set of aggregating contracts, if necessary.

That's everything that happens 'on-chain'. Off-chain, the architecture is different. This off-chain architecture requires oracle nodes connected to the Erthereum network. These ChainLink on-chain nodes are powered by the standard open source code implementation – of a core node software for interfacing with the blockchain, scheduling and balancing what goes on with various external services.

The work which ChainLink "nodes' perform are called assignments. Assignments are smaller tasks, known as sub-tasks, processed as a pipeline. A few node software sub-tasks are 'built-in' – e.g. HTTP request (broker), JSON parsing, and conversion to various blockchain formats. There are a few external adapters required by the off-chain architecture. They are [these external adapters) external services with a minimal REST API. Juels *et. al*. (2017) call these services – i.e. identify their importance: "By modeling adapters in a service-oriented manner, programs in any programming language can be easily implemented simply by addressing a small intermediate API in front of the program. Similarly, interacting with complicated multi-step APIs can be simplified to individual sub-tasks with parameters."

Next, ChainLink discuss sub-task schemas. ChainLink currently operates with a schema system based on JSON schema[133] to specify what inputs each adapter needs, and how they should be formatted. Juels *et. al*. (2017) state: "Schemas (act in deployment mode) to take adapters specifying an output schema – to describe the format of each sub-task – output. In both the on-chain and off-chain cases, availability and correctness statistics for oracles will be visible *on-chain*. Users / developers will then be able to view them in real-time, through an appropriate front end, such as a Dapp in Ethereum or an equivalent application for a permissioned blockchain.

Why distributed oracles don't ensure confidentiality? Yes! This is a question Juels *et. al*. (2017) are stating out loud – in their white paper! "Confidentiality is fundamentally hard to achieve in an oracle system. If an oracle has a blockchain front end such as a smart contract, then any queries to the oracle will be publicly visible. Queries can be encrypted on-chain, and decrypted by the oracle service, but then the oracle service itself will "see" these publicly visible events. Even heavyweight tools such as secure multiparty computation – which permits computation over encrypted data can't solve the problem given the existing infrastructure. At some point, a server needs to send a query to a target data source server. Thus, it must see the query,

[133] Source: "JSON Schema," See: https://json-schema.org/. Discussion: JSON Schema is hypermedia ready, and ideal for annotating your existing JSON-based HTTP API. JSON Schema documents are identified by URIs, which can be used in HTTP Link headers, and inside JSON Schema documents to allow recursive definitions.

irrespective of whatever confidentiality the query previously enjoyed. It will also see the response to the query.

ChainLink point out that HTTPS – the protocol for secure web communications – does not enable data signing. HTTPS does have an underlying public-key infrastructure (PKI) that requires servers to possess certificates that could, in principle, support data signing. There is a transport layer security (TLS) solution with the- –N extension[134] to overcome this. But TLS-N is not standardized yet. TLS-N cannot support out-of-bound confidential management of user credentials or queries. Instead, it requires users to query a data source *themselves*. This can present risks, for example, if a query attempt to initiate – e.g. query (*a.k.a.* 'confidential flight information') appears in the text of a stored smart contract – anyone accessing (by the user or someone else on a website) seeing this confidential information via their *automated* query of, say, the website, could have just stumbled upon this information, which could have inadvertently triggered its own 'release' by the smart contract, inadvertently, to the wrong parties.

ChainLink state that "highly secure systems are not yet available." This impedes, Advanced Systems Management Group (ASMG) would strongly argue, trustworthy smart contracts coming into existence on our immediate horizon. Today, centralized oracle-service-providers predominate. But a centralized point of control does not equate with full-fledged 'tamper resistance'. Juels *et. al*. (2017) in the ChainLink white paper state that: "a final change that might work is to change data at the source. If a data source digitally signed the data it is provided, then the relaying server wouldn't need to be trusted. This capability, with the encryption of a possible TLS-N roll-out, is not yet available."

Since that was a very complex overview we ended up with, are there simpler ways for the blockchain to access external data sources? Yes, they are called Data Service Providers (DSPs). They compile data from a single data source or a network or multiple data sources. The consumer chooses the data they want, the Data Service Provider's (DSP's) smart contract gets the external data. Then, the Data Service Providers (DSPs) implement. How? The consumer might pay for data via a per-query request, and the DSP *pulls* the data from its data sources and supplies the consumer in two manners. First, a subscription service: This is attended by a fixed price option, or access-on-demand. The second is the consumer requests the Data Service Providers (DSPs) data, and the DSP *pushes* the data to the consumer, possibly periodically, as

[134] The transport layer security (TLS) solution – applied for non-repudiation, suffers from several disadvantages: i) reusability – the application layer solution only supports defined protocols / applications ii) principle of minimum exposure *contradicted* – the application layer requires that private-keys are exposed to the application layer, which means the TLS layer is responsible for managing cryptographic keys. The adversary can capture the encrypted TLS traffic and decrypt it later, gaining the TLS traffic secret. Source: "Trustworthy Internet Movement," 2017 – SSL Pulse (2017); www.trustworthyinternetorg.org/SSL-pulse/. See *also*: "TLS-N: Non-repudiation over TLS Enabling ubiquitous content-signing for disintermediation," By Hubert Ritzdorf, Karl Wust and Arthur Gervais, *et. al*. IACR ePrint report 2017/578. See: https://eprint.iacr.org/2017/578.

outlined in the terms of the negotiated agreement. This has left us, at Advanced Systems Management Group (ASMG) with very shallow expectations regarding 'security on the chain'.

Let's examine the historical record. Banks and cryptocurrency exchanges are increasingly intertwined. As users seek fiat on- and –off ramps, and regulators are paying more attention to the banking sector and its exposure to virtual assets the cryptocurrency investigations Company CipherTrace, claim – in their reaction to this current OCC (2020) Digital Activities Review Initiative – that they have uncovered eight (8) out of ten (10) US retail banks, in which *several mixing services* (MSs) have made their mark '*mixing* bitcoins.' When you send your money to an anonymous service, if they are well-intentioned, they will send you someone else's tainted coins, without even knowing it. Now, whatever those coins were used, can be traceable back to you. Additionally, *mixing* large amounts of money may be illegal, as it may contravene anti-structuring laws.[135]

If a money service business (MSB) makes use of their bank account – as a conduit for accepting cash payments in exchange for crypto coin, to support the illegal trade-off issuing fiat for crypto remittance valuations – they often do this by a simple wire transfer, or by walking cash deposits to a depository institution. Many banks and other regulated financial institutions (FIs), unwittingly, provide a conduit for these illegal transfers (transactions). Analysis by CyberTrace further reveals that a typical large US bank processes over $2 Billion annually, in undetected cryptocurrency-related transfers.[136] Financial institutions (FIs) need to understand their cryptocurrency counterparty exposure, as it reached in to credit cards, debit cards, ACH, wire transfers and SWIFT transfers.

Recently a few firms have built software that can track the movement of crypto coins, in aid of law enforcement. When creating a wallet, users are given an address allowing them to receive coins. Sending coins from your personal wallet to your (coin) exchange wallet allows the exchange to be *linked* to your identity.[137] Companies use *chain analysis* to identify wallets linked to criminal activity on the Dark Net. These chain analysis tools provide data

[135] Several money laundering laws do not apply until the amount of money involved exceeds $10,000. The laws include three reporting requirements and one substantive crime. Launderers have responded to these laws in part by "structuring" their transactions--breaking them up so the amount involved in each transaction is less than $10,000. One such law, the cash transaction report (CTR) anti-structuring statute, may anticipate issues for the other anti-structuring laws to support. Source: "Money Laundering: The Anti-Structuring Laws," By Sarah N. Welling, University of Kentucky College of Law. Dated: Spring 1993. See: (for notes /citation) Alabama Law Review, Vol. 44, No. 3 (Spring 1993), pp. 787-799. See *also*: https://uknowledge.uky.edu/law_facpub/28/.

[136] Source: "How Impending Virtual Asset Regulations Impact Banks – Even Those That Don't Think They Do Crypto," By John Jefferies, [online article] CyberTrace. Dated: June 24, 2020. See *also*: *Ibid*., [Foot Note # *85*, *143*].

[137] Here is an example. The Monero platform, for example, uses Ring CT - making Monero 'private by default'. When you transmit cyber coins by Monero, six (6) other random signatures are pulled from the blockchain and included in your transaction. This causes an interloper to face a hurdle. Another example is for companies, such as Blocksteam, to use *side chains*, which are new models of trust allowing digital assets to be moved from one blockchain to another blockchain.

visualization[138] and live risk scores. These data visualization engines, such as Maltego, serve to combat deleterious actors (and the actions they cause) known as a 'mixing service'. A mixing service (MS) occurs when money launderers' – also known as Mixers, Tumblers and Foggers – act by putting *tainted* (identifiable as fraudulent or poisoned) cryptocurrency funds 'in' with regular crypto currency funds. The intention of an MS is to make it difficult to follow the trail back to the funds original source.

These Maltego *transforms* diversionary or exculpatory efforts act at the level of: bitcoin address; bitcoin transaction, and; bitcoin wallet 'space'. Maltego *transforms* allow you to calculate the current state of a crypto coin or crypto transaction e.g. capturing its risks and attribute details. The bitcoin address is usually stored on a public cryptographic key, then the person who knows the private *key pair* can send those bitcoins to another address. Keys are usually stored on computer's or mobile devices' software distributed app (Dapp).

The bitcoin transaction *trace* – i.e. performed upon a public record held in the bitcoin blockchain – produces a transaction ID for a *trace* request that will normally have one (or more) outputs. The bitcoin wallet gives a destination address, source(s) address, and risk scoring. You gain wallet information by *tracing* the address of all transactions. All these three (3) data sources: bitcoin address, bitcoin transaction, and bitcoin wallet[139] – can integrate into Maltego *transforms* – making investigations seamless.

Does this alleviate Advanced Systems Management Group's (ASMG's) concerns that progress on 'securing the chain' is being made? Again, the answer is: No!

Distributed ledger technologies (DLTs) employ hash[140] algorithms, and public-private key pairings, neither of which are supposed to lend themselves to their exposure. This may be hard to conclusively prove. There are significant meta data vulnerabilities on the blockchain, some of which we have already spoken to. Advanced Systems Management Group (ASMG) have no direct experience with meta data exposures on the blockchain to draw from, but we are confident we have a role to play in addressing this issue. Here is a listing of four (4) blockchain meta data vulnerabilities, of specific concern to us as data management experts: i) unproven

[138] Maltego Desktop Client is the visual interface in which all gathered information is linked and combined**.** It is a Java application that runs on Windows, Mac, and Linux. Maltego allows users to create graphs step-by-step in an intuitive point-and-click logic. More specifically for our purposes, Maltego is a software product used for open-source intelligence and forensics, developed by Paterva. Maltego **f**ocuses on providing a library of transforms for discovery of data from open sources in a data mining vein. Maltego produces a library of transforms (code snippets, working like APIs) which links capabilities to different platforms. Maltego uses the idea of transforms to automate the process of querying different data sources. See: https://www.maltego.com/products.

[139] A wallet address may not be one-hundred (100) per cent accurate. A grouping of bitcoin addresses into one grouping may be controlled via: i) single user or ii) a service. To compute wallet addresses? You may use 'multi-input clustering' method, which allows you to analyze multi-input transactions with known patterns.

[140] A hash is a string of numbers and letters that are pulled from the message**,** file**,** or document based on a mathematical algorithm**.** See *also*: *Ibid*., [Foot Note # *145*] 'Hash definition simplified.'

cryptography ii) security misconfigurations iii) insufficient (i.e. unprotected) logging alerts, and; iv) weak boundary defense.

Going through this list briefly, the first topic is 'unproven cryptography.' By this we mean foundational cryptographic compromise, which puts disputed provenance into a model, in an infected state. For example, unproven cryptography may be inserted *in* to a hash algorithm, or *in* to a key pairing. This requires a *fix* from node operators. The second meta data weakness, or *failing* concerns 'security misconfigurations.' If code libraries are compromised, or put *in* an infected state, a determination must be made as to any open ports – left unattended, unobserved or unprotected – and a thorough, attentive examination of the situation made. The third meta data weakness, or *failing*, may occur with 'insufficient logging alerts'. This may be affecting Processing and Mechanisms. The latter component, 'mechanisms,' may involve – hash algorithm (behavioural) malfunctions which may scramble or interfere with the normal functioning of – inputs: test /training data sets, and – outputs (data compilations). The next functional mechanism to check, for anomalies in operations, are the public-private key pairing/settings, and determinations made regarding whether their features and functions are disabled, compromised or severely weakened. If 'insufficient logging alerts' are not at fault, i.e. the public-private key pairing/settings are functioning normally, then the code base itself may be compromised or infected. *Infected code* may be releasing themselves when connections with recipients/visitors or users are engaged at deployment time, or when any internal programming instruction set may be activated – at the same instance – at deployment time. Criticality assessments are crucial, including: monitoring, and updating *all* the logging recipients alerting mechanisms, protocols, actions and activities. The fourth metadata-induced vulnerability is generically described as 'weak boundary defense.' *Weak boundary defense* is something DevOps (developers) need to never, ever leave "holes" in their Client coding duties, tasks and responsibilities. *Weak boundary defense* is also something DevOps (developers) can never overlook as they build mobile device apps, web apps, chain views or administrative tools. Sound straight forward? Not really! Ask a DevOps professional when was the last time they went the extra mile to secure everything they do (build). The answer will probably shock you: almost *never*!

Advanced Systems Management Group (ASMG) would be pleased to learn more about these four (4) metadata –enabled security breaches. Our expertise in data management issues would lend credence to *interested parties* consulting with us further.[141] Our concerns are that these topics go far beyond accounting treatments, and verge on technological preparedness and

[141] A further list of issues received a brief mention, at the conclusion to sub-section 5-1. 'Stablecoin projects and asset tokenization technologies.' Details are very sketchy, so it is hard to organize the information properly. ASMG suspect they concern, not ordered in any meaningful manner, these issue areas: i) forked currencies; ii) token pre-sale anomalies (*a.k.a.* initial coin offerings (ICOs) being financed); iii) pseudonymization and privacy breaches; iv) transformative forgings, and; v) crypto *fueling.* Source: "Accounting for Crypto Assets – IFRS (#) Publication," By Jiri (George) Daniel and Amanda Green, EMEIA (UK) E&Y *FS Assurance* FinTech Team. Plus, [sub-section authors:] Hitesh Patel, and Paul Brody, *et. al*. [online – E&Y (UK) Assurance Tax Transactions Advisory Service. Dated: 2018. See: https://www.ey.com/Publication/vwLUAssets/ey-ifrs-accounting-for-crypto-assets-new/$FILE/ey-ifrs-accounting-for-crypto-assets.pdf. See *also*: *Ibid*., [Foot Note # *104*, *107*, *108*, *116*, *117*, *182*].

threat detection avoidance, deterrence, or even counter-attack measures, something which technology-embedded solutions can counter with full quality assurance, if designed and implemented (and monitored) properly. Accounting principles, designed to achieve the same thing? Can't be done! What's even more troubling, is the current research literature and regulatory compliance writers have singularly, and unsatisfactorily, ignored addressing or discussing this issue amongst their peers.[142]

There is one further issue we would be remiss if we ignored. The Virtual Asset Service Provider (VASP) community – another way to describe crypto currency or crypto asset exchange service providers – have initiated a private-sector driven program they call the Financial Asset Task Force (FATF). In June 2019, the Financial Asset Task Force (FATF) called for implementation of the 'Travel Rule'. The Travel Rule requires VASPs / crypto currency exchanges, to share specific sender / receiver information for cryptocurrency transactions over a specified threshold. The Financial Asset Task Force (FATF) and their Travel Rule is promoting 'marked competition' among crypto start-ups. Since this is a market-driven effort – by its very nature – and resembles more of a *pseudo-regulatory* initiative at heart, Advanced Systems Management Group (ASMG) have chosen to not comment further on this topic. ASMG do not respond to 'market maker' issues or entities.[143]

[142] There are a few scattered, partially informed, viewpoints on these issues. The first, is an argument for tracing Bitcoin transactions: 1) Source: "Yes, Your Bitcoin Transactions Can be Traced – And Here are the Companies that are Doing It," By Matthew Himes [online – bitcoinist.com]. Dated: June 28, 2018. Secondly, a taxonomic classification of protocols for distributed hash tables (DHTs) organized according to the topics: 'secure', 'selective' and 'audit access functions,' is available here: 2) Source: "The Evolution of Embedding Metadata in Blockchain Transactions," By Tooba Faisal, N. Courtoisand and A. Serguieva [online – arxiv.org]. Dated: 2020. See *also*: *Ibid*., [Foot Note # *198*]. And thirdly, a new architecture -based on decentralized locality sensitive hashing classification(s) -as well as, a set of recommendation methods- arrived at according to 'how data' can be managed by users [via recommender systems (RSs). 3) Source: "An Efficient Blockchain-Based Privacy-Preserving Collaborative Filtering Architecture," By Fran Casino and Constantinos Patsakis, University of Piraeus, [published in] IEEE Transactions on Engineering Management, PP (99) Dated 2019. Pages 1-13. [online]. See: https://www.researchgate.net/publication/336733228_An_Efficient_Blockchain-Based_Privacy-Preserving_Collaborative_Filtering_Architecture; – may, in all *three* cases – provide grounds for further investigation and research.

[143] Source: "Is the Travel Rule Good of Bad for Crypto? Both," by Malcolm Campbell-Verduyn, University of Groningen, NL [online posting – Coindesk]. Dated: January 27, 2020. NB: It is not clear, Professor Campbell-Verduyn states, whether the 'Travel Rule' truly "squares-the-circle," bridging identity data collection and (cryptocurrency) circulation data collection issues effectively, vis-a-vis data protection and data privacy goals and regulatory guidelines. ASMG sees no proof to the contrary, to change our negative opinion regarding the FATF / Travel Rule. See also: https://ciphertrace.com/revised-fatf-standards-on-virtual-assets-12-month-review/. See *also*: 'Travel Rule interpretation, implementation and compliance' - https://parallelsummit.io/. Discussion: ASMG suggest the OCC investigate the FATF 'Travel Rule' for insufficiency: i) legal compliance *standing,* ii) regulatory enforcement *comprehensiveness*, and; iii) a determination re: 'market maker' *relevance*. OCC may wish to consult Scott Rembrandt, US Treasury Department's Head of Delegation to FATF, for an insider's assessment of this effort. See also: Ibid., [Foot Note # 48] '4th Amendment Does Not Protect Bitcoin Data, Says US Appeals Court,'
- Reviewed at Q 4. – Crypto assets / crypto currencies section of this submission. Quoting: CipherTrace Crypto Advisory 7/13 [2020], John Jefferies, editor/ author. Dated: July 13, 2020. See *also*: *Ibid*., [Foot Note *# 85*, *136*].

5-4. Wallet and other access allocation means

The crypto 'wallet' has taken on an almost folkloric connotation, yet even though many believe it to be very simple to understand, why is it so easy to muck up? A crypto wallet is the software program used to store crypto currencies, called crypto *coins*. Even with a straight-forward expose of what the wallet *is*, it has other connotations. Invariably, a crypto wallet can also be accurately described as being a 'communications application.' Or, we might call it a banking application. Wallets demonstrate their utility by instituting actions (trading) or interactions (network transmissions) with *other* (crypto) asset stakeholders (or crypto currencies) – i.e. crypto coins or crypto coin arbiters – on the blockchain.

A lot of things are at work there! If the crypto wallet is organized as a *private wallet*, the user-owner (of that wallet) has their own private key to the private wallet, which they can never lose. All crypto assets, or items transacted through the wallet's software, *trigger* movements (*a.k.a.* exchanges) of, say crypto coins, made by the user/owners' private key instructing these transactions to occur. A second form of wallet is called an 'exchange wallet'. Exchange wallets are a service entity – conducting the transactions on behalf of the user/owner of the wallet. In this case, the trading exchange – or, crypto exchange service provider – has the right to control the user/owner's private key, on their bequest and behalf, in pursuing the wallet's user/owner's instructions on their crypto asset trading activities.[144]

When a new crypto currency wallet is set up, a pair of keys is generated – public and private keys, in their exact paired configuration, the one to the other – each with their own features and functions. The public key generates the wallet's address. The private key creates the user/owner's digital signature, and verifies transactions on the user/owner's behalf. Once the transaction has been verified by the user/owner – or by the crypto exchange service provider, in the case of the exchange wallet example (acting on the user/owner's behalf) – the private key comes into play. The private key then acts on the *hash* contained in the digital signature,[145] signifying that the transaction may proceed and be added to the blockchain ledger.[146] If a private wallet or an exchange wallet are not suitable for the wallet user/owner's purposes, a decentralized exchange (DEX) *trading platform* may be selected. This topic is covered in a separate section, next. (See: Q. 5.5 'Decentralized exchange technology').

---

[144] An example of a crypto trading activity on the blockchain, may involve Bitcoin crypto transactions or Ethereum crypto transactions. In the latter case, an exchange involving Ethereum would move Ethereum ERC20 tokens – Ethereum's (ETH's) crypto coins – whereby '1' Ethereum (ETH) is moved from A's wallet to B's wallet. In this example, the record of the transaction occurring has been recorded on the 'exchange' database, i.e. the exchange's blockchain - where the transaction history is recorded - indicating the transaction concluded successfully.

[145] Digital signatures create a "hash" of the message. A hash is a string of numbers and letters that are pulled from the message**,** file**,** or document based on a mathematical algorithm**.** See *also*: *Ibid*., [Foot Note # *140*].

[146] Bitcoin and Ethereum use a specific algorithm to verify transactions, the Elliptic Curve Digital Signature Algorithm (ECDSA). The Elliptic Curve Digital Signature Algorithm (ECDSA) may be deployed with (or without) encryption, something most people don't realize – i.e. encryption is not automatically provided, or elected, by an Elliptic Curve Digital Signature Algorithm (ECDSA) implementation or selection event.

Most crypto currency attacks have occurred when a hacker *hits* an online wallet (private wallet) or a wallet service (exchange wallet or decentralized exchange/DEX *trading platform*). When this *hit* by a hacker occurs, the hacker attempts to transfer the *secret* private keys to their own wallet. Since one of the commonest attack vectors is to steal funds from the blockchain, via crypto account theft, a common defensive measure would be to never store crypto currency balances in an online 'private' account. The wallet service provider can strengthen the wallet's security stance, by instituting two factor authentication (2FA), or via *push* technologies on mobile device dapps,[147] in which the user/owner's mobile device dapp can approve an access request *pushed* out by the exchange wallet's authentication service.[148]

We began this section's discussion by stating a wallet is a *communication application*. In this regard, it relies on Peer-to-Peer (P2P) network communications functionality. The Peer-to-Peer (P2P) network is a group of nodes that are linked together in a manner where the permissions and responsibilities, for processing data, are equal among *all* nodes. Saying this another way, Peer-to-peer (P2P) computing or networking, is a distributed application architecture that partitions tasks or workloads between peers. Peers are equally privileged, equipotent participants in the application.

The fundamental difference between a Client-Server (C-S) network model[149] and a Peer-to-Peer (P2P) network model,[150] in general, is that each connected machine in a Peer-To-Peer (P2P) network has the same rights as its peers, and can be used for the same purposes. Whereas in a Client-Server (C-S) network, all traffic runs through a few servers, which can quickly become congested, during times of high demand.

What the Peer-to-Peer (P2P) Network affords us, is the option that if one route becomes bogged down – in the Peer-to-Peer (P2P) networking context we are examining – the network can easily redistribute the traffic load to nodes that are less congested. Any node within a Peer-to-Peer (P2P) network has access rights to transactions, as they possess their shared *permissions* to conduct their activity – i.e. signify that the transaction may proceed, or took place, and the transaction's history is added to the blockchain ledger. This ensures that Peer-to-

[147] Many of the mobile distributed applications (dapps and/or Dapps) that do exist, have wallet-enabled crypto asset trading solutions *built-in,* or if they lack this functionality, are linked to service providers with this capability. If developers aren't making their dapp to perform wallet-enabled *crypto asset trading* expressly, then they need to design and build these features into their dapps. Another option is for a crypto wallet user/owner to use a dapp browser, to surf a catalog of dapps, and interact with them. Examples of (two) commercially available (wallet-accessible) dapp *crypto asset trading* platform solutions, are Coinbase and Opera.

[148] Source: "What's a crypto wallet (and how does it manage digital currency?)" By Lucas Mearian, Senior Reporter [online – Computer World]. Dated: April 17, 2019.

[149] In a Client-server (C-S) network, one (1) computer is assigned to be the server, to which less powerful computers / workstations act as *client*'. They are connected like *spokes* to the server's *hub*. The spokes (*clients*) may run programs and access data that are stored on the centralized *server*. The Client-server network has its own network operating system, supporting directory services i.e. a *special* database controlling *who* has access to *what*.

[150] A peer-to-Peer (P2P) network has no special operating system – like the centralized server has in the Client-server (C-S) networking model. Peers are coequal and equipotent, in a non-hierarchical, peer-to-peer (P2P) networking model.

Peer (P2P) traffic transaction *flows* are conducted without (undue) delay, possibly achieving more efficient downloads. The power to control traffic or transaction *flows* does not rest on one centralized monitoring authority – as it does in the case of the Client-server (C-S) networking model. Nor can those who own (or operate) the most servers, as occurs commonly in the Client-server (C-S) networking model, receive unduly favourable rewards. This makes Peer-to-Peer (P2P) networks censorship resistant, but are they secure?[151]

Since all nodes can ostensibly direct traffic on the Peer-to-Peer (P2P) network, the application programming (product) interface (API) may have the chore of facilitating the parsing – *parsing* defined as the analyzing of a string of computer languages or data structures – which may restrict communications allowed, to say, a specific content format. But here is the rub. No device (mobile device or computer/workstation) on the Peer-to-Peer (P2) network is designated to be the sole *central monitoring* authority, to allow or 'gate' [restrict] traffic, therefore hackers can send their malware, or conduct distributed-denial-of-service (DDoS) attacks, on Peer-to-Peer (P2) networks, with impunity. This lack of oversight is what has led to many black-market practitioners utilizing these unprotected, and indefensible, Peer-to-Peer (P2P) publicly available networks as their own – *conscripted* "dark web" Peer-to-Peer (P2P) networks – which they influence, control and hold hostage. These dark web actors then run rampant, and inflict all manner of illegal activities and illegal transactions on the Peer-to-Peer (P2P) networks hosted on the web, with untold economic damage defunding their unsuspecting hosts.[152]

A wallet is – for all intents and purposes – is an *access infrastructure*. Access infrastructure is a term to define the 'what' function of a (crypto) wallet – i.e. a crypto wallet dapp was developed to act as a safe mechanism to store users' private keys – using encryption methods. This, it is hoped, offers to security to digital currency transactions. A crypto wallet should have security protocols integrated to make it hack-proof. These security features may include: i) multi-asset support; ii) QR code scanner (checking addresses automatically), and; iii) Near-Field Communication (NFC) support – e.g. applying Near-Field Communication (NFC) operationally[153] – when the wallet acts as the mechanism to complete the transfer, i.e. sending or receiving, crypto assets.[154] Other security protocols also sometimes supplied include: 12-word mnemonic

[151] Source: "What is Holochain and why does it matter?" By P2P Foundation staff, [online]. Dated: February 15, 2018. See *also*: *Ibid*., Foot Note # *169*] '(P2P Foundation-2018) specific implementations of Peer-to-Peer (P2P) networks are reviewed here. See [full citation-Elastos]: See: https://cyberrepublic.press/elastoscarrierpart3/. And, for Holochain: https://blog.p2pfoundation.net/what-is-holochain-and-why-does-it-matter/2018/02/15.
[152] Source: "Elastos In a Nutshell: Carrier Network Part 3 (of 3)," By Elastos community, [online – cyber republic]. Dated: October 30, 2019. See: https://cyberrepublic.press/elastoscarrierpart3/. Discussion: This paragraph appears under the *citation* caption 'Cons of Peer-to-Peer (P2P) Networks – Point 1. Illegal Activity'.
[153] Near Field Communication (NFC) *operates* based on physical proximity of the asset allocation system to the asset transfer (mobility) device, which requires a sender to *tap* the NFC tag and retrieve the wallet address of the recipient, thus completing the transaction. Source: "Cryptocurrency Wallet Development: Securing Your Crypto Assets," By Mudit Kumar [online a.k.a. Oodles Blockchain). Dated: July 3, 2020. See *also*: *Ibid*., [Foot Note # *154, 175*]. See: https://blockchain.oodles.io/blog/cryptocurrency-wallet-development/.
[154] Source: "Cryptocurrency Wallet Development: Securing Your Crypto Assets," By Mudit Kumar [online - Oodles Blockchain). Dated: July 3, 2020. See *also*: *Ibid*., [Foot Note # *153, 175*].

phrases; two-factor authentication (ubiquitous in Banking today); coin recovery; digital signatures / multiple signatures / biometrics, etc.

Let's take it even further: the wallet is little more than a private key. The security, when all is said and done, is how 'you' [crypto holder] store your private key. This is a 256-bit-key (your private key). Then a public key is generated from your private key, when activated, allowing a user to spend monies. To store your wallet, you could use a USB key, for example Trezor wallet or Ledger Nano5. Now, to store your public key, you'll need software. Two ways to store a public key – via the hot wallet method – online, providing the user (you) with a wallet showing a 'history of service'; or secondly via the cold wallet method. A cold wallet is disconnected from the online internet. Instead a cold wallet may have a paper transcription of your key names and numbers.

A wallet should be able to perform crucial functions including: proving identity, interacting with dapps, trading tokens, buying tickets, unlocking your car and logging into Facebook – all without ever leaving your app.[155] Mobile wallets promise to be useful, once they can overcome being *hacked* or being (outright) *stolen*.

Coinbase, a popular crypto wallet service provider, has over eleven (11) million users, with thirty (38) million currency *makers*, with several buy / sell cryptocurrency options giving chase. Changelly, another crypto currency player, has a feature letting users complete most of their purchases without identity checks or other Know-Your-Client (KYC) procedures. Gemini, a third crypto Company, touts itself as 'very secure,' acting in their capacity as a fully-licensed US financial institution (FI) *a.k.a.* it has FDIC-insured deposits, fully compliant with banking standards. CashApp – the most downloaded app on Google Pay and the iOS App Store – is a mobile device application providing the option to improve, or go-one-better-then PayPal. A fourth crypto player, Venmo allows transactions to *sync* to a bank account.

Critics of Coinbase,[156] back to our first example cited – the Company with a popular crypto wallet service – do not care for higher fees, or extensive (at times very slow) verification on its

[155] Source: "Four things you need to know about mobile dapps," By Adriana Hamacher, article on Decrypt [online], Dated: Feb 14, 2019. See: https://decrypt.co/5181/four-things-mobile-dapps-apps-crypto. NB: Quoting James Sangalli, co-founder AlphaWallet. See *also: Ibid*., [Foot Note # *163*, *164*].

[156] Source: "The technology of retail central bank digital currency," by Raphael Auer, Rainer Böhme. Bank for International Settlements (BIS) Quarterly Review, Dated: March 1, 2020. See *also*: *Ibid*., [Foot Note # 19, 57, 185, 420] '(Auer/Böhme-2019/Page 3 *their* Foot Note # 5) *a.k.a.* KYC/AML identity frameworks.' Auer/Böhme-2019: "An additional key element is a watertight and ideally globally coordinated Know Your Client / anti-money laundering (KYC/AML) identity framework(s), that keeps illicit activity out of this (virtual currency provider) novel ecosystem." Discussion: Coinbase's extensive (at times, very slow) Know Your Client (KYC) verifications are no excuse for any 'lack of' an internationally enforceable Know Your Client / anti-money laundering (KYC/AML) regulatory regime compliance effort put in place. NB: This issue is summarized, in full, at Foot Note # 85. See *also*: Q4. 'Crypto assets / crypto currencies' for its applicability to the two crypto corporate examples presented.

Know Your Client (KYC) system. Then there is Binance.[157] Binance, as the reader will note, has already been discussed for frequent lapses projecting its own self-serving administrative ethics, and their *faux pas* of committing frequent, and repeated, security transaction failures. Whew! That's a lot of stuff packed in there, on half a dozen decentralized finance (DeFi) companies, but signifying what exactly?

What about these so-called *smart-contract* interoperability projects? Just for review, a smart contract is a "an addressable blockchain entity that contains a set of storable data representing a logical state and a set of automated instructions used to alter that state. The instructions allow it also to interact administratively with other addressable entities, and emit events that distributed applications can subscribe to, thereby triggering appropriate behaviours. The state, instructions and transactions are all maintained and secured by the underlying immutable blockchain technology, responding to the requirement to automate interactions among peer-to-peer (P2P) actors consensually. Plus, they typically require a Virtual Machine (VM) interpreter to drive their execution.[158]"

Smart *automated* contracts – within their execution environments – are somewhat predictable, perhaps leading to legally-binding status. This may eventually come to fruition, allowing a smart contract to one day to have a direct legal equivalence to stocks and shares in the investors' market, and escrow services in the credit realm, but we aren't there yet. There is speculation among the experts that the *next* logical advance will be to treat 'smart *automated* contracts' as replacements for traditional contracting vehicles, enforced automatically, without relying on a trusted third party.[159] On a practical level, it must be remembered that, since smart contracts are pure computer code, the logic imputed into the code is of vital importance. Fusing computers with traditional legal contract thinking may unveil many new possibilities, but getting there is the question.

---

[157] Source: "As TikTok 'Spyware' Rumor Swirls, Crypto Apps Safety in the Spotlight," By Stephen O'Neal [online – Cointelegraph]. Dated July 24, 2020. See: Q4. 'Crypto assets / crypto currencies' for discussion. See *also*: *Ibid*., [Foot Note # *79*] '(Spying *a.k.a.* non-approval use of) camera, recording and clipboard issues'.

[158] Source: "Smart Contracts – How to Deliver Automated Interoperability," By Dominic Perini and Michael Jaieola [online – Erlang Solutions]. Dated June 15, 2020. See: https://www.erlang-solutions.com/blog/smart-contracts-how-to-deliver-automated-interoperability.html. See *also*: *Ibid*., [Foot Note # *97, 159*]. Discussion: Smart contracts were analyzed in an in-depth manner - see Section 5.3 'Secure data on chains' - for more information on this topic, *a.k.a. smart-contract* interoperability projects.

[159] We can go further and introduce the concept of the oracle – an oracle being an agent that finds and verifies real-world/external occurrences, and submits this information to a blockchain to be used by *smart contracts*. Voila! A perfect use case application of ASMG's data-centric security (DCS) tagging and labeling services, delivered in a secure, information sharing and safeguarding context. Source: "Smart Contracts – How to Deliver Automated Interoperability," By Dominic Perini and Michael Jaieola [online – Erlang Solutions]. Dated June 15, 2020. See *also*: *Ibid*., [Foot Note # *97*, *158*]. Or, as Perini / Jaieola (2020) state: "Oracles need to be trusted, which in some circumstances requires a high level of trust must be extended to the blockchain's external supporting systems, one example being Data Service Providers (DSPs)." [ASMG would counter with our own question]" Why the external systems? Why not extend the high level of trust to the 'data'? NB. Oracles were analyzed in an in-depth manner - see Section 5.3 'Secure data on chains' - for more information on these emerging developments, which are attempting to secure smart contracts on the blockchain.

Wallets interact with the main client front-end. They do this by allowing apps to send requests to the wallet itself using standard libraries, web3.js being the most popular. For payment transactions, here are the steps, more-or-less: i) the wallet lets an app know – via a response 'hand-shake' or communication – that the front-end can "present – Payment – submitted" ii) the wallet makes the remote procedural call (RPC) to a computer program which calls a sub-routine to execute in a different address *space* – commonly on another computer on a shared network – which is coded 'as if' this event were a normal (local) remote procedural call (RPC). This occurs without the programmer explicitly coding the details of the remote procedural call (RPC) interaction. This is a form of client-server interaction – i.e. caller is the client, RPC action executor is the sender – or payment *procedural* implementation.

In object-oriented terms, remote procedural calls (RPCs) are remote method invocations. Why does this matter? Different processes have different address spaces. If the remote procedural calls (RPCs) are hosted on the same (computer) machine, they have distinct virtual address spaces. Even though the physical address space is the same – i.e. different (incompatible) technologies have used this – *a.k.a.* conducting Common Object Request Broker Architecture (CORBA) process and/or procedural *requests*. CORBA remote procedure invocation passes through the intermediate layer as an Object Request Broker event. This alerts the wallet's remote procedural call (RPC) to engage blockchain server, to submit the approved transaction. The blockchain node receiving this request – i.e. 'procedure invocation' – monitors and submits transactions to the blockchain itself.

Most Dapps[160] today are web apps for a reason: i) this 'web app' organizational mode or appliance structure does not require the User to download a *new* app every time they need to conduct a transaction, and secondly; ii) Users can use 'your app' – built by you, the DevOps provider / designer / service entity – without having to create a *new* wallet every time a transaction request is made.[161]

Just for a quick review, computers have three (3) components – the Network layer (hosting IPFS/Filecoin or Swarm); the Storage layer (IPFS/Filecoin), and the Compute layer – [*continuing*] for the newest Web 3.0 machine-to-user experience, coding to "data" within documents is now

[160] A Dapp on a mobile device? Accessing 'extensions' to the programming code base is not possible, nor allowed, for an 'informed and technologically adroit' User of that Dapp. If you (an 'informed and technologically adroit' User of that Dapp) were allowed in by the DevOps builder / sponsor of that Dapp, once you entered the Browser View, you would sign-in with the prompt "personal_sign." It's just that simple. For a Dapp on a desktop? To perform the same activity – User of that Dapp *sign-in* – you would use a Chrome extension, for example MetaMask, or an equivalent browser plugin. These browser plug-in products allow the user to make Ethereum-styled transactions, through regular websites. NB: MetaMask (and equivalent products) simply allow a crypto wallet to access – via a browser extension – blockchain access, with / without a key vault, secure login and token wallet. For one vendor's take on this - See**:** https://metamask.io/.

[161] Do you note something fundamentally important occurring here? You - the wallet User/Owner - now have an implicit *trust relationship* established with the third party 'DevOps provider / designer / service entity's handling of your personal, highly private (and presumed-to-be confidential) transaction information. Are all wallet Users/Owners aware of this? ASMG would suggest: "Don't count on it!".

within reach. This allows this information 'coded-in' to be linked to information in other databases. If you next add a machine-readable *metadata* content message *a.k.a.* descriptive – the *descriptive* serves to add meaning to "something" in the Web 3.0 content – this makes it possible for a computer to process knowledge, using human-like deductive reasoning, and inference.[162]

Again, a necessary review of terms and terminologies is mandatory here. Ontology describes the concepts and relationships for knowledge domains, including: associated vocabularies and computerized specifications [denoting i.e. *clarifications*] to – the meaning of terms used in the vocabulary. The tagging of information described enables ontology inference rules and data organizational tools to provide logic and structure that can discover meaning and synthesize information on web pages and create domains of pre-organized knowledge on different topics that can be updated on an ongoing basis. This is aided by information sharing and information safeguarding – e.g. the provision of semantic security for Web 3.0 requirements – *a.k.a.* hosted on Web 3.0, also known as the Semantic Web.

Advanced Systems Management Group (ASMG) are sure it will only be a matter of time before the above becomes commonplace, but data has yet to be made 'secure' in these situations. Why? ASMG feels Berner-Lee (and others of that persuasion) are wrong when they suggest information tagging is the rate-limiting step, as it involves far too much coding for Web 3.0 machine learning (ML) applications to deal with. We digress, but point made!

Given all that, what is a wallet? High value – high stakes – low maturity. That leaves no doubt as to why this topic – addressing 'Wallet and other access allocations' – bothered Advanced Systems Management Group (ASMG) at the beginning of this section. Our concerns remain significant, and if basically unaltered, then we have considerable work to do to get to the bottom of all of this!

A short recap of what we have covered so far in this section Q5) '5-4. Wallet and other access allocation means' may prove instructive.

A wallet should be able to perform crucial functions including: proving identity, interacting with dapps, trading tokens, buying tickets, unlocking your car and logging into Facebook – all without ever leaving your dapp.[163] Mobile wallets promise to be useful, once they can overcome being 'hacked' or being (outright) 'stolen'. A popular solution here is to have the

[162] ASMG would also point out the following key facts: this is an entry point 'attack surface' or 'attack vector,' for a cyberthreat actor. As well, it places *all* confidential and personal information in the hands of the Dapps developer – DevOps professional Dapp designer and/or Dapps' service provider– as well.

[163] Source: "Four things you need to know about mobile dapps," By Adriana Hamacher, article on Decrypt [online], Dated: Feb 14, 2019. See: https://decrypt.co/5181/four-things-mobile-dapps-apps-crypto. Discussion: Quoting James Sangalli, co-founder at Alpha Wallet, on novel uses of a wallet. See *also*: *Ibid*., [Foot Note # *155*, *164, 474*].

wallet contain a dapp browser, so that you can surf a catalog of dapps and interact with them. Examples of this functionality are Coinbase and Opera.[164]

Does this mean that the wallet is becoming to Web 3.0 what browsers (such as Chrome and Mozilla) were for the internet (of old)? To answer this, first we must acknowledge that simple smart-contract interoperability projects are *certain to transition* towards (hoped for) seamless sharing of information across blockchains. Or, for the blockchain enthusiasts' wildest dream to be realized, that the end goal for the crypto wallet user is to not even know they're using a blockchain.

We have yet to explain how Dapps are fundamentally different from web apps. A centralized app, like the multi-messaging app for text, pictures and video (Snapchat), offers you a small file (the app) to download, that sends data through centralized servers. A decentralized app (Dapp) like TenX,[165] runs on a decentralized blockchain (Ethereum).[166] A distributed app (Dapp)[167] would run locally on your personal device, and would offer peer-to-peer connections. Dapps today would not exist as prevalently today without Ethereum, or something similar. If Bitcoin represented a centralized bank, Ethereum is like a decentralized computer, essentially a network of agents that does more than move money around but can carry out automated "smart contracts."[168]

[164] Many of the mobile dapps that do exist are wallets linked to crypto asset trading because, up to now, dapp developers that aren't already wallets need to either access one or build one in. Source: "Four things you need to know about mobile dapps," By Adriana Hamacher, article on Decrypt [online], Dated: Feb 14, 2019. See *also*: *Ibid*., [Foot Note # *155*, *163, 474*] '(Hamacher-2019" the killer wallet hasn't [yet] arrived'.

[165] Singapore-based TenX is a multi-purpose Dapp which includes a cryptocurrency payment platform that consists of: a wallet**,** physical debit card**,** bank account**,** ATM access, and more. TenX envisions its products making it easier for you to use your cryptocurrencies in the real world. See *also*: *Ibid*., [Foot Note # *169*].

[166] Trying to stay outside the Ethereum *versus* Bitcoin blockchain / distributed ledger technology suitability argument is near impossible. Vitalik Buterin, the co-founder of the Ethereum platform, had hoped his 5-year old platform would become the entity for decentralized applications (Dapps). Instead, it is now more familiar to the world as the smart contract blockchain, wildly popular for capital raising via initial coin offerings (ICOs). That doesn't mean that no decentralized development is happening on Ethereum, quite the contrary. Source: "Five Popular Dapps on Ethereum You Can Use Today," By Ryan Smith (online – Coin Central]. Dated: November 5, 2018.

[167] More than 1,500 dapps have been built on the Ethereum network, but the use case for most is insular. The five most popular Dapps include: IDEX (building a stack of financial services), Ethlance (decentralized marketplace for jobs), Auctionity (auction house for collectibles/crypto-collectibles), and LocalEthereum (a service using smart contracts to lock-up [escrow] a seller's Ethereum until paid in fiat), and Aragon (creating its own decentralized autonomous organizations/DAOs) – e.g. incorporating a business in a foreign locale, but doing it as a 'point-and-click' internet-type of entity). See: https://coincentral.com/five-popular-dapps-on-ethereum/#:~:text=Five%20Popular%20Dapps%20on%20Ethereum%20You%20Can%20Use,3.%20A.

[168] Source: "Blockchain Watchers Say Decentralized Apps Are Around the Corner," By Rubaia Islam (online – Money in Crypto). Dated: 2018. See: https://moneyincrypto.com/2018/06/26/blockchain-watchers-say-decentralized-apps-are-around-the-corner/. See *also*: *Ibid*., [Foot Note # *506*].

To sum up the situation we face currently, the way dapps have been designed to be run is not safe. Apps or Dapps [169] that run directly on a device, are subject to data leaks because no runtime out there can interface with the hardware, without being vulnerable to hackers. That's why no matter how secure the protocol is, if it is just running atop the existing OS (Android, iOS, Windows, SELinux, etc.) it will always have at least one vulnerability.[170]

And now – the device – the *wallet*. I think we're done with that issue, for now.[171]

5-5. Decentralized exchange technology (DEX)

It's mid 2020 (time of writing) and as of now, most people depend on centralized fiat currencies to manage their finances. For those wanting *crypto* they need convertibility. To do so, most people are subject to Know Your Client / anti-money laundering (KYC/AML) regulations. But once you do that, you are out of decentralized, and into centralized, finance territory. Back up a minute: decentralized exchanges (DEXs)?

In terms of technology, a decentralized exchange is a decentralized application (dApp) created on a public blockchain**.** So far, so good. Trustlessness and immutability are achieved through smart contracts, initiated via Dapps, engaging a wallet, or medium in which that exchange is hosted. Only now, by engaging the services of the decentralized exchange (DEX) platform, the user/owner takes back ownership for trades, once entrusted with the exchange wallet option, and the user/owner is responsible for, and conducts their crypto exchanges and trades themselves.

---

[169] Distributed Apps (Dapps or dapps, both spellings used interchangeably in this report) are apps that run locally on your personal device (as opposed to in the cloud). A centralized app like Snapchat offers you a small file (the app) to download that sends data through centralized servers. A decentralized app (Dapp) like TenX runs on a decentralized blockchain (Ethereum). See *also*: *Ibid*., [Foot Note # *165*] 'More information on TenX.' Discussion (*contd.*): A distributed app (Dapp) would run locally on your personal device, and would offer peer-to-peer (P2P) networking connections. See *also*: "What is Holochain and why does it matter?" By P2P Foundation staff, [online]. Dated: February 15, 2018. Discussion (*contd.*): ASMG were not convinced of the merit of this approach. Harnessing BitTorrent is a poor substitute, for the significant streaming advances, in media and communications business use-cases (Kafka Stream comes to mind). We will leave it to others to convince us. Here is the citation: [P2P Foundation a.k.a.] - https://blog.p2pfoundation.net/what-is-holochain-and-why-does-it-matter/2018/02/15. See *also*: *Ibid*., [Foot Note # *151*].

[170] Source: https://www.reddit.com/r/Elastos/comments/8r9x5b/elastos_vs_holochain/. Quoting '
Blogger post - level 7 - C00mbsie; Dated: (2 points·2 months ago).

[171] Discussion: The complete list of Apps or Dapps running on a device which are susceptible to data leakage, run-time failings/failures, or performance vulnerabilities are analyzed in Q11) sub-section 11.1 'Cyberthreats' – See: *taxonomy* 'a.k.a. Open Web Application Security Project (OWASP) foundation' recommendations: **i**) broken access controls; **ii**) XML external entity (failures)' **iii**) sensitive data exposure; **iv**) broken architecture [*sub-divided* into four items: 1) separated storage; 2) customized configurations (points *a* through *f*); 3) controlled access and user scope, and; 4) security misconfigurations] and; **v**) Injection (with unstructured communications, data, authorizations).

Agrawal (2019):[172] A decentralized (crypto) exchange (DEX) is many things, but I believe an exchange that has the following features qualifies to be a decentralized (crypto) exchanges (DEXs):

- An exchange that allows its users to control their crypto funds.
- An exchange that doesn't have a single point of failure, e.g. a centralized server hosting and/or database that are prone to hacks.
- An exchange that has no trusted third-party setups.
- An exchange that no government can shut down (e.g. Chinese exchange shutdowns).[173]
- An exchange that is not controlled by a single or group of companies.
- An exchange that respects the privacy of its users and doesn't ask for numerous registrations and KYC verifications.

Benefits of decentralized (crypto) exchanges (DEXs): 1) User Controls Funds 2) Anonymous 3) No hacks or server downtime. *Plus*, decentralized (crypto) exchanges (DEXs) make crypto users their own bank. *Secondly*, decentralized (crypto) exchanges (DEXs) honor the privacy of their users and bypass the need of doing Know Your Clients (KYCs) registrations, etc. Is this important? Absolutely! The ability to provide seamless liquidity for many crypto coins (tokens) – that are not able to list themselves, after initial coin offerings (ICOs), on centralized exchanges because of several rules/regulations set forth by these [centralized exchange] authorities – is, in a word, shocking!

This system for "DEX" – highlighted *above* by Agrawal (2019) – is a brand new (relatively speaking) system. So, what are the down-sides? Agrawal (2018) covers these:

- There are serious liquidity problems due to lack of volume.
- There is a lack of advanced trading functions such as margin trading, margin lending, stop losses, bot trading, etc.
- Most decentralized (crypto) exchanges (DEXs) that are now in use are in their beta testing stage, and users stand the risk of losing their funds because of insufficient testing.
- There is no central authority or support system, so it's hard to get your problems resolved.

Are there *other* things to be concerned about? Sure.

The decentralized (crypto) exchanges (DEXs) do not rely on a third-party service to hold the customer's funds. Instead, the decentralized (crypto) exchanges (DEXs) conduct their trading activities directly between users (peer-to-peer), through an automated process. Such a system can be established by: i) creating proxy tokens (crypto assets that represent a certain fiat or

[172] Source: "Why Are Decentralized Exchanges the Future of Cryptocurrencies?" By Harsh Agrawal [online – Coinsutra]. Dated: September 6, 2019). See: https://coinsutra.com/decentralized-exchange-cryptocurrency/.
[173] Source: "China is shutting down domestic Bitcoin exchanges," By Shannon Liao [online – theverge.com]. Dated: September 11, 2017. See: https://www.theverge.com/2017/9/11/16288898/china-shutdown-rumored-bitcoin-exchanges-crackdown.

cryptocurrency value) or ii) assigning value to (crypto) assets (that can represent shares in a company, for example) or iii) utilizing a decentralized multi-signature escrow system, among other solutions.[174]

Since Advanced Systems Management Group (ASMG) are a security services entity, naturally 'security services' would be what we would be drawn to look at next. Kumar (2020)[175] lends us a hand:
A decentralized crypto exchange's *security* remains limited, due to the underlying distributed ledger. Therefore, it is important to ensure the ultimate security of a decentralized exchange, by using an efficient underlying distributed ledger, e.g. Stellar blockchain. Also, to ensure transaction security is met, smart contracts should be regularly audited via security and operational reviews, and distributed ledger platforms must be monitored for their overall operational consistency and technical proficiency and functionality.

The decentralized (crypto) exchange (DEX) expert Mudit Kumar (2020) continues: Due to a decentralized crypto exchange platform developing on top of a decentralized exchange *protocol,* let's examine this next. A decentralized exchange *protocol* refers to a software program that we host on or integrate into one or more distributed ledgers. It facilitates automated peer-to-peer (P2P) transactions on the distributed ledger. Further, users get the ability to retain sole custody of their private keys throughout the transaction process and thus, ensure privacy. Additionally, users have access to the readily available information.

Kumar (2020): A decentralized exchange protocol also integrates with an on-chain and off-chain order book database, and a GUI (Graphic User Interface) and APIs. Put simply, we can break a decentralized crypto exchange application into four components:

- Platform and technology implementation of blockchain
- The mechanism of counterparty discovery
- The algorithm for order matching
- The protocol for transaction settlement protocol

A decentralized exchange application may not be completely decentralized, in all four components. It is because, for various decentralized exchange applications, one or more

[174] Source: "What is a Decentralized Exchange?" By Antonio Madeira [online - CryptoCompare] Dated: March 12, 2019. See: https://www.cryptocompare.com/exchanges/guides/what-is-a-decentralized-exchange/. NB: This system contrasts with the centralized model in which users deposit their funds and the exchange issues an 'IOU' that can be freely traded on the platform. When a user asks to withdraw his funds, these are converted back into the cryptocurrency they represent and sent to their owner.
[175] Source: "Analyzing the Essentials of Decentralized Crypto Exchange Platform Development," by Mudit Kumar [online – Oodles Blockchain] Dated: April 21, 2020. See: https://blockchain.oodles.io/blog/essentials-decentralized-crypto-exchange-platform-development/. See *also*: "Cryptocurrency Wallet Development: Securing Your Crypto Assets," By Mudit Kumar [online - Oodles Blockchain). Dated: July 3, 2020. See *also*: *Ibid*., [Foot Note # 153, 154].

components can be off-chain/centralized or decentralized. Numerous decentralized exchange applications, however, focus only on token trading within one chain.

(Kumar 2020) *again*: A user needs to identify an order [for their transaction], and essentially, this 'particular *counterparty*' (whom has placed the order) initiates the trade. In some cases, a decentralized exchange (DEX) may not have order books. Instead, it may feature a reserve-based model. A reserve-based model enables the supply and demand of various tokens, readily available for the execution, based on the reserve's quoted *buy* and *sell* prices, for this 'particular *token*'. These reserve-based models should be maintained on-chain, which requires smart contract solutions, to enforce the execution and settlement of any/all trades. This also benefits the trading / transacting parties, as they can also automatically determine their trade's price with a smart contract.

A few more points: 1) Instances of on-chain order books include: Bitshares and Stellar, with their decentralized exchanges (DEXs). When two orders intersect in price, a decentralized platform automatically executes and settles the trade. Secondly, 2) Hosting an on-chain order book on a decentralized network means that one needs to trust centralized, off-chain actors, for accurate and reliable publishing or broadcasting of the order books.

That was a whirl-wind walk through distributed exchange (DEX) technologies.
People can trade crypto-to-crypto using dozens, if not hundreds, of wallets and (multiple) exchanges that are available. So why isn't everybody using decentralized exchanges?
Well it's early times, as these articles were all written in the last two years or so. For most of us, in the trading public, people wanting crypto usually need convertibility. To do so, most people are subject to Know Your Client / anti-money laundering (KYC/AML) regulations. But once you do that, you are out of decentralized and into centralized finance. Get creative: shun centralized?!! Buy crypto from an ATM, but the exchange rates may be higher (approximately 5-10 % higher) than with a centralized exchange. Coinbase allows you to do this, and Coinbase also allows recurring buys. Today Coinbase holds your cryptographic keys; therefore, allowing you to use fiat money to purchase / make trades with Coinbase. Again, enter fiat, enter Know Your Client / anti-money laundering (KYC/AML) regimes and procedures. Plus, if you don't own your keys to your wallet (Coinbase does), you don't own that crypto. (What?).[176]

For the OCC, here may be the most chilling fact of all. Thibodeau (2019) states: "Decentralized exchanges cannot provide governments or other central authorities with user information upon request, even if they wanted to, or were required to by law. They don't require identifying data

[176] Source: "Understanding Decentralized Exchanges," by Mary Thibodeau [online – HedgeTrade]. Dated: February 23, 2019. See: https://hedgetrade.com/understanding-decentralized-exchanges/. NB: Waves DEX allows you to trade crypto to crypto. However, without the fiat function, Americans must get crypto sent directly to their wallet to get started, and don't have the option to buy or sell anything with fiat. As a result – Waves DEX does not hold your personalized information. Trades (and trade-offs) in an emerging, still-to-achieve-maturity, crypto trading-*issuance* service offering.

from users (unless users want to transact in fiat there), thus it [the crypto trading information, it must be assumed) is not stored anywhere.

5-6. Fundamental / foundational (security) infrastructure

This sixth point, hived out of the topic distributed ledger technologies (DLTs) – the fundamental infrastructure to anchor distributed ledger technologies (DLTs) *securely*– will be met via a brain-storming session, if you will. What we are aiming to brainstorm here is the very idea that distributed ledger technologies (DLTs) require a foundational security layer. Isn't this overly obvious? Not so!

First let's examine centralized financial institutions (FIs) – and the regulators which serve the industry – cannot *today* perform *real-time* analysis across all data stores, which causes them to suffer a potentially devastating weakness, or glaring inconsistency, in the knowledge they possess. This knowledge gap requires remediation. To overcome this knowledge gap, organizations must tailor and customize their *Search* and *Query* results, and not have these efforts always simply parrot what they think (or guess) as the status-quo conditions at work in the data service they are monitoring. Although knowing what is '*in*' your corporate data repositories may be an efficient use of an Employee's time, and may stem data processing downtimes, if the data you are looking at is immaterial to your business (or regulatory activities or proclivities?) what have you gained? What may be needed is the pairing of instantaneous *Search* and *Query* alerts, critical, boundary-pushing searches, and then – maybe even receiving – relevant information on your desk, exactly when you need it.

It is entirely possible that the user-of-data could be from two opposing data stakeholder constituencies, each addressing completely different business tasks and technical-administrative scenarios. The first might be Security and Privacy Officers. These Security and Privacy Officers represent data owners, data stewards and data custodians. This group have the stated goal of needing to apply *defense-in-depth* solutions to protect their data, which will efficiently (and quickly) exchange and receive the *specific* data elements they need, to perform their assigned work.

Their opposite counterpart(s) are the Operational users of data. This group are steadfast in their determination to have *their* data, via full data discovery, unhindered by any accessibility issues affecting them, or their membership enclave – e.g. their Community-of-Interest (C-o-I). They expect to have this accomplished with a minimum of fuss, and may only be peripherally aware of their certification and authorization (C&A) data access requirements, as per any training on such matters that they may have voluntarily received.

Let's move beyond definitional, or organizational, points of contention. Before leaving centralized financial institutions (FIs) – and the regulators which serve the industry – which we just summarized are (so far) unable *today* to perform *real-time* analysis across all data stores, is

this really an acceptable state of affairs for regulatory agencies to accept? Advanced Systems Management Group (ASMG) would state unequivocally: Absolutely not!

Let's turn our attention now to the decentralized finance (DeFi) crypto asset or crypto currency organizational entity or financial sector. We are hemmed in here by the decentralized finance's (DeFIs) crypto wallet's handling of information, which is stymied by its aggressive advocacy – in some circles – for the widespread implementation of smart contracts. Can this achieve real-time monitoring of data assets in a manner which improves upon the stilted real-time monitoring of data repositories (data assets) achieved to date by centralized, or mainstream banking?

This leads to a very thorny issue: That issue is: crypto wallet asset *staking*. Smart contract determinations and enforcement activities are always a challenge, more so since in the decentralized finance's (DeFIs) crypto wallet's case, the wallet is the repository which holds digital currency. What then is crypto wallet *asset staking*?

In the crypto currency world, 'staking' refers to locking up a digital asset. In effect, it means you have agreed to *hold* the digital currency / token in a *wallet* on its respective blockchain network. This may also be called a Proof-of-Stake (PoS) activity, although for our purposes, we are treating this as an investor would, i.e. investing in a crypto asset as a security, to be held like any other (traditional – stock or bond) investment security, to reap the reward i.e. earning a dividend or interest. Proof-of-Stake (PoS) oftentimes references Native-Coin (Ethereum platform) as the base for the staking effort. The staking action allows the digital coin (digital token) holder to, for example, earn a 'block' of rewards – issued either in the currency / tokenization transaction called 'Ether' (or an equivalent crypto token amount) – assessed against the length you have kept you 'principally-owned' digital asset *staked*, and therefore out of possible circulation for its redemption value.

This can be an arduous process. Therefore, crypto service providers have addressed this market niche by offering Staking-as-a-Service (ST-a-a-S) platforms. These ST-a-a-S platforms lower the technological barriers experiences by the user, so virtually any user/subscriber to their service can earn the digital token amounts caused by their commitment to 'stake' their own crypto asset valuations. Exchange-staking for the unit holder enables them as investors to leave their Proof-of-Stake (PoS) "stakeable assets" in their trading account wallets, to earn "interest," in the form of fresh tokens. Since the Staking-as-a-Service (ST-a-a-S) platform has made this technologically possible, the ST-a-a-S platform provider earns a small percentage fee for their service.

The entire consensus mechanism and fault-tolerant mechanism employed by blockchain relies on the 'best interest of the entire network.' Blockchains, e.g. distributed ledgers, allow users/subscribers to verify they receive the full amount of their earned *staking* rewards (fresh

tokens). Stakers – taxpayers involved in Proof-of-Stake (PoS) validation of blockchain transactions – are operating in uncharted waters.[177]

This is not a satisfactory answer. We turned next to Angelovska-Wilson / Weiss (2020) for their guidance.[178] After a methodical review of U.S. federal securities laws and money transmission laws applied to PoS arrangements, in which token holders Delegate their digital assets to Staking-as-a-Service (ST-a-a-S) platforms/providers, who stake on that Clients behalf, here is what we found. The SEC in their recently released Framework for 'Investment Contract Analysis of Digital Assets' takes the position that staking is a common enterprise. Common enterprise means Staking-as-a-Service (ST-a-a-S) providers usually take a percentage of all earned Rewards and combine Valuation Rights of holders in their record or 'block'. Interestingly, Angelovska-Wilson / Weiss (2020) believe that as staking approaches one hundred (100) per cent holders participation, the likelihood of earning a profit goes down. This is still rent-seeking activity, as not to 'stake' would also be deleterious to the investor's position. The Supreme Court has ruled that investors do not need securities law protections of they can exercise control over the profit-generating activity.[179]

Staking-as-a-Service (ST-a-a-S) providers are responsible for running the software that validates transactions and earns Rewards. Meaning? If the ST-a-a-S entered non-performance territory, negotiating affecting the asset holder, securities laws would apply, to all prepaid service contracts. But are these conditions not mitigated by contractual agreements and remedies, not securities laws? Since staking activities assume inflation rate applied against asset 'staking' holdings, of approximately five to fifteen (5 – 15) per cent,[180] on average, Clients/investors are required to pay federal and state taxes on the receipt of Rewards which further diminishes any expectations of profit.

FinCen has taken the view that Staking-as-a-Service (ST-a-a-S) is a money (transmitter) service business (MTSB), executing the staking activities execution, between the Network and the Client. The US Treasury Department believes transactions between two parties is not a money transaction business (MTB) activity.[181] That's enough!

---

[177] Source: "Taxation of Virtual Currency Staking Activities." By Andrea Kramer, McDermot Will and Emery LLB [online – jdsupra]. Dated June 24, 2020.
[178] Source: "The potential implications of security proof-of-stake-based networks," [Chapter 12] By Angela Angelovska-Wilson and Evan Weiss [online – Global Legal Insights]. Dated: 2020 – part of the Publication "Blockchain and Cryptocurrency Regulation 2020." See: globallegalinsights.com. Discussion: '(Angelovska-Wilson/Weiss-2020) provide a very thorough outline, from a crypto expert on staking (Weiss) and a lawyer's insight (Angelovska-Wilson) on this issue *a.k.a.* Staking-as-a-Service (ST-a-a-S), its duties and responsibilities, as legally mandated and recognized.' Well done!
[179] Source: SEC vs. Unique Financial Concepts, Inc., 196 F.3d 1195, 1201 (11th Cir. 1999). [internal citations, quotations and brackets omitted].
[180] Source: "Application of FinCEN's Regulations to certain Business Models Involving Convertible Virtual Currencies," FinCEN. Dated: May 9, 2019. See: FN-2019-G0001; Page 3.
[181] Source: U.S. Treasury Department – 31 C.F.R § 1010.100 (ff) (5) (i) (B) (2011).

Advanced Systems Management Group (ASMG) have no opinion on which side is right. We do, however, challenge any preconceived notion that the underlying network – the network hosting the exchange guiding how the distribution of a wallet's proceeds may occur – is a very problematic topic to address! Is it regulated? Good question!

Somehow wallet staking seeks to be regulated sufficiently enough to prove – by its very essence – that it is, in fact, robust and secure. Angelovska-Wilson / Weiss (2020) have come the closest to nailing this topic. They suggest: "Staking-as-a-Service (ST-a-a-S) providers [that] offer several different software services including: **i**) state of threat multi-sig **ii**) encryption and authentication **iii**) customer service **iv**) software services (dashboard and application [programming] product interfaces / APIs) **v**) monitoring and alerting systems and **vi**) Reward audits and distribution (collectively the 'Services') – which are all technological benchmarks for quality service delivery" – should somehow factor *in* to all of these discussions. The point we are emphasizing – 'should' – is the giveaway!

Why? Again, let's ask the experts! Angelovska-Wilson / Weiss (2020) suggest: "Staking-as-a-Service (ST-a-a-S) providers take an active role by: **i**) ST-a-a-S providers are arranging the transactions by utilizing software to stake the virtual currencies/assets/tokens on a 'specified' network or platform supporting that network **ii**) monitor the nodes on the network to ensure they are only validating currencies (crypto assets / tokens) they are asked to, on the exact (specified) network the Staking-as-a-Service (ST-a-a-S) provider is tracking **iii**) the ST-a-a-S provider is endorsing transactions by continuously verifying transaction behaviours on that specific network to earn Rewards. The Services offered by the ST-a-a-S provider to clients/subscribers provides clear evidence that they (the ST-a-a-S provider) offer and execute multiple services independent of money transmissions."

We have travelled through some choppy waters up until now. Let's return to a topic raised in the sub-section addressing: 5.1) 'Stablecoin projects and asset tokenization technologies (*a.k.a.* 'asset allocation means [devices],' as used and/or deployed to *transact* cyber-currency exchange activities.[182] [Original text – from earlier – *reproduced here*]: A new development is the Miniature Autocratic Government (MAG) token. MAG tokens call for an initial coin offering (ICO) delivered via peer-to-peer (P2P) networks, with a developer designing a miniature economy of sorts, in which the token to-be-issued is to constitute the medium of exchange (e.g. the means of payment) for the hard drive-specified storage space which serves as the 'service being rendered/purchased'.

Continuing the analysis: The Miniature Autocratic Government (MAG) tokens – which calls for an initial coin offering (ICO) to be delivered via peer-to-peer (P2P) networks – are set up and

[182] Source: "Accounting for Crypto Assets – IFRS (#) Publication*," By Jiri (George) Daniel and Amanda Green – authors (Ernst and Young-E&Y EMEIA), and; Hitesh Patel, Associate Partner – E&Y EMEIA (UK) FinTech Team; and Paul Brody, Partner – E&Y Technical Leadership (IFRS & Blockchain) *et. al*. Published by E&Y (UK) Assurance Tax Transactions Advisory Service. Dated: 2018. See *also*: *Ibid*., [Foot Note # *104, 107, 108, 116, 117, 141*] *a.k.a.* 'E&Y – section 2.2.2.2. "Miniature autocratic government" (MAG) tokens* (Page 9)'.

proceed via a process, or procedure, copying the seigniorage format. A seigniorage format, in the [historical] example we will cite for illustrative purposes, allows the government [financial currency *issuance* authority] to *earn revenue* when they sell bank notes at a premium, over their "overhead" of salaries, distribution, marketing etc. (and input materials cost of cotton, paper, printing. etc.).

In the case of the issuance of the Miniature Autocratic Government (MAG) tokens, the MAG issuance costs – associated/incurred with an initial coin offering (ICO) delivered via peer-to-peer (P2P) networks – can be set at the developer communities' whim (discretion), and set unilaterally. They may be broached – in ASMG's inexpert opinion (we admit) – to be viewed as a *precursor* to some form of customer 'rent-seeking behavior,' plus MAG tokens may carry an *undercurrent* to their actions approaching tax avoidance (again – this is ASMG's inexpert opinion. Admittedly!). The Ernst and Young (E&Y-2018) Report suggests that the re-investment of Miniature Autocratic Government (MAG) Initial Coin Offering (ICO) "commissions" is akin to the role played by infrastructure investment and foreign direct investment promotion agencies.

The "sources" providing their storage services – *a.k.a.* as a tokenized service offering – are escaping any clear-cut monitoring of their services delivery. Is this (MAG) token developers' offering legit? And who monitors this (MAG) token proscription and *issuance*? A regulatory authority? None that we can see! These (MAG) token developers are essentially registering and extracting rent-derived income from their token-holding Client base, with no monitoring or regulatory compliance assessments being made. Tracking could have been applied – by a data-centric security (DCS) tagging / labeling *virtual* audit trail mechanism – but after the fact? And most certainly, this audit trail should have been imposed immediately, as extra-territorial issues may be in play! What if the data storage / crypto storage was being delivered out-of-state, and/or or out-of-country (out-of-jurisdiction)? And what if these hard drive-specified storage space leasing options *leached out* information or asset holdings to off-shore locations, beyond the purview of foreign treaty obligations? Theft? It would appear this may be the case! At that point, enter a US regulatory agency, asked to intervene on the US citizen's behalf, yet how are US regulators to proceed? The crypto asset allocation(s) storage space may have just escaped (or relocated) to somewhere beyond the reach of the US Treasury Department or the OCC. In short, these (Mag) tokenized accounts are beyond redemption, and their holdings (and their data value) have just been made unattainable. Great.

Advanced Systems Management Group (ASMG) have created an interoperability vehicle worth examining. And certainly, a solution which could have plugged the hole created by MAG tokenization in this last example. This interoperability solution embraces the data-centricity paradigm, and envisions a data-centric security gateway / interfacing solution – as adopted in the defense sector – spreading into the financial services vertical. Advanced Systems Management Group's (ASMG's) improvement to the *status-quo* data classification and information exchange conditions practiced by Extract-Transfer-Load (ETL) methods and methodologies is unmatched by any other source in the world today. And it is backed by an open standard, and US Cert. – National Security Agency (NSA) EAL3 Certification and

Accreditation (C&A) *security assurance* ranking – among the world's most difficult Certification and Authorization (C&A) rankings to attain.[183] This solution would have stopped the leaching of tokenized assets out of the country, before any such attempt could have been initiated. Food for thought.

What is becoming increasingly clear to the data user community is the fact that: a) the protective layer applied, either as a security layer attached to the information objects in the files and data sets which users depend upon, and create hourly or daily, and/or; b) an encryption technology applied in the form of a security container, key management systems, cryptographic systems and tamper-proof audit trails etc. – which would only release information to a *need-to-know* party authorized by a certification and authentication (C&A) service, as they are pre-approved to receive [said] information or data files – may be the ideal way to go. Or, we could adopt a third approach: c) Data Administrators and the organizations Information Technology / Information Management (IT/IM) Security Team could adopt a unified security policy, enterprise-wide, that would be applied across all operations with respect to the treatment of data, without the need to deploy a new set of data or security services.

The Information Sharing and Safeguarding (ISS) Solution – Advanced Systems Management Group's (ASMG's) data-centric security (DCS) solution *per se* – addresses this third requirement, i.e. adopting a unified security policy, enterprise-wide, in its entirety. But it also, some would say fortunately so, incorporates two points: i) the provision of protective security layers (called defense-in-depth) and; ii) encryption, key management and trusted audit services are available for implementation, as part of the information sharing and safeguarding / data-centric security (DCS) solution.

Advanced Systems Management Group's (ASMG's) Common Object Interfacing/Interoperability Layer (COIL) provides services in concert with an Enterprise Service Bus (ESB), or COIL simply acts as an interface or messaging agent. It provides a data-centric security (DCS) capability in a messaging environment, and manages the attribution of message metadata required to implement DCS policies. Advanced Systems Management Group's (ASMG's) COIL *is* (software) services-based. The Advanced Systems Management Group (ASMG) data-centric security (DCS) solution pre-supposes a desire for *governance* and *accountability*. In the defense sector this is

[183] ASMG's data-centric security (DCS) solution – based OMG's standards –body ratified open standard, called the Information Exchange Framework (IEF) Reference Architecture (RA) – surpassed Technical Readiness Level (TRL) 6 to 7. The ASMG DCS solution has achieved Certification and Accreditation (C&A) security assurance \ ranking *a.k.a.* Common Criteria EAL3 – [US] National Security Agency (NSA) Labeled Security Protection Profile (version 1b). NSA's EAL3 standing covers security functional requirements for: 'Audit; User; Data Protection; Identification and Authentication; Security Management; Protection of the Target Evaluation (TOE), and; Cryptographic Support'. All *criteria* applied to: -an information system, part of a system or product, and all associated documentation that is the subject of a security evaluation. See: https://www.ncsc.gov/nittf/docs/CNSSI-4009_National_Information_Assurance.pdf. See also: See: https://www.us-cert.gov/bsi/articles/best-practices/requirements-engineering/the-common-criteria. '(*a.k.a*.) the Common Criteria, Evaluation and Assurance Levels by US-Cert.).

called situational awareness. The finance sector has this requirement, but they loosely (and not definitively) call it *business intelligence*.[184]

Understanding and controlling data, via its metadata, is of prime importance. Once the policies, rules, ontologies and vocabularies governing all data are specified and enforced, Advanced Systems Management Group's (ASMG's) data-centric security (DCS) solution can be acted upon, as a set of software-defined services, programming language-clarified directives, and applied to the minimally necessary data attributes required for an information sharing / information safeguarding exchange message to occur. Governance and accountability should be fully embedded into the financial realm's security architectural infrastructure, and not added as an afterthought.

Data, as a supply chain issue or *deliverable*, is created by applications (thick or thin, rich or basic), either using the application itself, or by using an agent (client-side), that profiles the data prior to storage or transmission. The extent of that implementation, and the products used to implement it, Advanced Systems Management Group (ASMG) are absolving from an IT governance issue, into an implementation issue.

Protection needs to be applied, either as security attribution attached to the information objects in the files and data sets which Users depend upon, and / or there needs to be a protective layer to apply such attribution, and afford the protection required, when the information is accessed. At the outset, this invariably means that User(s) understand the specified content and context of the information asset itself.

Let's examine what the Bank for International Settlements (BIS-2020) say about distributed ledger technologies (DLT): "Conventional and distributed ledger-based technologies (DLT) often store data multiple times, and in physically separate locations. The main difference between them lies in how data are updated. In conventional databases, resilience is typically achieved by storing data over multiple physical nodes, which are controlled by one authoritative entity – the top node of a hierarchy. By contrast, in many DLT-based systems, the ledger is jointly managed by different entities in a decentralized manner, and without such a top node. Consequently, each update of the ledger needs to be harmonized, between the nodes of all entities (often using algorithms known as "consensus mechanisms"). This typically involves broadcasting and awaiting replies on multiple messages, before a transaction can be added to the ledger with finality."[185] This is as accurate a description of data providence as one could hope for.

---

[184] Reviewing some text which appeared in the Introduction to this Submission (Reproduced *herein*): In the defense sector's case, situational awareness is at an advanced state of codification, ontological definitional accuracy and implemented level of accomplishment. Situational awareness allows defence sector participants to detect cyberthreat, or malevolent intent by adversaries, long before the finance sector's *business intelligence* response capability would learn of the incident.

[185] Source: "The technology of retail central bank digital currency," by Raphael Auer, Rainer Böhme. Bank for International Settlements (BIS) Quarterly Review, Dated: March 1, 2020. See: https://www.bis.org/publ/qtrpdf/r_qt2003j.pdf; *and/or* https://www.bis.org/publ/qtrpdf/r_qt2003j.htm. See *also*: *Ibid*., [Foot Note # *19*, *57,* 420].

The Bank for International Settlements (BIS) authors (Auer / Böhme- 2020) next address the vulnerabilities of conventional and DLT-based infrastructures: "The vulnerabilities are simply different. The key vulnerability of a conventional architecture is the failure of the top node, for example, via a targeted hacking attack. The key vulnerability of DLT is the consensus mechanism, which may be put under pressure, for example, by a denial-of-service type of attack."

Continuing, BIS state: "Ongoing assessments of DLT-based proofs-of-concept projects that are still ongoing, it remains to be seen whether scalable implementations will actually rely on the technology. Experiments are based on enterprise versions of distributed ledgers, which allow for decentralization but, in practice, are often run under centralized control." Ali and Narula (2020)[186] note that the platforms typically used "are useful for experimentation and prototyping because of their flexibility and features […]. However, what is helpful for prototyping might not be good for practice; these complex platforms make trade-offs when it comes to security, stability, and scale."

Let's get to one issue immediately: have Advanced Systems Management Group (ASMG) worked out a methodological implementation to support the distributed ledger? We are approachable, and willing to collaborate. ASMG have a DEMO version of the data-centric security (DCS) solution, which we are more than willing to demonstrate at OCC's earliest convenience.[187]

5-7. A Special Case: Cardano's Distributed ledger technology (DLT) Project

Another facet of blockchain that makes it difficult to fathom is that it is run amok by developers.[188] Most of the blockchain industry consists of high-end developers. Right now, all the tech you hear concerning blockchain, be it smart contracts or private keys, are still super complicated. But when you talk about mass audiences, you need to make blockchain (and crypto for that matter) very simple.**[189]**

[186] Source: "Redesigning digital money: what can we learn from a decade of cryptocurrencies?" By Ali, R., and N. Narula. Published by MIT DCI Working Papers, January 2020, Page 6.
[187] The ASMG DEMO is *ongoing* at the NATO Coalition Warrior Interoperability eXchange (CWIX) initiatives, and contracted activities sponsored by Department of National Defence (DND) Canada. Source: Michael Abramson, Special Advisor on Public Safety/ Security - Open Interoperability Standards to the Centre for Security Sciences (CSS - Department of National Defence/DND Canada); Co-Chair C4I Domain Task Force at OMG; Chair Emergency, Crisis and Major Event Management SIG, Chair Information Exchange Framework (IEF) WG (OMG); and Information Sharing and Protection Standards Development Principal author.
[188] ASMG thought we had finished with this question: Q. 5 – 'Distributed ledger technology (DLT) for banking.' It always seems the case that the proliferation of developers, placed into senior decision-making capacity, can take the conversation – and precious critical resources – on tangents that may seem unbridgeable. To our credit, we have given everyone their say.
[189] Source: "OKEx's Lennix Lai: Passive Income in Crypto Is the New Way to Earn," By Lennix Lai, OKEx Director of Financial markets, [interviewed by Cointelegraph's Erhan Kahraman]. Dated: March 22, 2020. See:

Following up on that point, *keeping-things-simple*, as much as Advanced Systems Management Group (ASMG) wish this to be the case, we uncovered a few radical ideas which – far from simple – at least challenged some long-held status quo thinking. We will drill down a bit into this *en masse*, and let the chips fall where they may.

A new approach to decentralized finance (DeFi) has been offered up by Charles Hoskinson (Cardano 2020), whom recently stated: "Cardano feel we can innovate on three (3) levels: **i**) use of smart contracts with terms and conditions of commercial relationships better controlled e.g. fraud-free, with commerce guaranteed; **ii**) use hardware security modules (HSMs).[190] Where Personal Identity (PiD) is not leaked, but used to authenticate and credential actors, and; **iii**) adopt modular regulation supporting decentralized autonomous organizations (DAOs) via rules encoded in computer programs that is transparent, controlled by organization members. This decentralized autonomous organization (DAO) can be customized to interact with user-written smart contracts, to add mutability, consumer protection and arbitration. This last point – modular regulation supporting decentralized autonomous organizations (DAOs) via a rules-based regime – will be scoped out in a *future* paper.[191]

Before we jump into the milieu created by Cardano's Charles Hoskinson, with this brute-force frontal assault on blockchain crypto asset issues affecting the financial sector and financial institutions (FIs), it is timely to state that a huge divide separates the new *era* of crypto transactions and the centralized edifice or *mainstream* financial services delivery effort. Plus, regulations pertaining to identities bumping up against blockchain's *laissez-faire* decentralized model of operations, are leading to a clash of cultures. This dilemma means something quite different to 'the ledger's' aficionados. They view their challenge as a *trilemma*: i) anonymized data to always be genuine ii) user's unrestricted access to genuine anonymized data and; iii) the blockchain must be decentralized, scalable and secure.

The Cardano Project - as we have come to call this effort - came to our attention after we read a comment by a Canadian banking regulatory counterpart to the OCC. Ben Gully, Assistant Superintendent at the Office of the Superintendent of Financial Institutions (OFSI), raised an issue in February 2019, suggesting: "Technology will enable or accelerate further decentralization of financial market participants, and blur the boundaries of a traditional regulated financial institution *specifically*. Instead of worrying that banks carry enough capital, watchdogs (regulators) now need worry about the type of cloud storage, or the anti-virus software, that lenders (Financial Institutions) use, but do not entirely control. Third Party

---

https://cointelegraph.com/news/okexs-lennix-lai-passive-income-in-crypto-is-the-new-way-to-earn. See *also*: *Ibid*., [Foot Note *# 347, 509*].

[190] Source: "Scaling Bitcoin with Secure Hardware," By Joshua Lind, Ittay Eyal, Peter Pietzuch and Emin Gun Sirer, [online – Hacking. Distributed]. Dated: December 22, 2016. See: http://hackingdistributed.com/2016/12/22/scaling-bitcoin-with-secure-hardware/ from Cornell University.

[191] Source: "Why We are Building Cardano," By Charles Hoskinson, [online – Cardano]. Dated: 2020. See: cardano.org. See *also*: *Ibid*., [Foot Note # *193*, *195*, *196*]. See also: Ibid., [Foot Note # *415*] (Keys-2018) Calling out Ethereum acolytes for their narrowness in not investigating Cardano (i.e. Cardano's views on what ails the crypto space, at present).'

vendors or intermediaries can quickly affect a financial institutions' (FIs') operations, its ability to grow its business, and potentially its bottom line."[192]

Mr. Gully (Office of the Superintendent of Financial Institutions /OSFI) didn't seem to be pointing at the crypto players as a worry with the above statement, but he might need to reassess that comment, in furtherance to the comments we wish to present next.

What Project Cardano is initiating or advocating is the '*build*' of a stable crypto currency ecosystem. If Ethereum's founder Butyrk has a destiny to build a world computer, who's to say Hoskinson's (Cardano's) dreamscape is any less sound?

Sharma (2019) sees the Project Cardano effort as follows:
i) a Control Layer – much more comprehensive than today's over-emphasis on the settlement layer, which is too restrictive in what it addresses
ii) a Credit system
iii) a Universal cypto currency wallet (Daedalus) with Automated trading facility and Crypto-to--fiat conversion capability.

Sharma (2019) notes Project Cardano errs on industry research and development effort prognostications, sometimes over-selling them as if they are implementable 'now,' which they aren't. They include:

i) Standardizing protocols – Hoskinson views these as programmable 'in' to Cardano's blockchain and apps
ii)Algorithms a.k.a. online exchanges (and wallets) will be automated to check the 'mechanization' of social process – e.g. KYC/AML for trading and daily transactions.
iii)Advanced ML automation – to drastically reduce downtime, forking and disruptor issues
iv)Roadmap – in a genesis phase (currently incomplete).

On the *daily transactions front*? Competitors may be: Litecoin, Dash or even Ripple. Any of which could become the bridge between existing financial institutions (FIs) and crypto currencies.

[192] Source: "Inside the power struggle between big banks and fintechs to modernize financial services," By Geoff Zochodne [online – Fintech News]. Dated: May 17, 2019. See: https://www.fintechnews.org/canadas-big-banks-are-lagging-its-peers-in-adopting-new-technologies/. Discussion: Zochodne (2019) has reviewed the mandate of The Office of the Superintendent of Financial Institutions (OSFI/Canada), and they are excluded from possessing an ability to act to promote financial services growth. In the UK, the Financial Conduct Authority (FCS) faces no such restriction, and can regulate *and* promote, financial matters, in a far different 'hands-on' manner. Not sure what the role of OCC is in this regard, but we assume it mirrors the Canadian regulatory model, until we are advised to the contrary.

Let's begin with a few overall observations made by Charles Hoskinson (Cardano 2020) in his report.[193] The power to bundle a payment system, identity management program, credit and risk protection, into a single application running a cell phone is not just useful, it is life changing. The reason we are building Cardano, Charles Hoskinson argues, is that we possess a legitimate shot at delivering – or at least advancing –this vision for a decentralized autonomous organization (DAO) customized to interact with collaboratively forming consumer protection and arbitration standards, aiding the use of user-written smart contracts, and advancing modular regulation – all three promulgated together – across financial systems of the developing world.

Currently there is no way to perform cross-chain transactions between crypto currencies and the global finance ecosystem. Crypto exchanges which crash or charge exorbitant fees are the only intermediaries available to attempt these cross-chain transactions. An assortment of regulations pertaining to customer and transaction identities has further distanced the crypto currency ecosystem from its global counterpart. Cardano's solution? Side Chains. Side chains will conduct transactions between two parties off chain. Cardano's Hoskinson is exploring ways for institutions to selectively divulge metadata, related to transactions and identities, to enable use of crypto currencies for trading and daily transactions.

This is our specialty at Advanced Systems Management Group (ASMG), understanding data and metadata. We have done a deep-scan of the distributed ledger, to examine what metadata on blockchain looks like. We have come up with three negative conditions which have caused us to challenge the hypothesis that data – e.g. metadata – somehow is fit for this hypothetical purpose.

If we wish to store data on a block on the distributed ledger, we may approach this as Marx (2018) has suggested,[194] by encoding it into a *receiving address* on blockchain. This is the opposite of using 'some' payload file, inside a block, of the distributed ledger. This first point – encoding [metadata] into a *receiving address* on blockchain – is in response to the fact that blockchain address size is *tiny*, and since we don't own the address we send our metadata [transaction or file event] to, even though we pay a fee to do this, remember that the sent transaction (metadata to the *receiving address*) will get stored at every 'full' node on the planet e.g. everyone downloading a blockchain node has your transmission [metadata].

The economics of the – encoding [metadata] into a *receiving address* on blockchain – is also very astronomical. We may pay a base price, plus an amount per byte, but if we have a smart contract's worth of metadata to store, the execution time is enormous, as is the price! And

[193] Source: "Why We are Building Cardano," By Charles Hoskinson, [online – Cardano]. Dated: 2020. See *also*: *Ibid*., [Foot Note # *180, 195, 196*] '(Cardano-2020) 'decentralized autonomous organizations (DAOs) explained'. See *also*: Ibid., [Foot Note # *415*] '(Keys-2018) Calling out Ethereum acolyte for narrowness in not investigating Cardano (what ails the crypto space, at present).'

[194] Source: "Storing Data on the Blockchain: The Developers Guide," By Lukas Marx [online – malcoded]. Dated: July 5, 2018.

splitting the file up? Won't accomplish much, except extraneous proliferation of our 'personalized' metadata / file set, and the Ethereum *public* blockchain hosting all this cannot (and will not) protect confidential data. If you wish to build yourself a private blockchain, you would have the ability to control the assignment of 'copy' rights to your personalized' metadata / file set. But remember anti-privacy regulations? The GDPR (and similar legislation in California, and coming elsewhere) do not accept the persisting of data, when it is not warranted or required for any pre-defined use. Blockchain has structurally not been designed to delete information, ever. Your last option is to encrypt your data / smart contract metadata, or file set – but now you have just inherited a distribution issue with encryption keys, we will examine in our next negative use case.

The second point, arising from our attempt to store metadata on the blockchain – storing *hash*-only, and not the metadata/data set – raises questions concerning how you will query what you are doing. The Blockchain is no SQL server. This means that to query (to get the data back in our sight / possession) requires the transaction event to be identified as going *in* as the hash/*id* indicates. By definition, a data *hash* is a *generated string* statement, computed using our data as input. The output hash/*id* is identical. This means we can see if our data was re-accessed (by us) had modifications done to it. If using a relational database to monitor this, we could just assign the hash/*id* an assignation of our raw data. If using a relational database for storage, we can now query this information and add another relational database column to store the transaction 'identification/*id*'. The *quid pro quo* here is that your storage mechanism (just created) loses its pivotal qualities: decentralization and transparency.

The third point, arising from our attempt to store metadata on the blockchain – storing sub-sets of our hash/*id* of the metadata/data set (or parts of the data set) – should we specify that we want 'parts (subsets) of the data block only' [stored], can get us back some semblance of decentralization.

This returns us with enough of a perspective on the difficulties we face, with metadata storage on the blockchain, to take up the pursuit of understanding the Cardano Project more thoroughly. Charles Hoskinson begins the White Paper by reviewing what Ethereum has accomplished to data with proof-of-stake (PoS). In Mr. Hoskinson's opinion: "Ethereum has encountered enormous complexity attempting to become a universal world computer. Ethereum suffers from trivial concerns destroying its ability to operate. Enterprise users cannot commit millions of dollars to protocols where roadmaps are ephemeral (*And/or – if those protocols / roadmaps are*) 'Petty or radicalized.' Bitcoin has distanced the need for stable identities, metadata and reputation in commercial transactions. In some most cases the metadata – how much value is moved between accounts, the attribution of who is involved, compliance information, reporting suspicious activity – is more important than the *commercial* transactions themselves.[195]"

[195] Source: "Why We are Building Cardano," By Charles Hoskinson, [online – Cardano]. Dated: 2020. See *also*: *Ibid*., [Foot Note # *180, 191. 193, 196*] '(Cardano-2020) on metadata importance'. See also: Ibid., [Foot Note # *415*]

The Cardano Project continues to berate the manipulation of metadata, which could be as harmful as counterfeiting currency, or rewriting transaction history. Making no accommodation for actors (ASMG concur fully here) who want to voluntarily include these *metadata* fields [in what they do] seems counterproductive to mainstream adoption of blockchain. And, fails to prove or agree with the necessity to guarantee consumer protection.

So far, what Cardano (2020) has done to address 'all-of-the-above' is to create the Cardano Settlement Layer (CSL) and, Cardano has fashioned protocols called the Cardano Computational Layer (CCL). The Cardano organization have now opted to embrace the following seminal points, throughout their workforce:

1) A regular review of their source code contained in Cardano Github
2) Review all Cardano documentation, to be correct, to be useful
3) Verify the claims that the (Cardano) protocols produced by scientists (enterprise architects?) are suggesting, and are implemented fully.[196]

Advanced Systems Management Group (ASMG) can work with this!

Cardano (2020) mention a list of topics ASMG support, once we are fully aware of all their essential features and functions. They include (in no rank ordering of importance): scripting language, and transactions between addresses in the distributed ledger requiring scripting inputs and improvements; the Kiayias, Miller and Zndros (KMZ) *sidechain* advances, adopted as a fundamental foundational layer; a public key signature scheme (details addressed in Hoskinson's 2020 Report); the 'separation of concerns' as it relates to TCP/IP and other matters (details addressed in Hoskinson's 2020 Report). ASMG have much to do to get caught up on the terms, ramifications and technological significance of these issues. Our motivation is at elevated level, to be as fully supportive in any way that we can.

A few topics did appear in the final sections of the "Why we are Building Cardano" Report, which we feel prepared to offer a few *conditional* remarks herein, subject to receiving more information in the near term to address these topics more substantially. They are the following, points which Project Cardano outlines (or sketches briefly) as follows:

-(See: Page 33) a prospective interoperability 'relay system', functioning as a form of atomic cross-chain trading, in a sidechain scheme. Advanced Systems Management Group (ASMG) clearly wish to be consulted on this topic.

'(Keys-2018) Calling out Ethereum acolyte for narrowness in not investigating Cardano (what ails the crypto space, at present).'

[196] Source: "Why We are Building Cardano," By Charles Hoskinson, [online – Cardano]. Dated: 2020. See: *Ibid*., [Foot Note # *191, 193, 195*] '(Cardano-2020) on correct, verifiable, up-to-date protocols and implementations, as peer-reviewed and recommended by experts'. See *also*: Ibid., [Foot Note # *415*] '(Keys-2018) Calling out Ethereum acolyte for narrowness in not investigating Cardano (what ails the crypto space, at present).'

-(On Page 37) *metadata* – not enough detail provided – Cardano are strongly encouraged to consult with Advanced Systems Management Group (ASMG) on this. ASMG are foundational experts on 'all things *metadata*.'

-(On Page 38) Authentication and Compliance with 'sealed glass proofs (SGPs)' – Intel's new instruction set architecture extension,[197] aims to provide strong confidentiality and integrity assurances for applications to 'side-channel attacks'. Cardano take the lead here – we need to learn more.

-(On Page 39) Marketplace decentralized autonomous organizations (DAOs). Cardano take the lead here – we need to learn more.

To state the obvious (once again) – Cardano have opened the *aperture* for a collaborative, truly conformant (and ethical) future for distributed ledger / blockchain technologies (DLTs) to emerge. Digital coin, and all crypto assets, will benefit. Cardano Project economic transactor(s) – and their appointed transacting agents – will be treated democratically, and with total consumer protection and ethical compliance, from across the distributed ledger technology (DLT) ecosphere. This may prove a worthy technology demonstrator project for the OCC – and any incumbent supporting agencies and regulatory *confreres* of the OCC – to examine 'up-close' and with informed discretion.

Advanced Systems Management Group (ASMG) feel particularly committed to pursue the one important initiative which may be coming out of all of this. That is the statement by several Italian researchers, Bartoletti / Pompiano (2017) that "A large part of identified transaction are without attributed protocols with legitimate meta(data)-protocols, but there is no registry of meta(data)-protocols to serve as a reference for identification. An off-chain Distributed Hash Table (DHT) registry of meta(data)-protocols should be set-up, e.g. as these meta(data)-protocols act to embed themselves in transaction on the blockchain.

Secondly, this calls for a corresponding unique indicator/identifier for each of these protocols since Distributed Hash Table (DHT) registrants may also grow in their depth to store smart contract templates, or conditions for the (exchange of) characteristics of entities underlying smart contracts, or software programs implementing *intelligent agents* capable of controlling various types of smart contracts.[198]"

---

[197] Source: "Sealed-Glass Proofs: Using Transparent Enclaves to Prove and Sell Knowledge*" By Florian Tramer *et. al*., Stanford U, Cornell U, EPFL and Cornell Tech – 'Joint Research Project *findings*.' Dated: 2016 See: https://eprint.iacr.org/2016/635. *(NB: Work done while the *first author* was at EPFL). Discussion: Proposed future paths to the transparent enclave model, or through extensions to smart contract and trusted hardware platforms. See *also*: "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, in S&P-16. IEEE, 2016. See *also*: "The Ring of Gyges: Investigating the future of criminal smart contracts," By A. Juels, A. Kosba, and E. Shi, in CCS-16. ACM, 2016.

[198] Source: "An analysis of Bitcoin OP_RETURN metadata," By Massimo Bartoletti and Livio Pompiano, University Cagliari, Italy, Dated: March 4, 2017. See *also*: "The Evolution of Embedded Metadata in Blockchain Transactions," By Tooba Faisal, N. Courtoisand, and A. Serguieva. [online – arxiv.org]. Dated: not provided. See *also*: *Ibid*., [Foot

Advanced Systems Management Group (ASMG) would hope we would be joined by any (and all) interested parties, motivated to at least evaluate Charles Hoskinson's Project Cardano. If, in fact, this is (or is not) a genre-defining effort, we shall see. Hopefully the Cardano Project may lead to a protocol adoption-standardization effort of merit. If so, that is something Advanced Systems Management Group (ASMG) would heartily endorse.

Q6. – Payment technologies a.k.a. 'getting interoperability right'

In answer to Q3 'what digital issues not addressed,' Advanced Systems Management Group (ASMG) provided extensive analysis of web developments in quite specific detail. That effort will now pay off. BigTech platforms enjoy a deep and market-maintaining lead in the strong relationship that they, and Third Party vendor(s), build into their services delivery platforms.[199] What we mean by this 'services delivery platform' is the on-the-rail, i.e. payments rail, used to perform payments transactions.

To address this, let's describe the greater payments ecosphere – who does what? where? how? – then dissect the payments rail thoroughly.

The Bank for International Settlements (BIS) authors (2019 – Frost *et. al*.,) state the obvious. BigTech companies are currently the largest companies in the world by market capitalization. The largest six (6) technology companies *all* surpass the market capitalization – by a significant margin – of all the world's largest, individual, globally systemically important (G-Sib) financial institutions (FIs). The term "BigTech" is defined by BIS (2019) as consisting of large existing companies, 'whose primary activity is in the provision of digital services, rather than mainly in (providing) financial services.'

The penetration by Big Tech into the US payment services realm has proceeded at a rapid pace. The market for US mobile payments, measured by payment volumes – a measure which is a closely watched indication of how digital payments performed more broadly – was $172.36 billion for the second quarter (2019), mostly in line with Factset forecasts of $171.49 billion for the year. The fact it hasn't grown even larger is due to the North American marketplace's widespread use of credit and debit cards,[200] which has put a brake on the development of

Note # *142*]. The second paper '(Faisal *et., al*.) calls for: "DHT database of protocols with secure and selective authorization or audit access." Discussion: A distributed hash table (DHT) is a distributed system that provides a lookup service, somewhat like a hash table: key-value pairs are stored in a DHT, and any participating node can efficiently retrieve the value associated with a given key. The main advantage of a DHT is that nodes can be added or removed with minimum work around re-distributing keys. Keys are unique identifiers which map to unique values, which in turn can be anything from addresses, to documents, to arbitrary data.

[199] Source: "Big Tech and the changing structure of financial intermediation," By Jon Frost, Leonardo Gambacorta, Yi Huang, Hyun Song Shin and Pablo Zbinden, BIS Working Papers No 779, Page 19. Dated: April 2019. See *also*: *Ibid*., [Foot Note # *58, 203, 211*].

[200] Source: "How China leapfrogged ahead of the United States in the FinTech Rate?" By M. Chorzempa, PIIE- China Economic Watch, Dated: 2018. See *Ibid*., [quoted in BIS Working Papers No 779, Frost *et. al*.,] Page 8.

payment services overall, compared with for example China.

So how big is the mobile payments market? eMarketer estimates suggest (US) mobile payment volumes eclipsed $112 billion. Apple Pay[201] has 22 million users that made an in-store payment in the last 6 months, compared with 11.1 million for Google Pay and 9.8 million for Samsung Pay. Mobile payments *niche* company – and current market leader – PayPal[202] announced in the first quarter of 2019 that they had reached a Client base of 40 million users.

In countries where the incumbent bank-based payment infrastructure is dominant, such as the United States, innovations in payment services – like Google Pay, Amazon Pay, Apple Pay, Samsung Pay, and payments on Facebook messenger – all rely on existing payment rails.

The Bank for International Settlements (BIS -2019) suggest Big Tech's movement into the financial services realm often starts with payments, in many cases overlaying such services on top of existing payments infrastructures. Increasingly thereafter, they have expanded beyond payments into the provision of credit, insurance, and savings and investment products, either directly or in cooperation with financial institution partners. This creates a huge challenge for regulators, as BigTech firms are also increasingly important third-party service providers to financial institutions (FIs). Amazon Web Services is the largest provider of cloud services in the world, including to many financial institutions (FIs). Microsoft and Google are also large cloud services providers. All three firms also offer specific tools using artificial intelligence and machine learning to corporate clients, including financial institutions (FIs).[203]

The issues for public policy are multi-faceted when it comes to BigTech. In Advanced Systems Management Group's (ASMG's) opinion, we have no choice but to analyze the backbone of mobile payments, and will start by laying out the architectural taxonomy of the Internet-of-Things (IoT), as an infrastructure architecture criticality, first.

Let's examine payments from an architectural perspective. Nemertes Research (2019)[204] claim that each Internet-of-Things (IoT) project has a specific customization effort. But underlying all IoT projects are:

---

[201] One smartphone maker has noted in discussions that payments services are not meant to be profit- making, but simply to make the core product more attractive for users, and to keep up with similar offerings by competitors.
[202] Source: "PayPal stumbles six (6) per cent after missing on revenue, slashing full-year outlook," By Kate Rooney, CNBC Markets [online]. Discussion: PayPal's revenue came in at $4.31 billion for the first quarter (2019), versus the expected $4.33 billion projected by FactSet.
[203] Source: "BigTech and the changing structure of financial intermediation," By Jon Frost, Leonardo Gambacorta, Yi Huang, Hyun Song Shin and Pablo Zbinden, BIS Working Papers, No. 779, [online]. Page 2. Dated: April 2019. See: *Ibid*., [Foot Note # *58*, *199, 211*] Discussion: (BIS-2019) Frost *et. al*. did not examine the payments *rail* – and other infrastructure service delivery (platform) issues – to anything close to the specificity the OCC, or any other regulators' in North America (or internationally) for that matter, would require. In the financial sector, the derivatives product *space has extensively documented* this topic. This is something which needs to be referred to, by all *other* banking Lines-of-Business, and preferably before the payment stream's *rail* gets implemented.
[204] Source: "Nemertes IoT Research Study 2019" By Johna Till Johnson, CEO / Founder [online]. Dated 2019. See: https://nemertes.com/research/nemertes-iot-research-study-2019/. See *also*: *Ibid*., [Foot Note # *206*, *206*, *218*].

i) application and analytics – AI, ML and visualization e.g. "R (a language and environment for statistical computing and graphics)," IBM SPSS, SAS and dashboards, such as produced by: Amazon, Google, Microsoft, Oracle and IBM products (and their multiple competitors);

ii) integration components – oftentimes 'fit' to ERP solutions/systems, as supplied by Oracle, Fusion Middleware, LinkSmart, Apache Kafka, Dynthings Open Source IoT platform, etc.;

iii) Security – firmware and security services products, etc. provided by Forescout, Symantec and Trend Micro (to name but a few);

iv) infrastructure components – sensors, actuators [physical devices] for communicating, controlling, capturing information. This information capture may be conducted via networks and platforms, e.g. wireless / WiFi / 4G (and *soon* 5G), etc.

This last group – information capture and transport or *infrastructure components* – is further sub-divided into:
a) physical networks – where sensors (and devices, like mobility) reside, which require extensive processing and analysis to survive and thrive, and;
b) "transport" functionality (technology) from IoT location to 'platform, at-the-edge, on-the-cloud or, on more than one depository (cloud?) requiring actuators,[205] etc.

The above Nemertes Reseach (2019)[206] architectural taxonomy itemizes *all* elements contributing to the make-up of the Internet of Things (IoT) platform. The IoT platform conforms to the ISO 20022 standard specifying the electronic means by which banks, and financial institutions (FIs), and their financial intermediaries, are instructed to adopt (the electronic means) to exchange relevant (payments-related) messages – on top of payments – and (thereby) enable this new *messaging* services layer to co-exist on top of the real-time payments system, or real-time payments *rail*.

Real-time payments – and payment systems in general – rely on back-end applications to create a sense of the 'Plenty-of-data-phenomena" condition which positively affects mobility systems and mobility data-generating channels, and sensors which, feed mobility devices with the prerequisite data they need to function overall. The Internet-of-Things (IoT) platform capability provides the 'gating' for the future growth of so much of the Information Technology / Information Management's (IT/IM's) sectoral AI footprint, as to be virtually impossible to separate out in any meaningful way. The German research company IoT Analytics found more than four-hundred and fifty (450) companies offered Internet-of-Things (IoT) platforms world-wide in July 2017. These companies have focused on addressing: i) how to create and manage

[205] An actuator is the mechanism by which a control system acts upon an environment. The control system can be simple (a fixed mechanical or electronic system), software-based (e.g. a printer driver, robot control system), a human, or any other input.
[206] Source: "Nemertes IoT Research Study 2019" By Johna Till Johnson, CEO / Founder [online]. Dated 2019. See *also*: *Ibid*., [Foot Note # *204, 218*].

Internet-of-Things (IoT) platforms and apps ii) how to operate and run Internet-of-Things (IoT) platform analytics, and; iii) securing your data via Internet-of-Things (IoT) platforms and service delivery activities. As well, Internet-of-Things: iv) (IoT) platforms *a.k.a*. dashboard data eneration (or visualization) [207] capabilities are also indelibly swallowed up in the mix as well!

Advanced Systems Management Group (ASMG) highlight this whole pea-soup of Internet-of-Things (IoT) platform offerings due to the fact they have created their own *self-important* role to shepherd data – whether we want them to or not – a role they are inept to supervise properly. This leaves the entire Nemertes Research (2019) IoT classification / characterization of stakeholders operating in the Internet-of-Things (IoT) space as being entirely suspect, critically wanting. The whole role of distinguishing and identifying the stakeholders / players in the IoT space – conducted by the Nemertes Research (2019) IoT classification effort – sits a little off.

In their portrait of *integration components,* Johnson (Nemertes Research-2019) casually refers to one IoT platform – Dynthings Open Source Internet-of-Things (IoT) platform – with that most bland adjective *open*. Vogel (2020) has conducted an extensive examination on the topic 'what is an open Internet-of-Things (IoT) platform' and comes to the striking conclusion that "to the best of our knowledge, no comprehensive study, or research finding, related to *open* IoT platforms exists today, nor does an objective certifiably accurate description of what makes an IoT platform – in fact – '*open*' has been conclusively proven.[208]"

Vogel (2020) develops a keen awareness and analysis of IoT platform stakeholders and platform developers which is revelatory. Some of the most prominent *key* stakeholders within the IoT ecosphere[209] are categorized (by Vogel *et.al*.) as follows:

1) platform providers – provide integration design/development and analytics etc.
2) application providers – provide more domain-specific solutions / applications
3) device providers – offer embedded devices/ sensors / smart devices (appliances)
4) system integrators – support end-to-end integration, as well as testing
5) operators – provide networking and connectivity

Let's examine each of these stakeholders – and the degree to which the term '*open*' applies to them – as per Vogel (*et.al.'*s) definitional boundary-setting. *Open* is not just a marketing

[207] Dashboards provide two main process advances: 1) instant visualization of IT key performance indicators (KPIs) – for example, providing a snapshot of 'total sales revenue received versus total sales invoiced', etc., and. 2) web app depiction of application analytic 'data', 'trends' and 'summaries – the first screen shot which appears when a dashboard app is loaded for viewing. A dashboard is a tool, nothing more.
[208] Source: "What is an Open IoT Platform?" By Bahtijar Vogel, *et. al*., Future Internet - 12,73; doi:io 10.3390 /fi20400743. Dated: 2020. See: www.mdpi.com/journal/futureinternet. See: *Ibid*., [Foot Note # *209, 219*] '(Vogel-2018) *quoting* S. Kans' study of Stakeholders influencing the Internet-of-Things (IoT) ecosytstem developments.'
[209] Source: "Analysis of Stakeholders Within IoT Ecosystem," By S. Kans, et. al., Published in Digital India, Springer: Berlin/Heidelberg Germany, Dated 2018, Page 251-276. See *also*: *Ibid*., [Foot Note # *208, 219*] '(*quoted* in Vogel *et. al*., 2020).'

characteristic or marketing 'hype' terminology point, to be bandied around with impunity – as Vogel (2020) has demonstrated conclusively. Here are Vogel's results: Here is how to determine if a service / or vendor's offering (or their operations) are, indeed, open.

1) *Platform providers* – the most famous being those companies that create and maintain the Android Mobile app – started with good intentions. They adopted open-source Linux tools and toolkits widely. Android does not, today, offer source code level implementation to their smart phone's application programming (product) interfaces (APIs). They rely on the DevOps community to figure things out. ThingSpeak, a big developer supporting Android, went commercial in 2015, and its source code has not been updated, and the newest code is not open.

2) *Application providers* – are happy with *just* open APIs. Sorry! That comment doesn't mean much. Application providers focus their efforts on: i) core (app) developments, ii) other Third-Party developers' products and implementations, and iii) data aggregators. Not a group to rely on for their professional opinion, concerning what the term *open* signifies.

3) *Device providers* – are, in the main, concerned with the open layer, and do not concern themselves with the openness of open source (code) or open APIs.

4) *System integrators* – deal with many moving parts. Openness to them differs with the nature of their 'current' task. If they focus on compatibility primarily, the openness of the standard is foremost in their minds. They tend to define open source (code), open APIs or open layers to self-serving (and usually not-to-be-quoted and attributed) ends. Troubling, as they do wish to control source code directly, and in a proprietary fashion.

5) *Operators* – are not directly affected by this discussion, as they view openness as non-essential.

Why should this be brought to the attention of the OCC? Advanced Systems Management Group (ASMG) have a very straight forward interpretation: He / She who controls the *code,* controls the power to leverage – and unduly influence – the system. The system – in its entirety – consists of a full suite of features and functions, including foundational elements of: design, configuration, implementation and, maintenance. In an ideal world, all the stakeholders laboring in this space would be examined judiciously, and closely. Instead, ASMG has elected to

focus on two stakeholder groups,[210] and one pivotal payments transformational effort, currently getting off-the-ground.

That transformational – i.e. pivotal – payments effort is the real-time payments (RTP) *rail*, currently under construction / implementation, which we will analyze next. The two stakeholders we have chosen to analyze, a little later, represent a wide and all-encompassing sweep through a great deal of today's modern Infrastructure Technology / Infrastructure Management (IT/IM) Internet-of-Things (IoT) and mobility device services *platformication* effort, currently being launched. This is a very diffuse technological landscape to assess, but it must be pinned down conclusively, if regulatory agencies ever expect to master this domain! Advanced Systems Management Group (ASMG) believes this analysis will vindicate itself – as few other efforts have (so far) – surpassing what others have attempted to accomplish.

In short? Advanced Systems Management Group (ASMG) believes we can accomplish one sacrosanct task with this effort. We can illustrate the over-whelming importance – i.e. enabling all whom read this Report – to understand the 'how' and the 'where' (i.e. location) in which *software* and *services* intersect, and together combine their efforts to deliver the *network* delivery *installation* which makes all the dots line up, in the mobility / Internet-of-things (IoT) services delivery landscape. This is a big jig-saw puzzle, to be sure. But so be it! First, let's complete an analysis of the payments *rail*.

Historically, countries where the incumbent bank-based payment infrastructure is dominant, such as in the US and Canada, innovations in payment services like Google Pay, Amazon Pay, Apple Pay, Samsung Pay, and payments on Facebook messenger – plus market-leader in the

[210] Stakeholder groups might not be the right terminology we are looking for. ASMG believe technology development issues frame the approach which Companies adopt. These Companies are steadfast in their pursuit of solving difficult problems. The two Stakeholder (corporate) examples we have identified, are not the architects (nor the *inventors* nor *innovators*) of the solutions they advance. They will do – as stand-ins – to help us explain the rapid pace of technological change that is afoot. The two corporations, nevertheless, are implementers – via the comprehensiveness of their platform installations – of remarkable technological pieces of the puzzle. Advanced Systems Management Group (ASMG) are profiling the Kafka platform (more-or-less emphasizing one Company's views, a Company named Confluent). Secondly, we will review the secure access service edge (SASE) technology development issue, and end with a short synopsis of one vendor's solution, offered by Cato Networks. These are technologies which are approaching 'state-of-the-art' status, in their combined handling of data management challenges, overall. The first *stakeholder* example (see]: i) [Foot Note # *220, 233*] '(Confluent-Kafka contributor Robin Moffat) *a.k.a.* 'The changing face of ETL' and; [Foot Note # *226, 233*] 'No More Silos.' Other Confluent corporate contributors appear at: ii) [Foot Note # *210, 230*] 'Confluent (proprietary) take on using: Kafka, KafkaSQL and Kafka Stream. Next are a few Independent contributors – with their seminal take on all of this – weighing-in on Kafka (or Kafka-like) solutions: iii) [Foot Note # *225, 231, 237*]. NB: Keeping score here can be a bit of a challenge, but it is worth the effort. For the next 'i.e. second *stakeholder* example *a.k.a.* secure access service edge (SASE) advances' see: iv) [Foot Note # *240 – 243, and* on peer –to-peer (P2P) networking, software-defined networking (SDN) and SDN controllers - # 244 – 247]. Mastery of this material is not essential, but grasp the general landscape, the ride is worth it. We end with the second *stakeholder* example *a.k.a.* secure access service edge (SASE) provider Cato Networks [Foot Note # *248*] '(Cato Networks-SASE) optimal architecture to secure and connect the new enterprise perimeters.'

FinTech *payments* space PayPal – all rely on existing payment rails.[211] Advanced Systems Management Group (ASMG) feel there is an explicit obligation by the OCC to unpack this payment *rail*, which may rank up there as one of the more detailed analysis presented in this Submission so far.

A payment rail is a payment *platform* component, or backbone, or may even be termed a payment *network*. A payment network moves money from a *payer* to a *payee*. Either transacting party could be a consumer or a business, and both parties are able to move funds on the payment network.

PayPal – and Venmo and Zelle and WePay – are electronic centralized payment systems conforming to ISO 20022 electronic payments (standards) requirements. They have, classically, transacted across the US and internationally, by adopting a centralized payments platform as their defining architectural principles and existent methodology. The Automated Clearing House (ACH) is the centralized *status quo* payment rail which clears payments – both credits and debits – in batches with financial institutions (FIs), FinTech parties, and payments enablers or intermediaries, and only finally settles after payments clear.

The new payments entrant is the US is The Clearing House (TCH). Or, as we are about to realize, a newly emergent virtual payments rail – which is progressively challenging the payments systems operational *status quo* conditions – in somewhat spectacular fashion. This new entrant payments *rail,* currently under construction, emphasizes real-time payments as the new era's lifesaver, for convenience and cost-effectiveness.

The Clearing House (TCH) new payments entity [called *naturally* RTP, for real-time payments] is operated on behalf of a banking association, and twenty-five (25) banking (RTP)-part owners, with a network that reaches to the Federal Reserve. Real-time payments (RTP) only works for credits (not debits), and is geared very specifically to advancing the role of demand deposit accounts (DDAs). Fifty (50) per cent of DDAs in the US today have a hand-shake established with the real-time payments (RTP) network / platform, or payments *rail*.

In Canada, the leading way to make bill payments, and other transactions, is through the bank's debit card linked to the Interac front-end, a client-facing application the Big Five banks (and a few other banks in Canada) established co-operatively to simplify payments in Canada and abroad. By the end of 2019,[212] there will be a real-time *rail* connected to the Bank of Canada. Guidance will be available for how service providers can use the application programming (product) interfaces (APIs) involved in the data layer of the system. Payments Canada acts as the non-profit, industry association to lead the creation of this back-end real-time payments

[211] Source: "Big Tech and the Changing Structure of Financial Intermediation," By Jon Frost, Leonardo Gambacorta, Yi Huang, Hyun Song Shin and Pablo Zbinden, [quoted: BIS Working Papers No 779], Page 3, 4, 8. Dated: April 2019. See: https://www.bis.org/publ/work779.pdf. See *also*: *Ibid*., [Foot Note # *58*, *199*, *203*].
[212] Source: "Canada's payments modernization effort chugs towards 'real-time' *rail* by end of 2019," By Brian Jackson [online] IT World Canada. Dated: September 18, 2018.

rail.

One thing being experienced in Canada is that banks need to get their data lake ready to receive and present data to other players on the real-time (payments) *rail*. Plus, fraud monitoring must be looked at as payment volumes scale up. Payments Canada's answer is to explore a "cover-all" defaulter pay model to back-up the system.

Just as in the US, innovators are pressing on with their efforts in the real-time payments *space*. Starting with a prolific Canadian example first, an example of these innovative-flush start-ups is the Toronto / Montreal / London (UK)-based "Payment Rails SDK" Company. Payment Rails is undeterred by the head-start by big players (banks, FIs, intermediaries and Big Tech) whom are attempting to cannibalize, through their early lead, ownership or proprietorship on the real payments *rail*. Even with their initiative afoot, enjoying direct linkage to central bank's in both countries – to the Federal Reserve (The Clearing House) and the Bank of Canada (Payments Canada) – encouraging the growth of these innovative start-ups is a huge public good.

Payment Rails SDK has published all – and we mean *all* – coding screen shots, exceptions management glossaries, etc., demonstrating how a real-time payments rail system operates.[213] Payment Rails – in start-up mode but innovating significantly – offers a cloud-based platform to businesses to pay any customer, or person, globally. They call it a "mass payout API" –based system. Finextra reports Payment Rails, which just started its beta testing, is focused on online markets, on-demand and sharing economic platforms, ad networks, affiliated platform players, app stores and businesses with international payment needs, putting it in an *alternative* payments industry niche that includes (competitors) Activehouse, Tipalti and WePay. Payment Rails charges a transaction fee up to $1.00 for transfers in the US or Canada, and $4.00 for transfers to 63 countries globally – a significant discount from the normal bank fees for wire transfers which can approach $45.00 for a similar transaction service.

In both the US and Canada, a strictly "credit push" payment system using the US's The Clearing House (TCH) real-time payments (RTP) payment system, or north of the border the Payments Canada real-time payments (RTP), both will have one non-productive (non-economic conducive) effect on the traditional banking industry. Since these two real-time payments (RTPs) focus on 'credit' payments, and credit payments have been a cash cow for financial institutions (FIs) and their intermediaries, a shift is afoot which is significant. Being a strictly "credit push" payment systems, both the US real-time payments/RTP (and Canadian real-time payments/RTP) payment systems will erode banking industry 'credit' payment performance, which is what has caused these banking entities in the US and Canada to start searching for cost-savings, via real-time payments (RTP) advances in the first-place, to offset lost payment stream fees / payment stream revenues.

Movement towards real-time payments (RTP) will require changes to nearly every internal

[213] Source: "New Rails for the API Economy," By Payment Rails staff [online] Payment Source Publication. Dated: January 13, 2017. See: https://api.paymentrails.com/v1/.

banking system. JP Morgan's experience[214] in the US (and internationally) with real-time payments (RTP) roll-out [to date] is insightful: 30 internal banking departments involved; 250 systems modules impacted; 20 client tests / 700 test uses / 600,000 files tested; client communications to thousands, (*etc*., etc.). Since funds paid are irrevocable, fraud loss may be incurred at the expense of the *sending* financial institution (FI). Therefore, *senders* [FIs / banks] need to have a very good authentication toolset ready, and excellent authorization capabilities.[215]

The ability to generate income from real-time payments (RTPs) is not well-defined. Real-time payments (RTP) is a gateway service. Profitability for real-time payments (RTP) will be based on core processors, Financial Institutions (FIs) uptake, and lateral movement into adjoining payments market *space*. Companies building integration tools for banks to make the RTP connection are: ACI, FIS, Fiserve and JackHenry.

Inventions may run the gamut from fraud investigation solutions to customer-facing applications, that: sell / resell / or sell directly. Consumer markets? Person-to-Person (P2P) credit activities are loss-leading for banks, in general. Real-time payments (RTP) may take away lucrative wire transfer business (from the bank's coffers). Wire transfers can perform credit and debit functions, real-time payments (RTP) only credit payments. But this won't be enough. The avalanche in the expected adoption rates of real-time payments, which has occurred in every other market globally in which it has been introduced, cannot be taken lightly.

Summing developments up, in the past, if the bank owns the consumer's core checking account relationship, they get control of the process, data and settlement activities and actions which transpire.[216] However, in the new real-time payments (RTP) *rail* ecosystem, let's turn to the opinion of a payments industry insider. Mike Venaccio, UFS (integration company architect) suggests "In the context of change in the payments market, we see the value of deposit balances being superseded by the value of the data. Prioritizing data collection, ensuring customer confidentiality – both are the key drivers for real-time payments (RTP) success.[217]"

This brings us to exactly where we want to be: a discussion of payments systems (e.g. payments technology infrastructure) architectural wiring itself, as it affects – i.e. serves – data payments tasks. Nemertes Research earlier provided a taxonomy itemizing elements contributing to the make-up of the Internet of Things (IoT) platform.[218] We next whittled this down to prominent

[214] Source: "Report reveals that slow payment transformation risks shrinking margins further," authored by Icon Solutions [online]. Dated: September 17, 2019. See: iconsolutions.com.
[215] Source: "Justifying Real-Time Payments in the US," By Sarah Grotta, Mercator Advisory Group [online]. Dated: May 2017. See: mercatoradvisory.com. See *also*: *Ibid*., [Foot Note # *217*].
[216] Source: "The Age of Real Time Payments is Here: Is Your Bank Ready?" By Tim Mills, The Clearing House, and Eric Skrum, Wisconsin Banking Association, [online]. Dated: January 3, 2020. See: wisbank.com.
[217] Source: "Justifying Real-Time Payments in the US," By Sarah Grotta, Mercator Advisory Group [online]. Dated: May 2017. See *also*: *Ibid*., [Foot Note # *215*]. '(Grota-2017) Mercator Advisory position on real-time payments'.
[218] Source: "Nemertes IoT Research Study 2019" By Johna Till Johnson, CEO / Founder [online]. Dated 2019. See *also*: *Ibid.,* [Foot Note *# 204, 206*].

key stakeholders within the Internet of Things (IoT) ecosphere.[219] So here's the payoff. Our in-depth exploration of the *new* real-time payments (RTP) *rail* will address two firms, the Apache Kafka *integration components* entity, and; the *infrastructure components* entity, Cato Networks. (NB: Cato Networks also has the plumb job of serving as a network *infrastructure* and connectivity components *operating* entity/organization, at the same time).

Before we can approach both the *integration components* entity example (Apache Kafka), and; the Cato Networks *infrastructure components* example (which fortuitously also includes Cato Networks' network *operator* delivery 'dual capacity' roles, twinned together) we have some background to cover first.

The back-end stack of an enterprise has a very big impact on how an organization functions. At one time, this back-end infrastructure stack consisted of: the hardware, the servers, the data storage drives, the routers, and all the networking ancillary support equipment, etc., *a.k.a.* the organizations 'Big Iron'. As Big Data began its assault on enterprise resources, more than just hardware resources were called for. Built-for-purpose databases, and data engines – *a.k.a.* data processing infrastructures and their applications and resources – were called upon to handle the prospectively 'ruinous onslaught' of data velocity and data volume, unleashed on the organization by Big Data.

At the front-end (*top*) of the organization, more Users have been expressing their need for more data, in accessible forms and formats. At the back-end (*bottom*) of the enterprise's infrastructure stack, the more data which the network was committing to send (and/or receive), as the respective case demanded, the greater the need for advanced data processing power. That is a very simplistic overview, but generically accurate, nonetheless.

Let's introduce a middle layer, to decouple the movement of real-time data between the top and the bottom – e.g. the top or *front-end stack,* and the bottom or *back-end* stack – and, essentially, here we insert Apache Kafka.
Before proceeding, there is one more point important point to make. On the architectural side of things, "Data is not only generated by systems, but when combined with other data (and insights), can usefully *power* systems.[220]" Extract-Transfer-Load (ETL) was the architecture era's last customizable transport services toolkit, but now it needs re-engineering. Extract-Transfer-Load's (ETL's) change, for the modern automated data insights-driven enterprise architectural context, must: **i**) notify us as soon as event 'x-y-z' happens; **ii**) display polling aggregates

[219] Source: "Analysis of Stakeholders Within IoT Ecosystem," By S. Kans, et. al., Published in Digital India, Springer: Berlin/Heidelberg Germany, Dated: 2018. *See: Ibid.,* [Foot Note *# 208, 209*].
[220] Source: "The Changing Face of ETL," By Robin Moffat, Confluent [online]. Dated: September 17, 2018. See: https://www.confluent.io/blog/changing-face-etl/. See *also*: Ibid., [Foot Note # *226, 233*] '(Moffat-2018) lists Confluent –Kafka *architecture elements* and Confluent-Kafka *benefits.*' See *also*: "No More Silos: How to Integrate Your Databases with Apache Kafka and CDC," By Robin Moffatt [online – Confluent]. Dated: March 16, 2018 *a.k.a.* [Foot Note # *210*, *226*]. See *also*: "The Changing Face of ETL," By Robin Moffat, Confluent [online]. Dated: September 17, 2018 - *a.k.a.* [Foot Note # *220*, *233*]. NB: Two more Confluent contributors are *featured* at [Foot Note # *210*, *230*].

(scores) on dashboards, and; **iii**) take charge (i.e. after delivery and transport) of output data from ML algorithm modeling, and more astute deep learning algorithms, review that data (or ask us to do so), and make 'data as a resource' more *insightful*.

Continuing with this *forward look*: if we add new data sources to our (reviewable) data stores or data repositories, which we have painstakingly assembled – I.e. from mobile app information, public app data, etc., – what happens at the *target* system data processing level *itself*? If data is created by an app, and we want it to be available to other apps, e.g. we want it *cleansed*, or we want it to have *business logic* added to it, or both, what do we do? Plus, we know we will want to relay that data resource, with these data cleansing and business logic transformations applied to the data, then move the whole thing to another data app, or data repository, or [data] resting place, and we do this how?[221] Also, we may wish to extract from merchant transactions information, data we need to send to a data assessor / data validator, whom is being asked to respond to anomalous transaction behaviors, by us?

And maybe, the data assessor - data validator may have to 'write' that data event/response to an Elasticsearch[222] store, for peer review by another expert-level adjudicator, to pass judgement upon?

To accomplish the above, let's introduce a middle layer. This middle layer will decouple the movement of real-time data between the *top* and the *bottom* (the front-end stack and the back-end stack, respectively) and, essentially, here comes the capability requirement we have identified for Apache Kafka.

What Apache Kafka needs to address, to meet Big Data at the draw-bridge – in the organization's data processing context – is to fill the task of moving, handling or directing the management of real-time data, correctly and adequately, at speed and scalability. In other words, applications are now required to "hook" into a data stream, Big Data, and consume (information) in the stream in three ways: i) in-batch processing mode; ii) in-real-time processing mode, and iii) in-near-real-time processing mode. Consuming information is *extracting information* and finding (and removing or befitting from) the value contained in that data. We are describing something which has moved way further than the scenario we began with, involving 1:1 data mapping to data transport activities, handled by Extract-Transfer-Load (ETL) architected solutions. We are now in multi-modal, distributed data processing territory. But that is not all. We need a processing system to order the acceptance of data as 'events' in that data flow (or data streaming) context.

---

[221] This may be a fraud detection service (or fraud detection system), for arguments sake.

[222] Elasticsearch is a distributed, open source search and analytics engine for all types of data, including textual, numerical, geospatial, structured, and unstructured. Elasticsearch is built on Apache Lucene and was first released in 2010, by Elasticsearch N.V. (now known as Elastic). It has a set of simple REST APIs, functions in a distributed nature, with speed, and scalability. Elasticsearch is the central component of the Elastic Stack, a set of open source tools / open source products from Elastic, designed to help users take data from any type of source and in any format and search, analyze, and visualize that data in real time, via data ingestion, data enrichment, or data storage process steps. See *also*: *Ibid*., [Foot Note: # *249*].

But *what if*, since Big Data to the untrained eye still constitutes an unwieldy resource to manage, we are trying to reach millions of users? Then our data stream starts to approximate a fire hose onslaught of incoming (and outgoing) data. How do we make sense of this, and read data sensibly and accurately, in the data queue?

The capability we require has now morphed into an added level of complexity, and is now calling for a solution closer to a 'distributed messaging queuing stack.' This distributed messaging queuing stack – and yes, that is how the Apache Kafka enthusiasts and DevOps people who built it describe it – will now orchestrate and organize Big Data flows, in a data streaming / data processing delivery mode.

The goal we are reaching for has changed considerably, once again. We are clearly no longer performing 1:1 transference of data *events* in data pipelines, but are instead creating (or benefiting from the creation of) a hub with the *data processing platform* at the hub's centre. This data platform, for all intents and purposes, is a data streaming platform. We will decouple the sources and targets to produce 'the data,' and receive or consume 'the data,' the one (consumer) from the other (producer). This will allow greater flexibility to build, and evolve, a data processing capability, integrated with database functional attributes, to allow data queueing and data querying of data resources, as theses data resources move through the enterprise's data pipe.

The gloves are off now. Here is what we have.

Apache Kafka provides a 'cascading of notifications,' decoupling each [data notification] *event* – an *event* being an information or data element resource, in transit to its intended audience for their interpretation and usage of that data resource – in a context delivery sequence, which 'fulfills' a data delivery and data *interpretive* clarification mandate. Secondly, these *events* are themselves facts – i.e. a dataset, for this analysis – which constitutes a *payment*. We store these facts (e.g. payments) in the very infrastructure we have deployed to send/receive them – e.g. the system used – for their *broadcast* deployment. This, Stopford, another Kafka expert (Confluent 2017) claims is a *shareable dataset*. It keeps the *broadcast services* in sync.

The benefit of this (Kafka Streaming) platform, is that our messaging backbone – and stream processing API – 'reshapes, redirects, and reforms' this data stream into its constituent sub-streams, or data 'recasting tables.' We 'rekey' to 'redistribute' i.e. "join streams back [together] again," something which Kafka initiates describe as *parallelism.*
The Kafka Stream API chains a collection of asynchronous services together, then ships them as streaming service data sets – with summarizing (and filtering) event handling 'materializing tables' – via a guarantee of correctness. This may be initiated as an 'event-log' activity: **i**) constituting an HTTP request or; **ii**) running them on a stream processor – in a separate processor – using Kafka SQL* (KSQL).
*Short review here: KSQL is an SQL implementation, enabling Apache Kafka users to process their streaming data using SQL, rather than Java or Python APIs.

As a payment process – e.g. payment transaction *event* – winds its way forwards in the data pipe, each supporting role or *transacting entity* observes their own temporal view (of this *data event*). But how is this all sewn together?

The core application programming (product) interface (AP)I for data – i.e. Apache Kafka – acts to stream data, as a data processing event, managed via a mobile device management infrastructure (i.e. solution).[223] One example of this, and there are many others on the market, is Juniper Networks' Junos Device Manager (JDM).[224] The stream processor which Kafka runs – using Kafka SQL (KSQL) as a payment process tool and toolkit – e.g. payment *event* transaction utility or set of utilities – processes data streams and provides invaluable, real-time analytics tools, toolkits and support.

Let's review a few things. Apache Kafka is the platform used to coordinate multiple producers[225] receiving *events*-styled data processing *inputs*, via real-time sources, and

[223] A mobile device management (MDM) solution is a class of software services that enables IT administrators to monitor, manage and secure employee-owned bring-your-own-device (BYOD) and company-owned mobile devices, across different service providers, original equipment manufacturers (OEM's), and operating systems within an organization. MDM forms a subset of Enterprise Mobility Management (EMM), which includes additional services like app management, managed configurations, email management, and secure content management. Both EMM and MDM form a further subset of Unified Endpoint Management (UEM), which extends MDM and EMM functionalities to all different types of devices working within an organization. People sometimes use the terms UEM, MDM, and EMM interchangeably. Source: https://www.codeproof.com/uem/mobile-device-management.

[224] The Junos Device Manager (JDM) is deployed after you have installed a device into your network. At this point, you need to manage the device (mobility device, for example) within your network. Device management can be divided into five tasks:

- Fault management—Monitor the device; detect and fix faults.
- Configuration management—Configure device attributes.
- Accounting management—Collect statistics for accounting purposes.
- Performance management—Monitor and adjust device performance.
- Security management—Control device access and authenticate users.

Source: https://www.juniper.net/documentation/en_US/junos/topics/concept/understanding-device-mgmt-junos-nm.html. Discussion: This may be getting quite technical, but here goes: 1) The agent (your Junos OS) responds to requests from the network management system (NMS) which are dedicated computers - a router is a good example of an NMS - which your network is able to use to monitor the device. 2) To transform the router into an agent, you place the router into the Simple Network Management Protocol (SNMP) community - an Internet standard protocol for managing all devices on an IP network. 3) You set *snmp* to community public authorization read-only. This command uses one of the common SNMP communities, e.g. the 'public' option. The second part of the command defines how the agent (your Junos OS) will respond to requests from the NMS system. An authorization of *read-only* means that the device will send its information to the NMS, but the NMS will not be able to modify any settings on the device (which it could do if you specified an authorization of *read-write*). Source: https://www.dummies.com/programming/networking/juniper/how-to-manage-junos-devices-with-simple-network-management-protocol/.

[225] Producers are multiple components reading from external sources: some of them are real-time sources delivering data via queues, WebSockets or rest services; others are data locations like sFTP that we read periodically, to fetch information. Consequently, we deploy multiple Kafka producers each delivering data to a different topic, that will contain the raw data produced by the source. Source: "Ingesting Raw Data with Kafka-connect and Spark

consumers[226] that 'ingest' those *events-styled* data processed resources, then these [same] consumers manage *their* handling of the *events-styled* data processed resources, in a manner which advances understanding and knowledge. Some of these data resources are pulled from online resources, or from the enterprise's internal data lake.

With the emergence of artificial intelligence (AI), the time frame to conduct data processing efforts has shrunk dramatically, to an extent where an immediately processed *output* is expected to fulfill heightened end-user expectations. Earlier there were batches of *inputs* that were fed 'in' to the system, that resulted in analyzed – i.e. processed data – sent as *outputs.* End-user recipients / Consumers [have] waited patiently to receive these "analyzed – i.e. processed data – sent as *outputs,*" after a specified delay. Currently, this delay (latency), is caused by waiting for the inputting of data, and this latency period may expand the wait for the data processing events to complete their actions, at the *output* stage.

Data feeds, and the *output* times accompanying the data feed / transactions –processing period, or the data compiling processing time-frame, have *combined* to represent one of the main criteria for "implementing the better way" *a.k.a.* to "do" data streaming! To ensure high performance with data streaming, the (data) latency period must be minimal, to the extent of almost being *real-time* in its processing execution of the data 'processing (or data compilation)' tasks it is challenged to complete. This is 'the *how*,' and 'the *why*,' for data streaming. It also explains, concisely we hope, why it is now needed, and not just needed but implemented, cross more and more operational environments than ever before. It also has spawned a more extensive use of applications across the financial service sector in general.[227]

When we move past this point in our discussion, it all gets very technical, and that cannot be helped. When it was first created, Apache Kafka® had a *client* application programming (product) interface (API) for just Scala and Java. Since then, the Kafka *client* (API) has been

Datasets," By Ronald Angel [online – Medium publication]. Dated: October 15, 2019. See: https://medium.com/swlh/ingesting-raw-data-with-kafka-connect-and-spark-datasets-1c2b7aa9ba3b.

[226] The consumer needs to know – what are your requirements for the streamed data? Are you wanting to simply stream data from the database so that you can use it in a traditional analytics/ETL sense? Or are you building event-driven applications? The former gives you more leeway on how you implement. The latter almost certainly necessitates a log-based CDC approach, because you need not only *every* event (rather than just the state at an arbitrary point in time), and you also need *delete* events. NB: The log-based change data capture (CDC) technique can be the basis to synchronize another system with the same incremental changes, or to store an audit trail of changes. The audit trail [for the log-based CDC] may subsequently be used for other uses - e.g. to update a data warehouse or to run analyses across the changes e.g. to identify patterns of changes. Source: "No More Silos: How to Integrate Your Databases with Apache Kafka and CDC," By Robin Moffatt [online – Confluent]. Dated: March 16, 2018. See: https://www.confluent.io/blog/no-more-silos-how-to-integrate-your-databases-with-apache-kafka-and-cdc/. See *also*: Ibid., [Foot Note # *210, 220, 233*].

[227] Source: "Analyzing Data Streaming using Spark vs Kafka," By Staff at Cuelogic Technologies, [online – Medium publication]. Dated: June 5, 2019. See: https://medium.com/cuelogic-technologies/analyzing-data-streaming-using-spark-vs-kafka-bcfdc33ac828.

developed for many other programming languages,[228] although Java and Scala (and Clojure)[229] are still predominant. If not running on Java Virtual Machine (JVM) code, the Kafka KSQL (KSQL) interface may run standalone, and/or it may be controlled remotely. Kafka KSQL runs in a "Kafka alerted mode," and can process the manipulated streams one message at a time. Both routes, or modes, of *event* message transporting, offer the opportunity to *model* business (payments process) *operations* in an asynchronous, non-blocking – i.e. co-ordination 'free' – manner.

Here is a more sophisticated payment example to consider. Say we have a service which sends emails to an affinity (Platinum or *top drawer* Private Banking) customer, assigned special treatment. First, we order the operations and compare the operations (customer treatment) to a Table of Customers *filter* declarative for 'Private Banking / Platinum Clients.' Next, we *code* i.e. 'construct' the email, to the Platinum Client, using domain specific language (DSL) and/or create this: a customized 'Message' via *off-the-shelf-text* java virtual machine (JVM), using KSQL (targeted to the Platinum Client). Here, with this specialized 'Message' example, we implement the emailer Node.js with KSQL running shotgun.

A few things of note here. The Kafka Streams needs its own local storage: a) for buffering as it keeps historical data 'on hand', and b) it monitors messages by the 'time-interval metric' [such as] 'how late the message was received,' or [another measure] 'how long – the message (that is) – was in the queue'.[230]

That's the basics, on how the tools work. We can put all of this together more comprehensively to validate and process payments, in response to HTTP request(s), mapping the synchronous world of a standard REST interface, to the asynchronous world of *events*, and back again. This may, for example, consist of a systemic fraud check on a payment, run in parallel. This would be

[228] One development was *Apache Storm,* a distributed stream processing computation framework written predominantly in the Clojure programming language. The project was open sourced after being acquired by Twitter. It uses custom created "spouts" and "bolts" to define information sources, and manipulations to allow batch, and distributed processing of streaming data. An *Apache Storm* application is designed as a "topology." The topology acts as a data transformation pipeline. At a superficial level, the general topology structure replicates the steps performed by a MapReduce job, with the main difference being that data is processed in real time as opposed to in individual batches. Additionally, Storm topologies run indefinitely until killed, while a MapReduce job 'directed acrylic graph' (DAG) must eventually end. There are other comparable streaming data engines such as Spark Streaming and Flink.

[229] Scala and Java are essentially class-based languages, they interoperate more easily. Or, perhaps, more seamlessly. A Java class is a class to Scala, and a Scala class is a class to Java. Problems might arise when it comes to Scala's singletons or Java's static members, particularly when there's a framework involved expecting things to work in a certain way. Clojure is a functional Lisp-like language, it is *not* object-oriented. Scala is an object-oriented language, which has functional programming features. All interesting, probably, but slightly beyond the nature of what is required for this section of our Submission.

[230] Kafka Streams performs buffering via "State Stores". This approximates a disk-resilient hash-table, keyed by its message. Source: "Building Microservices Ecosystem with Kafka Streams and KSQL," By Ben Stopford [online – confluent.io]. Dated: November 9, 2017.

handled by a validator aggregator, moving it to a 'validated' or a 'failed designations' repository *place*, and reporting this event appropriately.

Functionally speaking, Kafka Streams must implement *code* to expose the HTTP endpoint, or by taking the action '*view this*' (for example), via an external database. It might deploy Kafka Connect.[231] The architecture here is more complex than 'create, read, update, and delete' (CRUD)[232] systems. The benefit being, that if you do not require a response or 'GO statement' to be sent immediately back to the User – re: for such topics' as 'notifications,' 'payments modifications' and 'payments details,' etc. – this portends being able to scale *atomic* operations across many threads, and/or many organizations, with no remote locking and no remote reads. One single micro (and macro) workflow *may be* accomplished, spanning companies, identities and geographies. In short, single functions which are 'side *effect-free*' can be composed into service ecosystems that operate as one.

There are two camps we have visited with this review of Kafka's *event handling* messaging. The first call services directly via HTTP REST APIs – with / without Remote Procedure Calls (RPCs). The other camp adopts or utilizes the Service-Oriented Architecture (SOA) and Enterprise Service Bus (ESB) approach, that takes charge of the message que. For camp 1, a requirement exists to deploy load balancer, due to the fact event handling messaging operates in a long processing pipeline, and needs normal operations to be assured, i.e. no 'drops (re; losing component parts but maintaining 'at least one' operation occurring continually / normally). Plus, service discover is needed by the HTTP REST APIs call service camp, to know when something needs a call, for communicating something [or *other*].

The second camp, camp 2, is the old-fashioned service-oriented architect (SOA) with Enterprise Service Bus (ESB) approach to centralized messaging, with security slightly simplified. Slightly simplified means access control lists (ACLs) are applied which suggest who can read/write Kafka's *event handling* messaging, as per the access control lists (ACLs) we are provided. You also may grant only connections to the message que, and firewall the rest (of the message/messages).

[231] This stage bridges the synchronous, blocking paradigm of a RESTful interface with the co-sync non-blocking processing performed server side. Kafka Connect (or Connect API) is a framework to import/export data from/to other systems. It was added in the Kafka 0.9.0.0 release, and uses the Producer and Consumer API internally. The Connect framework itself executes so-called "connectors" that implement the actual logic to read/write data from other systems. See: https://www.instaclustr.com/solutions/managed-kafka-connect/?utm_source=bing&utm_medium=cpc&utm_campaign=CA-SN-Kafka%20Connector&utm_term=Kafka%20Connector&utm_content=Kafka%20Connector%2.

[232] In computer programming 'create, read, update, and delete' (CRUD) are the four basic functions of persistent storage. CRUD operations are often used with SQL, as CRUD operations identifies all the major functions that are inherent to *relational databases,* and the applications used to manage them, which include: Oracle Database, Microsoft SQL Server, MySQL, and others. See: https://www.sumologic.com/glossary/crud/.

Here is the important point we are trying to make. Apache Kafka (open sourced by LinkedIn) totally decouples *senders* from *receivers*. Senders need not know who is receiving the message. Kafka is deployed in industrial, or mega-industrial strength environments. In Netflix's case, Kafka serves as a firehouse-style data pipeline, processing over two trillion messages a day!

Using Apache Kafka, messages are written to a log-style stream, called a 'Topic,' and the *senders* writing to the 'Topic' are completely oblivious as to who (or what) will read the messages from there. You may set access control list (ACL) limits, which intruders / consumers "write to" or "read to" according to which 'Topics of the System (they choose),' giving you 'loosely' (loosely – ASMG's *comment* / *editorial statement,* added here for effect) centralized security control over *all* messaging.

In summary, Kafka – at a high level[233] – is architecturally designed like this:

- Web application emits review directly to Kafka
- Kafka Connect streams snapshot of user data from database into Kafka and keeps it directly in sync with change data capture
- Stream processing adds user data to the review event and writes it back to a new Kafka topic
- Stream processing filters the enriched Kafka topic for poor reviews from VIP users and writes to a new Kafka topic
- Event-driven application listens to a Kafka topic and pushes notifications as soon as a VIP user leaves a poor review
- Kafka Connect streams the data to Elasticsearch for an operational dashboard
- Kafka Connect streams the data to S3 for long-term ad hoc analytics and use alongside other datasets.
- Kafka – *the benefits* include:
- Data enrichment occurs once the enriched data is available for any consuming application
- Processing is low latency
- Notifications to the customer ops team happen as soon as the VIP customer leaves a poor review, leading to a much better customer experience and higher chance of retaining their business
- Ability to scale easily by adding new nodes as required for greater throughput.

Building an Extract-Transfer-Load (ETL) pipeline that incorporates stream processing is a useful process, when using Kafka. ETL has needed to change due to the inclusion of real-time data. (Check). All the data that is written needs to be extracted, transformed and loaded

[233] Source: "The Changing Face of ETL," By Robin Moffat, Confluent [online]. Dated: September 17, 2018. See: https://www.confluent.io/blog/changing-face-etl/. See *also*: *Ibid*., [Foot Note # *210*, *220, 226*] "(Moffat-2018) how Kafka generates systemic data (and other) insights, e.g. to usefully *power* systems.'

immediately. (Check). The goal is to avoid creating 1:1 pipelines, and instead create a *hub* with the *platform* at the center (Double check). By adopting an *event streaming* platform, we decouple the sources and targets for data, and thus introduce greater flexibility to build upon, and evolve, an architecture.

What we have just described assists us in reaching an understanding of the modern-day technology anchor for modern payments, serving its transformational role. Internet-of-Things (IoT) platforms fill the gap, to permit IoT devices to connect to other IoT devices, and applications, and to pass information-using *standard* internet protocols.

Before we leave this discussion of Apache Kafka, and Kafka SQL (KSQL), Advanced Systems Management Group (ASMG) have the uncomfortable feeling we have, somehow, though totally inadvertently, left the impression that this is all established orthodoxy. It is not!

Kafka SQL (KSQL), which is written entirely in Java, is a distributed real-time SQL engine, built by the vendor Confluent, to support streaming functions. Kafka SQL (KSQL) allows streaming functions such as windowed aggregations to stream table joins. Why do this? Most relational databases are used for doing on-demand lookups and modifications to data that is stored. Neha Narkhede, CEO (Confluent): "Kafka SQL (KSQL) is meant to do continuous querying e.g. turning a relational database '*inside-out*'. This is done by taking the relational database transactions log, and that transactions log's tables – with their derived views – and update all of this to be modeled-as-streams. Kafka SQL (KSQL) sits on top of the Kafka streaming table. You read data from Kafka Stream – where every update is independent of all others, every update is (probably) an update to a previous update, and so on. At some point in the future you query all of this, these tables, and you now have something that is continuously updated as new events arriving on the stream. As streams come in, queries either produce more events or update the tables. Kafka SQL (KSQL) is designed for data that is changing all the time. To do all of this? The SQL windowed functions common on relational databases need to be heavily modified to support streams."[234]

There is an opposing view. Jesse Anderson, Managing Director of the Big Data Institute, believes Narkhede (Confluent) has taken a completely indefeasible approach to this issue (stated above). Anderson (2019) sees a huge missing piece: checkpointing.

Checkpointing (described in this quote): "Kafka is a distributed log. You can replay any message that was sent by Kafka, either as 'stateless' or 'stateful'. For stateless processing, you just receive a message and then process it. As soon as you get *stateful*, everything changes. Now – in stateful mode – that message needs to be dealt with by storing the state. Storing the state means having to recover from errors while maintaining state. Confluent's Narkhede claims 'We have all of the messages to reconstruct the state'. Really? Confluent even add: 'You can use a *compacted topic* to keep the messages stored in Kafka, to be limited to the -1 per "key"

[234] Source: "Why I Recommend My Clients NOT use KSQL and Kafka Streams," By Jesse Anderson [online]. Dated: October 9, 2019. See: jesse-anderson.com. See *also*: Ibid., [Foot Note # *235, 236*].

limitation/designation. If you have -1 message per "key", and you have 100 billion keys, you will have 100+ billion messages still in the state topic, because all state changes will be put in the state change 'topics.' In short, as the number of keys grows, so does the 'size' of your state."[235]

To put all of this in operational terms? If a node dies, all those messages Anderson (2019) has just described (above) must be replayed "from the topic" and inserted into the database. It's only once all these mutations – re: *duplication of events* – has occurred, that event processing can start again. Think of this in a disaster scenario. Anderson (2019) asks us to consider the following response (to a total kill-off situation having occurred): "All machines running Kafka Streams as a job die, or are killed off. All nodes must "replay" state mutation messages before a single message can be processed. Hours of downtime? (Anderson says most analysts he talked suggested a minimum of four (4) hours downtime would be incurred, in this disaster scenario Mr. Anderson just sketched out). Plus, all the in-coming messages – backed up in the queue and waiting to be read – while this mess gets fixed?" Anderson (2019): This is the requirement, urgent at that, for processing frameworks which implement *checkpointing.* Competitor Flink calls this *snapshotting*, the exact same thing.

A checkpoint/snapshot invokes "writing out to durable storage [S3/HDFS, for example] the entire state up to the point of "disaster" striking. And the disaster taking out all the nodes in the system.

Why? And why – do we even need – checkpoint/snapshot applied? When there is a massive error, the program will start-up, read the previous checkpoint/snapshot (usually in the 1,000s), and start processing again. Overall, Anderson (2019) says the checkpoint/snapshot procedure lasts seconds to minutes. Why this is important: Downtime for systems with checkpoint/snapshot capability should be as short as possible. Distributed systems need to recover from failure almost immediately. Otherwise, why have them in the first place?

Confluent's Cofounder and Chief Technology Officer, Neha Narkhede, has made some somewhat contradictory statements. First, Ms. Narkhede claims data is not just created by humans, it's also created by machines. As a result, data is orders of magnitude larger than ever before. No argument there. But Neha Narkhede continues by stating: "Databases being the place where processing is done," but Jesse Anderson argues (2019), this last comment is a misleading statement! Anderson (2019): "There are small data architectures (and more data warehouses) that use the database for processing. But Big Data architectures? Show me an implementation! (Hint: There are none). Because they don't scale (in the context we have been discussing a.k.a. *checkpointing/snapshotting*).

Anderson (2019) continues by stating: "There are so many technologies in the Big Data ecosystem, because each one solves or addresses a use case. If the organization eliminates a

[235] Source: "Why I Recommend My Clients NOT use KSQL and Kafka Streams," By Jesse Anderson [online]. Dated: October 9, 2019. See: jesse-anderson.com. See *also*: *Ibid*., [Foot Note # *234, 236*] '(Anderson-2019) *calls out* Confluence on the issue of lacking a checkpoint / snapshot solution for windowed SQL functions.'

few 'tech parts,' all this does is drastically slow down, or eliminate, the ability to handle a use case. KSQL – even after its being renamed by Confluent's Narkhede as ksqlDB, and claiming to have had new features added, to address functions needing a fix – Anderson (2019) doubts very much that Confluent's Narkhede has done anything in this 'fix' in any meaningful, or measurably viable way. Kafka SQL will still be of limited utility to organizations. Why? Again, Confluent's ksqlDB is marketed as providing an API that makes streams look like a table — but the confusion still stands: Kafka is *NOT* a database, and APIs don't help business users. Instead, they only deepen the stranglehold Confluent has on their customers, and fail to provide visibility.

Kafka by Confluent – in the Confluent sense of it Kafka deployment implementation's – Anderson (2019) suggests, is pursuing a land-grab. This means 'claim you do more, claim you are a database,' and 'claim your pricing model needs adjusting' (upwards), and finally, 'claim you have more use cases' (which you don't) – and take the land. And on one final note, KSQL wants to take the initiative, and declare its sole expertise addressing 'random access reads' – a.k.a. the *current-status-of-data* metrics. Anderson: They can't! Database optimization for random access reads is a non-trivial problem, and very large companies with large engineering teams, are built around this problem. Bottom-line (from Jesse Anderson's point of view?): This – Kafka ksqlDB – 'should either be (placed) in the broker process,' or 'at the application level,' with a solid and durable storage layer! Proven architectures *get* current-status-of-data / random access reads – e.g. look for a database doing this now – via a processor with *checkpointing/snapshotting* installed. Use Kafka correctly, and not on one installed via one Company's manipulative marketing[236] messaging.

In the first week of December 2018, Apache Kafka supplier Confluent 'upped' its Amazon Cloud supply license fees for its Kafka-based streaming platform. Three other open source commercial software vendors followed suit. Backaitis (2018)[237] had this to say: "Amazon built some proprietary code, stuck it around Kafka (for streaming), and brought it to market as a paid service, which Confluent claim was 'their space'. Open source enterprises are citing major cloud providers – Amazon, Microsoft, Alibaba and Google – as all doing this same thing, only altering their type of offering. By baking code into Kafka (streaming) to make it proprietary (to those wishing to buy it from Amazon), who benefits?"

Jesse Anderson, Managing Director of the Big Data Institute, is quoted directly by Backaitis (2018): "The problem is that open source companies have to continue to develop the original project – be it Kafka or Hadoop. Those are expensive software engineers and their salaries

[236] Every time Confluent releases something, they should have *, +, %, @, after every statement so that you can look-up all caveats they are glossing over. And this is an open solution – open framework? (Last comment from ASMG). Source: "Why I Recommend My Clients NOT use KSQL and Kafka Streams," By Jesse Anderson [online]. Dated: October 9, 2019. See *also*: *Ibid*., [Foot Note # *234, 235*] '(Anderson-2019) calls out Confluence on glossing over facts with new issue identification via manipulative marketing tactics.' See *also*: "Kafka KSQL is Not SQL Here's a better way to achieve Kafka Analytics," By Mark Palmer [online – Medium publication]. Dated May 14, 2019.
[237] Source: "Is Apache Kafka's Confluent Product still open source, and does it matter?" By Virginia Backaitis [online – Medium article]. Dated: December 18, 2018. See: digitizingpolaris.com. Discussion: Virginia Backaitis is narrating the trek to the digital economy from ActBrilliant.com. We'll take all the narration we can get!

don't directly make the Company money. Not just that, all of their work goes into the common pool of code that makes the project benefit from those contributions." Amazon? "{Anderson): When Amazon creates a managed service, they focus on making it easy to start, or deploy the technology. With Kafka, for example, Amazon Web Services (AWS) makes it easy to start and run a Kafka cluster."

Here are a few disturbing facts which will frame the discussion we will take in the remainder of this answer to Q6) 'Payment technologies a.k.a. 'getting interoperability right.'

One third of WiFi networks globally are unsecured. Internet of Things (IoT) endpoints will reach seventy-five (75) Billion in number by the year 2025, which includes: sensors, actuators, cameras, printers, scanner, wearable robots, and other unheard of devices, but which of course – also includes mobility devices – such as tablets, embedded chips and smart phones. As of very recently, very little has been done to address Enterprise Mobility Management (EMM)[238]. This is, quite frankly, worrisome.

The worry being that potentially harmful applications (PHAs) – which may be trojans, ransomware-embedded-in-trojans, adware, clickware, and all manner of denial-of-service attack vectors which proliferate widely today. The first ever attack of the latter variety – *a.k.a*. denial-of-service – occurred in 2016 when Dyn DNS servers were knocked offline. In the aftermath to this incident, the 'Dyn Denial of Service' (DDoS) became the vernacular expression, shortened into the acronym DDoD, to describe this harrowing event. The Dyn DNS servers were taken offline globally, as were many major organizations, their websites and a huge number of customer service entities. Here is a partial list of the Dyn Denial-of-Service (DDoS) attack's victims: The New York Times, Twitter, Pinterest, Reddit, Tumblr, GitHub, Etsy, Spotify, PayPal and Verizon.[239]

Why is this important? Gartner coined the phrase secure access service edge (SASE) in 2018-2019. Secure access service edge (SASE), in brief, suggests we move the security focus from data centers "over" to the identity of the user, or the devices themselves. When users/devices are seeking access at the edge of the network,[240] they become the fulcrum or center-of-attention. The definition of an *entity,* as Gartner (2019) redefines the term, is: 'people, groups of people (branch offices or work-from-home) devices, applications, services, IoT systems or 'things,' *connected* to – or leading from – edge computing locations. Security administrators seek to broker trust, vis-a-vis tracking and logging communications events – in and out of – the

[238] Source: "Do You Know What's in Your Pocket?" By Soti staff writers [online – soti.net]. Dated: 2020.
[239] Source: "DDoS Attack Glossary: Top 12 Attack Vectors," By Robert Hamilton [online – CPO's magazine]. Dated: August 17, 2018. Discussion: See the article for a discussion of twelve (12) different DDoS constellations which strain the defensive resources of security teams today.
[240] Source: "What is SASE and Why Should You Care," By Info Systems Architects, staff [online – isacybersecurity.com] Dated: February 7, 2020. See *also*: *Ibid*., [Foot Note # *9*].

network, including (if possible): i) content filtering ii) prevention / detection of threats and iii) intrusion abatement or remediation.[241]

What Lerner (Gartner-2019) is driving at in this listing of security administrators 'roles' and responsibilities' in brokering trust in the whole data management flow, really focuses on software architecture, that software's security controls, and the over-arching security compliance protocols which keep things running smoothly. These are the really important issues that have emerged from Gartner's advocacy efforts, with this whole secure access service edge (SASE) 'call for vendor participation' paradigm. As a newly emergent vendor offering,[242] here is the basic mission template or goal for what the secure access service edge (SASE) implementation is trying to accomplish: "[SASE is] a collection of network function virtualizations (NFVs) that are service-chained and delivered to the end-user as a managed service. A network function virtualization (NFV) Is defined as planes (i.e. layers), in network terminology, mapped into network architecture. This network architecture creates 'secure' Internet Protocol (IP) tunnels, with a specific application utilizing that tunnel to, for example, drive 'low-latency,' in communications functioning, or drive 'high bandwidth' in communications functioning, or drive '(multiple) points-of-presence' in communications relationships, etc. etc.".

The author of this paradigm description, Stone (Mushroom Networks-2020)[243] suggests: "You want real-time packets (a packet being a communications' data unit, or message content event unit, or stream of data units/packets) to achieve, in their transport layer connotation, a state which fully addresses all attributes defining 'transmissions', 'low-latency,' or 'high bandwidth,' or '(multiple) proof-of-point' *peering*[244] relationships, effectively and elegantly.

Network communications infrastructure has hardware (servers, routers, systems) matched up with software, and applications / services. This network is rapidly expanding, as mobility and mobility device saturation points are reached. The Internet-of-Things' (IoTs') sensors, cameras

[241] Source: "Say Hello to SASE (secure access service edge)," By Andrew Lerner, Gartner [online – gartner.com]. Dated: December 23, 2019. See *also*: *Ibid*., [Foot Note # *9*].
[242] Source: "Secure Access Service Edge and SD-WAN," By Rob Stone, Mushroom Networks/hardware and router solutions [online – Mushroom Networks]. Dated: 2020. See: https://www.mushroomnetworks.com/blog/secure-access-service-edge-and-sd-wan/. See *also*: *Ibid*., [Foot Note # *243*]
[243] Source: "Secure Access Service Edge and SD-WAN," By Rob Stone, Mushroom Networks/hardware and router solutions [online – Mushroom Networks]. Dated: 2020. See *also*: *Ibid*., [Foot Note # *242*] '(Stone-Mushroom Networks-2020) network function virtualization (NFV) explained from a router/hardware device suppliers' perspective'.
[244] Peering is a process by which two internet networks connect and exchange traffic. This allows the two internet networks to hand off traffic between each other's customers, without having to pay a third party to carry that traffic across the network for them. Transit, the more usual way of connecting to the internet, involves an end-user or network, paying another – usually larger – network operator to carry all their traffic for them. Network operators who *peer* can select a path for: low-latency, improved bandwidth, or for {multiple) 'points-of-presence' features - one or all three, or several others - to improve network efficiency and control over who, how and what data passage occurs. For more on this- See: "What is peering?" By LM Jigback, CEO NoNod SE [online – netnod.se]. Dated 2020.

and smart phones, etc., are all mobility devices which engage with, and forward data – e.g. information transmission *packets* – which takes us to the next issue we need to examine: software-defined wide area networks (SD-WANS). Software-defined wide area networks (SD-WANS) feature: i) an SD-WAN – a user activity tracking mechanism ii) Firewall-as-a-Service – i.e. the assembly of integrated capability – e.g. intrusion prevention, web content filtering, application control(s), anti-virus / malware threat protection services, etc., iii) Access Security Broker(s) – which monitor data in the cloud, and iv) Secure Web Gateway – which acts as an enforcer of application controls. The SD-WAN approach specifies 'user identities,' and individual devices are its *focus*. Identity analytics, and user activity tracking, are key.

Then, if we are really motivated to do so, we introduce multiple dashboards, serving a company's own private network of 'eyes' (and ears), or their private network / cloud-serviced network *hybrid* – which may even choose to "segment employee internet access from guest WiFi traffic, or use Internet Protocol (IP)-based computer securing of users (and their packet endpoints) – via virtual routing and forwarding. Virtual routing and forwarding (VRF) is a technology that allows multiple instances of a routing table to co-exist, within the same router, at the same time.

Here, in simplified terms, is what is taking place. Visualize, if you will, the following: "this *attachment* (in a blog, for example), or this malware (in that *attachment* in the same conversation's attachment *blog*) are two *points*." The secure access service edge (SASE) monitors everything, using 'user activity tracking', 'Firewall as a Service,' 'Access Security Broker,' and 'Secure Web Gateway,' *to and from*, one cloud-native software stack to another cloud-native software stack – e.g. data *packets* move back and forth, in transit (paid for) or peering (not paid for) transport arrangements, between different vendor products or service offerings, the latter if a managed service offering is involves, between (multiple) stacks.

Software-defined networks (SDNs) provide programmability to the network from a central point. The nodes or data plane devices – using SDN – only forward packets, and the complexity of the control plane is handed over to the *controller*. It is the controller we should be examining up close. The controller installs the rules and policies. But as controllers suffer from central control 'link' failures', identifications (of devices or identities matched to a sensor, camera or device/smart phone) may need restoration actions. The controller is the *pivot* for all information on the SD-WAN network.

Software defined networks (SDNs) simply move the control logic from network devices to the central controller itself, separating the control plane from the data plane. Data flows through what is termed southbound applications / programming interfaces (SB-APIs). Link failures to a 'device' in communications mode, should failures happen, are quite routine, for example video conferencing or Voice-over-Internet-Protocol (VOIP).

In the past, vendors have been resistant (or been hesitant) to provide source code for their DevOps products and applications. They have not wished to have their developers' work

altered. Also, since traditional network architectures reign supreme, where tight coupling of control and data planes is the norm (rather than the exception), sluggish networks have been experienced, as the path to find 'alternative nodes' is complex – and hard to unravel – in the cases in which a transmission experiences a link, or node failure, in the network. Also, in traditional networks – for example with an improper utilization of bandwidth – every node may flood the network with packets, to find an alternative path to read and connect to.

Since software defined networks (SDNs) shift the data plane to the centralized controller, nodes (in theory) may have load balancing applied. Spinning Tree Protocol (STP) and reverse-STP have a "seconds" time interval, to be activated, to detect discontinuities in communications *connections.* Therefore, modern-day controllers may prove their inefficiencies. Instead, multi-protocol label switching (MPLS) have been devised. Multi-protocol label switching (MPLS) favours 'flow rules,' installed at the 'link,' via tagging and monitoring. Packet tagging and monitoring features are applied to data packets, and summarily counted at reception i.e. when they arrive at their destination, or endpoint (transport) *target*. If failure detection identifies a switch-level problem, an algorithm in the software defined network (SDN) finds the source and destination of the failed link. It isolates all hosts connected – via a mapping function – finding the switch responsible for the failed communication(s). The SDN controller will then have to install the flow entries, or the alternative path route markers, to correct the discontinuity in communications.

The controllers are indispensable. A single domain controller is only responsible for one autonomous system (AS) in its administration. However, the management of different heterogeneous domains is tedious. The lack of a common northbound interface [route] may be the culprit. Similarly, the network update process may be insecure, due to communications between different control planes.[245] That's the overview. Now what about Software Defined Network (SDN) controllers?

Controllers update policies according to *condition* changes in the network. Since Software Defined Networks (SDNs) rely on algorithms to reconfigure or 'forward' traffic on the network, through programmable interfaces, the rate-limiting factor is the availability of alternative paths. The flow rules, updated on the switches, determine the forwarding actions, conducted on the traffic, and apply these actions before the traffic reaches its final point of destination (e.g. its 'endpoint' transport *target*). Ali (2020)[246] suggests that link failure recovery is dependent on the time taken to perform data packet transport endpoint target failures, via failure detection proceedings.

Since Software Defined Networks (SDNs) relies on – latency, scalability, routing updates, Ternary control addressable memory (TCAM) space, flow operations matching, configurations,

[245] Source: "Safe routing reconfiguration approaches with defined networks," By S. Vissicchio *et. al*., published by IEEE - INFOCOM, Toronto, Canada; April 27-May 2, 2014, Page 199-207.
[246] Source: "Software-Defined Networking Approaches for Link Failure Recovery: A Survey," By Jeha Ali et. al., published by Sustainability – Issue # 12 [online]. Dated: May 22, 2020. See: res.mdpi.com.

robustness to back-up path failures, routing information access, processing of switches and the overheads associated with comingled routing, controller and switch integration – and involves, many things. There are a lot of places where inter-domain and intra-domain systems and components architectures may be susceptible to performance vulnerabilities, hijacking of controller features, forged traffic flows, etc. etc.

Cyberthreats may exploit vulnerabilities of Software Defined Network (SDNs) controllers in two ways. First, subject *bugs* may control the network through the Software Defined Network (SDN) software. Secondly, the *centralization* of 'network intelligence' in controller's may be hijacked, leading to accessibility to the servers being compromised, and since these servers host the control software – managing (i.e. mismanaging?) the entire network[247] – mismanagement occurring at this interstice is very deadly, and could seize up the entire network. This has led to Imran (2017) identifying six (6) security threats: i) faked or forged traffic flows ii) attacks on vulnerabilities on switches iii) attacks on control plane communications iv) attacks on controller vulnerabilities v) lack of mechanisms for ensuring security between the management applications and controllers, and vi) attacks on vulnerabilities in administration (central) stations.

Looking at each one: **i**) faked or forged traffic flows – Denial-of-Service (DoS) attacks can be quite difficult to control when controller resources / switches are circumvented, once an attacker gets to the application server, they have access to all holdings (details of users) right where these information stores are lodged. **Ii**) attacks on vulnerabilities on switches – by using a single switch the attacker slows-down the network with 'dropped packets'. Alternatively, attackers inject forged requests / traffic to cause overload conditions. This, essentially, defeats the software's trust management capabilities and routines. **Iii**) attacks on control plane communications iv) attacks on controller vulnerabilities – attackers can take 'leaked' data via a black hole, e.g. attacker uses oligarchic trust models with multiple trust-anchor certification authorities, one per submission assignment to a (specified) controller *instance*. The other method reported involved threshold cryptography applied across controllers to secure (corrupt) the communications. **Iv**) attacks on controller vulnerabilities – possibly the most severe type of attack: involves the application of the common intrusion detection system being "weakened / compromised" *a.k.a.* an exact event-combination is attacked triggering a behavior which renders classified (sensitive) information 'accessible/revealed'.

Since Software Defined Network (SDN) controllers trade on *abstractions*, malicious applications can provide translation commands (to those abstraction comments/data frameworks) which then issue command configurations to the fundamental structure of *everything* the controller is doing. The controller can only fight back through: a) replication (detection, removal or unmasking unusual behavior) b) bring in a diverse programming language (with corrections) c) refresh / recover the system (to active state). **v**) lack of mechanisms for ensuring security between the management applications and controllers – management application and

[247] Source: "SDN Controllers," By Ayesha Imran, University of Jyvaskyla, Department of Mathematical Information technology [thesis-online], Page 33. Dated: November 9, 2017.

controller –defined attacks '*is*/*are*' susceptible to attacks directed at disrupting the 'trust' relationship between components. The autonomic trust management process may verify management applications – to – controller's 'trust' bonding protection mechanisms. **Vi**) attacks on vulnerabilities in administration (central) stations – these administration (central) stations need to install double credentialing / double verification procedures, after attacks are detected.

Software Defined Network (SDN) controllers' many vulnerabilities *underscore* the existence of a significantly widened – e.g. augmented – Software Defined Wide-Area Network (SD-WAN) attack surface, compared with traditional network surfaces. Advanced Systems Management Group (ASMG) have elected to analyze one vendor offering, to carry this point home. This was a happenstance selection process. A recent trade sheet just landed in our in-box, announcing Cato Network's Secure Access Service Edge (SASE)[248] solution.

Cato Network's Secure Access Service Edge (SASE) solution proclaims itself to be *the solution* to address the corporate datacenter's requirements, "hosting" all sensitive data and applications. The operative word being to 'host" and not exchange – or safely (and securely) offer data interoperability – across all data-domains. Cato Network's Secure Access Service Edge (SASE) will, it is suggested, be the way to handle all sensitive data and applications at the perimeter, the enterprise's perimeter. The Cato Network's Secure Access Service Edge (SASE) solution will draw on the mantel of networking and security systems, and secure the web gateway.

Cato Network's continue by stating: "The combination of cloud applications and the expanding mobile workforce creates new traffic patterns that completely expose the traditional datacenter perimeter." Gartner / Cato Networks refer to SASE as the solution. SASE will address: SD-WAN, Global Private Backbones (basically, ERP systems with *eyes*), Service Web Gateways (e.g. AWS Direct Connect and/or Azure Route are mentioned), and Firewall-as-a-Service (virtual firewalls weaved into a *web*) and more.

This will accomplish the identity-driven solution for the cloud, supporting all *edges* and [to be] distributed globally. Cato network's predicates this on the newly minted concept called the "Point-of-Presence (PoP)". The Point-of-Presence (P-o-P) takes information at the edges, and connects this information to the nearest P-o-P, so all traffic is secured (and optimized) at the (global) P-o-P backbone, before that information travels to its destinations. They compare this to traditional appliance-based security, which optimizes security to a single traffic path. Instead, all traffic paths are routed through the P-o-P. The "Point-of-Presence (PoP)" gives you the capability to *look* at data *en-route*, but does nothing, Advanced Systems Management Group (ASMG) would argue, to map out the complete data life-cycle, including categorizing data's provenance, e.g. where it (data/information) sits, exclusively and conclusively.

Advanced Systems Management Group (ASMG) still feel somewhat thwarted in our efforts to make the technological landscape understandable, up until this point in our Submission. Why?

[248] Source: "SASE-The Optimal Architecture to Secure and Connect the New Enterprise perimeters," by Cato Networks [corporate website], Dated: July 2020. See: go.catanetworks.com. See *also*: *Ibid*., [Foot Note # *16*].

Things have simply moved so far, and so fast, from the routine commentary everyone is comfortable with: here is a routine relational database, here is a simple Internet search activity, here is a simple communications network protocol. However, unless we turn back the historical dial fifteen (15) years or so, nothing is simple anymore.

Case in point: We made the point a little earlier that "Data is not only generated by systems, but when combined with other data (and insights), can usefully *power* systems." We need to do some remedial analysis here. The Big Data environment, and the Big Tech players, and Big Tech delivery infrastructures which some major players in the economy have built – like Walmart for example – are doing tons of text searching where the traditional databases are not performing up to task. What has been brought to bear in this regard are enterprise-level Infrastructure-as-a Service (I-a-a-s) products to provide log analysis on huge sets of unstructured data.

Here is how it works: "During an indexing operation, Elasticsearch converts raw data – such as log files – into internal documents, and stores them in the basic JSON-type data structure as (JSON) data objects. Each document is a simple set of correlating keys and values; the keys are numerous data types – strings, numbers, dates or lists. Adding documents to ElasticSearch is easy – and it's easy to automate. Simply do an HTTP POST that transmits your document as a simple JSON object. Searches are also done with JSONL send your query in an HTTP GET with a JSON body. The RESTful API makes it easy to retrieve, submit and verify data directly from a command
line.[249]

We have travelled though the technology stack of the Big Tech companies with the overview we have just completed. That overview skipped examining how the back-end (*bottom*) of the enterprise's infrastructure stack was aligned with the front-end (top) of the enterprise's infrastructure stack, which we will now make up for. The back-end happens on the server (on site, or in the cloud) and databases. It's the machinery that works behind the scenes – everything the end user doesn't see or directly interact with. The server-side manages all those requests that come from users' clicks, returning the appropriate data responding to those user clicks, to the front-end where the *search* began. Any time you request something from a website– whether you're searching for a product in an online store, or searching for hotel locations within a specific state – the database is responsible for accepting that query, fetching the data, and returning it to the website.

[249] Source: "Elasticsearch: What It Is, How It Works, And What It's Used For," By Ralf Abueg, [online-knowi.com]. Dated: March 7, 2020. Discussion: At its core – Abueg (2020) tells us – Elasticsearch is a server that can process JSON requests and give you back JSON data. Not clear enough? Try this: For Elasticsearch purposes, an *index* is a collection of documents – e.g. Customers, Products, Orders – then Elasticsearch performs a *hashmap* (like a data structure that takes you from a word to a document) – via Elasticsearch's distributed, inverted indices, something like a *Query on Steroids*, performed in near real-time, with searches in milliseconds, not minutes or hours. See *also*: *Ibid*., [Foot Note # *222*].

Middleware essentially describes any software on the server that connects an application's front-end to its back-end. Here we examined Kafka, a middleware layer, at length. Middleware, and certainly Kafka demonstrated its proficiencies here, also let's cloud applications and on-premise applications "talk," and provides services like data integration.

Trying to store, process, and analyze all the unstructured data an enterprise is faced with led to the development of schema-less alternatives a.k.a. advances to the structured query language (SQL) status quo. These alternatives are referred to as NoSQL, meaning "Not only SQL." Unstructured data from the web can include: sensor data, social sharing, personal settings, photos, location-based information, online activity, usage metrics, and more. Trying to store, process, and analyze all this unstructured data is a daunting task! NoSQL databases took on this job, and arranged everything into a document-oriented management approach. The NoSQL database approach sets *no* limits on the types of data you can store together, and thereby allows you to add different 'new' data types as your needs change.

As we discovered earlier, Kafka SQL (KSQL) is meant to do continuous querying – e.g. turning a relational database '*inside-out*'. This KSQL accomplished this by taking the relational database transactions log, and that transactions log's tables – with their derived views – and providing updates on all of this to be modeled as 'streams.' Kafka SQL (KSQL) sits on top of the Kafka streaming table. Then, you read data from Kafka Stream – where every update is independent of all others, every update is (probably) an update to a previous update – and so on. At some point in the future, you process everything, as new events keep arriving on the stream.
In short, Kafka SQL (KSQL) takes the relational database transactions log's derived views – and updates all of this via modeled-as-streams outputs – with the more data generated, the more the network commits to send (and/or receive) data feeds. As the respective case demands, greater and greater, more advanced, data processing power is delivered.

This moved us forwards to examining next, the whole secure access service edge (SASE) topic. Since the network is more and more committed to sending (and receiving) a steady stream of data, something is needed to replace the failings of Software Defined Network (SDN) controllers. Cato Network's showed us their secure access service edge (SASE) solution. Through the combination of cloud applications and the expanding mobile workforce, Cato Network's outlined their service model as addressing: SD-WAN, Global Private Backbones (basically, ERP systems with *eyes*), Service Web Gateways (e.g. AWS Direct Connect and/or Azure Route are mentioned), and Firewall-as-a-Service (virtual firewalls weaved into a *web*) and more. This – Cato Network's suggests – will accomplish the identity-driven solution for the cloud, supporting all *edges* and will (may?) be distributed globally. And where are we exactly? Back at Elasticsearch.

Elasticsearch has a set of simple REST APIs, which it uses to deploy functions in a distributed nature, with speed, and scalability. Elasticsearch is the central component of the Elastic Stack, a set of open source tools (a.k.a. open source products) from Elastic, designed to help users take

data from any type of source – and in any format – and search, analyze, and visualize that data in real-time, via data ingestion, data enrichment, or data storage process steps.

If you are an employee of a major Big Tech Company, all of this is veering on the steps of being day-to-day routine. But to all the rest of the economy? A lot of catch-up activity is at play! That is the technology behind the massively complicated payments technology infrastructure. To segue from here into a payments solution? And that solution – requiring data interoperability, as data moves from one platform to any other payment platform – is done how?

Two things may be jumping out here as our answer to - Q6) 'Payment technologies a.k.a. 'getting interoperability right' draws-to-a-close. First, the title is a misnomer! Interoperability was not mentioned once in this section's answer. Advanced Systems Management Group (ASMG) believe it is simply not possible today to achieve. Why?

Let's throw up on the white board a few virtual facts – as in *factoids*. A factoid is either a false statement presented as fact, or true (but brief or trivial) item repeated often enough it becomes unassailable. Our virtual facts (factoids) – all four of them – may have answers proving to be 'none-of-the-above' or 'all-of-the-above'.

Virtual Fact 1: A process to prevent additional data propagation events from occurring, may require 'purging data' or 'debugging data'. Do this often enough, and then you might wish to *next* examine data 'roles', or examine how data is accessed by (data's) Users,' or decide whether that data has been *untouched*.[250]

Virtual Fact 2: Data which is sensitive – and protected – by 'something like' the Payment Card Industry's Security Standards (PCI-DSS) regulation, may have safeguarding issues, which we need to promptly attend to or alternatively, just ignore.

Virtual Fact 3: Hadoop clusters for (*interpretive*) data reporting – i.e. *throw* data out in the open (cloud or edge), in a decrypted state – and 'wait and see' what happens. These data sets are shared, seemingly with impunity, and without discernable security protections or controls.

Virtual Fact 4: Running analytical processing on data does not necessitate (that) the entire research group – receiving that data – requires all the Sensitive (data) elements associated with the research underway. Data sharing and securing, by equivalence theory (or just by observing), is not required by all, only by a few.[251] If you don't need it, you don't *get it* (Data – that is!).

[250] Source: "A New View and Guidelines for Data Centric Security," By Michael Ferrell, James Madison University [online - Infosec Techreport], Department of Computer Science, Masters' thesis. Page 115. Dated: June 2007. See: citeseerx.ist.psu.edu. Discussion: Acolyte of the IBM Data-Centric Security Model (DCSM) logical view.
[251] Source: "The Need for Data-Centric Security," By Varun Haran – interviewing Robert Shields, Informatica. [online – APACinfosec]. Dated: November 6, 2015. See *also*: *Ibid*., [Foot Note # *253*].

Fun aside, what we are looking at here is the common Information Technology / Information Management (IT / IM) orthodoxy. This IT / IM orthodoxy is so well engrained, that even raising the specter that 'by applying the concept of data-centric security' – to secure, share and safeguard data – is simply not on. Let's loop back around and look at the generic message contained in these four *factoid* examples.

Three underlying solutions[252] are trotted out by the Information Technology / Information Management (IT / IM) *cognoscenti* to address. Data security, they claim, must be peripherally subscribed to, by the four factoids (above): **i**) tokenization; **ii**) masking and; **iii**) (data elements) encryption.

i) Tokenization – Virtual Fact 2 [as the *illustrative* example – e.g. Data which is sensitive, and protected, may still have safeguarding issues left unaddressed] calls for a data 'token' to be substituted for a sensitive piece of information. For example, you may substitute a randomly-generated number, i.e. assign a personal-identifying credit card number. This will be sixteen (16) digits long, with the last four digits of the credit card *inserted* into that randomly-generated numbering sequence. Tokenization is embedded in-line with transaction (processing) systems, usually inserted into a data *stream* in the data pipe, as opposed to inserted into a database or data repository.

The Payment Card Industry's Security Standards (PCI-DSS) regulation has managed *some* security protection, blanketing credit card transactions with tokenization. Consumers / Banking officials – even third-party transactors' (Fintech's) – continue to pass credit card information through complex, difficult to secure environments. And this data packet transit leaves data packets unprotected. Merchants sought out tokenization solutions, to circumvent transaction breaches. The solution Merchants employed, took the credit card information being sent for reconciliation – via the bank and/or Fintech – replaced it in mid-'stream,' i.e. the unsecured data packet transaction was replaced via a token.

This token could be a unique [cellular level] scrambled number, or a randomly-generated number –with the four last digits of the credit card as the embedded identifier – which was sent as the proxy, for the credit card number itself. Where this proves problematic is that the tokenization approach does not lend itself to other more complex situations. For complex data sets, which may require data management features to create different types of tokens – dynamically – possibly serving multiple audiences, the challenge becomes precipitous.
Do we want to be doing this? (tokenization)?

ii) Masking – Virtual Fact 4 [*illustrative* example – e.g. Sensitive data may not be required to be seen by all] is the situation in which a research group "say, running analytics on data, we should *not* instantly assume requires *all* research group members accessing *all* (or particularly the sensitive portions of the data sets') all the time." To share everything – sensitive or not –

[252] Source: "Trends in Data Security," By Marco Tietz, Khurt Williams and Scott Yoneyama, [online – Securosis L.L.C.]. Dated: September 14, 2014. Page 8 -10, 16. See: cdn.securosis.com. See *also*: *Ibid*, [Foot Note # *256*].

expands the cyberthreat attack service massively.[253] The popular option for retaining 'aggregate' data values – e.g. substitute 'something' for a Social Security Number (SIN) personal identifier – by using a random-generated number; or a random person's name (taken from a phone book); or, replace a 'Date-Of-Birth (for age masking)' with such-and-such – removes a *sensitive value* from contention. This could work for low-level analytical tasks, where you don't require a 'secure-everything' approach, within your system. Or, you don't trust where your data is being stored. You (the data User) alone know how to 'unmask' your data store. This might work for personal identifier information (PII), personal health information (PHI) or personal credit information (PCI) compliance requirements.[254]

Again, there are issues with data masking. The Users' credentials may need to be uncovered during database querying, which involves (or could involve) desensitizing information. The organization may term this as 'risk-based' data masking, or 'least privilege' or 'need-to-know' data masking. Possibly these events may occur over multiple jurisdictions, and may involve multiple, as opposed to uniform – or singular – data types. The down-side of data masking is that the User needs to know which masks re suitable for various regulations and laws. Plus, if anonymized attributed – such as masking elements, such as number of bank accounts a Consumer has – or some personal information appears in a date set (of information) this could be reversed engineered by a motivated party. That motivated party may then trace that information back to the data record the data masking is attempting to secure.
Do we want to be doing this? (data masking)?

iii) (Data Elements) Encryption – Virtual Fact 1 [*illustrative* example – e.g. Prevent additional data propagation by debugging and/or purging data at its source; Encrypt? Decrypt?], and;
iii) (Data Elements) Encryption – Virtual Fact 3 [*illustrative* example – e.g. Hadoop clusters for '*interpretive* data' reporting; Encrypt? Decrypt?].

These two examples – 'debugging and/or purging data at its source' and 'Hadoop clusters for '*interpretive* data' reporting' – are not the panacea they are made out to be! Sensitive data may exist on files or disk volumes, so a logical thought would be to employ a data cipher applied to files or disk volumes, and essentially secure data. However, remember one thing: That data you just encrypted may have transitioned over via some sort of *data substitution* effort, moving across a wide variety of applications.

Some US mandates in the US are quite comfortable accepting encrypted data. It does – also – get used regularly in cloud transport applications. The down-side to data encryption (applied on

[253] Source: "The Need for Data-Centric Security," By Varun Haran – interviewing Robert Shields, Informatica. [online – APACinfosec]. Dated: November 6, 2015. See *also*: *Ibid*., [Foot Note # *251*] '[Haran-2015] secure data selectively (electively) distributed as a security control measure – Informatica suggestion'. See *also*: *Ibid*., [Foot Note # *251*].
[254] Two methods of data masking may be used: Persistence masking – data is masked where it is stored, Secondly, Dynamics masking – real-time data is masked, i.e. data masking is altered prior, or during, the data in delivery stage of data transmission.

data elements-in-transit, i.e. data *packets*) is that it cannot de-identify, or de-sensitize that data packet, for analytical or test purposes. European Union (EU) jurisdictions are not allowing encrypted (personal) information to cross national boundaries. This European restriction also applies to tokenized data sets. And, data masking initiatives, as well, are frowned upon by the European Community (EC). Compliance issues plague data encryption efforts, since the ciphers used must come from *trusted* sources, plus if keys (or key management regimes) are used alongside the data elements encryption, who will vouch for the efficacy of these systems,[255] as well?
Do we want to be doing this? (data elements – encryption)?

Tietz, et. al. (2014) have suggested: "Focusing on data is logical, but it is still an unusual way for firms to consider security."[256] The only unusual thing here, is that last statement!

Two things may be jumping out here as Q6) Payment technologies a.k.a. 'getting interoperability right' wraps up. First, the title is a misnomer! Interoperability was not mentioned once in this section's answer. Advanced Systems Management Group (ASMG) believe *interoperability* is best deferred to Q8 to address this topic, as framed by a grouping of solutions to address *data management issues* in a panoply of different ways. And secondly, Advanced Systems Management Group (ASMG) believe *interoperability,* as it applies to mobility devices – the centre piece of the payments infrastructure today – needs a separate section to address its operational security failings. This latter issue we propose to address in answer to Q11 'Changes to banking (post Covid-19)'.

ASMG will now address information *interoperability* in a full-fledged manner. We will approach this topic in a three-pronged presentation. First, we will offer a short overview of the genesis of the data-centric security (DCS) solution. This section will examine, in preliminary fashion, how the data-centric security (DCS) solution was created, and how it has progressed to the status it occupies today.

Next, in the second section, we will get under-the-hood, and examine a few 'tool box' items – rules and policies and all manner of 'conceptual' to 'implementable' elements – which are fully derived from the Object Management Group's (OMG's) *open standard* ratification of the

[255] Jonathan Gould, OCC's Senior Deputy Comptroller announced on July 23, 2020 that national banks can hold the unique crypto-graphic keys for a crypto-currency wallet. Alexandre Lemarchand was quoted by a publication recently: "For the crypto currency industry to truly mature, institutional investors are going to have to get involved – exchanges, brokers, asset managers, over-the-counter (OTC) traders, *custodians* and others – must enforce institutional-grade controls on all transactions. Otherwise, QuadrigaCX, with one bad actor and $163 million vanishing, might this (not) repeat again?" Source: "Digital Custody," By Asset Servicing Times reporters, [online – assetservicingtimes.com]. Dated: 2020. See *also*: "US Banks Can Now Offer Crypto Custody Services," By Sarah Coble [online – infosecurity-magazine.com]. Dated: July 23, 2020.
[256] Source: "Trends in Data Security," By Marco Tietz, Khurt Williams and Scott Yoneyama, [online – Securosis L.L.C.]. Dated: September 14, 2014. See *also*: *Ibid*., [Foot Note # *252*], Page 16. '(Tietz, *et. al.*-2014) data-centric security called – erroneously – on the carpet for its *unusual* security capability.'

Information Exchange Framework's (IEF's) information sharing and safeguarding *a.k.a.* data-centric security's Reference Architecture (RA).

The third and final section will address why this is a new security paradigm, and why it is needed across the entirety of the Information Technology / Information Management (IT/IM) security establishment.

The data-centric security solution (DCS) Advanced Systems Management Group (ASMG) offers was born out of our organization's journey supporting the defense sector. The military has long pursued the *exercise of authority* based upon certain, verifiable tasks. These tasks, in the theatre of dispute resolution *a.k.a.* warfare, address two principle activities: *Command* following a process of verification of knowledge, and; *Control* exercising the actionable mission to obtain decisive advantage. Advanced Systems Management Group (ASMG) became involved in liaisons with defense sector principals, as our story unfolds.

Advanced Systems Management Group (ASMG) envisioned, at a very early stage in our organization's history, that unless we secured data – in all its manifest representations (e.g. forms and formats, content and contextual identifiers, etc.) – then to achieve data security at a defense-in-depth level across an enterprise, was unattainable. Advanced Systems Management Group (ASMG) decided we needed to come up with a definitive way to address data security issues, and decided to concentrate on both the *data* / *metadata* – integration infrastructure, and the *data* / *metadata* messaging and networking (transporting) infrastructure – combined. We also felt strongly that key advances being made with Multi-Independent Levels of Security (MILS) architectural modeling would be vitally useful. These developments made a strong and lasting impression on our Company.[257]

Multi-Independent Level Security (MILS)[258] guiding principles were identified as an architectural methodology to achieve a system of highly secure *distributed components*, assembled together,

[257] Source: "MILS: Architecture for High-Assurance Embedded Computing, By Vanfleet, Beckwith, Calloni, Luke, Taylor, and Uchenick. See also: *Ibid*., [Foot Note # *258–260, 271*]. See: http://www.crosstalkonline.org/storage/issue-archives/2005/200508/200508-Vanfleet.pdf. The original citation is from: MARS/2013/12-05-IEPPV 6th Revised Submission, OMG Document Number: MARS/2013-12-05; Annex G-Page 313; *and* Page D-10. See *also*: [alternate *citation*]: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.590.2027&rep=rep1&type=pdf.

[258] Source: "MILS: Architecture for High-Assurance Embedded Computing," By Vanfleet, *et. al*. See also: *Ibid*., [Foot Note # *257, 259 –260, 271*] '(Vanfleet *et. al*.-2005) Multi-Independent Level Security (MILS) architectural methodology defined.'

to achieve – in a [hardware-driven] combination[259] – *information sharing* alignment for the provision of critical *information assurance*. Advanced Systems Management Group (ASMG) were challenged, years back, to adopt this same guiding principle, and architectural methodology. The big difference was that we chose to apply MILS methodologies and principles – not to hardware and hardware-related components – but to data itself.

Vanfleet *et. al*., (2013) identified the set of critical attributes which ensured that *information assurance* would always be achieved. These four (4) attributes, supporting secure *distributed components* attaining *information assurance,* are: "[*information assurance* is guaranteed when security attributes serve to be] Non-bypassable, Evaluable, Always-invoked, and Tamper-proof – spelling the acronym NEAT." Vanfleet *et. al*. (August 2005) stated this very succinctly as follows: "Security policy enforcement that is not NEAT is not effective.[260]"

Non-bypassable, Evaluable, Always-invoked, and Tamper-proof (NEAT) attributes, applied to defining *information assurance* for Advanced Systems Management Group's (ASMG's) *data* securing and safeguarding efforts, are captured here:

• Non-bypassable: The data-centric security (DCS) solution intercepts traffic between the workstation and the target data service. Information requests that comply with the security policy may proceed. While traversing the interception point, data is cryptographically transformed. Only valid requests can traverse the intercept, and any attempt to access the data directly will only disclose an encrypted object.

• Evaluable: Each DCS component is implemented as a well-designed, well specified, well implemented, minimalist, low complexity module that is accessible through a well- defined, *open* protocol. It is possible to do assurance testing against each DCS (Information Exchange Framework/IEF) interface via the use of validation and verification harnesses.

• Always invoked: Every DCS (Information Exchange Framework/IEF) -relevant data request is

[259] Source: "MILS: Architecture for High-Assurance Embedded Computing," By Vanfleet, *et. al*. See *also*: *Ibid*., [Foot Note # *257–258*, *260, 271*]. Discussion (*point*): 1) Hardware components may include access control guards, down-graders, crypto devices, etc. ASMG were usurping these same *design principles* and critical *attributes*, but making their transference to data design or data management applications and methodologies in the service of securing *data*. Source: "ASIS–for–GNAT User's Guide," By Ada Core staff [online]. Dated: 2020. See: http://docs.adacore.com/live/wave/asis/html/asis_ug/asis_ug.html. See *also*: http://www.adacore.com/gnatpro-high- security/mils#sthash.BUzkPb7t.dpuf. See *also*: *Ibid*., [Foot Note # *264–265*]. Discussion (*point*): 2) '(Adacore.com) National Information Exchange Model (NIEM) Program Office – *definition of* Semantic(s) – comprising one or more Transactional(s), that may be statically filtered (e.g. they *should* define security and privacy filters operating with specific metadata at runtime).' The important point raised here is that NIEM is a common vocabulary, that enables efficient information exchange across diverse public and private organizations. To implement NIEM, ASMG built the vocabulary tools and tooling components, next (called the Information Exchange Policy-Based Packaging Vocabularies (IEPPV – see: omg.org).

[260] Source: "MILS: Architecture for High-Assurance Embedded Computing," By Vanfleet, *et. al*. See *also*: *Ibid*., [Foot Note # *257 – 259, 271*] '(Vanfleet *et. al*.-2005) - Non-bypassable, Evaluable, Always-invoked, and Tamper-proof (NEAT) attributes.'

checked by the appropriate security processes and information protection services. The selection of what constitutes an IEF-relevant data request is entirely defined by the implementation. DCS does not place restrictions on what actions can be made subject to policy-based access control.

• Tamper-proof: The DCS (Information Exchange Framework/IEF) system generates an audit trail for all security relevant events that is established through a chain-of-custody. This capability detects the addition, deletion or modification of audit trail information. While this does not provide absolute proof that data tampering may have occurred, it does support the detection of unauthorized modification by Security and Incidence Event Management (SIEM) products, that may be used to audit data records, in support of incident handling and forensic tracking activities.[261]

Advanced Systems Management Group (ASMG) – in the pre-2013 time-frame – recognized that the data assembly *process* required its own specialized vocabulary. This vocabulary, tied in with Model Driven Architecture (MDA) advances,[262] supports the Model Driven Architecture's (MDA's) inherent strength – supporting the serialization of packaging and processing (data) models – i.e. achieving semantic interoperability.[263]

Semantic interoperability, in Advanced Systems Management Group's (ASMG's) definitional and analytic realm, is a crucial concept. It supports the entirety of our work supporting the strategic interests of our defense sector Clients,' pursuing their Command and Control (C&C) situational awareness initiatives.

What ASMG were uncovering, in our work as a voting (and ratifications-participatory) member of the Object Management Group's (OMG's) standards setting organization, was that to secure

[261] Source: Secure Access Management for a Secure Operational Network: A Scientific Paper, By Charlebois, Daniel -DRDC CSS et. al., Defence R&D Canada – CSS. Technical Report (Document # TR 2013-037 – unclassified), Date: December 2013, Page 10-11. See also: Ibid., [Foot Note # *280*]. Discussion: Security and Incidence Event Management (SIEM) vendors, and SIEM products / services suppliers, have maintained a studied silence 're: this critical integration capability/opportunity' which the DCS solution represents, for security and incidence event management (SIEM) reporting.

[262] Model Driven Architecture (MDA) provides the transformational ability to serialize [data] models as interface code or policy / rules languages, that can be executed by multiple services (i.e. decision and enforcement points) or platforms. Source: Information Exchange Framework (IEF) – Information Exchange Policy Packaging Vocabulary (IEPPV), See: MARS/2013/12-05-IEPPV 6th Revised Submission, OMG Document Number: MARS/2013-12-05; Page 6.

[263] Semantic interoperability, in the context in which we are examining it, is the requirement to enable information integration, machine analytics, inferencing, knowledge discovery, and data federation to all be addressed. Semantic interoperability is not only concerned with the packaging of data (structure and syntax) but also addresses the simultaneous provision of intent and meaning (semantics) attached to that data. Source: Information Exchange Framework (IEF) – Information Exchange Policy Packaging Vocabulary (IEPPV), See: MARS/2013/12-05-IEPPV 6th Revised Submission, OMG Document Number: MARS/2013-12-05; Page G-5. This is not to be confused with Technical Interoperability, a term which defines an agreed communication protocol which exists between established communications infrastructure, allowing systems to exchange bits and bytes, and the underlying network and protocols are unambiguously defined. Source: *Ibid*., [this Foot Note # *201*] Page G-6.

data, we needed to introduce policies applied to data. Policy enforcements – of one or more -application and/or -systems "specific" *security policies* – would inherently, and by their intuitive design, authorize information flow *only* between components in the same security domain. Or, as taken and adapted from the [hardware-driven] application of Multi-Independent Level Security (MILS) first principles[264] – *information sharing* alignment for the provision of critical *information assurance* wouldn't just apply to trustworthy hardware security monitors (e.g., access control guards, down-graders, crypto devices, etc.[265] would but would apply to data / metadata in a *defense-in-depth* NEAT attributes-compliant information assurance connotation as well.

That has been a prickly unravelling of the birth of the data-centric security (DCS) solution. Now let's proceed to the second part of this presentation, and examine the under-the-hood, 'tool box' items – rules and policies and all manner of 'conceptual' to 'implementable' elements – which are fully derived from the Object Management Group's (OMG's) *open standard* ratification of the Information Exchange Framework's (IEF's) information sharing and information safeguarding [*a.k.a.* data-centric security's (DCS's)] Reference Architecture (RA). The next big task Advanced Systems Management Group (ASMG) undertook was to address head-on the requirement we identified as an urgent need for a single, holistic and unified security orientation for managing data, with modular design techniques, and layered security defenses. This advanced security solution would employ mandate-level, mission-level and

[264] Source: "ASIS–for–GNAT User's Guide," By Ada Core staff [online]. Dated: 2020. See: http://docs.adacore.com/live/wave/asis/html/asis_ug/asis_ug.html. See *also*: http://www.adacore.com/gnatpro-high- security/mils#sthash.BUzkPb7t.dpuf. See *also*: *Ibid*., [Foot Note # *259, 265*] '(adacore.com) National Information Exchange Model (NIEM) Program Office – *definition of* Semantic(s) comprising one or more Transactional(s), that may be statically filtered (e.g. they *should* define security and privacy filters operating with specific metadata at runtime).' Discussion: The important point raised here is that NIEM is a common vocabulary that enables efficient information exchange across diverse public and private organizations. To implement NIEM, ASMG built the vocabulary tools and tooling components, next (called the Information Exchange Policy-Based Packaging Vocabularies (IEPPV – see: omg.org).

[265] Source: "ASIS–for–GNAT User's Guide," By Ada Core staff [online]. Dated: 2020. See *also*: *Ibid*., [Foot Note # *259, 264*]: '(adacore.com) the *build pattern* for a semantic specification of an exchange agreement modeled after the *build attributes* adopted by (interoperable) NEAT-compliant hardware and hardware components.

departmental-level policies[266] treating all information assets as critically important. To do this, Advanced Systems Management Group (ASMG) built the Information Exchange Packaging-based Policy Vocabulary (IEPPV) components and constituent elements, and presented these for the Object Management Group (OMG) to conduct its peer-reviewed, open standards organization ratification exercise next.

The Information Exchange Framework (IEF) Reference Architecture (RA) – which includes the data ontologies and data models captured by the Information Exchange Packaging-based Policy Vocabulary (IEPPV) components and constituent elements – is that result, ratified by the Object Management Group (OMG)[267] in July 2017.

The Information Exchange Framework (IEF) Reference Architecture (RA)[268] provides Foundational security services which deliver: **i**) the provision of a *defense-in-depth* protective data security layer, and; **ii**) additional encryption, key management, and trusted audit services – equally blended *in* to the reference architecture's security service mandate – as the unified, implementable data-centric security (DCS) solution.

The first Foundational security service – *defense-in-depth* protective data security layer – in this context, the Information Exchange Policy and Packaging Vocabulary's (IEPPV's) has many

[266] A *policy* is a definitive course or method of action selected from among alternatives, and follows given conditions to guide and determine present and future decisions. (Source: Information Exchange Framework (IEF) Final Revised Submission (FRS), Source: OMG Document Number: MARS/2017-02-21; Page 315). *Policy Driven* refers to a process involving formal documents describing a plan of action (Policy_Instrument) translated into machine readable rules (/instructions) and enforced by software services and systems. This process results in full traceability from Policy_Instrument to instrumentation (policy decisions and enforcement points). See: *Ibid*., [Information Exchange Framework (IEF) Final Revised Submission (FRS), See: OMG Document Number: MARS/2017-02-21]; Page 316. Discussion: There are a number (i.e. a multiple) group of paths through which authorizations for *information sharing* occurs, depending on: i) the number of items (/data and/or metadata elements being requested simultaneously); ii) the source and target for the requested InformationElements - e,g. "file/ or other data configuration element" - being handled; iii) the capabilities of each of the selected IEF components processing that data exchange; iv) the availability and fidelity of the user's (e.g., network, devices, systems, services and *users*) authorizations, privileges and attributes to receive that information, and; v) the complexity and fidelity of the user's own policies. Many of the preceding items will be addressed in the individual component specification section(s) put together during the DCS design phase. The preceding list of items outlines the process attributes (and location attributes) for shared and secured data, while data / metadata will be: i) encrypted using a symmetric key; ii) The file/data element is (or will be) appropriately marked, and; c) The file/data element will be maintained in a Secure Access Container (SAC). See: *Ibid*., [Information Exchange Framework (IEF) Final Revised Submission (FRS), See: OMG Document Number: MARS/2017- 02-21]; Page 282-283. [http://www.omg.org/spec/IEFRA/]. See *also*: *Ibid*., [Foot Note # 282].

[267] The Object Management Group® (OMG®) is an international, open membership, not-for-profit technology standards consortium, founded in 1989. OMG standards are driven by vendors, end-users, academic institutions and government agencies. OMG Task Forces develop enterprise integration standards for a wide range of technologies and an even wider range of industries.

[268] Source: https://www.omg.org/spec/IEF-RA/.

capabilities to review. The IEPPV captures *all* semantics, ontologies, models, rules[269] and policies driving the data-centric security (DCS) solution.

Breaking down the Information Exchange Framework (IEF) Reference Architecture's (RA's), data-centric security (DCS) services and components a step further, the next three features consist of: **iii**) separation *via* controlled information flow [implementable *via*]: **iv**) separation mechanisms that support both untrusted, and trustworthy, components, and; **v**) information flows /*messaging* implementable (e.g. designed and architected) to ensure that the *total security solution* is non-by passable, is one-hundred (100) per cent evaluable, and is *always* invoked and tamper-proof.

These three data-centric security (DCS) services and components – points **iii**) separation *via* controlled information flow; **iv**) separation mechanisms that support both untrusted, and trustworthy, components, and; **v**) information flows /*messaging* implementable – are derived, or influenced by the Multi-Independent Levels of Security (MILS) system principles which Advanced Systems Management Group (ASMG) embedded into the data-centric security (DCS) solution strategy. In particular – point **iv**) separation mechanisms and; point **v**) information flows / *messaging* – are *both* at one or more separation mechanisms' implementable e.g., *via* Separation Kernel, *via* Partitioning Communication System, and/or *via* Physical Separation. In effect, the data-centric security (DCS) solution maintains data process point *separation* and, data *assurance* and data *integrity* requirements and mandates, at the highest critical acceptance levels.

The second Foundational security service – additional encryption, key management, and trusted audit services – have been added to, and expanded, over time. The Object Management Group's (OMG's) Command, Control, Communication, Computers and Intelligence (C4I) Task Force started an effort in 2007 towards drafting a specification for Data Tagging and Labelling,

[269] A *Rule* is defined as one of a set of explicit or understood regulations or principles governing conduct within an activity or sphere. Telling us exactly... what? Or, Rules are the build pattern for an information exchange that conforms to the semantic specification of an [information] exchange agreement (e.g., the Information Exchange Data Package, which in this Report is referred to as the IEPPV). This exchange agreement is specified for us by the National Information Exchange Model (NIEM) Program office, the issuer of the semantic underlying the IEPPV. Source: Information Exchange Framework (IEF) – Information Exchange Policy Packaging Vocabulary (IEPPV), See: MARS/2013/12-05-IEPPV 6th Revised Submission, OMG Document Number: MARS/2013-12-05; Page D-10. Rules are further characterized by the term, Distribution_Specification. A specification is something which governs the assignment of information dissemination and data handling tasks via User Application(s), service Interfaces, and Middleware. An IEF component relies upon a 'gateway'. A 'gateway' provides a single integration point for security services, and is hosted on other parts of the user infrastructure / environment. This single security point provides the ability to pass message traffic, conveying both: i) security redaction and filtering, and; ii) proxies or protocol translations; at various network layers. (Source: Information Exchange Framework (IEF) Final Revised Submission (FRS), See: OMG's Document Number: MARS/2017-02-21; Page 308). Rules are further characterized by the term Information Exchange Policy Set. This is a general term identifying a group of InformationExchangePolicies (note: *no spacing*). InformationExchangePolicy represents a serialization of Policy Models, defined by adopting the IEPPV. Source: Information Exchange Framework (IEF) Final Revised Submission (FRS), See: OMG Document Number: MARS/2017-02-21; Page 310.

for Security and Privacy. A Request for Information (RFI) was issued in 2007, and a Request for Proposals (RFP) in 2010.[270] The effort was suspended, but is now being revived (circa 2017), due to strong interest from several military organizations.

To understand the nature of "Data Tagging and Labelling, for Security and Privacy" a quick introductory overview on how the data-centric security (DCS) solution applies an audit trail may prove instructive. There is a Trusted Audit Service (TAS) audit event(s) processing logic incorporated into the Information Exchange Framework (IEF) Reference Architecture's (RA's) 'IEF implementation scenario.' briefly reviewed next. We mentioned the Tamper-Proof nature of the data-centric security (DCS) / Information Exchange Framework (IEF) solution, presented as a NEAT design parameter earlier.[271] 'Tamper-Proof' is also a very adept description of the data-centric security (DCS's) solution's information sharing and safeguarding *audit trail* capability, capturing – and providing – explicit *data* information assurance.

The data-centric security (DCS) audit enumerates data to include the record and block chain data, that form the *chain-of-custody*. This transformational logic also includes the ability to detect security incidents that need to be flagged, to the parties which need to be notified. Those parties may include: domain security officers. Domain security officers are *alerted* via a standard event logging mechanism. In terms of preventing malicious activity against the target environment – the data-centric security (DCS) / Information Exchange Framework (IEF) Reference Architecture (RA) components and elements – are uniquely placed to detect attempts to: **i**) send illegal instructions, **ii**) catch the tampering of data, and **iii**) monitor *all* suspect activity. Processing of notification messages is *not* part of the data-centric security's (DCS's) – e.g. Information Exchange Framework (IEF) Reference Architecture's (RA's) – duties and responsibilities. However, the data-centric security's (DCS's) – Information Exchange Framework (IEF) Reference Architecture's (RA's) – IEF implementation scenario can leverage: **iv**) all known interfaces, which can then be made to work within enterprise monitoring *computer-off-the-shelf* (COTS) Security Information and Event Management (SIEM) solution packages. SIEM software applications may be used, effectively, to provide another avenue to monitor (and log) events that are occurring.

The Information Exchange Framework (IEF) Reference Architecture (RA) is now readied and prepared to address cross-platform, cross-domain and cross-national boundaries' interoperable (or interactive) "data-sharing" – *e.g.* the insightful implementation of information interoperability – at the *data* level, and to service, and reflect *fully*, information sharing and safeguarding of whatever enterprise application, wherever it should arise.

---

[270] See: 1) Object Management Group (OMG): "Data Tagging and Labeling for Security and Privacy RFI." OMG document omg/07-09-04, September 2007. And, 2) Object Management Group: "Data Tagging and Labeling for Security and Privacy RFI." OMG document omg/07-09-04, September 2007. www.omg.org/cgi-bin/doc?omg/07-09- 04.pdf].

[271] Source: "MILS: Architecture for High-Assurance Embedded Computing," By Vanfleet, *et. al*. See *also*: *Ibid*., [Foot Note # *257–260*] '(MILS Architecture "NEAT attributes" at the data-centric security/DCS *design stage*) - audit trail event(s) processing *a.k.a.* creating a *chain-of-custody*'.

Why is this so certain? Here are the reasons why.

The Information Exchange Policy and Packaging Vocabulary (IEPPV) extends to allowing: **i**) distribution of data across the enterprise as a shared service, allowing business intelligence tools, mashups, and portals to interact with identical data in real-time; **ii**) the creation of a single source of data "truth" for major data domains, i.e., provides the ability to establish and maintain one trusted source of data for specific work flows, getting everyone on the same page; **iii**) reduces the operational problems that may stem from 'batch' data updates between systems. Even minor discrepancies in data between out-of-synch batches, in enterprise systems, can cause serious problems, especially in financial transactions, and; **iv**) Information-as-a-Service (I-a-a-S) allows the simplifying and streamlining of data exchanges between enterprise systems, reducing many of the cost factors that have inhibited the thorough sharing of back-end data with (/between) consuming systems in the past. By establishing a single, trusted source of data as a shared service, it is possible to set up separate consumers of that data in number(s) of separate applications, with comparatively little effort.

The IEF deploys an XML [eXtensible] Messaging and Presence Protocol (XMPP),[272] treating the messaging infrastructure as the critical core. This core leverages the eXtensible Messaging and Presence Protocol (XMPP), a protocol which may be organized in a star configuration, with all endpoints connecting through a central XMPP server. The data-centric security's (DCS's) solution will ask the Information Exchange Framework (IEF) services to first connect to the XMPP server, which sets up a persistent connection or session (for message transport) and then authenticates the action to the server.

The XMPP server provides the message services protocol for all data-centric security (DCS) / Information exchange Framework (IEF) services, ensuring that messages are only delivered to their intended recipient.

The eXtensible Messaging and Presence Protocol (XMPP) sessions leverage Transport Layer Security (TLS) to ensure that message traffic is encrypted. The DCS / IEF solution also requires authentication at the session layer, so that the identity of the participant in the XMPP domain is determined when the connection to the domain is established. Achieving this level of trust is required *prior* to any exchange of messages taking place, and offers a double layer of security:
1. Protection of the information at the transport layer connection; and
2. Authentication of the session that specifies the identity of the XMPP network participant.

In the current implementation, Policy Enforcement Points (PEPs) and Security Service Gateways (SSGs) are identical, in that they share the same connect to and (/use) the eXtensible Messaging and Presence Protocol (XMPP) messaging infrastructure. Each component's XMPP identity, and

[272] Source: "What Can You Do With XMPP?" By Barrett, Dated: 2009. See: http://fyi.oreilly.com/2009/05/what-can-you- do-with- xmpp.html. Discussion: The eXtensible [XML] Messaging and Presence Protocol (XMPP) is a protocol for message exchange within the messaging infrastructure's service-oriented-architecture (SOA). See *also*: *Ibid*., [Foot Note # *273*].

its associated set of credentials, are specified in a local configuration file that is loaded at run time, and used to connect to the XMPP domain, and access the messaging services of the Information Exchange Framework (IEF) Secure Message Service Bus (SMSB). Once a data-centric security (DCS) / Information Exchange Framework (IEF) component is connected to the XMPP domain, they may send and receive messages to support its [e.g. *their*] role conforming with service-oriented-architecture (SOA)[273] duties and responsibilities.

The eXtensible Messaging and Presence Protocol (XMPP) servers require a centralized repository to store the identity, and provide authentication, for the participants in the XMPP domain. In the deployed architecture, this service is the Lightweight Directory Access Protocol (LDAP)[274] directory, with a separate directory branch (e.g., organization unit/OU) for each of the XMPP servers that provide messaging for their respective Secure Message Service Bus (SMSB). The Lightweight Directory Access Protocol (LDAP) service is an instantiation of the OpenLDAP 4.2.3 server,[275] and is hosted on its own separate machine, and used exclusively by the data-centric security (DCS) solution implementation. The eXtensible Messaging and Presence Protocol (XMPP) servers access this Lightweight Directory Access Protocol (LDAP) service over the Management Network, using the standard LDAP protocol.

Where Web services are concerned, data-centric security (DCS) solutions can resort to the Information Exchange Framework's (IEF's) non-repudiation capability, functioning as an IEF secure message bus (ISMB).

The Information Exchange Framework's (IEF's) secure message bus (ISMB) issues its communication to the Trusted Logging Services – via component TLS_LogMessage(s) – which accomplishes three (3) things:
- performs operations on InformationElements protected by the IEF
- makes changes to the operational characterization of an IEF component, and
- changes (allowable, and can be made) to the Data Policies or Access and Release Control policies.[276]

[273] Source: "What Can You Do With XMPP?" By Barrett, Dated: 2009. See: http://fyi.oreilly.com/2009/05/what-can-you- do-with-xmpp.html. See *also*: *Ibid*., [Foot Note # *272*].
[274] Lightweight Directory Access Protocol (LDAP) is largely implemented with open source solutions, and therefore, has more flexibility than Active Directory (AD). LDAP is a Directory Service, based on a client-server model, that runs on a layer above the transmission control protocol (TCP) / internet protocol (IP) stack. The Lightweight Directory Access Protocol (LDAP) provides a mechanism used to interconnect network devices, and to search, and modify, Internet directories. LDAP is prevalent – in fact, Microsoft Active Directory is an LDAP-based solution.
[275] Source: OpenLDAP is a free, open-source implementation of the Lightweight Directory Access Protocol (LDAP) developed by the OpenLDAP Project. It is released under its own Berkeley Software Distribution (BSD)-style license called the OpenLDAP Public License. LDAP is a platform-independent protocol. Several common Linux distributions include OpenLDAP Software for LDAP support.
[276] Source: Information Exchange Framework (IEF) Final Revised Submission (FRS), See: OMG Document Number: MARS/2017-02- 21; Page 210-211.

In short, the Information Exchange Framework (IEF) secure message bus (ISMB) acts to isolate communications between Information Exchange Framework (IEF) components.[277]

With the multiple layers of identity and session protection in evidence, the Information Exchange Framework's (IEF's) data-centric security (DCS) solution service(s) have a high degree of confidence, that they: **i**) are connected to the correct messaging server; **ii**) (have) no rogue services running to illicitly receive message traffic, and; **iii**) are architecturally-solid, with all the built-in protections in place /*maintained* to guard against man-in-the-middle attacks.

Simple Object Access Protocol (SOAP)[278] provides the Messaging Protocol layer of a web services protocol stack for web services. It is an XML-based protocol consisting of three parts: **i**) an envelope, which defines the message structure and how to process it, and; **ii**) a set of encoding rules for expressing instances of application-defined datatypes. Simple Object Access Protocol (SOAP) is a protocol specification for exchanging structured information for implementing web services, across computer network(s). Simple Object Access Protocol's (SOAP's) purpose is to induce extensibility, neutrality and independence. It uses XML Information Set for its message format, and relies on application layer protocols, most often Hypertext Transfer Protocol (HTTP) or Simple Mail Transfer Protocol (SMTP), for message negotiation and transmission. Simple Object Access Protocol (SOAP) allows processes running on disparate operating systems (such as Windows and Linux) to communicate, using eXtensible Markup Language (XML). Since Web protocols like HTTP are installed and running on all operating systems, Simple Object Access Protocol (SOAP) serves an important function to allow clients to invoke web services and receive responses independent of language and platforms.

There is one more step to look at: 'Submit the Request to the Back-End Application.' Once transformed and expanded with supplemental information from other data-centric security (DCS) / Information Exchange Framework (IEF) solution services, the message may be submitted to the back-end application. The request is encoded into the appropriate message format, and wrapped in a transport envelope such as Simple Object Access Protocol (SOAP) within HTTP. In this form, the message can be delivered to the target application using

[277] A full listing of the interface actions conducted by the IEF Secure Message Bus (ISMB)-Interface may include a multitude of message options, including (but not limited to): i) CTS-Request (e.g. CTS is the Cryptographic Transformation Service which encrypts / decrypts InformationElements as authorized by policy. The CTS is a bridging component that will link cryptographic action requests from Policy Enforcement Points (PEPs) to a Federal Information Processing Standard (FIPS) -compliant level (e.g. At FIPS level 4, which protects a cryptographic module against a security compromise. This is also referred to in the literature as "140.2", a US government computer security standard governing cryptographic modules); ii) ISSG Request / Response (e.g. ISSG, or the IEF Secure Service gateway, which provides the integration point between the IEF installations and the user security services and infrastructure). Source: Information Exchange Framework (IEF) Final Revised Submission (FRS), See: OMG Document Number: MARS/2017-02-21; Page 26. SEE ABCs report Page 19.

[278] SOAP (simple object access protocol) – in the context of *prospective* APIs communicating with one another – acts in a brokerage role *a.k.a.* in terms of the Client-server *spine.* See *also*: *Ibid.*, [Foot Note # *445*] 'Simple Object Access Protocol (SOAP) for an in-depth description and analysis.'

extended security protocols such as Secure Socket Layer / Transport Layer Security (SSL/TLS) to ensure the integrity and confidentiality of the information.

With all of that said, the issue of batching large volumes, or frequent flows of data, may need a quick recap. The Information Exchange Policy and Packaging Vocabulary (IEPPV) extends to allow: **i**) distribution of data across the enterprise as a shared service, allowing business intelligence tools, mashups, and portals to interact with identical data in real-time; **ii**) the creation of a single source of data "truth" for major data domains, i.e., provides the ability to establish and maintain one trusted source of data for specific work flows, getting everyone on the same page; **iii**) reduces the operational problems that may stem from 'batch' data updates between systems. Even minor discrepancies in data between out-of-synch batches, in enterprise systems, can cause serious problems, especially in financial transactions, and; **iv**) Information-as-a-Service (I-a-a-S) allows the simplifying and streamlining of data exchanges between enterprise systems, reducing many of the cost factors that have inhibited the thorough sharing of back-end data with (/between) consuming systems in the past. By establishing a single, trusted source of data as a shared service, it is possible to set up separate consumers of that data, in number(s) of separate applications, with comparatively little effort.

The network capability of the Information Exchange Framework (IEF) Reference Architecture (RA) is very robust. As we have mentioned once already, the data-centric security (DCS) solution addresses both – the *data* / *metadata* integration infrastructure and the *data* / *metadata* messaging and networking (transporting) infrastructure – combined.[279] Although the specific protocol or format of the message content will depend on the nature of the entity or service being leveraged, all messages are delivered through the same communications mechanism. The DCS solution uses a *store-and-forward* system, in which the secure messaging infrastructure provides the delivery of messages between IEF components.

And the final, or third part of this sub-section presentation on the data-centric security (DCS) solution, will run the gamut, from providing a few essential interpretations as to why data-centric security is a security paradigm with some very strong selling points, and ending with a summation of why it is dearly required in our present circumstance.

[279] Source: '(MARS/2013/12-05-IEPPV 6th Revised Submission),' OMG Document Number: MARS/2013-12-05; Annex G- Page 313. *This* is a foundational principle on which the data-centric security (DCS) solution was designed. Repeated here, to capture the fact that data-centric security (DCS) accommodates 'data in a network/messaging context,' and data in *all other* 'cloud/edge/distributed ledger' or' database/application-specific/mobile-device-specific' contexts – *a.k.a.* constructs – which a security paradigm might, feasibly, be expected to address. See: *Ibid*., [Foot Note # *283, 532*].

The Advanced Systems Management Group – Department of National Defence (DND-Canada) security *concept of operations* (CONOPS)[280] Report, provides some of the *play-by-play* support, to this third section's description of the data-centric security (DCS) solution. We believe data-centric security (DCS) is a foundational, and distinctly different paradigm for achieving information security.

The Information Exchange Framework (IEF) Reference Architecture (RA) – and its full set of features and functions – the CONOPS Report (2016) suggests, will provide information sharing and information safeguarding advances *in a security paradigm context* to: i) unmodified client applications, and: ii) back-end data services – the latter occurring with minimal impact on existing operations. All forms of data sharing and (data) authorization *events* will – under the data-centric security (DCS) solution – cause a sequence of actions to occur. They are: a representative interaction between Information Exchange Framework (IEF) components [conducted via] 'file access' actions – e.g., Create, Copy, Cut, Delete, Move, Open, Paste and Save.

There are a number (e.g. *a multiple*) 'group of paths' through which authorizations occur, depending on: **i**) the number of files being requested simultaneously; **ii**) the source and target for the requested InformationElements - i.e. "file(s)" - **iii**) the capabilities of each of the selected Information Exchange Framework (IEF) components; **iv**) the availability and fidelity of the user's – e.g., network(s), devices, systems, services and *users* – authorizations, privileges and attributes, and; **v**) the complexity and fidelity of the user's own policies. Many of the preceding items will be addressed in the Individual Component specification section(s) of the Information Exchange Framework (IEF) Reference Architecture (RA) documentation. The preceding list of items outlines the *process* for accessing a *single file* located in the Information Exchange Framework's (IEF's) protected file share. If the file resides in one of the protected Information Exchange Framework's (IEF) file share locations, then: *a*) The file *is* or *will be* encrypted using a symmetric key; and/or: *b*) The file *is* or *will be* appropriately marked; and/or: *c*) The file *will be* maintained in a Secure Access Container (SAC).[281]

Advanced Systems Management Group's (ASMG's) Object Management Group (OMG)-sponsored standards-body ratification efforts – as strikingly prominent today as when first sketched out at standards-body meetings held quarterly by the OMG, throughout 2013 and up to the present day – cast an even deeper shadow, which we would be remiss if we did not cover next.

[280] Source: "Secure access management for secure operational networks (SAMSON): Security concept of operations (Security CONOPS)," By Daniel Charlebois *et. al*., Defence Research and Development Canada – Ottawa Research Centre, Scientific Report *unclassified*, DRDC-RDDC-2016-R001, Dated: January 2016, Page 1. See *also*: *Ibid.*, [Foot Note # *261*].

[281] Source: Information Exchange Framework (IEF) Final Revised Submission (FRS), See: OMG Document Number: MARS/2017- 02-21; Page 282-283. See: http://www.omg.org/spec/IEFRA/. See *also*: *Ibid*., [Foot Note # 266].

Drilling a bit deeper into this, the data-centric security (DCS) implementation – basing it [*herein*] on a Client-server *spine* – often uses Common Object Request Brokerage Architecture (CORBA) services for distribution assurance, distribution logic; Distribution Data Services (DDS) for publish, subscribe data functions; Hyper-Text Transfer Protocol (HTTP) servers, services and components for web-enabled data handling and data management tasks.[282]

In the latter case, web applications, we are addressing software-intensive systems, and unified modeling language (UML) components or elements, are among the most efficient choices of the modeling language componentry available for the web today. The DevOps professional may integrate their web software applications with the aid of UML. In this case, the DevOps professional will use UML modeling for functional requirements, for example to capture interactions between an actor and the system of interest.

Other constraints, such as business rules and implementation constraints, must be represented separately. Continuing with this topic a bit, the distinction between Web sites and Web applications is subtle, and relies on the ability of a user to affect the state of the business logic on the server. Certainly, if no business logic exists on a server, the system should not be termed a Web application. For those systems on which the Web server—or an application server that uses a Web server for user input—allows business logic to be affected via Web browsers, the system is considered a Web application. Typically, Web application users enter a varied range of input data: simple text, check box selections, or even binary and file information.

The architecture for a Web site is straightforward. It contains the same principal components of a Web site: Web server, a network connection, and client browsers. Web applications also include an application server. The addition of the application server enables the system to manage business logic and state. Why have we reviewed this here? Owing to the connectionless nature of client and server communications, a server doesn't have an easy way to keep track of each client request, and to associate it with the previous request, since each, and every, Web page request establishes and breaks a completely new set of connections.

The Web's Use Case requires accurate mapping and representation. The Web Use Case consists, at any one time, of – implementation models; -deployment models; security models, and; the *Site Map* – all requiring accurate mapping and representation. Unified modeling

[282] A system architect should not view the use of CORBA, DDS or Web Services as mutually exclusive. A single application can use CORBA for remote invocation, for distribution of logic and for 'smart pull'. Similarly, it is not mutually exclusive to deploy DDS for 'smart push' or 'sensor,' 'camera,' or 'smart phone,' mobility device data engagement. Data, no matter where it resides, is effectively monitored, and an audit trail of its information security and information safeguarding activities is kept. Thirdly, no mutually exclusive functionality applies to the use of web services in the DCS solution's implementation, as web services may – to cite but one example, to 'deploy a graphical user interface (GUI) for the crafting or reports for a large, diverse (and distributed) Community-of-Interest (CoI) to consume that report. And on a second point of clarification, a DCS implementation may use Hyper-Text Transfer Protocol (HTTP) servers and components – such as Extensible Mark-up Language; SOAP (simple object access protocol); Web Services Description Language (OWL), and JSON (for mobility) etc., – enabling communications between large Communities-of-Interest (C-o-I's).

language (UML) can be very prolific in its expression and execution of the system's business logic – in the web-specific elements or technologies we are examining.

This truly a unique paradigm shift, which we have just described. It involves in-depth domain-specific vocabularies and metadata (tag-values). If expressed in a modeling language, such as UML (See: IEPPV OMG Document Number: Mars/2013-12-05; Annex C – UML Profile),[283] this alignment may be directly integrated into an Enterprise, Business, Information or Security Architecture. In this case, the *domain specific* concepts become the *class names* on the various: Specifications, SemanticElements, TransactionalElements, WrapperElements and Attributes which the DCS solution has fully annotated and described.

We are getting a little ahead of ourselves, jumping so deeply into Information Exchange Framework (IEF) components, as *listed* in that last paragraph. All the *above* discussion will be returned to, summarized and reviewed, in the final section of this Submission.

Q7. – AI / ML security / governance and regulatory complexity

Artificial Intelligence (AI) may be the question the OCC have raised which will have the most difficult set of responses to assess. Why?

Robotic process automation (RPA), employing early-stage artificial intelligence (AI) and machine learning (ML) disciplinary advances and toolkits, found its first deployment with the financial services sector about a decade ago. This produced a mixed set of results. Robotic process automation (RPA) is not smart in a cognitive sense. Robotic process automation (RPA) doesn't embed regulatory compliance, or simplified data management tasks, into data sets. Although some robotic process automation (RPA) advances – which seek to dramatically improve the Customer service experience – may have achieved limited success, others so far have fallen short of the mark. Advanced Systems Management Group (ASMG) do not agree with this somewhat contentious evaluation by banking critics. We believe artificial intelligence (AI) and machine learning (ML) –through their algorithmic modeling and data enrichment efforts – are now fully foundational in their importance, and are *part and parcel* of financial institution (FI) business processes – plus underpin so much of the critical infrastructure and enterprise architecture components found in a financial institution(FI) today.

[283] The Information Exchange Policy and Packaging Vocabulary (IEPPV) was modeled using unified modeling language (UML) coupled with a profile that implements the Ontology Definition Metamodel (ODM) profiles for the Resource Description Framework (RDF) and OWL, and generates the RDF/XML artifacts as OWL 2.0-compliant documents. The resulting ontologies have been tested using the W3C RDF Validators and several OWL-DL compliant reasoning tools. Metadata developed for the IEPPV utilizes the OMG Architecture Board recommendation for specification metadata. See: http://www.omg.org/techprocess/AB/SM/20120614/SpecificationMetadata.owl. NB: [This paragraph *adapted* from] - Source: Information Exchange Framework (IEF) – Information Exchange Policy Packaging Vocabulary (IEPPV), See: MARS/2013/12-05-IEPPV 6th Revised Submission, OMG Document Number: MARS/2013-12-05; Page 17 – 18. See *also*: *Ibid*., [Foot Note # *279*, *532*].

ASMG have mentioned, or talked about, AI and machine learning (ML) technological developments in each of the answers we have completed, up until this point in our Submission. Here's a quick recap of the information we have presented:

Q1) 'Recent technological advances' – this question prompted Advanced Systems Management Group (ASMG) to review the transformational effort undertaken by one of the Big 5 Canadian Bank's whom realigned their Lines-of-Business (L-o-B) Customer Service offerings dramatically, aided and abetted by microservices and DevOps organizational performance recalibration efforts and architected improvements.

Financial institutions (FIs) are being inundated with unstructured data. This data involves varied and diverse data sets, drawn from: emails, call centre generated information, social media resources, chats, etc. This large swath of data provides tens of millions of information sources, impacting Customer service activities daily. Unstructured data represents over eighty (80) per cent of all data which financial institutions (FIs) deal with, and oftentimes it is hard to order, or even comprehend its meaning. *Data appliances* enter the picture, and when coupled with *agile* computing microservices and DevOps architected improvements, played a pivotal for the Big 5 Canadian Bank Advanced Systems Management group (ASMG) are most familiar with, causing that bank to successfully launch its smart core data management platform. The data appliances used to assist in this transformational effort included: Tibco EBX, a data management enterprise toolkit, and; Tibco Spotfire(s) – many of them – the latter a business intelligence toolkit [See: Foot Note # 14, 15].

AI and machine learning (ML) inference engine analysis, and the Lines-of-Business Data Domain-focused process improvements which the Big 5 Canadian Bank pursued were touched directly by sequentially *staged* transformational business process improvements – led by an array of critically deployed *data appliances* – ushering in unforeseen revenue generation savings, spread dramatically across the Bank. Collectively, these efforts have taken *data* from a non-contextual and underutilized status, and translated them into a contextually meaningful state of knowledge. This allows the institution's data to bring added business value to drive effective decision-making [See: Foot Note: 23]. By codifying, processing, and analyzing data in this manner, AI and machine learning (ML) inference engine analysis, combined with the Bank's introduction of sequential, staged process improvements, created for the Bank the desired *one-version-of-the-truth* Customer Service delivery objective, which had been the Bank's driving ambition to accomplish, for some time.

Q2) 'Hurdles to tech advance and innovation' – is a question which brought Advanced Systems Management Group (ASMG) face-to-face with innovation, writ large! We examined the Internet-of-Things (IoT) and mobility device developments, and the fast-paced adoption of model-driven application product (programming) interfaces (APIs) – both developments witnessing applied production-level AI and machine learning (ML) modeling and analytics-driven advances. These advances have been incorporated into many banking and financial

institution (FI) operational systems and business processes [See: Foot Note: # 29, 30]. This is the first indication that production-level AI and machine learning (ML) algorithmic modeling efforts have moved well beyond the static, overly simplified methodologies and implementations which AI and machine learning (ML) introduced via robotic process automation (RPA) pilots and programs of an earlier era.

Advanced Systems Management Group's (ASMG's) answer to Q2) 'Hurdles to tech advance and innovation' also focused on a quick primer of the *application of innovation* to one specific financial industry (FI) matter – *data governance*. Data governance reaches across many of the banking sector's Business Use Cases. ASMG believes that the link between operational issues and data management issues is very direct [See: Foot Note # 33]. We next expanded our examination to look at microservices / DevOps enterprise architecture-defining issues. Continuing in this vein "i.e. data governance mutually supports both the banking and regulatory domains" [See: Foot Note # 37]. Advanced Systems Management Group (ASMG) glanced – only briefly (admittedly) – at the topic of AI and machine learning (ML) playing an increasing role in fraud identification, transaction monitoring, and loan underwriting and monitoring. [See: Foot Note # 47. Plus, comments – June 2020 *re: the ACPR AI/ML* – consultations review process].

Q3) 'What digital issues not addressed' – is a pivotal question which brought Advanced Systems Management Group's (ASMG's) attention full circle, to examine the data ecosphere: the intelligent Cloud / intelligent Web. This is the turf where Big Tech reigns supreme! We walked through Tesla Director (former Google employee) Andrej Karpathy's guided view of *neural nets* and related AI / ML topics [See: Foot Note # 68]. Other topics we touched upon next included: supervised machine learning [ML] tasks [See: Foot Note # 69], intelligent chip advances, and; AI systems' automated *code writing* performed via web programming conducted on Web 3.0 [See: Foot Note # 70]. A few more controversial and complicated issues required examination. They include: digital-era developments with visual recognition / semantic model vectors (SMVs) [See: Foot Note #71, 72]. And last-but-not-least, the exciting, fast-paced advances occurring in Integrated Development Environments (IDEs) [See: Foot Note # 74]. All these cutting-edge developments may soon impact many of the financial service sector's governance and regulatory compliance boundaries, as the technology juggernaut continues to gain speed.

Q4) 'Crypto assets / crypto currencies' ushered in the new decentralized finance (DeFi) *crypto space* of the economy. Advanced Systems Management Group (ASMG) will readily admit this question was a real challenge to organize, and capture, a cohesive, true-to-topic world view.

Decentralized finance (DeFi) is massing its frontal assault, deploying many vectors of disruptive change, all at once. Few sectors of the economy have been prepared for anything like these disruptive influencers, in advance. We offered only a very brief sampling of industry developments and observations, since a rethinking of the financial service industry's rules of engagement is well underway. We elected to sample the crypto progress being made by one or two key players, and left well enough alone.

Coinbase CEO Brian Armstrong, besides offering his best advertorial for his Company Coinbase, in his "11 Predictions for the 2020s" mentions: "The next one hundred (100) million people who get exposure to *crypto* will not come from caring about it [crypto], but will be attracted to crypto by default: trying to play some game, using a decentralized social network, or earning a living."[284] Here's one prediction the Coinbase executive missed: 'make a payment on a distributed application (Dapp)'. [See: Foot Note # 85, and stablecoins discussion, Foot Note # 98 – 101 *inclusive*].

Additionally, Coinbase's Brian Armstrong suggested – re: Armstrong's "11 Predictions for the 2020s" blockchain predictions for the next decade, presented in answer to Q5) 'Distributed ledger technology (DLT) for banking' *a.k.a.* [sub-section] 5-1. 'Stablecoin projects and asset tokenization technologies' (Anderson's point #5) 'Crypto assets / crypto currencies' musings: "almost every tech start-up will have some sort of cryptocurrency component.[285]" Coinbase CEO Brian Armstrong leads us on a bit here, Advanced Systems Management Group / ASMG believes. Armstrong (2020) states: "Privacy will be integrated into one of the dominant [distributed ledger] chains (and/or) into a privacy coin. (Huh?) Or, into a blockchain with built-in privacy features. These privacy features – *to be* built "*in*" and designed "*in*" to the distributed ledger 'i.e. decentralized blockchain' – will eventually get mainstream adoption." And here's another controversial point Coinbase CEO Brian Armstrong made (Armstrong's point #9) which gave ASMG extreme *pause*, and may be a source of consternation to the OCC as well: "Maturation of *crypto* will bundle together exchanges, custodians, brokerages and clearing houses – i.e. these (entities) will be separated out, from a legal and regulatory point of view[286]."

Q5) 'Distributed ledger technology (DLT) for banking' – in our very first paragraph to this question's answer – Advanced Systems Management Group (ASMG) laid out a litany of issues which we feel we needed to address. To summarize our views succinctly, in one paragraph, here is a try – [Reproduced *somewhat* as it appears in Q5, although not word-for-word *herein,* but more as an *ad lib* summary] –

[284] Source: "11 Predictions for the 2020s by Coinbase CEO Brian Armstrong," By Sead Fadilpasic [online – Crypto News]. Dated: January 6, 2020. See: http://cryptonews.com.

[285] Brian Armstong's *point five* prediction for blockchain developments in the 2020's suggests: Crypto start-ups will: i) raise money using crypto; 2) utilize crypto to achieve product market *fit* by issuing tokens - to early adopters of the product - turning them into evangelists, and; 3) bring together global communities and marketplaces at a pace never seen before in traditional venture capital *start-ups* financing. See *also: Ibid*., [Foot Note # *284, 286*] *a.k.a.* prediction / point five '(Armstrong-2020) 11 Predictions for the 2020s'. See *also: Ibid*., [Foot Note # *98 – 101 inclusive*] 'Stablecoin projects and asset tokenization technologies discussion'.

[286] Brian Armstong's *point nine* prediction for blockchain developments in the 2020's argues: Maturation and evolution of the crypto market structure will happen, resembling more closely the traditional financial world, with a number of functions currently bundled into one (exchanges, custodians, brokerages, clearing houses) being separated out from a legal and regulatory point of view, which will lead the U.S. Securities and Exchange Commission (SEC) and other regulators to feel more comfortable with creating a cryptocurrency index fund for retail investors. For example, Coinbase Custody is already a separate company, while Coinbase Pro will separate into a brokerage and exchange. See*: Ibid*., [Foot Note # *284, 285*] *a.k.a.* prediction / point nine '(Armstrong-2020) 11 Predictions for the 2020s'.

"Distributed ledger technologies (DLT) are, essentially, provided in the service of the *data* supply chain. As such, it is a very large and monolithic data *supply chain*, which is located within a financial institution's walls. It serves the integration of information, handles copious amounts of machine learning (ML) analytics and algorithmic test data, training data and the algorithms' data *outputs*, and the like. Plus, data supplied from inference engines, through search efforts (knowledge discovery) and/or through the data supply chain's handling of the profundity of data forms and data formats (data -at rest, data -in redaction [or could be 'deletion'], data -in motion, or data -in storage) – however and wherever 'data' ultimately appears, or where and in what manner 'data' is configured – all headed, as theses data resources may be, to federated information libraries, or 'other' data repositories, requiring more and more critical resources to make sense of all of this."

After this quick glance at what we have already learned from our earlier set of responses to the first five questions posed by the OCC – touching upon AI and machine learning (ML) issues – Advanced Systems Management Group (ASMG) have come to a striking observation: We wish to tackle question five (Q5) 'Distributed ledger technology (DLT) for banking' *in its entirety*, by addressing five (5) issue areas where 'AI and machine learning (ML) security, governance and regulatory complexity' are writ-large:
i) Credit underwriting / Credit monitoring;
ii) Anti-Money Laundering (AML) / Fraud;
iii) Customer identity (ID) and Due Diligence;[287]
iv) Trading and Hedging monitoring, actions and activities and;
v) Forecasting / Marketing.

These five (5) represent the *What* topics which represent the foundational *focal point* for AI and machine learning (ML) advances to address. They are also somewhat bifurcated – or split – between opposing camps: the traditional, or centralized banking mainstream and the decentralized financial (DeFi) asset allocation and financial services environment.

Why is this last observation so important? The challenge *is* for regulatory authorities in the financial services realm to come up with regulatory instruments (efforts) which can not only subsume the centralized banking environment's regulatory challenges and issues, but also capture and subsume today's decentralized financial (DeFi) services environment issues and demands. This latter set of vested interests, and their economic capital, claimed by DeFi stakeholders, is placing economic demands upon which are upsetting the financial service industry's *status quo* conditions and arrangements, going forward. There are many long-established, vested, traditional banking interests which see their livelihoods under *threat* by these newly emergent DeFi stakeholders, investors and service delivery actors and agencies.

[287] ASMG addressed these two topics - point iii) *Customer identity (ID) and Due Diligence* – elsewhere in this Submission. The *first* sub-topic, Customer ID – was addressed under the heading "Identity projects." (See: Q5 'Distributed ledger technology (DLT) for banking' - sub-section: 5.2 'Identity projects'). The *second* sub-topic, 'Due Diligence' – was addressed under the heading "Customer ID / Due Diligence." (See: Q7 'AI – ML security / governance and regulatory compliance' - sub-section: 7.3 'Customer ID / Due Diligence).'

This is an extremely fluid, and highly transitional period, in which economies and economic conditions are far from certain. This is a realm which the which the OCC has no choice but to travel through, and ultimately end up at a point which delivers regulatory certitude, rules-making and rules-setting mastery and clarity.

Let's turn now to examine these five (5) AI and machine learning (ML) issue areas up close.

7.1 Credit Underwriting / Credit Monitoring

This is a topic which falls easily within the OCC's regulatory backyard. This topic is which any but the most seasoned financial analyst, or credit issuance expert, need address at their peril! With that advisory note out of the way, Advanced Systems Management Group (ASMG) will tred lightly.

Corporate debt has sky-rocketed, with more than half of investment-grade debt – corporate debt above junk status – now approaching $3 Trillion. This led noted financial analyst Scott Minerd, Guggenheim Partners, to suggest recently that: "Even seemingly sound companies are finding credit expensive or difficult to obtain.[288]" To put this $1 trillion of (corporate) investment-grade debt in perspective, heading into the 2008-2009 Great Financial Crisis (GFC), Americans – more likely with some assistance from the mortgage-originating and credit instrument-issuing lending community-at-large – carried $1.3 Trillion in outstanding subprime mortgages as the catastrophe developed, which came very close to seizing up the global economy.

In 2020, the *new* accounting standard called current expected credit losses (CECL)[289] came into effect. The current expected credit losses (CECL) regulatory regime will require banks, and other financial institutions (FIs) to assign values to loan obligations over the course of a loan's lifetime. This will more accurately account for the value of the loan on the financial institution's books, but in today's coronavirus pandemic global economic conditions, is that what we really want? Joshua Ronen, Professor (Accounting) New York University, suggests: "Paradoxically, current expected credit losses (CECL) provisions may cause loan deteriorations, on offer to corporations and small businesses, which may cripple their lending opportunities, causing an

[288] Source: "Financial System Faces Biggest Test Since 2008 as coronavirus spreads," By Alan Rappeport and Jeanna Smialek [online – New York Times]. Dated: March 9, 2020. See *also*: *Ibid*., [Foot Note # *290, 304*]. Discussion: Here's the math: $1.0 Trillion in investment-grade (corporate) debt, plus $1.2 trillion in outstanding leveraged loan (corporate) indebtedness, plus … other obligations (must get this number to $3 Trillion – c'mon, New York Times writers – you can do better than this?).

[289] Source: "US Current Expected Credit Losses (CECL) implementation guidance," Deloitte Staff, [online]. Dated: 2020. See *also*: *Ibid*., [Foot Note # *294, 295*] '(Deloitte-2020) *more* interpretations *Re*: US (CECL) implementation guidance.' Discussion: (Deloitte-2020) generally-accepted-accounting-principles (GAAP) guidelines – will their complexity be reduced – *a.k.a.* – due to the *new* CECL credit modeling functions?' See *also*: *Ibid*., [Foot Note # *296*] '(OCC) *Re*: US (CECL) implementation guidance.' See *also*: *Ibid*., [Foot Note # *297*] '(Jacobs-2019) *Re*: US (CECL) implementation guidance.'

economic *hit* upon the most strapped borrowers, since they are often over-extended, and the worst credit risk in the marketplace, as it is."[290]

A Moody's (2018)[291] summed up loan monitoring issues very effectively here: A good loan monitoring regime will quickly identify deteriorations in the borrowing entity's financial health. Today, regulators are requiring more data, faster, while ensuring that the capital (financial) offsets that credit originators offer – to monetize or insure 'loan underwriting' activities – are performed with greater due diligence than ever before. With new technological advances, financial statements may be captured by optical character recognition (OCR) and using "push" apps or application product (programming) interfaces (APIs), to read financial statements and their interpretive notes, in an automated manner. This document reading, document verification and document examination effort – through either scanned PDF files, or as non-readable PDF files or via PDF (or other) file formats subjected to optical character recognition (OCR) processing, or automated machine learning (ML) "push" apps or application product (programming) interfaces (APIs), may cause 'current expected credit losses' (CECL) regulatory provisions to be that much easier to track, monitor, and enforce.

Why it matters: Deloitte (2019) examined the European Community's (EC's) Single Supervisory Mechanism (SSM)[292] to good effect. The lessons learned in that region may prove helpful to our discussion, examining the US's 'current expected credit losses' (CECL) provisions. What the European Community (EC) attempted with the (EC's) Single Supervisory Mechanism (SSM) was a wholesale *shift* towards placing the regulatory focus back on banking's "lending" core. This was in response, partially we suspect, to Europe's aversion that a repeat of the subprime mortgage crisis ever find its re-occurrence. Deloitte's (2019) review of the EU's Single Supervisory Mechanism (SSM), states that the European Central Bank (ECB) were very concerned about the high-level incidence of Non-Performing Exposures (NPE's) across the region.

Non-Performing Exposures (NPE's – European Central Bank terminology) are credit issuing situations in which lending contracts, or other counterparty exposures – that are problematic, in the sense of unexpectedly deviating from contractual cash flows due to counterparty

[290] Source: "Financial System Faces Biggest Test Since 2008 as coronavirus spreads," By Alan Rappeport and Jeanna Smialek [online – New York Times]. Dated: March 9, 2020 – Quoting Professor Joshua Ronen, NY University. See *also*: *Ibid*., [Foot Note # *288, 304*] '(Rappeport/Smialek-2020) "(CECL) more accurately measures corporation loan / loss provisions.'

[291] Source: "Redefining loan monitoring through an integrated solution," by Moody's Analytics [online]. Dated: November 2018. See: moodysanalytics.com.

[292] The Single Supervisory Mechanism (SSM) has final supervisory authority over banks in the EU, while national supervisors act in a supporting role. The European Central Bank (ECB) works in conjunction with the Single Supervisory Mechanism (SSM) to conduct stress tests on financial institutions (FIs), and take early interventions as the situation dictates. These interventions may include setting capital or risk limits on operations, or by requiring changes in management. A total of 122 banks are being supervise directly by the ECB, representing approximately eighty-two (82) per cent of banking assets in the region. All other banks not scheduled to be regulated under the Single Supervisory Mechanism (SSM) regime authority - more than six thousand (6,000) in the Eurozone alone – will be supervised by their respective national supervisors.

behavior – may require the Single Supervisory Mechanism (SSM) to step in, and review industry credit and lending loan obligations and practices. The goal of the EC's Single Supervisory Mechanism (SSM) review exercise *is* to monitor and prevent surges in new Non-Performing Exposures (NPE), thus causing increased, possibly non-performing lending contract *flows* to multiply.

Each bank surveyed by the Single Supervisory Mechanism (SSM) regulatory supervisory authority was tasked with aligning their risk pricing to their Significant Increase in Credit Risk (SICR) scores. The Significant Increase in Credit Risk (SICR) scores would reflect *adjusted performance* measures, such as: Return-On-Risk Adjusted Capital (RORAC), Risk-Adjusted Return-On Capital (RAROC) and Economic Value- Added (EVA) measures, driven by each bank's individually-calculated risk appetite. By monitoring in this manner, the (EC's) Single Supervisory Mechanism (SSM) sought specific key warning flags to be created and/or adopted as 'alerts' to raise awareness of actions or activities which may prove deleterious at the *cluster* Customer *level*.[293] These key risk indicators include: Loan to Value (LTV), Debt Service to Income (DSI), and Debt Service Coverage (DSC). The EC's Single Supervisory Mechanism (SSM) documentation suggests credit risk should be *cascaded* down to the organization's business lines. This provides a rationale for inclusion / exclusion of risks (and risk classes), placing them into the *corporate* Risk Appetite Framework (RAF).

Deloitte (2020)[294] states: "The adoption of the current expected credit losses (CECL) standard will likely affect internal controls and the need for data not previously used for financial recording purposes, *a.k.a.* Covid-19 economic factors, which will be major disruptors to financial stability." Is the industry prepared? Deloitte (2020) continuing: "The *new* current expected credit losses (CECL) standard is also expected to reduce the complexity of US generally-accepted-accounting-principles (GAAP) guidelines, by decreasing the number of credit loss models that entities can use to account for debt instrument commitments.[295]

Continuing with Deloitte's (2020) take on things, "Current expected credit losses (CECL) standards will affect *all* entities holding loans, debt securities, trade receivables, and off-balance sheet credit exposures and promises to be one of the most significant accounting projects of the next five years. It has many governance, modeling, credit analysis, information technology, and reporting interdependencies for all to answer." Perhaps recognizing this fact ahead of time, the OCC have published a methodology and workbook to explain how

[293] Source: "Credit Underwriting and Monitoring: The increased regulatory focus on credit life-cycles," authored by Deloitte (Athens) Greece office [online]. Dated: October 14, 2019. See: ww2.deloitte.com. Discussion: The Deloitte (Athens, Greece) authors suggest: "The EC's Single Supervisory Mechanism (SSM) documentation calls for 'Back-tested leading metrics, covenant compliance, and other monitoring activities,' [which] will result in the 'embedding of *early warning indicators'* in processes."
[294] Source: "US Current Expected Credit Losses (CECL) implementation guidance," Deloitte Staff, [online]. Dated: 2020. See *also*: *Ibid*., [Foot Note # *289, 295*].
[295] Source: "US Current Expected Credit Losses (CECL) implementation guidance," Deloitte Staff, [online]. Dated: 2020. See *also*: *Ibid*., [Foot Note # *289, 294*].

everything works. Plus, the OCC began hosting seminars in 2017, and published a full list of related links and resources.[296]

Accounting Today (2019) recently wrote: "By moving credit loss modeling to the lifetime of the loan's duration, the availability and quality of data, and segmentation and granularity of financial instrument data that share similar risk characteristics – including payment status, internal or external credit score, risk rating or risk classification determinations, financial asset type, collateral type, asset size, effective interest rate terms, geographic location, industry of borrower and borrower's vintage, etc. – among other topics, are all under the "lens" of current expected credit losses (CECL) provisions." Continuing: "For example, current expected credit losses (CECL) nodes and methodologies would include: i) loss rate ii) discounted cash flows iii) vintage analysis iv) probability of default/loss-given defaults v) provision matrices, and vi) regression analysis."[297]

"Companies," Accounting Today (2019) adds "auditors, and regulators are expected to observe current expected credit losses (CECL's) impacts, (to) verify the regime's report summaries and reporting commentaries and (its) interpretive notes, and make appropriate disclosures (or the OCC receives those disclosures) during the 2020 financial reporting year."

Advanced Systems Management Group (ASMG) were a bit stymied by all of this! We turned to an authority on the topic, in our effort to try to come to grips with the 'data management' and 'technology' side of how the current expected credit losses (CECL) regime might work. We found Tom Kimmer's (SAS-2020) comments extremely helpful: "There are a few data management and technology discrepancies which need to be effectively handled. They are, for example point ii) [raised by Accounting Today *a.k.a.*] '(discounted) cash flows' – cash flow modeling requires integration of data from both risk management and financial management perspectives, to capture accurately the model losses, and payment streams data, e.g. '*cash flows.*' However, this data is frequently housed in different systems. Plus, different systems have different data definitions, and are populated at different times, and have varying – maybe even conflicting, or out-of-sync – levels of detail. Dealing with missing, or incomplete, data – or if third-party 'publicly available' industry data is introduced into the current expected credit losses (CECL) data modeling efforts – this activity raises new issues of data definition accuracy and completeness, as data generated across data silos or originating in different data repositories, may have to be scrupulously checked for its accuracy."

Kimmer (SAS-2020) also points out that: Banks that have process silos, have trouble assembling a comprehensive view of the required data for current expected credit losses (CECL) analysis and review. Kimmer (2020) suggests adopting a centralized model library, a common data platform, centralized workflows, dynamic reporting capabilities, audit supervisory frameworks,

[296] Source: "Current expected credit losses (CECL) Methodology," By OCC Staff [online – occ.treas.gov]. Dated: May 8, 2020. See *also*: *Ibid*., [Foot Note # *289*].
[297] Source: "Voices – CECL standard expected to make a major impact," By Jonathan Jacobs, Jennifer Press and John Schrader [online-accounting-today]. Dated: November 12, 2019.

and robust governance and security controls, to reach "fully" current expected credit losses (CECL)-compliant status.[298]

Then again, Advanced Systems Management Group (ASMG) wonders, what about the big (and not-so-big) financial firms outside the banking sector's oversight mandate, which included asset managers, hedge funds[299] and big insurers[300]? Plus, what about the newly emergent on-line credit and lending platforms?

One thing that is not totally clear to us, is how *all* the 'edge players'[301] – Big Tech, FinTechs and newer lending platforms, e.g. smaller-to-medium-sized online-lenders, such as Prosper[302] and SoFi[303] – will fare, with their current expected credit losses (CECL)-compliant status? Each of these examples raise flags for regulatory agencies to look at.

Prosper, in what they call the Prosper Marketplace, operates a business-to-business (B2B) loan portfolio. Prosper Marketplace closed a deal in February 2017 with a consortium of institutional investors to purchase up to $5 billion of loans through the lender over the following 24 months. The deal included warrants to purchase thirty-five (35) per cent of the lender's equity, highlighting its desire to secure long-term funding.

---

[298] Source: "CECL: Are US banks ready? By Tom Kimmer, SAS. [online]. Dated: 2020. See: https://www.sas.com/en_sa/insights/articles/risk-fraud/cecl-are-us-banks-ready.html.
'(Kimmer-SAS 2020) CECL-compliant list of technological inputs, data systems and data process reporting tools and toolkit items.'

[299] The Department of the Treasury – OCC; Federal Reserve (Bank); Federal Deposit Insurance Corporation; and the Securities Exchange Commission 'amended regulations' implementing 'section 13 [revisions]' of the Bank Holding Company Act (BHC Act) re: the *new* amendment(s) lifted the section containing reference to restrictions placed on banking entities / non-banking Financial Institutions (FIs) or Companies - from engaging in proprietary trading and having certain interests in, or relationships with, a hedge fund or private equity fund's - "covered" funds. (The BlackRock exemption "anyone?"). Source: "BlackRock Authored the Bailout Plan Before There Was a Crisis – Now It's Been Hired by three Central Banks to Implement the Plan," By Pam Martens and Russ Martens, Wall Street on Parade [online]. Dated: June 5, 2020. See: https://wallstreetonparade.com/2020/06/blackrock-authored-the-bailout-plan-before-there-was-a-crisis-now-its-been-hired-by-three-central-banks-to-implement-the-plan/. See *also*: *Ibid*., [Foot Note # *463*] 'BlackRock enters full-fledged economic advisory participatory role *a.k.a.* Coronavirus pandemic Crisis support financing on behalf of the US Federal Reserve'.

[300] Source: "How Insurers Will Be Impacted by FASBs CECL Standard," By BDO (US) Staff, [online – bdo.com]. Dated: December 19, 2019.

[301] Source: "Beyond FinTech: A Pragmatic Assessment of Disruptive Potential in Financial Services- sub-section -3.4 'Lending'," By R. Jesse McWaters, WEF-Forum, and Rob Galaski, Deloitte, [online – WEF-Forum]. Page 115, 121, 123. Dated: August 2017. See *also*: *Ibid*., [Foot Note # *302*, and *quoted* in *303*].

[302] Source: "Prosper Inks $5 Billion Loan-Buying Deal with Investors Including Soros and Jefferies," By Staff writers [online – Wall Street Journal]. Dated: 2020. See: [Quoted in] *Ibid*., [Foot Note # *288*] '(McWaters/Galaski-2019) online-lenders – are we regulated?' See *also*: *Ibid*., [Foot Note # *301, 302*].

[303] Source: SoFi [copies a UK online vendor - Zopa's - business to business (B2B) lending model]: "Zopa raises $41.2 million for challenger bank launch," By Staff writers, [online – CNBC]. Dated 2020. See: [Quoted in] *Ibid*., [Foot Note # *301, 302*] '(McWaters/Galaski-2019) online-lenders – are we regulated?'.

SoFi, a major US online lender focused on student loans, applied for a banking license in June 2017 to diversify funding. The move comes after similar actions by several other major lenders, including Zopa – the United Kingdom's first online lender had set the stage by applying to become a challenger bank – in the UK.

With the rise in these online lending platforms, in the business-to-business (B2B) and business-to-community (B2C) lending space, this raises the risk that a "single-point-of-failure," may one day play havoc with the *prospective* introduction of *new*, conflicted systemic risk(s), introduced sight unseen, into the credit and loans marketplace. Is this something regulatory authorities need to keep an eye out for? Secondly, the expansion of non-financial firms, or pseudo-financial firms, in this controversial business-to-business (B2B) and business- to-community (B2C) lending *space*, should not – Advanced Systems Management Group (ASMG) questions – be allowed to return us to 'the wild-west days of the 1990s,' when retailers extended credits and loans to all manner of applicants, virtually unregulated and unmonitored.

Returning now to the New York University Accounting Professor's earlier observations, suggesting that the US current expected credit losses (CECL) provisions might negatively impact a loan's value over its lifetime – a measure which the CECL was attempting to circumvent – may not prove so wise in the context of today's Covid-19 fiscal environment. In short, CECL provisions may have inadvertently – in Professor Ronen's estimation – served up a slate in which a Lender's loan losses (provisions) are pushed so far negative, that as the economy is worsening, this may dissuade Lenders' from extending loan arrangements to corporations they were previously unhesitant to lend to. Not to stress the obvious here, any removal of current lines-of-credit, some of which were undoubtedly granted or issued (or extended) under terms met in the pre-Covid-19 economy, may have to be reset, but at what cost? To risk a catastrophic, industry-wide, lending crisis?

One recommendation floating around – to stem what we saw in an earlier era with derivative-generated losses incurred by banks (and others) during the Great Financial Crisis (GFC) – in which deleterious runs on credit availability were inflicted widely across the economy – might be worth revisiting today. We simply don't know, nor will ASMG speculate on this any further. But the solution some experts are telling us, is to involve the reintroduction of some form of credit funding – in which banks and financial institutions (FIs) would be able to invest in credit funds[304] – and sponsor, or take ownership stakes, in venture capital funds, which *might* pool ultra-rich investors' money to bet (invest in) what we hope would be economically rewarding business 'startups' *a.k.a.* business re-openings.

The Bank Policy Institute, a lobbying group representing Big Banks – which include Bank of America, JP Morgan, Wells Fargo and Citigroup – are anxious that lenders, such as themselves,

[304] Source: "Financial System Faces Biggest Test Since 2008 as coronavirus spreads," By Alan Rappeport and Jeanna Smialek [online – New York Times]. Dated: March 9, 2020. See *also*: *Ibid*., [Foot Note # 288, *290*].

in the words of JP Morgan's spokesperson Andrew Gray, "[The Bank (JP Morgan)] stands by efforts by [our} regulators to *help lenders* freely, fairly, better serve their customers – but this issue is up to regulators.[305]" The next day, March 4, 2020, the Federal Reserve moved to simplify capital rules, introducing changes to combine capital requirements determined by stress tests, and (*introduced*) a separate set of requirements.[306]"

Let's cut to the chase: Those *separate set of requirements* are the 'streamlined capital rules'. During the Great Financial Crisis (GFC – 2008-2009) banks and financial institutions (FIs) pursued investments in credit funds, by sponsoring or taking ownership stakes in venture capital funds, which *might* pool ultra-rich investors' money to bet on startups. That was then.

Today, in the pandemic-fueled crisis conditions of Covid-19, this methodology – the 'streamlined capital rules' – have been applied in a quantitative-easing type of funding mechanism. The Federal Reserve were not – in any way, shape or form – interested in making investment bets on startups. They had a vastly more purposeful goal in mind. That goal was to unabashedly assist the Federal Reserve provide a type of quantitative-easing *toolkit* mechanism, solution or financial vehicle – to ease the strain on the financial system – teetering under global pandemic closure conditions. And the Federal Reserve pursued this quantitative-easing type of solution – via 'streamlined capital rules' a.k.a. [risk reduction alleviation] – being its sole mission or purpose.[307] No criticism intended, from these quarters, as the means were more than justified by the Federal Reserve's quick-witted methodological action.

7.2 Anti-Money Laundering (AML) / Fraud

McKinsey (2016) state that risk management in banking has transformed itself substantially, since the 2008-2009 Great Financial Crisis (GFC). The transformation includes McKinsey's projection that by the year 2025, the number of analytics professionals working in Financial Institutions (FIs) will be ten (10) to twenty-five (25) per cent greater in every large Financial Institution (FI). Much of the impetus is due to compensations made to monitor and track increased levels of money laundering, sanctions busting, financing of terrorism and fraud.[308]

Banks are motivated to institute strict Anti-Money Laundering (AML) / Fraud protections, since they will not sacrifice the security of financial transactions on their watch. Customer expectations are ever mindful of seamless conduct, by banking and financial institutions (FIs), or

[305] Source: "Big Banks want regulation eased because of coronavirus – Experts call it opportunistic," By Renai Merie, [online – The Washington Post]. Dated: March 3, 2020.
[306] Source: "The Fed Simplifies Capital Rules, a Change Sought by Big Banks," By Jeanna Smialek, [online -New York Times). Dated: March 4, 2020.
[307] See: Q 10. 'What other changes need OCC address,' for an *in-depth* discussion of this topic.
[308] Source: "The Risk Revolution," By Kevin Buehler, Andrew Freeman and Ron Halme, McKinsey Insights [online]. Dated: 2016. See *also*: *Ibid*., [Foot Note # *312*]. Source: "The Future of Bank Risk Management," By Philip Harle, A. Harvas, A. Kremer, *et. al*., McKinsey Working Papers on Risk [online - McKinsey Insights]. Dated July 22, 2016. See *also*: *Ibid*., [Foot Note # *310*].

any other Third-Party financial intermediaries – including any transacting parties deploying automation solutions – since every banking customer has an elevated expectation of one thing, and one thing only: their banking activities must be conducted in a 'zero-failures, no-compromise' mode of services delivery.

Here is an example of a prodigious, expert use of automation: the UK and US FinTech Company Kabbage, collects financial transactions information from PayPal, Amazon and eBay trading platform 'information and data repository sources,' and from United Parcel Service (UPS) trading shipment volumes, recorded on the UPS transaction processing platform. This Big Data library of statistics, coupled with machine learning (ML) analytics-generated data *outputs*, is meticulously applied by the Kabbage Company's AI and ML platform to identifying anti-money laundering (AML) and Fraud detection incidences, then should any be detected or identified, 'early warning signal' notifications are applied immediately.

Why it matters: Can banks obtain regulatory – and Customer – approvals for machine learning (ML) and AI modeled algorithmic *outputs*, that use social media outlet data, and (possible) other data sources, in their virtual monitoring activities conducted online? This is not a trivial issue! Nor can it be answered without deep appreciation of the merits of the technology presented. One exposure from this data collection can seriously risk an institution's risk management *alignment* exercise, which many financial institutions practice in an 'always "on," [no downtime] 24-7 manner.' A financial institution (FI) cannot play fast and loose with data privacy and data protection issues. The technology the financial institution (FI) deploys must be fool-proof, as well.

A second issue we are witnessing today is the increasing dependence on business modeling which requires that risk managers understand, and manage, AI and machine learning (ML) modeling and inference engine processes, procedures, and their usage of data – all data – whether it be test data, training data, etc. at an unassailably proficient level of processing comprehension and understanding. It is not enough to have someone write the code, the business mangers themselves must understand how that code works, how it processes information (data), and its overall 'code of (operational) conduct.' This proficiency must extend to cover any/all operational modifications or alterations to the Banking Line-of-Business (L-o-B), through its interstices or application programming (product) interfaces (Aps), networking nodes etc. It all comes together to support AI and machine learning's (ML's) algorithms' code base, internal workings, including supporting apps, test data, training data etc. This functional knowledge must be maintained in a continuous-learning manner, across the organization, and be performed better than competitors (or industry peers) to shore up and maintain information advantage.[309] This second challenge – proficiency and mastery of algorithmic modeling – also extends to covering data quality issues, particularly the tricky handling of *unstructured* data.

[309] See: *Ibid.*, [Foot Note # *2*} '(ACPR-Banque de France) AI and machine learning (ML) algorithms' code base, internal workings, including apps, test data, training data (etc.) continuous learning.'

Currently, the data which most banks use for their operations is neatly arranged in tables, but there is a wealth of information that could boost client services dramatically. This information, termed *unstructured data*, may be found in: e-mails, phone communications or, is floating around in social media. Retrieving insights from these types of documents is impossible *without AI*, which can understand patterns and create responses to data, better than human agency.

The goal is to become paperless – although most large financial institutions (FIs) have been less paper-focused for some time now. By emphasizing digital data, and digital data holdings, and/or collecting data and information via optical character recognition (OCR) scanning, or other means – such as using "push" apps or application product (programming) interfaces (APIs), to read financial statements and their interpretive notes, in an automated manner, to cite but one example – is the wave of the future for financial institutions' (FIs') data management efforts. In short, data must be readily *searchable* and *actionable*. And those search activities may include data queuing, and data 'search' querying (or data 'search' retrieval) activities which need to be integrated into an enterprise-wide data management master plan.

Consequences in the future: McKinsey (2016)[310] suggest there is a significant downward pressure on bank's business models, with all these AI and machine learning (ML) inference engines, apps and machine learning (ML) modeling advances, which are straining operational budgets. The most effective response to this may be to: try an enterprise-wide data management master plan which has 'simplification, standardization and digitization' as its primary goals and objectives.

In Appendix B – Advanced Systems Management Group (ASMG) present a suggested Privacy-Enhancing Technology (PET) pilot – a pilot which addresses both the data privacy and data protections issues succinctly, which may also serve as a compelling argument to meet the digitization challenge head-on. This Privacy-Enhancing Technology (PET) pilot[311] may be pursued by banks, and their financial sector regulatory supervisory authorities, today.

---

[310] Source: "Corporate finance, capital markets, securities services," By McKinsey *internal* analysis. See *also*: "The Risk Revolution," By Kevin Buehler, Andrew Freeman and Ron Halme, McKinsey Insights [online]. Dated: 2016. See: *Ibid*., [Foot Note # *308*]. See *also*: "The Future of Bank Risk Management," By Philip Harle, A. Harvas, A. Kremer, *et. al*., McKinsey Working Papers on Risk [online - McKinsey Insights]. Dated July 22, 2016 - *a.k.a. Ibid*., [Foot Note # *308,*] '(McKinsey-2016) Risk Management – *try* an enterprise-wide data management master plan with 'simplification, standardization and digitization.'

[311] See: Appendix B – *a.k.a.* DS-08-2017 "Privacy, Data Protection and Digital Identities," Horizon 2020 Work Programme 2016-2017 'Secure societies – protecting freedom and security of Europe' [/Page 76] – ASMG's hypothetical submission (not submitted nor acted upon). ASMG's GDPR Privacy-Enhancing Technology (PET) *project* would have addressed the 'issue of privacy, data protection, and digital identities' as follows: i) Privacy violations caused by search engine identity exposures; ii) Responsible information sharing iii) Protecting *on-line* identities from cyberthreats, both in the public and private sphere iv) [ASMG's] (PET) Privacy-enhancing Technologies solution *a.k.a.* data-centric security (DCS) with usability, accessibility and safeguarding features *built-in* v) Open source and externally auditable vi) Leverage identity-based solutions vii) Reduce identity fraud / protecting citizen's privacy viii) Extended impacts ix) Data protection embedded in data governance.

7.3 Customer ID / Due Diligence

The OCC may have noted, if you have examined the foot notes carefully to Appendix B [See: Foot Note # 311] that Advanced Systems Management Group (ASMG) side-stepped the "Customer identity (ID) and Due Diligence" issue, in our Privacy-Enhancing Technology (PET) funding *proposal* submission documentation. The explanation for this is that by reducing human intervention – and tying risks to specific business (and regulatory) break points – is one thing, instituting a comprehensive Identity project (ID) globally across enterprises and institutions, is quite another, more dramatically comprehensive and far-sweeping a challenge to address. A strong automated framework for providing, and proving, a citizen's ID, is what the globe needs. Getting there, in practical terms?

Why it matters: ASMG believes the following point to be foundational: "let's take the *data ID* and protect it." This will provide a huge boost to regulatory agency fortunes. It will also allow the regulatory process to remove any doubts about a data set's full data life-cycle, and will also serve a very important role to rebuff threat vector attacks, on data repositories or data holdings. Data hacking is a constant worry for all organizations, as potential or prospective data leakage, data left or data hacking incidences oftentimes occur below the horizon, and may be virtually undetected for months and months on end. To deter this from happening, Advanced Systems Management Group (ASMG) advise a Joint Task Force Team of subject-matter-experts (SMEs) be formed, with Team members already available within your (and our) organizations. These subject-matter-experts (SMEs) must be brought together and tasked with focusing attention *collectively* on advanced data management issues.

McKinsey (2016) state:[312] "Digitization of risk functions – including early warning systems featuring *quality* data reporting, focusing on high-performing Information Technology / Information Management (IT/IM) enterprise architectures and data resource management Infrastructure components, is achievable. Let's review two terms which are frustratingly overdue for our consideration: the terms are '*logging*' and '*auditing*'. Logging refers most often to program level events, such as administrative actions and abnormal related events, that technical staff use for 'debugging' software programs. This identifies system problems before they are big enough to cause harm, such as system outages or failures, which can greatly hamper an institutions' productivity. Auditing most often refers to user-level transactions, such as 'change to a financial record that was made by e.g. "Joe Smith at 10:00 am on December 21, 2019." Most solutions have separate sets of logs that are maintained currently, including by cloud (platform) service providers (CSPs). For example, Google's Cloud Solution maintains an administrator activity log which tracks application product (programming) interfaces (APIs) via

[312] Source: "Corporate finance, capital markets, securities services," By McKinsey *internal* analysis. See *also*: *Ibid*., [Foot Note # *310*]. See *also*: "The Risk Revolution," By Kevin Buehler, Andrew Freeman and Ron Halme, McKinsey Insights [online]. Dated: 2016. See *also*: *Ibid*., [Foot Note # *310*]. '(McKinsey 2016) – increased regulatory tracking of money laundering, sanctions busting, financing of terrorism and fraud.'

'calls' and 'changes' to configurations, and a data access log that records and updated (or changes) information re: user-provided data[313].

Due Diligence Review (DDR) is a process, whereby an individual or an organization, seeks sufficient information about a business entity to reach an informed judgment as to its value for a specific purpose. Due Diligence Review (DDR) is not, by itself, an audit. It is much broader than an audit, and is business oriented – rather than accounting oriented. Due Diligence Review (DDR) is determined in consultation with the client. It is not confined to financial due diligence, but extends to operational due diligence, market due diligence, technical due diligence, legal due diligence, systems due diligence, etc. All these factors, or issues, form an integral part of the overall due diligence exercise. A Due Diligence Review (DDR)[314] should normally cover the following:

1. Titles & ownership.
2. Various Government consents/licenses.
3. Correctness and completeness of all information supplied.
4. Product/service warranties, damages and other claims.
5. Contingent liabilities.
6. Recoverability of all current assets.
7. Registration of Intellectual properties.
8. Employee benefit plans.
9. Litigation/appeals, etc.
10. Non-contravention of regulation, loan covenants, contracts terms, etc.

We can do McKinsey – and all the other experts one better – and implement a complete, robust data-centric security (DCS) solution, and do so in record time. Plus, it will meet all the Due Diligence Review (DDR) audit criteria we have just outlined.

Consequences in the future: McKinsey (2016) don't say it, but ASMG will: *secure* data, then the regulatory '*mix* and *fix*' follows without delay. This will ensure the regulatory process *drives* the financial health and welfare of both the financial institutions' (FIs) interests, and will hugely benefit the fiduciary tracking performance – by regulatory bodies – tasked with protecting banking and investment management organizations, the consumer, and the functioning of our economy, when it all is viewed from one unified program stance.

[313] Source: "Audit Trails: Managing the Who, What, and When of Business Transactions," By Irith Gillath, Syslink SAP Management Solutions (vendor), [online – smartsheet.com]. Dated: 2020.
[314] Source: "Due Diligence Referencer (correct spelling *Indo-Anglais*)," By Bombay Chartered Accountants Society [online]. Dated: 2015-2016. See: https://www.bcasonline.org/Referencer2015-16/Accounting%20&%20Auditing/due_diligence_review.html.

7.4 Trading / Hedging

For this sub-section, re: Trading / Hedging,[315] there are several key banking and financial institution (FI) Lines-of-Business (L-o-B) Data Domain issues under consideration. They are:
i) How will that Financial Institution's (FI's) Lines-of-Business (L-o-B) Data Domain – under consideration – *mesh* with other information domains?
ii) How will increasing exposure to one type of asset in a portfolio – at 'x' amount – affect key financial ratios?
iii) Can a system alert, drawing Users attention to queries / information request-response [answers] – which those Users should be asking themselves – be made within a trading and hedging technologically-secured trading platform delivery model, providing notifications via: **a**) screen-generating graphic user interfaces (GUIs) **b**) intelligent *push* apps – or – **c**) email, chat or chat-bot [automated] alerting mechanisms or systems?

Here is an example: Why has 'such-and-such' a topic been raised by a *central bank* prodding us (institutionally) for information about 'such-and-such' an issue, requiring our resolutions to be identified, deliberated upon, and implemented *almost* immediately?

First, some preliminaries to respond to, before we pull together every facet of this answer, and weave it together.

Trading and hedging activities are sliding sideways today, at an accelerated pace, into low-interest bearing territory. Or, they are valiantly attempting to maintain their position as low-interest-bearing investments, in today's high-risk trading environment. Governments are feeling the pressure, as trading and hedging need a constant vigilance to ensure they do not develop unwanted anomalies in their performance and volatility measures, and investment portfolio management safeguarding efforts are always necessary, and always in need of review as the fiscal environmental landscape adapts and changes. Banks, McKinsey (2016) tells us, will be closely examined for trading / hedging information asymmetries. Banks advice to their investor Clients will be closely examined, to ensure transparency of recommendations on trading information, and that all trading and hedging actions are rigorously executed in the way that all parties and counterparties expect the transactions to occur.

Should cross-boundary, or cross-subsidizing between banking products occur, this will be attentively examined by regulatory authorities, as well. No party or counterparty wants a repeat of the sub-prime lending situation which caused the 2008 Great Financial Crisis (GFC) to occur. The technology means to track all of this, and ensure regulatory compliance is seamlessly and affordably managed, is easily within reach.

[315] Hedging was not examined *per se* in this question's answer. See: Q7) 'AI / ML modeling Issues' answer. ASMG chose to examine the globally-inspired (and globally-influencing) US hedge fund industry, separately, in our answer presented as Q10) 'Other regulatory actions'. Examples of hedging - as a beneficiary to AI / machine learning (ML) modeling - were not within our area of subject matter expertise – allowing us to take a pass on providing further comment on this topic.

Advanced Systems Management Group (ASMG) have evaluated a Big 5 Canadian bank's specific trading platform, called Trafinas. This example – and there are numerous others on the market today – we will analyze briefly, in a moment.

First, a traditional trading system consists primarily of two blocks – one block that receives the market data. The other block – sends the trading order request to the exchange. For algorithmic trading, there are three (3) components: 1) the exchange; 2) the server, and; 3) the application. The data is analyzed by component #3 – the application. Trading strategies are fed from the user and are viewable on a graphic user interface (GUI), once a trading order is authorized / implemented. After authorization and trade conduct is completed, the trade information is sent to an order management system.

Sell-side marketers of trade activities need to express trades (with / without algorithm modeling assists) to 'drop' the trading information into their "buy -side" counterparty's order-entry system, and be ready to trade without constant coding (customization) on *new* order-entry screens, each time a trade sequence – or trading action – is conducted or required. The industry standard for trade order processing was set by the Financial Information Exchange (FIX) for XML, called FIX Algorithmic Trading Definition Language (FIXatdl) version 1.1, released March 2010.

Now let's examine the Trafinas trading reconciliation platform, one vendor's robotic process automation (RPA) solution to trade finance. Trafinas uses optical character recognition (OCR), and natural language processing (NLP) tools, to taking "screened" data and then applies rules and advanced analytics to the assembled trading data sets. Trafinas creates a configurable workflow of the process within its application. Next, Trafinas orders an audit trail of the sequence of events followed. This case management approach to monitoring and recording trading activities is accomplished as a microservices offering. Trafinas easily integrates with existing Client portals and trade finance "core" banking back-office systems.[316] Most often, software such as Trafinas will require the migration of data from an existing (legacy) system to a new system.

Why it matters: Data needs to be secured, before transport, to ensure it came from where it was supposed to originate. Also, determinations need to be made that there has been no tampering with information on the trade, or that trade's contingent 'status,' at the data / metadata level, and that no key elements of the data set for the trade have been tampered with or compromised, or even id data fragments – or disconnected sets of data respective (or

[316] Source: https://www.conpend.com/cgi-partners-with-scotiabank-on-intelligent-process-automation-proof-of-concept-for-trade-finance-transactions/ *a.k.a. Ibid*., [Foot Note # *379, 380, 381*] '(Conpend-Trafinas) ScotiaBank Trade Finance trading platform.' See *also*: https://appsource.microsoft.com/en-us/product/web-apps/conpend.trafinas2 *a.k.a. Ibid*., [Foot Note # *379, 380, 381*] '(Trafinas / ScotiaBank) modular, micro-service-based Trade Finance infrastructure, supporting existing Client Portals and Trade Finance, and Core Banking back office systems.' Discussion: The successful interaction of banks globally, is a basic prerequisite for secure and transparent processing of trade finance activities via trading platforms.

irrespective) of the trading occurrence – have been left behind. During the implementation phase, the project Team implementing a trading reconciliation platform such as Trafinas, must continue to verify the integrity of the data, assembled and kept together, which may potentially involve Third Party assists to moderate and ensure requirements are met.

Consequences in the future: Regulatory compliance is multi-faceted, and employs (sometimes) more than one regulatory organization or agency, in the supervising and monitoring of trading / hedging actions. The Volker Rule (Dodd-Frank) involved the Federal Reserve, Commodities and Futures Trading Commission (CFTC), OCC and the Securities and Exchange Commission (SEC) in the shepherding of the Dodd-Frank Act into law. OCC are no strangers to data integrity issues, and the OCC's work in this area is, undoubtedly an ongoing, and continual effort. We applaud your efforts.

7.5 Forecasting / Marketing

A very dramatic headline appeared in a Forbes publication on April 19, 2020 declaring: "Google, Facebook and Apple Need to Kill Blockchain." The journalist went on to list all manner of disasters soon to rain down upon Google and Facebook's cash cows – ad revenues. Apple's demise? Surely not the drop-off in sales of smart phones, as budget alternatives begin to crowd our one of the greatest money-makers of all times, the iPhone? The rest of the Forbes article, fortunately or unfortunately, was a bit of a dead-letter: Facebook's launch of Libra crypto currency (non-starter); Apple's efforts to expand their own credit card (anyone here of this, lately?), and; Google's 'smart debit card'.[317]

What the previous comments do introduce, truth be told, is the all-powerful ability of the 'origination and sales' process to captivate, and hold hostage, a consumer audience. Need an example of this? Try – AirBnB, Booking.com, or Uber!
Forecasting and Marketing are activities, taken together, generate significant revenue streams within a nation's economy. Today, rafts of stakeholders are involved with managing each purchase a consumer makes. Consumers are increasingly overwhelmed, and often feel more paralyzed than empowered. Sixty-five (65) per cent of customers – contacted by Toma *et. al.,* (2017) – claim they spent as much time as they'd expected to need for the entire purchase just getting ready to speak with a sales rep.[318]

Into this whole milieu, let's situate traditional banking. McKinsey (2016) suggests that banks will probably be closely examined for: information asymmetries, barriers erected to disallow (Customers') bank switching, activity monitoring *a.k.a.* inappropriate or incomprehensible advice on banking products and banking services, offered to banking Customers', and non-

[317] Source: "Google, Facebook and Apple Need to Kill Blockchain," By Billy Bainbrough [online – Forbes]. Dated: April 19, 2020. See: forbes.com.
[318] Source: "The New Sales Imperative," By Nicholas Toman, *et. al.,* [online – Harvard Business Review]. Dated: March - April 2017 *issue.*

transparent or unnecessarily complex product features and product (and service) pricing structures which confuse or defeat normal banking interactions or defeat the 'trust' relationship all banks seek to protect with their Client population.

The *new* FinTechs, or even *newer* crypto asset financial service entities, with the latter's deterministic pursuit of decentralized data paths, are moving to monetize everything they do in a bewildering array of revolutionary product configurations. These financial service entities – BigTech, Fintech or distributed finance (DeFi) crypto asset providers – don't want to replace banks, but they do wish to tap into the most lucrative part of the financial service value chain: 'origination and sales'. In 2014, these activities accounted for almost sixty (60) per cent of the banking sectors' profits. They also earned banks an attractive twenty-two (22) per cent return on earnings (ROE), much higher than the gains they received from the provision of balance sheet and fulfilment.[319]

Why it matters: Will the proliferation of new technological advances, providing cheaper, faster computing power and data storage, or even more advanced processing improvements – portend an acceptance – by Consumers – of better risk-taking decision-support efforts, lead to the realization that both sides of the financial sector *dichotomy of interests* (traditional / centralized *versus* distributed ledger / decentralized finance or DeFi) may really have the same goals and interests at heart? McKinsey (2016) reports: "Accessing external unstructured data offers substantial upside, not only for better credit-risk decision, but also for portfolio monitoring and early warning notifications. Machine learning (ML) identifies complex, non-linear patterns in large data sets, and makes more accurate risk models possible. These models learn via every bit of new information they acquire, which improves their predictive powers over time.[320]"

Consequences in the future: All is not rosy under those tinted glasses, McKinsey! For one, ML models have been dissected thoroughly by the ACPR Report authors.[321] Secondly, this whole issue of conducting a financial industry 'forecasting - marketing services' review, needs to be weighed against the benefits of supporting both sides on the '*dichotomy of interests'* equation. Advanced Systems Management Group (ASMG) might agree that the most effective way to do this is to follow the data, make the data 'known' and make the data 'secure.' The data-centric security (DCS) solution advances the goal that data is the product, and the beneficiaries of secure data is an inheritance for all. This may be the effective path to take – mapping out (and

---

319 Source: "Corporate finance, capital markets, securities services," By McKinsey internal analysis. See also: "The Risk Revolution," By Kevin Buehler, Andrew Freeman and Ron Halme, McKinsey Insights [online]. Dated: 2016. See *also*: [Foot Note # *320*].

320 Source: "Corporate finance, capital markets, securities services," By McKinsey internal analysis. See also: "The Risk Revolution," By Kevin Buehler, Andrew Freeman and Ron Halme, McKinsey Insights [online]. Dated: 2016. See *also*: *Ibid*., [Foot Note # *319*] 'Buehler et. al., (2016) will machine learning (ML) automation get us to the banking nirvana – optimal customer service?'

321 Source: "ACPR (Banque de France) Discussion document – "Governance of Artificial Intelligence in Finance (Dated: June 2020)." See *also*: *Ibid*., [Foot Note # *2*] '(ACPR-Banque de France) full dissertation on AI / machine learning (ML) algorithmic modeling.'

securing) the complete data life-cycle – and from there, working out the holistic technology solution, at a later stage of development.

7.2.1 A Short Diversion: The ACPR AI / ML Report

McKinsey (2016) alerted us to one opportunity, to adopt an architectural decoupling, a decoupling in which the legacy IT back-end is separated from the more speedy, agile (and flexible) customer-facing front-end. Advanced Systems Management Group (ASMG) believe the *gating* issue here, with the back-end being perceived as slow, while the front-end is perceived as speedy, is not really a salient issue.

McKinsey (2016) again, in remarkable turn-around (as in turn-around hardly truthful) state: "Data entering the bank need not follow strict rules (as would be required of data entering the enterprise data warehouse)." Wrong! It's not a question of users defining the rules when they extract the data from the (data) lake that is at issue. It's the matter of the rules and policies which are applied to data and metadata, as data assets, which is the defining issue. Defining and applying rules and policies to data and metadata is foundational, and not enough people understand the importance of this statement. Data – when it is /transported, /redacted and /stored – needs to be *always* secured, in existential, foundational or semantically-consistent state, and data's providence must be *fully* documented, for that data's Community-of-Interest to access and interpret it to its rightful, and specific, contextual and content-laden meaning.

The Why's of AI and machine learning (ML) activities which require regulatory organization scrutiny include: i) regulatory complexity; ii) lack of transparency; iii) auditing / audit trails; iv) 'other' [ASMG have filled these in here] - silo'ed proprietary platforms, inaccessible software code and irretrievable data assets – and; v) 3rd Party disintermediation.

The ACPR Report authors call for an *information sharing platform* as vital, to allow customers / users access to model and algorithmic [trading product / hedging product] *outputs*. The ACPR call this the *middle ground* involving audit tracks - produced independent from the ML algorithm modeling platform – as the *outputs of the whole* automation exercise. ACPR specifically call for machine learning (ML)-based *internal models,* becoming [as in *when* they *become*] invalid – following a major change in their input data properties and parameters. The instant 'invalid' ML modeling algorithm outputs are identified or recognized as "afflicted or compromised," from their original 'pre-condition' or state, this may require the immediate intervention of a pre-defined process. In the example involving a trading event, of for example a financial asset, the 'trade's configuration parameters' must be made accessible via a 'learning algorithm <hyper-parameter.>' This 'learning algorithm <hyper-parameter>' must be treated, in the same fashion, as a *rules-based* intervention would occur, in a centralized (or traditional or mainstream) banking transaction connotation.

This process, in a traditional *rules-based* model (for comparison purposes) would involve 'detection,' and/or 'security monitoring' components/elements [to be] triggered, acting to signify a disruptive event is *in-process*. This can be achieved in real-time, with the data-centric security (DCS) solution's alerting capabilities. The data-centric security (DCS) solution's alerting capabilities will: send secure messaging alerts to identify the model's outputs, or configuration parameters, as "conflicted/damaged." The DCS solution's alerting mechanism – and the proscribed 'update(s)' (e.g. 'make obsolete' and/or 'make redacted' and/or 'commit to storage or deletion') instructions – regarding how the offending data model's *output* should be perceived or managed[322] are unique to the Information Exchange Framework (IEF) Reference Architecture (RA) instructions and directives, upon which the data-centric security (DCS) solution is based.

The ASMG data-centric security (DCS) solution can then trigger a different notification alert (authorization and security *caveat-recognized*) to pre-determined – by design and by information sharing *consent* agreements) e.g. pre-loaded for distribution [e.g. 'alerts' to all those in the 'Community-of-Interest (CoI)' requiring a communication to be made] – as soon as their initiation is demanded by the Community-of-Interest (CoI). The Community-of-Interest (CoI), may consist of: **a**) compliance and/or risk management personnel / staff; **b**) 'other' administrators – systems administrators and systems operators, technical and support staff, (etc.,) and; **c**) domain (or business analyst) specialists. Each Community-of-Interest (CoI) party or counterparty, will receive their alert message, with the amount of detail they have the security clearance and authorization to receive. For example, the most secure information is targeted and delivered to the 'top level' of security-cleared employee(s)/*receiving* the most complete alerting message [pre-arranged to be received by them], and cascading down (in terms of the complexity of information contained in the message) from there. This is an operational compliance, security caveat decision/support tree, at its finest! It also, definitively, offers the organization the ability to "internalize" the operational functioning and situational awareness conditions of the AI and machine learning (ML) algorithmic models' *outputs*, features and workings.

This could all be implemented in the same manner, technically-speaking, as occurs in the example in which derivatives products' "*Push*" alerts today, or similar in execution to the way that the automatic alerting and triggering methodologies are conducted under Basel III regulatory requirements, in full-force, at present[323].

---

[322] Source: "ACPR (Banque de France) Discussion document – "Governance of Artificial Intelligence in Finance (Dated: June 2020)." See *also*: *Ibid*., [Foot Note # *2*] '(ACPR-Banque de France) Page 25, 29-30. See ACPR Report-section 8.4: *'Possibility of Default'* discussion.'

[323] Source: "What is Basel IV?" Dixit Joshi, and Steve Morris, Deutsche Bank, [online]. Dated: January 8, 2018. See: https://www.db.com/newsroom_news/2018/what-is-basel-iv-en-11456.htm. '(Joshi/Morris-Deutsche Bank, 2018) "The calculation of regulatory capital, as well as the potential use of a standardized approach as a floor (for Basel IV) is still being decided." NB: ASMG propose to take a closer look at this issue, the Basel IV calculation of regulatory capital requirements, in a standardized fashion. Our interest lies with possibly assisting – at some point – with the data-centric security (DCS) alerting / tagging and flagging mechanisms, which Basel IV will propose to institute, at some point in the future. Discussion: The Basel Committee on Banking Supervision (BCBS) have

Basel III has specified AI and machine learning (ML) -triggered reporting and notifications requirements, characterized here by ASMG as follows: The Basel III regulations ask for the automatic triggering of a report to their regulatory supervisory authorities when a documented threshold criteria has been met. (NB: This is ASMG's interpretation of the process – subject for peer review by Basel III regulatory experts *please*). When a) the documented threshold criteria have been met (or exceeded), i.e. a specific threshold made by an AI and machine learning (ML) modeling output data set, having an incongruous parameter adjustment having taken place, this will: b) trigger a regulatory report of AI and machine learning (ML) modeling output incongruities, data alterations and/or changes, based on that modeled configuration/parameter adjustment having taken place. This report will be sent to the regulatory supervisory authority with the power to investigate the matter. This is a strictly legislated conformance-based governance framework requirement: c) the supervisory body's governance framework will "specify": a) back-testing (required), and; b) regulatory reporting of the AI and machine learning (ML) algorithmic modeling output data's '*materiality-of-change*' response, to be put into effect.

ACPR authors delve more thoroughly into the 'other' basket of issues specified *next*:
i) silo'ed proprietary platforms,
ii) inaccessible software code and irretrievable data assets,
iii) third party disintermediation,

ACPR Report sub-section 8.4 'Probability of Default Workshop Results' suggests the whole matter of outsourcing software and algorithmic modeling (ML) platforms to third parties [residing] outside-the-organizational-walls produces unforeseen "externality issues." These include: a) Responsibility for disciplined 'investigation / continual monitoring' of the third party's operational (AI and machine learning/ML modeling) code base, which they (the third party contractor) may hold in premises off-site to the Client installation, b) validation of the software / algorithmic platform's functional efficacy and performance attributes and design features, and; c) monitoring of audit procedures and records-producing audit information (audits, physically themselves) may prove to be problematic, *a.k.a.* the complete data life-cycle analysis. This last point, life-cycle determinations of algorithmic machine learning (ML) output data sets, will necessitate a deep understanding of the algorithmic models' pre-design, and post-design assumptions and considerations, and will need to address all aspects related to the ML algorithmic model's actions and activities throughout the course of its mission.

ACPR authors leave one remaining 'other' category of issues specified *here*:

announced a five-year phase-in period, commencing on January 1, 2022 – with full implementation on January 1,2027 – for Basel IV. Basel IV introduces *new* rules concerning the capital ratios of all banks, as they shape their future business models. Among the changes are a specific risk weighted assets (RWAs) averaging model. This risk weighted assets (RWAs) averaging model will adopt internal models which cannot fall below seventy-two point five (72.5) per cent of the standardized model calculation. This new risk weighted assets (RWAs) averaging model will be 'the output floor.' Computing RWAs shall be based on a bank's revenues, or may reflect a bank's individual loss history (this is the input floor).

iv) integration (of the AI and machine learning/ML algorithmic modeling capability) must be designed / documented and be verifiably accurate. This will include identifying the 'what' [parameters, execution commands, etc.] and; should 'what' [parameters, execution commands, etc.] be not identified by the algorithmic modeling capability – or are simply excluded – this must be captured in the next 'how' description/implementation documentation, outlining in-house systems configurations, and their in-house security controls administration. Lastly, there may be a need for Basil IV observances, to fully ensure that compliant infrastructure supports *exist*, that will need to match *all* the intended business use-case[324] requirements, with the financial institutions' (FIs') regulatory compliance responsibilities. Note: Advanced Systems Management Group (ASMG) had to reread this section several times, to fully understand its meaning: comply with Basil IV regulations.

Q8. – RegTech and the OCC: Governance embedded in technology

One of the early cryptocurrency advocates, CoinLab founder Peter Vessenes, recently made a few interesting points regarding digital currency regulatory efforts. Mr. Vessenes (2020) has, in the recent past, provided digital currency consulting services for entities including the US Treasury Department, the Financial Crimes Enforcement Network, the Department of Homeland Security and the FBI. Peter Vessenes: "The mix of multiple regulatory agencies overseeing complex financial products – the Commodity Futures Trading Commission, OCC and the Securities Exchange Commission (SEC) amongst others – have what I'd call "good" motivations, protecting citizens from scams, Ponzi schemes and so on. It's very risky, expensive and time-consuming to try to innovate in America on the financial side.[325]" Mr. Vessenes applauds goals which include solving the problems of financial inclusion, open access, and the careful monitoring and control efforts applied to rent-seeking behavior, being among a few things that sprang to mind.

There are various sorts of intermediaries which routinely crop up in the discussion of appropriate financial sector regulatory monitoring activities. They are impacted by such actions as unexplained – i.e. unexpected, or less-regulated than-the-norm might expect – regulated entities, including: currency valuation (options) exchanges, International Swaps and Derivatives

[324] Source: "ACPR (Banque de France) Discussion document – "Governance of Artificial Intelligence in Finance (Dated: June 2020)." See *also*: *Ibid*., [Foot Note # *2*] '(ACPR-Banque de France) Page 25, 29-30. See ACPR Report-section 8.4: *'Possibility of Default'* discussion.' See *also*: https://www.db.com/newsroom_news/2018/what-is-basel-iv-en-11456.htm. Discussion: The Basel Committee on Banking Supervision (BCBS) have announced a five-year phase-in period, commencing on January 1, 2022, with full implementation on January 1,2027 for Basel IV. Basel IV introduces *new* rules concerning the capital ratios of all banks as they shape their future business models. Among the changes are: risk weighted assets (RWAs) using internal models cannot fall below 72.5 per cent of the standardized model calculation (this is the output floor). Computing risk weighted assets (RWAs) shall be based on a bank's revenues or may reflect a bank's individual loss history (this is the input floor).

[325] Source: "Peter Vessenes in the Focus of Cointelegraph China," By Cointelegraph (China Focus Talk Show] Dated: March 28, 2020. See: https://cointelegraph.com/news/peter-vessenes-in-the-focus-of-cointelegraph-china. See *also*: *Ibid*., [Foot Note # *96*].

Association (ISDA) Master Agreements,[326] and so on – that add complexity, and friction, to what at first blush seems the simplest of procedures – i.e. settling payments between banking clients.

Often people keep their money at different banks, and their stocks at different brokerages. A Bloomberg (2019) opinion piece suggests: "If you want to run a financial market, it seems to be more important to have a relatively open platform than it is to have a neat and efficient one.[327]"

The International Swaps and Derivatives Association (ISDA) Master Agreements are a special case. They allow parties to calculate the financial exposures they carry, with their over-the-counter (OTC) – derivatives, and other special instruments[328] – on a *net* basis: i.e. what is owed to a counterparty, and what the counterparty owes back, made under mark-to-market accounting treatments.

A pivotal moment for International Swaps and Derivatives Association (ISDA) Master Agreements occurred when the legal community internationally were challenged by the demise of the financial industry (FI) conglomerate Lehman Brothers. When Lehman Brothers fell into bankruptcy on September 15, 2008, during the Great Financial Crisis (GFC) in 2007-2008, it was cited at the time as the largest bankruptcy case in US history. Lehman Brothers' debt had a book value of approximately $ 619 billion of *debt-in-process* assets, and other reciprocal financial holdings.

Lehman Brothers were not alone, as the Great Financial Crisis (GFC) had a ripple effect, causing the bankruptcy proceedings of many other firms and financial stakeholders in the industry. Distressed mergers, restructurings, and government bailouts, as well as other financial institution (FI) delinquencies caused by inopportune investments, lead up to catastrophic financial loses, circling the globe. The SEC ruled that Lehman Brothers' bankruptcy, in North America at least, had not been *caused* by any accounting issues.[329] This was not the case, in other equity markets. where the firm had a significant presence.

[326] ISDA Master Agreements specify a schedule, list of confirmation routines, definitional booklets and credit support documentation to record contract activities. In its earliest form (1985, updated 1986) ISDA Master Agreements consisted of standard definitions, representations and warranties, and the itemization of default and remedies.

[327] Source: "JP Morgan Has a Coin Now," By Matt Levine [online – Bloomberg Opinion]. Dated: February 14, 2019. See: https://www.bloomberg.com/opinion/articles/2019-02-14/jpmorgan-has-a-coin-now.

[328] Derivatives are designed as financial contracts between two parties where each party does something for the other, either in the present or in the future. They are financial instruments whose value is dependent on the value of the underlying asset or group of assets. The underlying asset can be commodities, stocks, interest rates, market indices, bonds, and currencies. See:
"Types of Derivatives (The 4 Types of Derivatives Explained)," By Therobusttrader [online]. Dated: 2017. See: https://therobusttrader.com/types-of-derivatives/.

[329] Source: "Let's Walk Down Memory Lane with Ernst and Young and Lehman Brothers," By Caleb Newquist [online – goingconcern.com]. Dated: September 10, 2013.

Lehman Brothers International Europe, the firm's London-based center of operations, had roughly 8,000 International Swaps and Derivatives Association (ISDA) Master Agreements in place – around 67,000 open trades on the books – when they entered UK administration (bankruptcy) proceedings. Two attorney's familiar with the case, Parker / McGarry (2019), reported that the administrator for London-based Lehman Brothers International Europe (LBIE) – a firm named Lomas & Ors – faced a motivated counterparty (JFB Firth Rixson Inc., and others) litigating the issue of 'Event of Default'.

Lomas & Ors, Lehman Brothers' administrator for their UK bankruptcy proceedings, were appointed by London-based Lehman Brothers office, Lehman Brothers International Europe (LBIE). Lomas & Ors possessed a ninety-seven (97) page list of counterparties to Lehman Brothers International Europe (LBIE), with their itemized contractual commitments, spread across the globe. A close-out on this grand a scale has moved from a 'what if' theoretical exercise, into the real-world. It has now multiplied into a massive undertaking, affecting as it were – massive volumes of derivative trades and their consequences – for LBIE's and their counterparties interests, as they sought to close out all their International Swaps and Derivatives Association (ISDA) Master Agreements.[330]

Despite our earlier observation that, in North America, Lehman Brothers' bankruptcy was not deemed to be caused by *any* accounting issues, the application of Generally Accepted Accounting Principles (GAAPs) to Lehman Brothers International Europe (LBIE) Balance Sheet did not mirror the conclusions that were afoot in the UK Court's. Although in North America, Lehman Brothers' could be granted their status as an institution which constituted a highly-leveraged entity status, operating in a risky and volatile environment, this did not placate UK court proceedings.

Taking this issue up in the UK, Judge Briggs J (as he was then known) presided over the events of 'default and remedy' to which Lehman Brothers International Europe (LBIE) found themselves locked in litigation. The big gap in International Swaps and Derivatives Association (ISDA) Master Agreements *is* that they do not specify, or if they do with the barest of intentions, how early termination provisions on 'Event of Default' are to occur. Before we examine Judge Briggs J (as he was then known) judicial decision – 're: Lehman Brothers International (LBIE) / Lomas & Ors (for LBIE) *versus* JFB Firth Rixson Inc., and others' – let's have a quick look at the structure and substance of International Swaps and Derivatives Association (ISDA) Master Agreements.

One huge weakness of International Swaps and Derivatives Association (ISDA) Master Agreements is the lack of options present for a non-defaulting party (Lomas & Ors, for LBIE) on its defaulting counterparty (JFB Firth Rixson Inc., and others). This leads to delays, or in worst

[330] Source: "The ISDA Master Agreement and CSA: close-out weaknesses exposed in the banking crisis and suggestions for change," By Edmund Parker and Aaron McGarry [online – Mayer Brown]. Dated: January 2019. See *also*: [original citation-1st publication] Butterworth's Journal of International Banking Law, January 2009 edition. See *also*: *Ibid*., [Foot Note # *331*].

case scenarios, botched close-outs. Lehman's lost the right for protection against a rise in the relevant (prevailing) floating interest rates. Lomas & Ors, Lehman's bankruptcy administrator in the UK litigation proceedings, were dealt by Judge Briggs J (as he was then known) a very mixed message in the judicial decision.

Reduced to its bare essential, the precedent established by Judge Briggs J (as he was then known) determination, was that there should be (*inter alia*) no bankruptcy 'event of default' to ensure that Lehman Brothers International Europe (LBIE) would receive its *quid pro quo* for an interest rate hedge, for as long as it was in a financial condition to be able to do so (receive the benefit of the interest hedging derivatives contract). In short, the aggrieved party in the proceedings – Lomas & Ors [re: Lehman Brothers International (LBIE) / Lomas & Ors as administrator (for LBIE) *versus* JFB Firth Rixson Inc., (and others) – were deprived of the right for which they had contracted – namely the risk of protection against a rise in the relevant floating interest rate.

This next part of the administration (bankruptcy proceedings, in the UK judicial vernacular) verdict, Advanced Systems Management Group the counterparty (ASMG) are not completely understanding, as Judge Briggs J (as he was then known) ruled that Lomas & Ors – as administrative trustee for LBIE – were to be compensated for the 'cost of finding an alternative transaction' i.e. for [said] Clients' (LBIE's) interest rate hedging instrument – after having [Lomas & Ors as administrator (for LBIE) given the counterparty, JFB Firth Rixson Inc., (and others), 'credit for any unpaid amounts.'

Behind all the legalese, what does all this mean? Don't search us for any kind of definitive answer, or full-fledged understanding!

International Swaps and Derivatives Association (ISDA) Master Agreements are the worse-for-wear, across an abundance of issue areas. This sticky wicket – concerning the 'Event of Default i.e. 'default and remedy' – many in the UK began to cite as having received the definitive legal-judicial interpretation by Judge Briggs J (as he was then known). Legal experts in the UK have having roundly come to the defense of, and belief in, the importance of Judge Briggs J (as he was then known) precedent-setting legal decision.[331] The decision, Parker / McGarry (2019) suggest: "[ruling on Lehman Brothers International Europe (LBIE)] *has potentially* important consequences for all businesses that rely on derivatives, to manage risk, arising from their financial obligations.[332]

[331] Source: "The ISDA Master Agreement and CSA: close-out weaknesses exposed in the banking crisis and suggestions for change," By Edmund Parker and Aaron McGarry [online – Mayer Brown]. Dated: January 2019. See *also*: *Ibid*., [Foot Note # *330*] '(Parker / McGarry-2019) UK Judge's ruling on 'Event of Default - default and remedy.'

[332] Source: "ISDA Master Agreement – probably the most important standard market agreement used in the financial world," By Barry Donnelly, Head of Banking and Litigation (UK) [online – Macfarlanes]. Dated: April 2011. See: inhouselawyer.co.uk. Discussion: Lehman Brothers International [Europe] (LBIE), as it were, went into administration [bankruptcy] on September 15, 2008 during the Great Financial Crisis (GFC).

Advanced Systems Management Group (ASMG) are not sure how this is the case, since in the last (many) years, it has not been uncommon for counterparties to enter into a derivatives transaction, deem an International Swaps and Derivatives Association (ISDA) Master Agreement to apply, and never get to the issue of negotiating the actual terms and conditions of the applicable ISDA Master Agreement, in their totality.

Further to this, Parker / McGarry (2019) submit: "Any entity that enters as a party or counterparty to an International Swaps and Derivatives Association (ISDA) Master Agreement, will have comprehensive records of trading positions that are *live* (open book transactions). When these transactions are taking place, under the auspices of the International Swaps and Derivatives Association (ISDA) Master Agreement's terms and conditions, it is recommended by experts to carry out a *full audit*, to produce a central populated spreadsheet, that lists: **i**) every trade **ii**) every counterparty **iii**) the 'exposure' **iv**) what role each counterparty has (who is the calculating agent?) and; **v**) the crucial elements 'elected to (*fulfill*)' in the Schedule to the International Swaps and Derivatives Association (ISDA) Master Agreement. This [Schedule to the ISDA master agreement] should include whether stipulations have been made to apply automatic Early Termination, and any credit support annex (CSA) provisions.[333] This *full audit* – and its enforcement of provisions [parts **i**) through **v**) *inclusive*] – shall represent an 'audit enforcement,' in the opinion of Parker / McGarry (2019). It allows a Counterparty to be fully informed, and able, to make decisions quickly and decisively, if the credit worthiness of their opposite Party / Counterparty becomes a grave concern.

It would appear both regulatory organizations, the OCC and SEC, have the challenge which lies ahead, of being participatory witnesses – on this side of the Atlantic – as to how regulatory compliance enforcements measures ought to be devised with respect to the International Swaps and Derivatives Association (ISDA) Master Agreement enforcement actions generally, and the 'Event of Default i.e. 'default and remedy' International Swaps and Derivatives Association (ISDA) Master Agreement sub-sections specifically, at least as far as determining whom has what compliance mandate pertaining to these negotiated agreements.

To their credit, the International Swaps and Derivatives Association (ISDA) have been working on new standards to cover smart contracts and the distributed ledger. They are pursuing this through their Market Infrastructure and Technology Oversight Committee (MITOC), the ISDA organization's facilitator for coordinating regulatory, technological, and work-stream issues – re: future-proof standard documentation and data categorization efforts – going forward. Specifically, the International Swaps and Derivatives Association (ISDA) are now addressing

[333] The Credit Support Annex (CSA) is a legal document which defines the terms or rules under which collateral is posted or transferred between swap counterparties to mitigate the credit risk arising from "in the money" derivative positions. It is one of the four parts that make up an ISDA Master Agreement, but is not mandatory. However, under English Law, the Credit Support Annex (CSA) are considered transactions: Any collateral listed as 'Eligible Collateral' is delivered as an outright transfer of title. The collateral taker becomes the outright owner of that collateral free of any third-party interest.

distribution ledger technologies (DLTs), which allow code to be embedded in the distributed ledger. This, from a legal perspective, is served by two interpretations.[334]

The first viewpoint is that there is a difference between *smart contract* code (computer software code) and the elements of a legal contract being represented and executed by software. Certain operational classes in legal contracts lend themselves to being automated, others are non-operational – e.g. payments and deliveries. If these elements are captured in a private distributed ledger, regulators need to be able to access the *smart contracts* terms and conditions, and these terms and conditions need to be shared (interoperable) between firms and platforms.

The second legal interpretation holds to the premise that a *smart contract* is – in its essence – a depiction which includes *essential* 'smart contract' code (computer software code) known in legal terminology as 'software agents'. A software agent is designed to execute certain tasks if pre-defined conditions are met. Such tasks are often embedded.[335] Elaborating on this – in technical terminology – 'smart contract code' does *x-y-z*, as embedded within, and performed by, the distributed ledger technology (DLT) *tasked* to perform [*said*] duties. Tasks software agents may be asked to perform may include: **i**) crypto-currency creation; **ii**) casting a [procedural] vote on blockchain procedural or coin issuance matter, or **iii**) performing an electronic *blind auction* administrative mechanism or procedure.

The second legal interpretation / legal viewpoint goes further, suggesting re: *smart contracts hold* [demand] that for a legally enforceable *smart contract* to be implemented, or acted upon, it will need to embed one or more pieces of code *designed to execute* a set (or singular number of) pre-defined tasks (three examples have been provided: crypto-currency creation; casting a [procedural] vote re: procedural [administrative] blockchain matters, and; performing an electronic *blind auction*. These types of *smart contract* occurrences – and this is crucial – become legally enforceable rights – when legally mandated – up-front, and in this manner.[336] To sum this second viewpoint up, every smart *legal* contract can be said to contain one or more pieces of smart contract code, but not every piece of smart contract code comprises (or *is* [an essential part of]) a *smart* legal contract.

Now, let's stay with the importance of definitions – which are mandatory (not optional) – to explain a few more examples of *how things work*. The Financial Stability Board (FSB) and the Committee on Payments and Market Infrastructures (CPMI), and other relevant international

[334] Source: "Making Sense of Blockchain Smart Contracts," By J. Stark. [online – Coindesk]. Dated; 2016. See: http://www.copindesk/com/making-sense-of-blockchain-smart-contracts/.
[335] Source: "[Whitepaper] Smart Contracts and Distributed Ledger – A Legal Perspective," By Paul Lewis, Derivatives and Structured Products Partner, Linklaters LLP [online], Page 3 - 5. Dated: August 2017. See: isda.org. See also: Ibid., [Foot Note # *336*].
[336] Source: "[Whitepaper] Smart Contracts and Distributed Ledger – A Legal Perspective," By Paul Lewis, Derivatives and Structured Products Partner, Linklaters LLP [online], Page 3 - 5. Dated: August 2017. See *also*: *Ibid*., [Foot Note # *335*] '[Linklaters-Paul Lewis] pre-defined smart contract tasks (examples) *a.k.a.* legally enforceable.'

bodies, are developing a roadmap to enhance cross-border payments.[337] Cross-border payments by financial institutions (FIs) – we will exclude the blockchain payments vertical for now – FSB (2019) states: "(It) would be feasible to verify each digital signature, since computationally this is an appreciably costly operation, involving the processing of a transaction, yet we could do so, and twin this with monitoring and verifying each digital signature for all accounts, on an hourly basis, with a two-digit number of standard servers.[338]"

Now let's introduce distributed ledger technology (DLT) payments into the cross-border payments equation. Ali and Narula (2020) state: "Among the distributed ledger technology (DLT) -based payments projects that are still ongoing, it remains to be seen whether scalable implementations will actually rely on the blockchains' underlying technology.[339]" In short, verification of the centralized trading and financing transactions system *a.k.a.* for cross-border payments – *doable*; verification of decentralized, distributed ledger trading and financing transactions system a.k.a. for cross-border payments – at this point in time, *unattainable*.

Our next example draws from the securities transactions side of the financial settlements bench. The European Commission's European Securities and Markets Authority (ESMA) introduced the Securities Financing Transactions Regulation (SFTR), to reform and advance securities settlement discipline and compliance. The Securities Financing Transactions Regulation (SFTR) provides a compelling, and comprehensive, overview of the market *per se* – capturing with succinct and practical terms and terminologies, and interpretive guidance – the 'how to' guide book to approach securities trading and financial transactions. The objective the Securities Financing Transactions Regulation (SFTR) set for itself was to identify, and monitor, financial stability risks that may arise from shadow banking activities. The requirements that the SFTR measures specified affect a broad range of trades, and their corresponding trading, and reporting, organizations. The financial trading activities which the Securities Financing

[337] Source: "Enhancing Cross-Border Payments – Stage 1 Report to the G20," By Financial Stability Board (FSB) staff [online]. Dated: April 2020. See *also*: "Riksbank – World's Oldest Central Bank Study Digital Currency Results: (Chapter entitled) E-krona design models: pros, cons and trade-offs," By Hanna Armelius, Gabriela Guibourg, Stig Johansson and Johan Schmalholz. [online – Riksbank Economic Review 2020:2]. Dated February 2020. See *also*: *Ibid*., [Foot Note # *337*, *418, 419*].

[338] Source: "Riksbank – World's Oldest Central Bank Study Digital Currency Results: (Chapter entitled) E-krona design models: pros, cons and trade-offs," By Hanna Armelius, Gabriela Guibourg, Stig Johansson and Johan Schmalholz. [online – Riksbank Economic Review 2020:2]. Dated February 2020. See *also*: *Ibid*., [Foot Note # *337, 418, 419*] '(Riksbank 2020) E-krona design models and verifying digital signatures in centralized payment streams'. See *also*: https://www.coindesk.com/riksbank-worlds-oldest-central-bank-study-digital-currency-results, Page 91.

[339] Source: "Redesigning digital money: what can we learn from a decade of cryptocurrencies?", By R. Ali and N. Narula. MIT DCI Working Papers [online]. Dated: January 2020. See *also*: *Ibid*., [Foot Note # *186*] *and/or* (Riksbank 2020) "Riksbank – World's Oldest Central Bank Study Digital Currency Results: (Chapter entitled) E-krona design models: pros, cons and trade-offs," By Hanna Armelius, Gabriela Guibourg, Stig Johansson and Johan Schmalholz. [online – Riksbank Economic Review 2020:2], Page 93. Dated February 2020. Discussion: ASMG believes, and supports, the traditional financial sectors' discipline in defining things. We 'tune-out' – the oftentimes *opinionating* declarations – which exemplifies so much of what the blockchains' adherents (aficionados?) have to say. For example, misrepresenting the International Swaps and Derivatives Association (ISDA) deliberations on smart contracts, among other things. Kind of a challenge to dismiss these wild, seemingly outlandish claims, while keeping our analysis on track – throughout this Submission.

Transactions Regulation (SFTR) covers include: repurchase transactions, securities and commodities lending and borrowing transactions, buy/sell-back and sell/buy-back transactions, and margin lending trades.

Aside from the wide berth and extensive coverage the Securities Financing Transactions Regulation (SFTR) paid to the sector in general, the eligible reporting organizations under the Securities Financing Transactions Regulation (SFTR) umbrella were enumerated, and found to be more numerous in quantity, than were cited in previous regime documents and reporting methodologies. The new Securities Financing Transactions Regulation (SFTR) states: financial counterparties (FCs), non-financial counterparties (NFCs), European Union (EU) counterparties, branches of EU entities that are domiciled outside the EU, and branches of non-EU entities located in the EU, are *all* within its enforcement mandate for regulatory compliance and enforcement rulings and proceedings. This is a very comprehensive regulatory regime.

To date, the Securities Financing Transactions Regulation (SFTR) is the financial stability risks and shadow banking activities regime with the most complex set of requirements. It consists of one-hundred-and-fifty (150) attributes, has a tight T+1 reporting deadline, entails complicated reporting related to collateral reuse and, most importantly, requires the collection of more data by all affected counterparties — including across institutional data silos, or from outside, third-party sources. Furthermore, as the total volume of reportable trade and eligible transactions increases, the margin for error permitted by trade repositories (TRs) and regulators decreases.

Given the complexities of the Securities Financing Transactions Regulation (SFTR) requirements, reporting organizations' need meet legally-enforceable duties and responsibilities — as declared by the SFTR provisions — and must comply with reporting requirements which specify how the reporting must be optimized, and how it must be presented, in a seamless capture of content and context. Current systems in place to handle MiFID and EMIR[340] reporting requirements may not have the capacity to handle yet another regime, and the additional data required for Securities Financing Transactions Regulation (SFTR) reporting may not be readily at hand, or even accessible. Therefore, many reporting organizations may now be asking themselves how best to proceed.

Here are a few pointers regarding what might need to be addressed:

[340] As a short synopsis, the Markets in Financial Instruments Directive (MiFID) is a European regulation that increases the transparency, and standardizes the regulatory disclosures, required for firms exercising derivatives contracts and contracting obligations (and similar financial instrument contracts and contracting obligations), in the European Union (EU). The European Market Infrastructure Regulation (EMIR) is a body of European legislation. Collectively the European Market Infrastructure Regulation (EMIR) regime acts in a supervisory capacity, defining: i) over-the-counter (OTC) derivatives, *plus* ii) exercising supervisory guidance and authorization of the duties, roles and responsibilities which the market's central counterparties and trade repositories (TRs) must maintain. The European Market Infrastructure Regulation (EMIR) specifies the reporting requirements for derivative contracts, plus provides implementation guidance for risk management standards, thereby intending to reduce counterparty *operational* risk, and help deter (or prevent) systemic financial system failures or collapse.

- Is our infrastructure equipped to accommodate yet another trade and transaction regulation regime?
- Can our data collection, validation, enrichment, and submission process scale to accommodate SFTR?
- Can we take a different approach going forward?
- Reporting organizations may need to bolster their reporting best practices, itemizing their daily processes, and listing and tracking all the reporting they make to trade repositories (TRs).

The Securities Financing Transactions Regulation (SFTR) was set to go live in April 2020, however, due to the global COVID-19 crisis, the EU's sponsoring agency, the European Securities and Markets Authority (ESMA), has postponed the initial reporting date to July 2020. And while the reprieve does not eliminate the need to address the issues at hand, it presents an opportunity for organizations to examine their systems, and consider best practices, before reporting goes live.

Clearly, taking on the Securities Financing Transactions Regulation (SFTR) requirements and regulatory reporting duties and mandate, adds more weight to the compliance teams' daily burdens. And what might those daily burdens entail?

Many reporting organizations' compliance teams are continuously managing the high volume of required reportable transactions, across global trade and transaction regimes — but with no end in sight. For them, the pressure is great to stay on top of daily transactions, thus achieving full compliance, within tight timelines, and across (reporting) regimes. A typical day for a compliance officer at a reporting organization, may begin with the processing of the first batch of trades, including delegated ones. This first batch may often include a listing of the number of errors to be addressed. These errors, including pairing/matching, must be dealt with promptly because new batches of trades tend to follow in rapid succession, with the number of trades to be reconciled increasing, throughout the day.

If by midday, the compliance teams have caught up with batch processing and error reconciliation tasks at hand, they are on track to meet trade repository (TR) reporting requirements *next*. However, this may or may not be the case, as many attempt to manually rectify errors from the previous day, while continuing business as usual with a new set of trades for the current day, are tactically a challenge. Organizations' systems are often opaque, and lack traceable data drill-down, making the error rectification process very cumbersome. At the end of the trading day, potentially hundreds or thousands of problems with trade reconciliations might yet need to be monitored, or rectified, before being sent for overnight batch processing. Compliance teams log off hoping that their reconciliations will be error free, but given that data quality can be problematic, this *is*, unfortunately, not always the case.

As the following (next-day) workday begins, compliance teams may be required to firstly, deal with any problems that were flagged by trade repositories (TRs), on their overnight submissions

/ resubmissions. And then, the typically hectic trading day starts again, with some feeling they may be sinking into quicksand. A plan to increase transparency and facilitate financial stability should certainly have a positive effect on standardizing reporting. So how did trade and transaction reporting get so complicated for organizations?

The list of financial reporting regimes implemented over the past 10 years includes MiFID, Dodd Frank, EMIR, MAS, ASIC, and FinfraG.[341] With the addition of each new regime, counterparties have had to contend with:

- Expanding requirements
- Addressing data quality issues
- Determining reporting eligibility
- Resolving data quality exceptions

Is the Securities Financing Transactions Regulation (SFTR), as one commentator wishes us to believe, best described as: "SFTR - The Last Straw?" Hardly.

It may be said – regarding many reporting organizations – that they lack the adequate processes and procedures, currently in place, to handle the *expanded* and *diverse* reporting requirements under the new Securities Financing Transactions Regulation (SFTR) reporting guidelines. This is argued, by some parties, as especially true today, given that large data volumes need to be combed and assessed, to complete the regulatory compliance audit response to the Securities Financing Transactions Regulation (SFTR) authority. Many organizations report that their *mission critical* data is often opaque (siloed?). This mission critical data may, in fact, be entrenched in evidentiary processes and proceedings, that oftentimes are manual in nature. The Securities Financing Transactions Regulation (SFTR) reporting requirements will challenge, and unduly strain, trade repository (TR) organizational capacities. This – trade repositories (TRs) claim – will adversely increase the risk they will experience far more numerous compliance (security) breaches.

Advanced Systems Management Group (ASMG) applaud the Securities Financing Transactions Regulation's (SFTR's) data management review efforts. We believe – and would tell anyone who asks – that the Securities Financing Transactions Regulation (SFTR) enables parties, and counterparties including trade repositories (TRs), the opportunity to manage *all* data collection, data validation, data enrichment, and data submission requirements in the proscribed manner *effectively*. This will be accompanied with another benefit, i.e. treating critical data stores as

[341] The Monetary Authority of Singapore (*MAS*) regulates a broad swath of financial institutions, including: banking, capital markets, insurance and financial institutions (FIs) in the payments sectors. The Australian Securities and Investments Commission (*ASIC*) is responsible for supervising integrated corporate, markets, financial services and consumer credit regulations in Australia. In the financial services sector, *ASIC* licenses and monitors financial services businesses typically dealing in superannuation, managed funds, shares and company securities, derivatives and insurance products and services. Thirdly, *FinfraG* (i.e. Finanzmarktinfrastrukturgesetz) aims at regulating derivatives trading in Switzerland. The Financial Market Infrastructure Act (FMIA-Switzerland) supervises all activities conducted by *FinfraG.* FinfraG has drawn on the EU supervisory regime called the European Market Infrastructure Regulation (EMIR) and the American regulation, the Dodd-Frank Act.

their most important institutional asset. They should strive to lodge, or house, all data repositories and data stores in one place. Here is an example *in action*:

Securities Financing Transactions Regulation (SFTR) data can be implemented in a manner that enables reconciliation of unpaired and unmatched trades, and other related activities. This should be within reach, as one vendor explains, via their solution platform (which includes) a user-friendly dashboard.[342] These dashboards provide transparency for: i) end-to-end workflow management, ii) eligibility assessment, and; iii) trade repository (TR) reconciliations. Dashboards, such as that offered by AxiomSL – enable users to *facilitate* submissions, including delegated submissions – with automated connections and workflow discipline.

Highlights of the bundled vendor solution offerings – AxiomSL included – are as follows:
i) Eligibility Insight – the Securities Financing Transactions Regulation (SFTR) solution (by AxiomSL, other vendor offerings can do the same) handles end-to-end transaction reporting automatically, and with full traceability and auditability. By leveraging their dashboard and eligibility views, Operations teams (at the users' site) can focus on value-added issue resolution. The user can easily filter by: regime, asset class, entity, date, status, as well as other criteria;
ii) Exception Management – Securities Financing Transactions Regulation's (SFTR's) exception management capabilities (by AxiomSL, others vendor offerings can do the same) are designed to enable organizations to focus on reviewing and managing exceptions through a flexible and transparent User Interface (UI). Accepted reports, and exceptions management, are clearly presented, and a reason for 'the *exception*' to be singled out and reported, is given. Therefore, users can amend transactions for resubmission with an auditable and traceable history;
iii) Pairing/Matching Resolution – once a trade repository (TR) report is acknowledged (by AxiomSL, other vendor offerings can do the same), the Securities Financing Transactions Regulation (SFTR) solution analyzes end-of-day trade repository (TR) reports, and the dashboard displays any unpaired and unmatched reconciliation issues. With this type of clarity, reporting organizations can act and resolve any errors in a timely fashion. Trades can also be resent and resolved, via the same exception management capability, on the dashboard, providing counterparties with control over their Securities Financing Transactions Regulation (SFTR) compliance efforts, and;
iv) Securities Financing Transactions Regulation (SFTR) data reporting requires a Proprietary Solution platform: in this case, the vendor (AxiomSL) suggests their "Regime Agnostic Trade and Transaction Solution (RATTS).[343]

[342] Source: "The World's #1 Platform for Risk and Regulatory Reporting," AxiomSL. By AxionSL staffers [online]. Dated: 2020. See: https://www.axiomsl.com/.
[343] *Disagree*. Point **iv**) 'Securities Financing Transactions (SFT) Requires [i.e. calls for] - proprietary solution(s). Discussion: ASMG reminds OCC that processes and procedures - currently in place - to handle expanded and diverse reporting requirements under SFTR, unduly strain trade repository (TR) capacities when data 'from trade repositories' are silo'ed (dead-ended?), and lodged in hard-to-access e.g. *non-interoperable* data repositories, which 'proprietary' [vendor] data platforms exacerbate. ASMG would like to DEMO the data-centric security (DCS) solution, for OCC's internal implementation requirements, to begin to correct this critical failing and shortcoming which the proprietary platform solutions cannot alleviate.

Enterprises simply don't have the time or resources to introspect data, as it moves across the cloud, to the edge, or wherever else that data repository may exist. This causes data lineage, and data relationships, to be scrambled, and oftentimes they are not captured accurately. Data pipelines are also known to become 'data islands' unto themselves. Likewise, many first-generation data pipelines should be re-architected, as the underlying systems and schemas change. Without proper attention, they can even break[344].

RegTech, as it is coming to be understood, must be something qualitatively different from what it's replacing, and not just a faster and better version of the same thing. For example, can a RegTech solution address, in a Line-of-Business (L-o-B) context: i) How will a Line-of-Business (L-o-B) *mesh* with other Lines-of-Business (L-o-B) Data Domains, and what impact will they have overall, on such business metrics as the return-on- capital? ii) How will increasing exposure to one type of asset (i.e. in securities trading scenario) in a specific (or specified) portfolio, by what conditional (or expected) amount, might key ratios analyzed be affected? iii) Can a system be able to alert users to other questions (they should be asking themselves), such as: why a central bank is prodding (institutionally) for information about '*this-or-that*' (arcane and outwardly benign) criteria?

These are but a few examples that are buried deep in the data enterprise – consisting of databases, data repositories, and data lakes (and data silos, unfortunately) etc. – which data analytics and data algorithm computations attempt to analyze, to arrive at firmer contextual constructs for decision-makers, or to convey 'an explicit' content understanding, or simply '*make sense of data*.' Data may oftentimes be hidden in a treasure trove of complex, interrelated sources of interaction, and shared understanding. This makes the effort to solve data's semantic puzzle a repeating (and repeatable) challenge.

The very first risk associated data, is knowing its exact lineage, i.e. where did it originate? Has a data resource experienced any tampering or compromise? Data – to be fully understood in a semantically explicit manner – needs its meaning, its context, and its full semantic properties and identity to be vouched for. Then, it may be shared responsibly across a Community-of-Interest (CoI), in a secure information sharing capacity. If this occurs, the guesswork behind the transport (or transfer) of data, in a semantic sense, and the interpretation of data's meaning and consequence, is no longer tied to an issue of questionable providence or concern. What every data analyst would desire, is that data resources be responsive, be made easily understandable, and be effectively analyzed in ways that are sophisticated, yet not complicated. Now, moving on to blockchain.

[344] Source: "CIO: 3 Questions to Ask about your Enterprise Data Lake," By Ciaran Dynes [online – talend]. Dated: August 8, 2016. See *also*: *Ibid*., [Foot Note # *35, 365*]. See *also*: "Build a True Data Lake with a Cloud Data Warehouse," By Talend staffers [online]. Dated: not given *a.k.a*. [Foot Note # *366*]. See *also*: "Creating a company culture where the respect of personal data is top priority," By Maud Bailly, [online – talend]. Dated: 2020 *a.k.a*. [Foot Note # *367*].

The Harvard Business Review (2007) suggest "if there's to be a blockchain – technological, governance, organizational and even societal – *barriers* will have to fall.[345]" But only if the technological base to support the blockchain can be secure, regulated, and guaranteed *secure* again, with frequent maintenance and compliance audits performed along the way. The Harvard Business Review authors' (2017) correctly identify infamous bitcoin hacks exposing weaknesses in the blockchain itself, as well as suggesting that separate systems linked to parties using the blockchain, are also vulnerable to attack. They cite Nasdaq working with Chain.com – in pursuit of technology for processing and validating financial transactions (via blockchain) – and the Bank of America, JP Morgan, New York State Stock Exchange, Fidelity Investments and Standard Charter, all testing blockchain technology as a replacement for paper-based and manual transaction processing. These major financial institutions (FIs) are pursuing these transformative processing and validating of financial transactions on blockchain in such areas as: trade finance, foreign exchange, and cross-border settlements. The Harvard Business Review authors' (2017) also point out that the Bank of Canada may be proceeding (study phase, at present) to investigate their nation's digital currency, called CAD-coin.[346]

Returning to a voice from the crypto asset community we quoted earlier, Lennix Lai (OKEx)[347] asks: "Can we put everything on the blockchain that's in the centralized system right now? I don't think so. First, the centralized system right now is working quite well. It is slow sometimes, it might not be very efficient. But the size is so big, with volumes of trillions of dollars. It's a robust financial system right now. Also, because of the increased regulations, the traditional market is getting a lot more efficient than before.

A lot of regulation that we talk about is related to checking, to disclosure. For example, the bank needs to disclose their balance sheets, and the security firm needs to disclose the access of the client, the fund manager needs to disclose the buy and sell orders, and so on. If you think about the blockchain concept, you don't need a regulator to play this role because everything can be executed on a technological basis. It's immutable. It's transparent. Everyone can see it, along with regulators. Each move and transaction is logged on-chain. In summary, we can serve the exact same regulatory purpose with a fraction of the costs that the regulators are spending right now."

That just seemed too good an opportunity to pass up! That is a standard *trotted-out* viewpoint arguing that for blockchain to serve regulatory purposes properly, a viewpoint which Advanced

[345] Source: "The Truth About Blockchain," By Marco Iansiti and Karim Lakhani [online – Harvard Business Review] Dated: Jan-Feb 2007 (*issue*]. Dated: February 2017. See: *Ibid*., [Foot Note # *346*].
[346] Source: "The Truth About Blockchain," By Marco Iansiti and Karim Lakhani [online – Harvard Business Review] Jan-Feb 2007 *issue*]. Dated: February 2017.See: *Ibid*., [Foot Note # *345*] '(Iansiti/Lakhani-Harvard Business Review] blockchain activities abound in the financial sector.' See *also*: "Staff Analytical Note 2020-11 (English)," By Cyrus Minwalla – Bank of Canada, Dated: June 2020.
[347] Source: "OKEx's Lennix Lai: Passive Income in Crypto Is the New Way to Earn," By Lennix Lai, OKEx Director of Financial markets, [interviewed by Cointelegraph's Erhan Kahraman]. Dated: March 22, 2020. See: https://cointelegraph.com/news/okexs-lennix-lai-passive-income-in-crypto-is-the-new-way-to-earn. See *also*: *Ibid*., [Foot Note # *189, 509*].

Systems Management Group (ASMG) simply cannot fathom, is simply erroneous, at heart, and completely wide-of-the-mark.

Perhaps we should turn to Jay Hao, CEO OKEx *next* – whom happens to be Mr. Lennix Lai's boss – to lay-out a more accurate perspective! Mr Hao believes that blockchain's power is its ability to eliminate transaction barriers, improve efficiency and ultimately impact the development of the global economy. This is rich, coming from a Company CEO operating *integration* components and *infrastructure* components – following the Nemertes Research Internet-of-Things (IoT) taxonomic guideline – which would rule that OKEx are highly proprietary, market-controlling and monopolistic, at their core. We have reviewed OKEx once before in Q6) 'Payment technology a.k.a. getting interoperability right.'

OKEx has a vested interest – following the Nemertes Research Internet-of-Things (IoT) taxonomic guideline – in market-controlling *integration* components and *infrastructure* components, which grants OKEx an exceptional *competitive advantage.* This is worth considering, as we evaluate altruistic statements from the OKEx CEO. For a not-so-subtle reminder, OKEx controls its network-supporting initiatives via its OKEx Chain, and Client onboarding and Client enrollment activities conducted by its *superior* matching engine, which is not coincidentally, *fully* proprietary. OKEx also touts its support for the Lightning 2.0 Network. Lightning 2.0 is – right now – mostly commands 'prompt-based,' so it's a little distance away from offering a *good wallet* and a *good user*-friendly graphical user interface (GUI).[348]

A quick explanation here is in order: In computer networking, the two most common forms of data transmission are broadcast and unicast. Broadcast mode – computer's employing the network to disseminate data and information – is used to send data on a network to all other points, one-to-all. Unicast – a data transmission type where information is sent from one point on a network to another point – is accomplished one-to-one. Blockchain transmissions resemble broadcast-like forms, with info sent to nodes on the network. (All nodes!!).

This works the way legacy 'Ethernet hubs' have long handled data transmissions. The problem arises with the fact that Ethernet hubs don't *scale*. To send to one hundred (100) participants, you need to replicate everything 99 times!! It is simply unrealistic to even consider scaling a global payment network (such as Bitcoin) via broadcast-based on-chain transactions / communications (methodologies). If we do this – i.e. adopting a "flat LAN network" with every single person, host, device on their own broadcast domain – it simply isn't a suitable network transmission approach. Just by attempting to read this article, using broadcast domain transmission mode, every other single device would be forced to download / read it as well, crashing the Internet!!

[348] Source: "Lightning Network Explained – Is it Bitcoin 2.0," By Michael (no surname), [online – Boxmining]. Dated: September 4, 2018. See also: https://medium.com/@melik_87377/lightning-network-enables-unicast-transactions-in-bitcoin-lightning-is-bitcoins-tcp-ip-stack-8ec1d42c14f5.

Manukyan (2018)[349] suggests that by using the traditional Internet Protocol IP Suite,[350] we send and receive data packets. Internet Protocol (IP) is what allowed us to scale our small and largely primitive networks of the past. Lightning is what will allow us to scale our global Bitcoin network, now, and into the future. Lightning nodes in Bitcoin are the equivalent of Internet Protocol (IP) hosts – where we can finally conduct *or route* one-to-one and/or point-to-point transactions, to their appropriate recipients.

In the computer networking scenarios which we wish to describe next, *multicast* is group communication – wherein data transmission is addressed to a group of destination computers – simultaneously. Multicast can be one-to-many, or many-to-many, distribution. Multicast should not be confused with physical layer *point-to-multipoint* communication. To use multicast effectively, *multicast* must be engaged by employing network programming on the multicast backbone, or *MBone.*[351] The multicast backbone is a system that allows users – at high-bandwidth points on the Internet – to receive live video and sound programming.

Where is this going? It allows all Bitcoin network transmission *tasks* to be accomplished via a *unicast* networking approach. Unicast data transmissions – not reliant on 'blind' broadcast transmission of data – will instead *pre-select* who 'gets' the data / transmission packets.[352] In short, 'Lightning 2.0' enables unicast transactions supporting Bitcoin-delivered transactions, that previously were only supported in the non-scalable, broadcast transactions' mode. Manukyan (2018): "In traditional Internet Protocol (IP) implementations, we send and receive data packets; in Lightning 2.0 we send and receive *Bitcoin.*"

Manukyan (2018)[353] states: "There is a great wealth of knowledge to be gained in understanding how computer networks and the Internet work, that can be applied to Bitcoin's own scaling

[349] Source: "Lightning Network enables Unicast Transactions in Bitcoin – Lightning is Bitcoin's TCP/IP stack," By Melik Manukyan [online – Medium]. Dated: January 9, 2018. See: https://medium.com/@melik_87377/lightning-network-enables-unicast-transactions-in-bitcoin-lightning-is-bitcoins-tcp-ip-stack-8ec1d42c14f5. See *also*: *Ibid*., [Foot Note # *353*] '(Manukyan] Why Lighning 2.0 adopts the unicast network model.'

[350] Internet Protocol (IP) is the principal set (or communications protocol) of digital message formats and rules for exchanging messages between computers across a single network or a series of interconnected networks, using the Internet Protocol Suite (often referred to as TCP/IP). Messages are exchanged as data packets, or just packets.

[351] The *MBone* (short for "multicast backbone") is now referred to as the *Multicast Internet.* It is an arrangement whereby we use of a portion of the Internet for Internet Protocol (IP) multicasting (sending files - usually audio and video streams - to multiple users at the same time somewhat as radio and TV programs are broadcast over airwaves). The multicast internet uses a network of routers that support IP multicast, and it enables access to real-time interactive multimedia on the Internet. Tunnels must be set up on both ends: multicast packets are encapsulated in unicast packets and sent through a tunnel.

[352] Packets are A packet is the unit of data that is routed between an origin and a destination on the Internet or any other packet-switched network. Network packets are small (around 1.5 KBS for Ethernet packets and 64 KBS for IP packet payloads) amounts of data passed over TCP/IP networks. NB: This may have been defined once before, apologies if that was the case.

[353] Source: "Lightning Network enables Unicast Transactions in Bitcoin – Lightning is Bitcoin's TCP/IP stack," By Melik Manukyan [online – Medium]. Dated: January 9, 2018. See: https://medium.com/@melik_87377/lightning-network-enables-unicast-transactions-in-bitcoin-lightning-is-bitcoins-tcp-ip-stack-8ec1d42c14f5. See also: Ibid., [Foot Note # *349*].

constraints." Or to sum things up, Manukyan (2018) suggests: "Lightning 2.0. is what will power and transport effectively additional applications and protocols and additional layer-generated content. We must not forget that 'lightning hubs' are a false narrative. Lightning hubs, or the scaling approach of on-chain transactions, pushes us in the direction of an actual (ethernet) hub design, which defeats the purpose of the decentralization of the base layer, which is demanded of the distributed ledger."

By deploying Lightning 2.0 resources, OKEx – following the Nemertes Research Internet of Things (IoT) taxonomic guidelines once again – are reinforcing *their* dominant market-leading position, as a crypto services / crypto asset exchange, i.e. as an *operator* – and operators exercise significant influence over their Clients' activities.

Jay Hao, CEO OKEx goes on to state: "(We have also created) OKChain, independently developed by OKEx, which we view as fundamentally *completed* as one-hundred (100) per cent open-source (*A-Hem*!!). OKChain is a "commercial chain alliance" model, which will face *all* ecological nodes and provide efficient, free and boundless public chain ecosystems. It is a significant step for internationalization efforts.[354]"

The OCC, and other US regulatory bodies, have a big task ahead. Just these last few comments, especially with regards to rent-seeking behavior, first CoinLab founder Peter Vessenes giving it to JPM Coin. Next, OKEx defending – and then subtly deflecting away from their monopoly status – we can start to see that the world has a pressing and *real* requirement for consumer protection and asset management regulation, in terms of all things falling under the umbrella term *crypto*.

Let's give one last word to OKEx CEO Jay Hao, whom again goes on the public record (Cointelegraph) suggesting: "I was not surprised by the result of the U.S. Security and Exchange Commission's (SEC's) ban on Telegram tokens. Telegram is, Jason Hao believes, (elaborating on the nature of Telegram tokens) attempting to frame the Telegram Open Network as a practical tool for community members with *consumer uses*, while the SEC and the courts are more concerned about its financial attributes, believing that Telegram Open Network may flow out of control to the secondary market."[355] The take-away from Mr. Jao Hao, although let's not tar

[354] Source: "Sharing Thoughts on Security, OKEx' Jay Hao Says Customers Come First," By Vadim Kretokin, [online – interview by Cointelegraph China]. Dated: April 30, 2020. See: https://cointelegraph.com/news/sharing-thoughts-on-security-okexs-jay-hao-says-customers-come-first. Discussion: OKEx in this article reveal they have reached cooperation, via the OKEx "commercial chain alliance" model, with the world's seven largest legal fiat payment providers through their fiat gateway project. This fiat gateway project supports 30 fiat currencies, including United States dollars and euros, and accepts 17 payment methods including Visa and Mastercard. Also, "*we* [OKEx] have provided services to more than 20 million users in more than 200 countries and regions around the world, and that is still increasing." All under light regulatory approvals (ASMG wish to add that fact – our reflection on the side!). See *also*: *Ibid*., [Foot Note # *86*, *95, 355*].

[355] Source: "Sharing Thoughts on Security, OKEx' Jay Hao Says Customers Come First," By Vadim Kretokin, [online – interview by Cointelegraph China]. Dated: April 30, 2020. See *also*: *Ibid*., [Foot Note # *86, 95, 354*].

and feather CoinLab founder Peter Vessenes with the same brush, seems to be 'regulate, sure – but do it in a way that we condone, and approve it's ends'.

Advanced Systems Management Group (ASMG) reiterate our belief: trace the organization which is *speaking,* i.e. promoting itself, back to its roots. The way in which the OKExs (or CoinLabs) of the world are offering and structuring their technologies, and the effect that this technological prowess exerts over the financial system itself, applies significant pressure on regulatory efforts. By applying technical means to shore up their monetary and market-building *information advantage*, the very firms the OCC (and other regulators) are examining, are attempting to extract as much corporate 'self-serving rewards' as they can. Plan your regulatory program accordingly.

ASMG are not experts in regulatory issues, but we are experts on data and data security issues, and their complexities. A lot of regulation that we talk about is related to issuing payments, to monitoring investment products, and all these activities are about disclosure. For example, the bank needs to disclose their balance sheets, and the security firm needs to disclose the access of the client, the fund manager needs to disclose the buy and sell orders, and so on. That part Mr. Lennix Lai (OKEx) got right.

Any large financial institution in the US today is very familiar with banking regulations. Here are two examples. The Current Expected Credit Losses (CECL) regulation,[356] a new financial industry standard the SEC has cautioned will 'require credit issuers to estimate expected losses over remaining *life of loan* [obligations]', rather than rely on incurred losses (effectively).

The US Security and Exchange Commission's (SEC's) Allowance for Loan and Lease Losses (ALLL) provisions,[357] provides us with another banking regulation which most large banks are intimately familiar with. SEC's Allowance for Loan and Lease Losses (ALLL) regulation sets a valuation reserve, established and maintained by charges against a bank's operating income. The ALLL regulation monitors financial institutions (banks) to ensure that they have established,

[356] Current Expected Credit Losses (CECL) is a new credit loss *accounting standard* (model) that was issued by the Financial Accounting Standards Board (FASB) on June 16, 2016. This will significantly track losses a.k.a. via loss modeling, impacting both data collection (data need to be more granular) and modeling methodology (backward-looking over a short period of time, to forward-looking for the life of the loan). Revised interim final rule on CECL capital transition (March 2020) for the handling of 'loss claims' discusses timing, and extensions, as per when the CECL – the *new* credit loss *accounting standard* (model) will apply. Source: "Revised interim final rule on CECL capital transition," By RSM Consulting [online]. Dated "April 1, 2020. See: https://rsmus.com/our-insights/newsletters/financial-reporting-insights/revised-interim-final-rule-on-cecl-capital-transition.html. See *also*: *Ibid*., [Foot Note # *289*, *291*, *293-297*] 'In-depth analysis *a.k.a*. multiple viewpoints on Current Expected Credit Losses (CECL) provisions.'

[357] Allowance for Loan and Lease Losses (ALLL) is a valuation reserve, established and maintained by charges against a bank's operating income. It is an estimate of uncollectible amounts used to reduce the book value of loans and leases, to the amount a bank can expect to collect. The SEC warns: although management's process for determining allowance adequacy is judgmental - and results in a range of estimated losses - it must not be used to manipulate earnings, or mislead: investors, funds providers, regulators or other affected parties. See: https://occ.gov/news-issuances/news-releases/1998/nr-ia-1998-116-statement.pdf.

based on the estimated credit *risk* within total assets 'held by the institution,' a sufficiently large financial offset – calculated to accurately reflect the estimate of uncollectible amounts – used to reduce the book value of loans and leases, to the amount a bank can expect to collect. To conform with the SEC's Allowance for Loan and Lease Losses (ALLL) regulatory [provisions, large banks must be prudent in consideration or their data warehouse set-ups.

Additionally, in their efforts to be Allowance for Loan and Lease Losses (ALLL) provisions compliant, large bank's may wish to *synthesize* multiple loan systems and their servicers, since ALLL insists upon: a) consistent sources for internal/external reporting, and; b) long term storage of loan-level history.[358]

In today's extremely tight regulatory environment, following the global confluence brought on by securities (and trading and investment irregularities) a decade or so ago, or even after the recent pandemic-inspired economic collapse, regulatory actions take an equal or even more important precedence, over other financial institution (FI) priorities. The financial institutions (FIs), amongst themselves, are attempting to manage the lowest ceiling of required access and accommodation – extended to outside decision-makers (regulators) – as they endeavor to strictly guard their Customers' high-value (account) assets (HVAs). In a decentralized environment, Role-Based Access Control (RBAC) can provide an essential policy and administrative channel to support regulatory requests.[359] How this can be accomplished has not, so far, been conclusively demonstrated.

To get to a full understanding of data, or to achieve a comprehensive data management strategy, what might the toolkit items comprise of, to assemble an array of effective tools and resources, to make intelligible the data pipeline? The data pipeline – in a financial institution's (FI's) every-day working world, extracts a large operational toll in managing and updating its mission critical resources it manages. To achieve a full understanding of data, or to achieve a comprehensive understanding of data pipeline toolkit items, does require a little bit of work. The symbiotic relationship between the data pipeline, and its most important cargo – data – Involves a delivery model which changes with the architectural preferences expressed by an organization's enterprise architects. Plus, it varies if that enterprise architectural team works for a bank or investment management division of a financial institution (FI) a considerably sized Big Tech Company, a FinTech Operation, or for one of the new decentralized finance (DeFi) crypto asset and/or digital currency entities.

[358] Source: "ALL Today: Challenges and Solutions," (slide deck) By Tim McPeak, Sageworks [online]. Dated: September 14, 2016. See: https://s3.amazonaws.com/design.sageworks.com/images/blog/TheALLLToday915.pdf. '(McPeak-2016) Quoting a SageWorks Summit, Sept. 14, 2016 (Slide 12 of 36).'
[359] Source: "Role-Based Access and Containers as a Service," By Sara Jeanes [online – sumologic]. Dated: June 28, 2016. See: https://www.sumologic.com/blog/role-based-access-containers-service/.

Here are some of the available options: on-premise, at the edge or in the cloud hosting of AWS EMR,[360] Microsoft Databricks[361] platform configurations or installations, with the equivalent choice of 'on-premise, at the edge or in the cloud hosting' arrangements, or adopting a privately-designed/hosted data delivery mode or architected solution. Roughly-speaking, data pipeline tools will be divided into three groupings, not the most ideal demarcation, but it will have to do. They are: i) data productivity tools ii) data quality tools and iii) data connectors.

Data productivity tools are all over the map. They may include: i) Slack – a communications and collaboration tool; ii) Clockify – time-tracking software; iii) Google Calendar – an online Calendar function; iv) Google Drive – documents, sheets, slides, and a file-share *sync* service; v) Google Alerts – context change detector software solution, and; vi) DropBox – file history service. There are so many other examples available, they are simply too plentiful to tally up, and count.

Recently, new entrants have taken data productivity solutions, and bundled and expanded them, to include: i) augmented data catalogues ii) the inclusion / application of active metadata collaborative features (e.g. Zaloni); iii) adding software development kits (SDKs)[362] to add modern identity to native JavaScript, iOS and Android Apps (ForgeRock) – and other famous examples, such as Facebook with way too numerous a suite of software development kits (SDKs) to do justice by mentioning them here.

Facebook may serve as a useful example of a sophisticated data pipeline, and should not be passed up. Facebook's APIs communicate across the wider Facebook platform, utilizing the Social connections and Profile information data points of every Facebook User to conduct

[360] Amazon Elastic MapReduce (EMR) is one of the many services that Amazon Web Services (AWS – the Amazon cloud service provider/CSP *hosting platform*) offers. It enables users to launch and use resizable Hadoop clusters within Amazon's infrastructure. Like Hadoop, Amazon EMR can be used to analyze vast data sets. It also simplifies the setups and management of the cluster of Hadoop and MapReduce components. EMR configures and uses Amazon's prebuilt and customized EC2 instances. EC2 instances are firewall settings that control network access to *instances* automatically, and launches clusters in an Amazon Virtual Private Cloud/VPC - which is a logically isolated network you define. EC2 instances can take full advantage of Amazon's infrastructure, and other services offered by Amazon Web Services (AWS). Such EC2 instances are invoked when we initiate a new Job Flow to form an Elastic MapReduce (EMR) cluster. A Job Flow is Amazon's term for complete data processing that occurs through a series of computational steps, in Amazon's EMR. A Job Flow is defined by the MapReduce framework, and its input and output parameters. Source: https://www.cloudmanagementinsider.com/what-is-amazon-elastic-mapreduce-emr-briefly-explained/.

[361] Azure Databricks is an Apache Spark-based analytics platform optimized for the Microsoft Azure cloud services platform. Designed with the founders of Apache Spark, Databricks is integrated with Azure to provide one-click setup, streamlined workflows, and an interactive workspace that enables collaboration between data scientists, data engineers, and business analysts. Source: https://docs.microsoft.com/en-us/azure/databricks/scenarios/what-is-azure-databricks.

[362] Software development kits (SDKs) or *devkits* bring together relevant documentation, code, samples and processes, to create software applications on specific platforms. Most often, SDKs contain an API, whereas APIs are purpose-built, for a specific use e.g. 'allow communications between apps'. The API is the telephone line, while the SDK is the house itself. Source: "What is the Difference Between an API and an SDK?" By Kristopher Sandoval, blog post [online – nordicapis.com]. Dated: June 2, 2016. See *also*: *Ibid*., [Foot Note # *363*].

application functions. These may include "pushing" activity to send information in the form of news feeds, dealing with subscriptions to media outlets, collecting and collating group data – pages, photos, events logs – etc. The Facebook Communications API allows the possibility to limit data sharing on a per-User basis, allows Users to limit their Profile content and that content's *use*.

Facebook software development kits (SDKs) permit, for example, Facebook DevOps employees to create apps for iOS, for example, allowing a logging of application activations, the Facebook Communications API calls existing sources and functions, while the Facebook SDK is deployed to first *define* functions (which the User seeks), and mandates or *builds* the call-up for the source (and its function) itself. SDKs, in general, contain Libraries (to build functionality), Code samples (to increase understanding at implementation) and References (for easy linking and provision of explanations).[363]

Here is another new entrant paving the way with software development kits (SDKs), with 12 different SDK uses cases incorporated into their productization effort. The Company, mParticle, allows the building of a software development kit (SDK) to address a messaging audience, i.e. a messaging service which requires an email address, while another needs a Push token. This is accomplished by the mParticle's software development kit (SDK) built as ID Sync. ID Sync Search allows marketers to query User Profiles by any known identifier, such as email, mobile phone, or device identity, and return all matched User Identity values including the mParticle ID. The mParticle Profiler (ID) application programming (product) interface (API) gets the most up-to-date real-time User identities, User attributes, Device identities, and Audience memberships. Couple the mParticle Profile application programming (product) interface (API) with the mParticle ID, and you have everything you need to personalize the customer experience.[364]

Data quality tools, our second category of data pipeline tools under review, are also very broad in scope. Data quality tools serve to: standardize, cleanse, and enrich data in the data pipeline. They also cross-reference between datasets and data pipelines for the *task* of mapping Data Lineage, via data impact analysis reporting. Data impact analysis may include: data sampling, semantic discovery (of data), and data auto-profiling activities, however this list is far from exhaustive. Other areas that may be covered include: social curation (of data) with data sharing, data ratings assignments and data fields analysis (i.e. data endorsements). Here are two sample data lineage tools: i) Talend Open Source – provides file management and data flow orchestration on Windows, Mac OS and Linux for integrations / workflows, business / business intelligence; ii) Jaspersoft ETL (owned by Tibco) – data extraction, transformation and Loading tool offering: dynamic schema, data viewer, data language and multiple shared repositories.

[363] Source: "What is the Difference Between an API and an SDK?" By Kristopher Sandoval, blog post [online – nordicapis.com]. Dated: June 2, 2016. See *also*: *Ibid*., [Foot Note # *362*] '(Sandoval-2016) explanation of how software development kits (SDKs) work.'
[364] Source: "Use Cases for [mParticle] ID Sync," By mParticle staff [online]. Dated: June 8, 2020. See: doc.mparticle.com.

We'll complete this overview on data quality tools by looking at an example outside the financial service sector, for variety's sake. Talend offers an application programming (product) interface (API) which is a building block of code that helps that helps programmers connect their applications to data services. These data services connect businesses with customers, suppliers, and employees. Once data is accessible through an application programming (product) interface (API), it can be reused in a controlled way by potentially anyone within and beyond an organization. Billions of times each day, application programming (product) interfaces (APIs) facilitate the transfer of data between people and systems, serving as the fabric that connects businesses with customers, suppliers, and employees.[365]

Accor, a hospitality services conglomerate or multi-national enterprise (MNE) connects five thousand (5,000) Accor hotels and residences in one hundred (100) countries. These contacts hold many different types of data – personal data (credit card information, passport information), on-site satisfaction surveys, log calls from call centres, and loyalty points data. Accor engaged Talend[366] to collect 300 GB of data daily, on fifty (50) million customers, on fifty (50) different data (traffic) flows from eleven (11) business areas, including: reservations, payments, loyalty, marketing, preferences etc. All this was collected and collated by Talend on an Amazon Web Service (AWS) data lake via a Talend Data Catalogue.

For their (Accor hospitality service) data pipeline project, Accor's connected partners - their hotel network staff, networks gleaming data from the web and data retrieval from social media sites – all this information is stored in Accor's data lake, on AWS and connected to a Snowflake data warehouse – through Talend's Data quality tools. "There was a regulatory risk, but also an image risk for the Group," explained an Accor spokesperson. To mitigate these risks, Accor opted for Talend Data Catalogue, and invested a lot of effort in cataloging, creating a glossary, and developing documentation. Talend Data Catalogue brought about radical improvement in data lineage, enabling Accor teams to find customer data more quickly, and depending on the specific request, either retrieve personal information or destroy it. The Talend / Accor hospitality service data governance project was a joint effort, involving employees drawn from various business areas and IT, who worked together under the Accor Data Governance Board. The initiative also involved a team of one hundred (100) persons at headquarters, comprising business area representatives and data specialist teams, who were in turn supported by

[365] Source: "CIO: 3 Questions to Ask about your Enterprise Data Lake," By Ciaran Dynes [online – talend]. Dated: August 8, 2016. See: https://www.talend.com/blog/2019/11/19/build-responsive-intelligent-data-pipeline-focus-on-lifecycle/. See *also*: *Ibid*., [Foot Note # *35, 344, 365*]. See *also*: "Build a True Data Lake with a Cloud Data Warehouse," By Talend staffers [online]. Dated: not given *a.k.a*. [Foot Note # *366*]. See *also*: "Creating a company culture where the respect of personal data is top priority," By Maud Bailly, [online – talend]. Dated: 2020, *a.k.a*. [Foot Note # 367].

[366] Source: "Build a True Data Lake with a Cloud Data Warehouse," By Talend staffers [online]. Dated: not given. See *also*: "CIO: 3 Questions to Ask about your Enterprise Data Lake," By Ciaran Dynes [online – talend]. Dated: August 8, 2016 *a.k.a.* [Foot Note # *35, 344, 365*]. See *also*: "Creating a company culture where the respect of personal data is top priority," By Maud Bailly, [online – talend]. Dated: 2020. *a.k.a.* [Foot Note # *367*].

another eighty (80) data experts drawn from each business region and business functional area.[367]"

The third data pipeline toolkit categorization we will examine next, is loosely called 'connectors'. Data pipelines, in the popular idiomatic expression of DevOps professionals, are regarded, interchangeably, as 'data connectors'. It just goes to show how hard it is to define this third grouping of *connector* toolkit items.[368] So we won't even go there.
If all a data connector did was load data from applications and databases, into a central data warehouse, that would be a pretty simplistic wrap-up. Not true.

Here are a few of the complex issues the 'data connector' – data engineering (and DevOps) Team – may be tasked with addressing: i) standardizing connectors across an expanding, and diverse, inter-connected ecosystem or datasphere, where hardly anything is the same; ii) dealing with documented (and not-so-well documented or 'documents missing' challenges and special contingencies; iii) trouble-shooting *a.k.a.* validating data; iv) redacting and/or deleting data from data silos' (oftentimes dead-ended data silos), data lakes, databases and/or any other data geolocations (if they can be found, and accounted for).

Just in terms of this last point, point iv) 'redacting and/or deleting data,' this can be a very consequential activity, since if the data engineer's infrastructure and systems cannot detect the (data) deletion events – this may lead to troublesome *data remnants* being orphaned or left behind. If the data engineer's infrastructure components and toolkits (and software defined toolkits / SDKs) can't detect the (data) deletion events properly, this may leave behind these troublesome data remnants, which may prove deleterious to any / all existing data sets. They may be 'chock full' of unwanted data elements/data remnants, which may prove to be highly hazardous to data warehouse / data pipeline normalized 'and expected' functioning modes of operation, and as *unconsigned* data resources, they can seriously disrupt and negatively affect data impact analysis reporting or reviews your firm may be running.

When Companies build their own Extract-Transfer-Load (ETL) stacks, they employ four (4) to five (5) data engineers full-time. Configuring an ETL stack is a big job, and it gets bigger and harder to manage and maintain all the time. Standardized connectors, with well-documented data schemas, to trouble-shoot and validate data, and delete data – if your systems are prepared and set-up to accomplish these tasks, apply here as well. Ideally data connectors mark rows that are deleted instead of columns, which in the former case (rows) adheres to data queries requests you may wish to run. Data schema changes are not trivial! You may need to

[367] Source: "Creating a company culture where the respect of personal data is top priority," By Maud Bailly, [online – talend]. Dated: 2020. See: https://info.talend.com/rs/347-IAT-677/images/CS_EN_BD_CaseStudy_Talend_Accor.pdf. See *also*: "CIO: 3 Questions to Ask about your Enterprise Data Lake," By Ciaran Dynes [online – talend]. Dated: August 8, 2016 *a.k.a.* [Foot Note # *35, 344, 365*].
See *also*: "Build a True Data Lake with a Cloud Data Warehouse," By Talend staffers [online]. Dated: not given, *a.k.a.* [Foot Note # *366*].
[368] Source: "Data Pipeline Checklist," By Katie Chin [online – Fivetran]. Dated: not given. See *also*: *Ibid*., [Foot Note # *369*].

add a custom field to a source table (for example). However whichever vendor you are using will need to capture this adjustment, so it corresponds accurately to everything in your data warehouse. With some integration providers, the end User is responsible for monitoring (and adjusting) changes. You need to know if this is the case, in "your" case.

As far as data connector design features are concerned, it's common for an API data connector to offer a temporary disconnect when permissions change. Make sure your internal data engineering Team "get this." They need to physically contact the vendor / supplier (of data connectors) and ensure reconnections to the 'source' occurs, and you have not suffered data losses (or duplicated data fields, or irreplaceable data drift and/or data leakage, or outright data loss). These are very important data lineage events, tied directly to data integrity issues, which underpin your data warehouse, and data pipeline procedurally, and in operational dynamic terms as well.

Some data engineers *define* their data pipelines to provide a daily snap-shot approach, due to the fact this is easier to build. If your internal data engineering team are doing this, ensure all work communicates effectively with a third-party vendor (and their data connectors) and that all replenishment activities occur incrementally.

And lastly, Fivetran's Katie Chin asks: "Is your data connector provider a partner to your business success, or a commodity product only? If you only have one (data) connector, support might not be as crucial, but in today's ever complex data environment, don't count on it! Find the right data connectors – data pipeline Support Package that works, and monitor its compliance measures and metrics religiously.[369]

We have moved from a touchy-feely approach to regulation, with our initial commentary provided us from the crypto currency advocates – Peter Vessenes, Lennix Lai and Jao Hao – and pivoted to the hard-core realities faced by an actuary or a forensic accountant, based in the busy Operations (Legal and Administration/Regulatory Compliance) Department of a major bank, to drive home the observation that RegTech is not a topic to address lightly!
For example, banking institutions face a huge number of issues daily, as they go about their business. The financial services and investment brokerage and management industry segment, will – by necessity – remain fixated on their mandate to 'square-up' with systems and protocols (SWIFT, SEPA, FIX, etc.,) covering the complex set of business lines and business services offered in banking and investment management at present:
– Retail Banking; Real Estate; Risk and Compliance Departments (KYC/AML/CDD etc.); Trade Finance (Letters of credit / Letters of mortgage); Investment Banking, and Banking Admin Departments (HR and Digital Mailrooms, etc.), to name but a few. All these activities require

[369] Source: "Data Pipeline Checklist," By Katie Chin [online – Fivetran]. Dated: not given. See *also*: *Ibid*., [Foot Note # *368*] '(Chin-Fivetran) *knowing* and *doing* – all you need to know about data pipelines and data connectors.'

vigilance, and all are at high risk for information *compliance* and *assurance* (C&A) monitoring (and reporting):[370]

- Risk Governance *requiring* stress testing
- Finance Risk *asking* for monitoring of loan limits and collateral management
- Operational Risk *requires* reconciliations i.e. general ledger (daily) via metrics & dashboards
- Compliance risk *a.k.a.* regulatory reporting, and
- Financial Crime (seems crypto asset players get a *pass* here?) *performing*:

i) transaction monitoring ii) client screening / client onboarding / due diligence iii) investigative case management (across all banking activities) and iv) trade surveillance.

On the point referring to Compliance risk – *a.k.a.* regulatory reporting – risk regulation under Basel III (and other regimes), legal settlements engendered from compliance issue malpractices, or fines and sanctions ear-marked to deal with banking services complaints, or examinations of IT requirements to meet Sarbanes-Oxley (SOX) [certification requirements], etc., these are all tricky topics! They require banks and investment management dealers to combine data from far more internal systems than they are accustomed to integrating. As well, banking and investment brokerage functions are clamoring to create more powerful analytics, to deep-drill more extensively, into their legacy systems.

As we pointed out in our first comment appearing in Advanced Systems Management Group's (ASMG's) Answer to Q1 – 'recent technological advances' citing the Data Age 2025 Report[371] a collaboration between Seagate and IDC – the growth of the global datasphere [IDC (2018)] forecasts that more than 150B devices will be connected across the globe by 2025, most of which will be creating data in real-time. These estimates indicate the quite startling observation that five years from today, every connected person in the world, on average, will have a digital data engagement – over 4,900 times per day – which is approximately 1 digital interaction every 18 seconds.

Yet, for all intents and purposes, the cryptocurrency segment of the financial services and investment management industry is occupying a very wide berth, encompassing very little supervision from regulators, and not nearly anything close to the in-depth supervisory and regulatory lens which focuses its attention on banks and investment management firms, at present. Across the financial and investment brokerage sector of the economy, there are literally a huge basket of items to regulate and monitor. In short, eCommerce, *mobile*, batch,

[370] Source: This list is adapted from chart provided by (author) Joan McGowan-Celent, "High-Impact Risk and Compliance Robotic Process Automation (RPA) Use Cases." Dated: August 29, 2018.
[371] Source: "The Digitization of the World: From Edge to Core," By David Reinsel, John Gantz and John Rydning, IDC White Paper [online]. Dated: November 2018. See: https://www.seagate.com/files/www-content/ouar-story/trends/files/idc-seagate-dataage-whitepaper.pdf. See *also*: *Ibid*., [Foot Note # *7, 11, 25, 27*].

Third Party ingress, *web* (and Cloud) services, P2P network communications, etc. etc. This represents a lot of real estate to cover! Advanced Systems Management Group (ASMG) do not possess intimate familiarity with the set of regulatory issues OCC addresses, on a day-to-day basis. Our best approach *here* is to provide a horizon scan, and we will refer to – PwC (US) "Financial Services Technology 2020 and Beyond (2020)"[372] – Report to assist us in making that technological scan useful.

Advanced Systems Management Group (ASMG) will conclude this section Q.8 'Regtech and the OCC: Governance embedded in technology' on the not-so-satisfying admission that this is a very difficult topic for a technology firm such as ours to address. We will nonetheless proceed. These information *compliance* and information *assurance* (C&A) monitoring and reporting challenges, McGowan (2018)[373] has sub-divided into four (4) topics – appearing under a *financial crime* (reporting) presentation Joan McGowan made a few years back. These are a convenient ranking of a basket of issues, we will sort through next. They are: **i**) trade surveillance **ii**) client screening / *client onboarding* / due diligence **iii**) investigative case management (across *all* banking activities) and **iv**) transaction monitoring.

[372] Source: "Financial Services Technology 2020 and Beyond: Embracing disruption," By Julien Courbe, PwC US [online]. Dated: 2016. See: https://www.pwc.com/gx/en/financial-services/assets/pdf/technology2020-and-beyond.pdf. See *also*: *Ibid*., [Foot Note # *405*, *406*].

[373] Source: "Why Investigative Case Management Is So Important for Banks," By Joan McGowan, Celent. [online]. Dated: August 15, 2017. See: https://www.celent.com/insights/956630691.

8.1 Trade surveillance

Trade surveillance is a prime example of how regulatory requirements have multiplied and diversified, with more firms expected to monitor and report market abuse across more markets and jurisdictions, and at greater speeds, than ever before.[374] O'Hara/Hall (2017) have some very penetrating insights into the application of machine learning (ML) and AI to automate and monitor persistent trading threats and abusive trading behaviours. O'Hara/Hall (2017) cite the roll-out in Europe, in January 2017, of the Market Abuse Regulation (MAR) which applies to companies with securities, admittedly trading in the EU, but also has implications for U.S. issuers that may have debt and equity securities (admitted *to*) trading in the EU, including Eurobonds that have been (admitted *to*) trading on previously unregulated exchanges, such as the Dublin and Luxembourg exchanges.

The EU's Market Abuse Regulation (MAR)[375] outlines market abuse, market manipulation and insider dealing. It prescribes rules relating to, *inter alia*, the disclosure of inside information, the maintenance of insider lists and dealings in securities by persons discharging managerial responsibility (PDMRs) with the aim of enhancing market integrity and investor protection.[376]

The EU's Market Abuse Regulation (MAR) has extended the types of trades to be monitored from those conducted in regulated markets, to many other varieties of activities. These include the noteworthy category of over-the-counter (OTC) transactions, such as swaps. And although T+1 reporting of abuse is acceptable – for the moment – the direction of travel is clearly toward intra-day, and eventually real-time monitoring. In addition to the Market Abuse Regulation (MAR), the UK's Senior Managers Regime – effective for banks from March 2016 and for asset managers from 2018 – requires regulated firms to designate, and demonstrate, personal responsibility for trade surveillance, along with other key operational areas.

[374] Source: "The future of trade surveillance – Separating the Spoof from the Truth," By Mike O'Hara and Chris Hall, The Realization Group [online]. Dated: June 2017. See: https://www.therealizationgroup.com/wp-content/uploads/2017/06/FMI_The-future-of-trade-surveillance-170427.pdf. See *also*: *Ibid*., [Foot Note # *377. 378*].

[375] The EU's the Market Abuse Regulation (MAR) also extends the scope to cover orders to trade in one product to affect price of a related instrument, including transactions in underlying instrument to influence price or value of derivatives (or vice versa), even if carried out on the same venue. It includes surveillance requirements across securities that are not necessarily explicitly related, such as the monitoring of trading across instruments that have an economic relationship with each other (and not just securities/assets and their derivatives). Source: "Market Abuse Regulation (MAR): What you need to know," By Bloomberg Professional, [online]. Dated: April 11, 2016. See: https://www.bloomberg.com/professional/blog/market-abuse-regulation-mar-what-you-need-to-know-2/.

[376] Source: Source: "Market Abuse Regulation (MAR): What you need to know," By Bloomberg Professional, [online]. Dated: April 11, 2016. Discussion: Bloomberg (2016) have compiled a list of twenty (20) no-go activities, which include: collusion; floor/ceiling price pattern, ping orders, phishing, abusive squeeze, inter-trade venue manipulation, cross-product manipulation, painting the tape, improper matched orders, concealing ownership, wash trades, trash and cash, quote stuffing, momentum ignition, layering and spoofing, no intention of executing orders, excessive bid/offer spread, advancing the bid, smoking and; pump and dump. See *also*: *Ibid*., [Foot Note # *375*] '(Bloomberg – 2016) no-go listing of viable Market Abuse Regulation (MAR) infractions.'

Nick Gordon, Certico suggests in his opinion piece – quoted by O'Hara/Hall (2017) – that: "Regulators expect firms to demonstrate understanding and oversight, where the risks are most severe. Multi-legged orders involving a variety of counterparties, exchanges or instruments require 'particular scrutiny,' with risks assessed and monitored both at the individual transaction and holistically, at the parent order level. Nevertheless, alerts must be finely tuned, as there are good reasons – from both a business and compliance perspective – to avoid false positives."

O'Hara/Hall (2017) cite how technology is accelerating regulatory effectiveness. "In broad terms, systems and applications that deploy AI are making 'smart,' logical decisions based on analysis of the structured, and even unstructured, data they consume. This means the potent twinning of AI and ML systems, the latter effectively a subset of AI, can adapt to circumstances, think for themselves, even infer meaning from natural language processing (NLP). This, as we stated, potent twinning of ML inference engines and AI algorithmic modeling and processing advances can not only recognize patterns denoting potentially abusive behaviour, but can also identify new threats as they emerge. Or, explore evidence or contextual data, once unusual behaviour is flagged, for further investigation.[377]

Valerie Bannert-Thurner, the Global Head of Risk and Surveillance sSlutions at Nasdaq, adds an opinion to the O'Hara/Hall (2017) article, which is very timely. Bannert-Thurner (Nasdaq) suggests "ML can play multiple roles in trade surveillance, from identification of potential abuse to decision support to trade reconstruction. For example, Nasdaq is exploring the role of ML in the ranking and scoring of alerts that its trade surveillance solutions brings to the attention of customers. By learning from the past, i.e. how previous alerts were responded to and acted upon by clients, individually and collectively, ML-powered tools can rank future alerts in accordance with their likely importance and relevance to each client. This will further reduce the time spent on investigating false positives. It could also help us to further fine-tune alerts and provide guidance to users on the setting of appropriate parameters.[378]"

Enough of the market-scan and enviro-scan. Sure, ML-based tools are being developed to scour disparate sources of written and verbal communications, to parse the intent and meaning behind words and phrases used in emails, conversations, etc. It certainly goes without saying that an investigator, and a financial institutions' (FIs') compliance staff member, are becoming more and more attuned to sourcing explanations from fund managers or traders, about a specific stock, or what was going on at the time of an asset's trading execution or transaction clearing event. As it were, we are fully aware that (ML and AI) systems can also, admittedly,

[377] Source: "The future of trade surveillance – Separating the Spoof from the Truth," By Mike O'Hara and Chris Hall, The Realization Group [online]. Dated: June 2017. See: https://www.therealizationgroup.com/wp-content/uploads/2017/06/FMI_The-future-of-trade-surveillance-170427.pdf. See *also*: *Ibid*., [Foot Note # *374, 378*] '(O'Hara/Hall -2017) AI and ML inference engines combine to flag new avenues for threat emergence, threat discovery.'

[378] Source: "The future of trade surveillance – Separating the Spoof from the Truth," By Mike O'Hara and Chris Hall, The Realization Group [online]. Dated: June 2017. See: *Ibid*., [Foot Note # *374, 377*] '(O'Hara/Hall -2017) Nasdaq expert suggests ML-powered tools may provide governance and guidance on setting risk alert parameters.'

reduce information asymmetry, and give an insight into how today's trading by a fund manager compares to his/her normal pattern of trading performance, and their trade activity execution activities are undertaken responsibly and appropriately.

Let's look at a specific installed example. The one we have chosen is one close to home for Advanced Systems Management Group (ASMG): ScotiaBank's "four-pronged" AI -driven data capture, OCR, Automated Compliance, and Anti-Money Laundering (AML) approach, implemented within its Trade Finance business vertical.[379] ScotiaBank's Trade Finance project performs four (4) things: i) automated screening of documents against Trade Based Money Laundering Red Flags; ii) automated document checking against a contract such as a SWIFT MT 700; iii) provides business insight, through exposing extensive data from the trade documents, and; iv) compiles real-time Compliance monitoring on all data.

ScotiaBank's Trade Finance Group chose the Conpend[380] solution. Conpend's Trafinas (TRAde FINance ASsurance)[381] trading platform – and its applications – captures, identifies and classifies documents for Scotiabank's complete set of platform-based trading transactions. ScotiaBank Trade Finance have achieved, through Trafinas deployment, a configurable workflow within the application, allowing for seamless movement of work between Clients, Operations and Compliance. This workflow can be tailored in accordance with the banks requirements, providing a "single version of the truth" for audit purposes, and may be deployed both on-premise, and in the cloud.

There are plenty of other vendor products addressing this niche. One is a trading reconciliation platform called Onetick.[382] Onetick provides a web dashboard with pre-coded compliance rules covering – Market Abuse Regulation (MAR), MiFID II, SEC FINRA and IIROC regulations. Plus, Onetick offers parameterized alert thresholds, email notifications, and market data. OneTick can capture streaming market data from any source, with clients receiving ultra-low latency access to the latest 'tick data'. OneTick can collect every tick for all markets globally, regardless

[379] Source: https://www.finextra.com/pressarticle/76192/cgi-partners-with-scotiabank-on-intelligent-process-automation-proof-of-concept-for-trade-finance. See *also*: *Ibid*., [Foot Note # *316, 380, 381*].
[380] Conpend - established in 2016 - emerged from Proferus, an Amsterdam based company with expertise in professional services for trade finance, payments and cash management within banking and the financial sector. Conpend own the Trafinas platform, selected for ScotiaBank's Trade Finance project. See: https://www.conpend.com/cgi-partners-with-scotiabank-on-intelligent-process-automation-proof-of-concept-for-trade-finance-transactions/. See *also*: *Ibid*., [Foot Note # *316, 379, 381*].
[381] Source: https://appsource.microsoft.com/en-us/product/web-apps/conpend.trafinas2. Discussion: Trafinas is a robotic process automation (RPA) solution developed specifically for Trade Finance transactions. Given its modular, micro-service based design, Trafinas can easily integrate with existing Client Portals and Trade Finance or Core Banking back office systems. Use of existing infrastructure such as Document Management Systems for text extraction (OCR) and document storage is supported. Trafinas has been deployed both on-premise and in the cloud. See *also*: *Ibid*., [Foot Note # *316, 379, 380*].
[382] Source: https://ftp.onetick.com/web1/one_database_more.php. OneTick also has advanced data loading / Arcive DataBase Loading: OneTick builds intelligently compressed archives from data collected in real-time (e.g. Reuters, Wombat, direct market feeds, etc.) or from batch sources such as TAQ daily files, NYSE Open Book daily files, LSE daily files, etc. Data archival (materials) are completely transparent to users.

of asset class, data volume (including Options Price Reporting Authority / OPRA data from all US options exchanges), peak data rates or type of data (including full depth of book) data reporting / data response categories monitored, or placed under surveillance. Clients for Onetick's trading reconciliation platform include proprietary traders, hedge funds and investment banks and their customers.

Where does that leave us today, in the global pandemic world in which trade execution is situated? Coronavirus chaos is giving rogue traders cover in their never-ending shadow war with regulators and trade surveillance firms. Remote work is allowing them to operate away from the prying eyes of bosses and colleagues. At the same time, extreme market swings have sweetened the pot for rogue traders by raising the specter that trading on material nonpublic information could yield a huge payday.[383] Dibble (2020) reports: "Greenwich Associates said one global banking client logged 35,000 false positives on a single trading day in March, compared with 5,000 on average. In some cases, compliance staff took two to three weeks to review alerts normally evaluated on the same day. Add to this (Dibble 2020) makes the astute comment that the SEC received about 4,000 whistleblower tips from mid-March to mid-May 2020 — a thirty-five (35) per cent Year-over-Year increase, likely attributable to a spike in illicit activity, and an increased feeling of security for remote-working tipsters, what with the recent surge in whistleblower payouts by the SEC. In March (2020), the SEC took the unusual step of warning corporate executives against insider trading. Delays and outages have also hamstrung the SEC's efforts to monitor trading electronically. The Consolidated Audit Trail Project (CATP), designed to give the agency an oracular real-time window into daily trading activity, has been delayed until 2022, and faces privacy concerns on Wall Street.

Is this launching a *new era* for trade surveillance? It seems a logical question to begin asking, and should the OCC – and other regulatory organizations – begin now to start assembling a technological strategy, that might be a very effective way to address these ongoing technological developments.

8.2 Client onboarding

Client onboarding is the action or activity required by a bank or financial institution (FI) to create an identity for a new customer, and verify that current customers are who they say they are, when they access banking services. This customer identity enables the bank or financial institution (FI) to match customers to a predefined listing or menu of financial services, set up by the bank's depository and credit departments, and investment management divisions, to entice customers to access the *pre-defined*, personalized set of service offerings on tap.
A basic Know Your Customer (KYC) process, with customer background checks, allows the financial institution (FI) to measure the risk they pose. This first step is termed Customer Due Diligence **(**CDD). Usually this is all that is required.

[383] Source: "Shadow War Between Rogue Traders and Surveillance Firms May Decide Traders WFH Fate," By Jason Dibble. [online-eventus-in-the-news]. Dated: June 5, 2020. See: https://www.eventussystems.com/rogue_traders_surveillance_and_wfh/.

Users' (the bank's front-line employees) – should they identity a profile showing a higher-risk *e.g.* anti-money laundering (AML) or countering terrorist financing (CTF) irregularity – may take the next step, and accelerate to Enhanced Due Diligence (EDD). Factors triggering enhanced due diligence (EDD) are: i) beneficial ownership, ii) politically exposed person (PEP) identifier(s), iii) connections with high-risk countries, iv) high transaction amounts, and v) involvement in high-induced activities. Enhanced Due Diligence (EDD) may involve asking the customer for the verification of their identity, or verification of the source of income. The story doesn't end once you have *onboarded* a client, and established business relationships. Due diligence remains active, as there is always a chance of your client's profile changing – finding their name appearing on a politically exposed person (PEP) list, the Client involving themselves (or others) in high-risk transactions – or simply, committing a fraudulent transaction.

Customer onboarding has increasingly migrated away from in-person and in-branch activities. In-branch banking and investment management service interactions are being rapidly replaced by customer onboarding in the 'Client at home' or 'Client on mobility device' mode or setting. The mainstream or traditional banking segment has now joined the ranks of new financial institutions (FI) players, such as hybrid (crypto asset and traditional depository banking), Big Techs and FinTechs, in rapidly promoting an on-boarding process. This is taken a step further with *digital* onboarding. A customer's digital lifecycle – whether that addresses onboarding or electronic signing on digital transactions – relies on the merit of the entire digital interaction, as digital-first and digital-focused journeys usually lead to higher customer-satisfaction scores.

By linking the level of service offered to their customers directly with their drive to innovate, there is an important compliance requirement behind these actions. Financial institutions (FIs) are required to undertake security measures, and perform regulatory compliance reporting, *a.k.a.* addressing the Know Your Customer / anti-money laundering (KYC/AML), and Countering Terrorist Financing (CTF) regulations, in their jurisdictions. By maintaining scrutiny of client transactions and interactions, and monitoring their risk-taking activities, the institution's business and fiscal exposures can be rigorously protected. Should a crisis condition be uncovered, actions can be initiated to stem, and/or prevent the crisis from escalating, and the financial institution can ensure they are fully compliant with all applicable regulations, enforced by the regulator they are registered with. With the rise of financial crime, and the costs associated with compliance, as well as the growing threat of digital disruption, it has never been more important for financial institutions (FIs) to embrace technologies that streamline compliance processes.

One of the technologies that can help with safe onboarding is the deployment of network access controls (NACs).[384] In the past, companies used only desktops and laptops, connected and authenticated over a wired network. However nowadays, wireless networks and mobile technologies have introduced personal devices – the bring-your-own-device (BYOD) to a transaction – trend, the hallmark of Internet of Things (IoT) interconnectedness. In addition, increasingly stringent compliance measures, such as PCI-DSS, SOX, and ISO standards, require companies to openly communicate the security controls applied to all APIs, which conduct the Clients' interactions with the financial institution (FI). These API security controls must be registered with external auditing authorities. All these can be achieved via NAC solutions.[385]

Banks can accelerate client onboarding by capturing biometric identity documents (such as face and voice recognition) in the branch, or via the Internet-of-Things (IoT) mobility-enabled encounter. This begins with the customer onboarding registration phase of the interaction. For all subsequent branch interactions, some — or any of these — biometrics can be used to painlessly authenticate the customer.[386] But what if the customer isn't the problem, but the bank, or hedge fund, or financial institution (FI), or other financial sector Stakeholder might be the problem? Hold your hats, and read this next.

The 'Secrets of the World's Biggest Hedge Funds Exposed' reads the latest media headline! An exfiltration and {ransomware) encryption attack has just been reported. On Thursday July 23, 2020 came the first situation: Hedge Fund Angelo Gordon receives a message from its external fund manager, SEI Global Fund Services, that they have been breached. SEI Global's third party vendor (software and services supplier) A.J. Brunner (Pittsburgh/Atlanta-based) – a company provisioning SEI Global with their investment dashboard and enrollment *onboarding* portal – were the afflicted party. The A.J. Brunner investment dashboard and customer onboarding suffered a breach by hackers of "discrete pieces of user information," which were permanently stolen, with *no copy-left-behind*. The SEI Global Investor Dashboard was where online accounts were located, holding confidential and private high value asset (HVA) account information.

[384] Any network access control (NAC) product's goal is to defend the entire perimeter of an organization's network. NAC policy is a list of rules, specific to your enterprise, which dictates who can access which resources. This is typically done through a two-stage process: authentication and authorization. If either step fails, the request is blocked to preserve the safety of the network. This is what's known as zero-trust security. A few examples of service offerings include: Cisco Identity Services Engine; Pulse Policy Secure (for mobile devices); Aruba ClearPass twinned with Aruba Policy Enforcement Firewall and, FortiNAC (for physical and virtual environments) and ForeScout CounterACT's security silos on a 'single Internet-of-Things (IoT*) a.k.a.* '[IoT-Hardware automated] management portal.'

[385] Source: "The Best Ways to Secure Device Onboarding in the Enterprise," By Ofer Amitai, Founder-Portnox [online]. Dated: September 26, 2018. See: https://www.portnox.com/blog/cloud-security/the-best-ways-to-secure-device-onboarding-in-the-enterprise/.

[386] Source: "Explainer: Verification vs. Identification Systems," By Stephen Mayhew [online – biometricupdate.com]. Dated: June 28, 2012. See: https://www.biometricupdate.com/201206/explainer-verification-vs-identification-systems.

Countless other funds use SEI Global Fund Services for their funds administration. Dow Jones reported July 27, 2020 that the other Companies under suspicion of being hacked include: Graham Capital, Fortress, Centerbridge and even PIMCO. Hackers simply isolate the weakest link in the M.J. Brunner-supplied investment dashboard and enrollment *onboarding* portal platform, and all personal information contained there is manipulated and exposed for the world to see. Unidentified hackers took files from A.J. Brunner that contained user names and emails – and in some cases physical addresses and phone numbers – associated with the A.J. Brunner software's library functions, and portal and dashboard distribution mechanisms. Over 570 GB in data was published online. More importantly, Structured Query Language (SQL) files that include 'live' client data, including positions, trades and Profit and Loss (P&L) statements, were all directly affected by the breach and theft. As of June 30, 2020, SEI Global had $693 Billion in client assets under administration, and managed or advised on additional assets. Investors in funds which SEI Global Fund Services counted as their high value (account) asset (HVA) clients, include: pension funds, endowments and wealthy individuals and families. SEI Global say their intra-company network wasn't affected or compromised, and their network didn't detect a vulnerability (Finger-pointing?). A.J. Brunner had immediately notified the FBI upon discovery of the breach and theft, and will continue to work through the ongoing investigation effort.[387]

This attack is the latest ransomware incident affecting financial-services companies, initiated through their far less secure suppliers. Officials from the National Security Agency (NSA) have warned of this situation affecting vendors and service providers as an emerging threat vector, for some time. Those warnings were well placed.

8.3 Investment case management (Investigative case management)

Agencies involved in investigation processes deal with vast amounts of information, both in physical and digital forms. Two primary investigation process model requirements are: **i**) The solution must be specific enough that general technology requirements for each phase can be developed – such as forms and formats to eliminate manual processes, role-based security, notification controls, etc. – and reporting capabilities, to meet compliance and authorization (C&A) audit requirements, are adhered to; **ii**) The foundation of the solution must apply to any investigative process – the workflow must be built *in* to the system, built *in* to the decision-support efforts, and must be capable of withstanding minor customizations, yet still maintain systems integrity and compliance – while supporting data records-keeping functions, and observing systems best practices.[388]

Another way of summarizing this, to cover common traits of the business process which are required to be managed by the case management solution, should be to:

[387] Source: "Fund Administrators for Fortress, PIMCO and others Suffers Data Breach Through Vendor," By Dylan Tokar, James Rundle and Juliet Chang, The Wall Street Journal [online]. Dated: July 27, 2020.
[388] Source: https://www.columnit.com/case-management-a-progression-in-investigation-case-handling.html.

- Require some form of research or investigation
- Mandate an end-point, or an organization to monitor the *informed* decision making
- Require formal process tracking, for internal or external policies, auditing or compliance.[389]

In the US, the Consumer Financial Protection Bureau (CFPB) are heavily invested in analytics and digital technologies. For example, the Consumer Financial Protection Bureau (CFPB) created *eRegulations*, an online tool to help users find, research, and understand regulations.[390] Also the Consumer Financial Protection Bureau (CFPB) operates the open source data platform, called *Project Qu*. Project Qu lets users query complex data about mortgage loans, combine it with other data, and then summarize it. The OCC's sister regulatory agency – the SEC – operates its National Exam Analytics Tool (NEAT) through SEC's Office of Compliance Inspections and Examinations (OCIE). The National Exam Analytics Tool (NEAT) platform has invested significant resources to enhance its data mining and data analytics capabilities. SEC's National Exam Analytics Tool (NEAT) combs through data, then identifies potential insider trading, improper allocation of investment opportunities, and all other infractions it may choose to isolate. This is a well-established field of expertise – for regulatory organizations[391] such as the OCC – to navigate in. Far be it for a technology entity, and a standards-body member company such as Advanced Systems Management Group (ASMG), to offer advice to the OCC on how you pursue your work.

The best Advanced Systems Management Group (ASMG) might be able offer *here* – in response to Q.8) 'RegTech and the OCC: Governance embedded in technology' – might be to review the technologies behind two investment case management solutions marketed today. They are: **i**) *trading* – (investment) portfolio management platform(s) - *two* and; **ii**) *investment* – one example (Consumer wholesale and Retail) *client advisory* platform.

For the first example (of two): – *trading* (investment) portfolio management platform(s) – we will examine are: a) the BlackRock Solutions (BRS) Aladdin Platform; and secondly: b) the Sentient Investment Management Platform, since sold to a Company called Emerj.

The BlackRock Solutions (BRS) Aladdin Platform and the Emerj (was Sentient Investment Management) Platform are unlike one another, in almost every regard. Specifically, the latter

[389] Source: "The Value of Case Management in Financial Services," By Fiserv staffer [online]. Dated:2016. See: https://www.fiserv.com/en/about-fiserv/resource-center/point-of-view-papers/the-value-of-case-management-in-financial-services.html.
[390] Source: http://www.consumerfinance.gov/eregulations/.
[391] In Europe, regulators have put quite a bit of emphasis on how technology is used. The UK Financial Conduct Authority (FCA) are focused on ensuring financial institutions (FIs), including insurers' do not abuse their newfound 'big data power.' Source: FCA warns insurers' use of Big Data could penalize customers," By Caroline Binham [online – Financial Times]. Dated: September 21, 2016. See: https://www.ft.com/content/dd7d1c47-087c-3db8-9252-1ef9c4ea3b01. Other EU regulators are employing big data analytics to see if current regulations and supervisory measures are sufficient. See: https://eba.europa.eu/documents/10180/2157971/Joint+Committee+Final+Report+on+Big+Data+%28JC-2018-04+%29.pdf.

investment case management trading platform is highly innovative – moving *trading* into the deep learning (AI) realm. Our third investment case management solution serves a slightly different vertical, but in most respects, similar in its functionality to the BlackRock Solutions' (BRS') Aladdin Platform. This third trading and investment case management platform, occupies the second niche 'Consumer wholesale and Retail) *client advisory*. Vanguard Group's in-house designed and pioneered *new* robo advisor interacts with Clients only, no human agency allowed!

First, let's examine BlackRock's initiative. BlackRock is one of the world's largest investment management firms. They built their Aladdin Risk Management Platform[392] to service investment management professionals, with an operating system tailored specifically for investment management professionals' needs and requirements. The Company claims their Aladdin Risk Management Platform can use machine learning (ML) to assist the investment manager professional in their financial institution (FI) business dealings, and can solidify all their risk analytics and portfolio management decision-making activities into one place.

The BlackRock Solutions (BRS) Aladdin Platform's software tools enable individual investors, and the investment asset managers themselves, to assess the levels of risk, and integrate and connect functions, that help *manage money*. From portfolio management teams, to trading and compliance, operations and risk oversight employees of BlackRock, BlackRock Solutions (BRS) Aladdin Platform brings together people, processes, and systems. This triumvirate of stakeholders is assisted, and supported, by a seamless investment process.

The BlackRock Solutions (BRS) Aladdin Platform's functionality allows teams across investments, trading, operations, administration, risk, compliance, and corporate oversight branches or divisions of the Company, to use the same *consistent* process, and share the same *relevant* data.[393] The company claims that the BlackRock Solutions (BRS) Aladdin Platform can automatically monitor over 2,000 risk-related factors per day (like interest rates or currencies rates), and test portfolio performance under different economic conditions. For example, an investment management firm might find it possible to augment the capabilities of human investment managers using BlackRock Solutions (BRS) Aladdin Platform's informed decision-making, effective risk management, and efficient trading capabilities.

BlackRock Solutions (BRS) Aladdin Platform's capabilities extend to provide multiple, extensive sets of prediction parameters or metrics to Users', which determine their (the Users') portfolio's performance – much faster than if done manually – in real-time. The platform can potentially be fed with *input* data, in the form of trading performance histories, for any/all securities selected, and fully reflects the trading performance within a fund's holdings. BlackRock Solutions (BRS) Aladdin

[392] Source: "Machine Learning in Investment Management and Asset Management – Current Applications." By Raghav Bharadwaj, Analyst [online –Emerj]. Dated: April 3, 2020. https://emerj.com/ai-sector-overviews/machine-learning-in-investment-management-and-asset-management/.
[393] Source: "Aladdin FAQs," By BlackRock analysts [online]. Dated: 2020. See: https://www.blackrock.com/aladdin/resources/faqs.

Platform's extended capabilities, serve also to provide tracking data on risk factors – to predict future performance – under different economic test conditions.

An article in the Financial Times[394] reported that BlackRock is in the process of setting up a new BlackRock Lab for Artificial Intelligence in Palo Alto, California. The BlackRock Lab for Artificial Intelligence will be focused on developing new applications of AI and ML knowledge, as applied to newly emerging asset and investment management issue areas, as they become known and are identified.

In 2014, the Oregon State Treasury (OST) recommended that the Oregon Investment Council (OIC) contract to acquire the BlackRock Solutions (BRS) Aladdin Platform. Aladdin will perform the Oregon Investment Council's (OIC's) asset risk management investigation and discovery service. This was aimed at providing the Oregon State Treasury's (OST's) staff with risk analytics and portfolio management tools and toolkits, enabling the OST investment management Team members to be able to generate, in-house, customized risk reports (e.g., duration, geographic and sector exposures, scenario analyses, etc.) in support of the state's $90 billion investment portfolio. A 2015 Report from the Oregon State Treasury (OST) describing the Oregon Legislature Offices' implementation of Aladdin on their premises, said that it required six months to implement and bring on-line.

The BlackRock Solutions (BRS) Aladdin Platform, installed at the Oregon Legislature Offices (OLO), went live in September 2015. Results captured in the December 2015 OLO Report clearly state that investments totaling $42.2 billion, making up most of the Oregon Public Employees Retirement Fund's (OPERF's)[395] investment portfolio, were now successfully monitored using Aladdin. The Oregon State Treasury (OST) investment management staff had engaged a few outside consulting systems experts, along with a team from BlackRock Solutions (BRS) to complete the Aladdin investment risk management platform's installation on their premises.

The Oregon Public Employees Retirement Fund's (OPERF's) $25.8B portfolio of illiquid / alternative investments were found to be well-managed by the BlackRock Solutions (BRS) Aladdin Platform. Aladdin exceeded performance expectations and delivery objectives, which all three organizations – the Oregon State Treasury (OST), the contracting designee the Oregon Investment Council (OIC), and the recipient (or host) of the *trading* (investment) portfolio management platform (Aladdin), the Oregon Public Employees Retirement Fund (OPER) – had deemed prerequisite to rule the program an unqualified success.

Next – quantum computing *meet* trading – quantum investing!

[394] Source: "BlackRock bulks up research into artificial intelligence," By (author inaccessible]. See: https://www.ft.com/content/4f5720ce-1552-11e8-9376-4a6390addb44.
[395] Source: https://www.oregon.gov/treasury/invested-for-oregon/pages/default.aspx. See *also*: *Ibid*., [Foot Note # *404*].

Sentient Investment Management – a division of California-based Sentient Technologies[396] – is the corporate brainchild that gave birth to a new, highly innovative *trading* – (investment) portfolio management platform – which the Company installed for internal use. The investment portfolio platform, then called Sentient Ascend, consisted of a quantum investment deep-learning inference engine. Since sold to another firm, Emerj, that Companies executives describe the Sentient Ascend platform [as it was then configured] as "offering a dedicated, in-house built and designed, artificial intelligence platform to continually evolve, and optimize, the investment strategies it is assigned to analyze.[397]" Emerj state that the platform uses evolutionary intelligence, deep learning, and large-scale distributed computing, in its investment management strategy platform. Not too descriptive, that marketing advertorial!

The original progenitors of the Sentient Solution, describe it more illustratively. It is based on an AI *backbone* designed for quantitative trading, with a deep-learning inference engine, with unparalleled analytical penetrative powers. Its goal was to serve hedge fund investment advisory requirements. The *then* Sentient Technologies CEO, Babak Hidjat, PhD for Machine Intelligence post-graduate Fellowship from Kyushi University (Fukuoka, Japan), was one of three individuals whom contributed to the inference engine's design. There is evidence Sentient collaborated with MIT's Computer Science and AI Lab (CSAIL) for one year, in a health care pilot, but no records of *how* Sentient made the leap to commercialization in the investment management sector have surfaced.

And why is it so unique? The Sentient Ascend (as it was known in 2016) trading platform processes stockpiles of historical investment data – say the 'best performing hedge fund exemplars in an industry segment – then passes this information, through its quantum computing deep-learning inference engine, for additional AI processing tasks. The Sentient AI platform takes 40 trillion virtual trading strategies, boils them down to the 'Top Two List', then implements these top two virtual trading strategy examples / models to represent the Sentient Investment Management's hedge fund's trading strategy.[398]

It is an expensive proposition to maintain a quantum computing inference engine, of such a sophisticated and advanced design. Despite its remarkably extensive operational mandate, pursuing labour intensive tasks human agency struggles to come to terms with, the Sentient Ascend platform achievements were split-up, and sold off by its creators. Advanced Systems Management (ASMG) included this example in our trading platform technology scan to point out that some win, and some move *sideways*. One analyst, examining the applicability of

[396] In 2019, Sentient Technologies was dissolved, selling off Sentient Ascend – it's investment management platform – to a Company named Evolv. Sentient Technologies also divested much of its AI intellectual property to the firm Cognizant. Source: "IT leader Cognizant evolves AI beyond '*hill*' climbing," By Ray Tiernan, [online – CBS Interactive]. Dated: February 28, 2019. See *also*: *Ibid*., [Foot Note # *397*-*398*].
[397] Source: https://emerj.com/company/sentient-technologies/.
[398] Source: https://emerj.com/company/sentient-technologies/. See *also*: "IT leader Cognizant evolves AI beyond *hill* climbing," By Ray Tiernan, [online – CBS Interactive]. Dated: February 28, 2019. See *also*: *Ibid*., [Foot Note # *396*, *397*] '(Jonathan Epstein/Sentient) –genetic algorithms and deep learning assist a quantum investing trading solution,' and '(Cognizant) acquires *unspecified* assets from Sentient.'

Sentient Ascend to a much less demanding application, analyzing web site conversion rate optimization (CRO) *hits*, hinted that if you have more than one hypothesis, and perhaps more than one idea regarding how to execute [those hypothesis'] in an experiment, then Sentient Ascend's AI may be what the doctor ordered. That adds little information of an insightful or substantive nature, to help us unravel and better understand the Sentient Ascend story![399]

Unfortunately, for our purposes, this is one case of a better mousetrap definitively moving sideways! Since we are somewhat frustrated in our efforts to seek more comprehensive information from the Company Emerj, nor do we know what intellectual property from the Sentient Ascend platform's AI toolkit ended up with Cognizant, we best leave well enough alone.

Our third investment management platform example the *investment* – (Consumer wholesale and Retail) *client advisory* platform, built by the Vanguard Group, has its own compelling story. The Vanguard Group are the largest provider of mutual funds in the world, and the second-largest provider of exchange-traded funds (ETFs), their ETF's only super-ceded in size by BlackRock's iShares. The Vanguard Group pursued an aggressive strategy to build an in-house Personal Advisory Service (PAS), which would scale to be an automated *pure robo* adviser. This robo advisor – named (naturally) the Vanguard Digital Advisor – was described in a Securities and Exchange Commission(SEC) filing as having the ambition to take *robotic interaction* with Vanguard Clients *away* from human agency contact. Vanguard Group's goal is to, one day soon, make their 'pure' *robo advisor* – [as in] *robo advisor* conducting robotic interaction with Clients only, no human agency – a services offering fully available to all of Vanguard's retirement plan customers' enrollees, and other Client customers' investment plan employees/enrollees, across America.[400]

Vanguard's SEC filing shows how Vanguard will gain useful financial profile insights into these Vanguard Digital Advisor clients' needs: "You'll create a profile within the Digital Advisor (DA) Website and Digital Advisor (DA) Interface that provides us with information relating to your family, age, risk tolerance, specific financial goals, investment time horizon, current investments, tax filing status, other assets and sources of income, investment preferences, planned spending, and existing financial/investment accounts."

The Vanguard Personal Advisory Services (PAS) platform runs an automated AI algorithm, which arrives at a recommended trading track that fits the investor's risk-allocation, asset mix-allocation and time-horizon objectives. It goes further, inserting or exerting 'parameterization' of risk tolerances into the automated AI algorithms sequencing of tasks and responsibilities. The Harvard Business Review[401] have suggested: "The Vanguard Personal Advisory Services (PAS)

[399] Source: "Boost Your CRO Process with AI and Sentient Ascend," By Silver Ringvee [online –ReflectiveData]. Dated June 6, 2018. See: https://reflectivedata.com/boost-cro-process-ai-sentient-ascend.
[400] Source: "Vanguard trying out a new *robo-only* adviser that is even cheaper," By Erin Arvedlund [online –The Philadelphia Enquirer]. Dated September 18, 2019. See: https://www.inquirer.com/business/vanguard-digital-advisor-robo-investing-price-war-20190918.html.
[401] Source: "Artificial Intelligence for the Real World," By Thomas Davenport and Rajeev Ronanki, Harvard Business Review Jan.-Feb. 2008 issue [online]. Page 108 - 116. Dated: 2008.

cognitively constructs, and re-balances, a portfolio with tax efficiency planning in mind." This brings an *intelligent agent* – a cognitive (deep learning) intelligent agent to the decision-making foreground – to engage more directly with a *client onboarding* 'front-end' application. (Further details yet-to-be-released).

Harvard Business Review authors speculate about the problem with human agency – *a.k.a.* financial advisers – competing with these extremely sophisticated 'pure' *robo advisors*. The human element offered by the financial adviser takes too long, or is too expensive to *sub* (i.e. share) their subject-matter-expertise, across a work environment. This puts a damper on the firm's growth. Robo-advice may correct this deficiency. The Vanguard Group estimates that the Personal Advisory Services (PAS) platform handles $80 billion under management, today. This grants a substantial benefit, *across-the-board,* to many Clients it reaches. The success of the investment platform's launch hinged upon financial workflow redesign efforts, poured into the program, before the implementation phase started.

Where is this all headed? Possibly to a new future *cognitively intelligent* Company?

8.4 Transaction monitoring

This topic was saved for last. One of the biggest threats to the business longevity enjoyed by the traditional banking industry is the relentless pace of technological change which the new FinTech's have caused. FinTechs are widely championing: i) real-time payments and services ii) mobility-banking emphasized through their (oftentimes) stellar Client services platforms, and iii) state-of-the art networking advances which underpin the Fintech's operations and service mandates. Artificial Intelligence-delivered chat-bots are amongst the first things that greet you, when you visit them online. AI has not, until this point at least,[402] displaced traditional credit underwriting methods. For example, a traditional marker on credit-worthiness – the long favoured repayment history record – beats a social media behavior-generated metric which a FinTech might use, hands down. This won't, however, deter machine learning (ML) advances from entering the credit underwriting financial services space, a space the FinTechs are eager to grow into. It's still early days, yet the large custom data sets that the traditional banking and financial institution's (FI's) guard so zealously, are considered fair game for the aggressive FinTechs to find ways to exploit or expropriate.

By 2020, PwC (2018)[403] suggests that AI will automate a considerable amount of underwriting, especially in mature markets, where data is readily available. Even in situations where AI does not completely replace an underwriter, greater automation may cause human operators to

[402] Source: "Synergy and Disruption; Ten Trends Shaping FinTech," By Jeff Galvin *et. al*., McKinsey Financial Services [online]. Dated: December 17, 2018.
[403] Source: Financial Services (FS) Viewpoint *publication*: "Great by Governance: Improve IT performance and value while managing risk." See: https:// www.pwc.com/us/en/financial-services/publications/ viewpoints/assets/information-technology-governanceimprovement-pwc.pdf. See *also*: *Ibid*., [Foot Note # *413*].

refocus their efforts, possibly shifting their concentration to assessing and pricing risks in the less data-rich emerging markets. It would also free up underwriters to provide more risk management advisory services, product development advice, and other higher value support services for their clients.

Government regulators have not remained *above-and-beyond* the fray. Regulatory compliance requirements, and the increasing volume of information collection and case load investigative analysis and research have been conditionally transferred to that B2B robot down the hall! (See: Sub-section 8.3 'Investment case management - Investigative case management' – The Oregon Public Employees Retirement Fund (OPERF) / Oregon Investment Council's (OIC's) risk analytics and portfolio management platform.[404] This portfolio management platform has granted to the State of Oregon's regulatory agency and pensions administration Team an equal footing to that enjoyed by financial sector principals' operating within their State's jurisdictional boundaries.[i]

AI already plays a prominent role in the capital markets sector. One example of this are the algorithmic triggers deployed in *high-speed trading*. Next generation algorithmic trading systems are already moving from descriptive and predictive 'trading metric' reporting, to prescriptive analysis – improving their ability to anticipate and respond to emerging trends. And while algorithmic trading programs, once limited to hedge funds and institutional investors, are now accessible to private investors as well.[405]

AI is also prominent in investment management activities. The technology has been readily adapted as a core component of the fund design process. This is particularly the case with trading authorizations and trading hand-offs between (human) investors and their financial advisors. AI systems have, for quite some time, driven investment strategies and greater returns that complement active management. Plus, AI is contributing strongly to the decision-making efforts pursued by passive funds management, as well. This latter point, reinforced by an increasing body of research citing the relative advantages of passive funds, could force asset managers to radically rethink the benefit of their promotional efforts. Asset managers toiling away at selling, and pitching, active fund management products and services to their Clientele may be wondering if they merit their continued concentration on this effort.[406]

---

[404] Source: https://www.oregon.gov/treasury/invested-for-oregon/pages/default.aspx. See *also*: *Ibid*., [Foot Note # *395*]

[405] Source: "Financial Services Technology 2020 and Beyond: Embracing disruption," By Julien Courbe, PwC US [online]. Page 20 – 21. Dated: 2016. '(PwC 2016) triggers deployed in *high-speed trading,* and; AI core *component of fund* design process; and, algorithmic trading from descriptive and predictive 'trading metrics' reporting – all *three* combine to form 'prescriptive analysis.'
See: https://www.pwc.com/gx/en/financial-services/assets/pdf/technology2020-and-beyond.pdf. See *also*: *Ibid*., [Foot Note # *372, 406*].

[406] Source: "Financial Services Technology 2020 and Beyond: Embracing disruption," By Julien Courbe, PwC US [online]. See *also*: *Ibid*., [Foot Note # *372*, *405*].

Financial Institutions (FIs) can do their part. As financial institutions (FIs) continue to press on with automation advances, software architecture comes under the lens. Software architecture addresses such crucial elements as technology choice (in features and functions), system typologies to fit enterprise architecture goals and objectives, and the need for high level application programming (product) interfaces (APIs), which match correctly with high level object models. Theses design features are necessary to address, at an early stage, issues developers encounter in the software development life cycle (SDLC).[407]

Where the software development life cycle (SDLC) leads us, invariably, is in the direction of adopting risk management frameworks (RMFs) of some kind. If we wish a comprehensive listing of the security controls, which are a part and parcel of a developed risk management framework (RMF), we need go no further than to examine Microsoft Azure. As a major datacenter and cloud services provider (CSP), Microsoft Azure lists fourteen (14) mandatory security and privacy controls drawn from the Special Publication titled NIST SP 800-53 – Revision 4 – which provides the governance guardrails that Microsoft Azure depends upon.[408]

NIST SP 800-53 – Revision 4 'security and privacy controls' – protect an organization's operations, in business and government. They are offered from a functionality perspective – a.k.a. to strengthen security mechanisms by developing specialized sets of controls, or overlays – to handle operational mandates, and, from an assurance perspective – a.k.a. measuring confidence in the implemented security capability – which ensure that information technology components and information systems are matched to sound security engineering principles[409]. NIST SP 800-53 promotes a level of independence. For instance, it goes without saying that an Organization's responsibility is to assess all your data, and rank the most delicate pieces,

[407] Source: "At which place of the software development life cycle (SDLC) does Software Architecture take place?" [Quora blog] Ed Costello, Dated: May 21, 2016. See: https://www.quora.com/At-which-phase-of-the-SDLC-does-Software-Architecture-takes-place. See *also*: *Ibid*., [Foot Note # *411*, *412*].

[408] Source: https://azure.microsoft.com/en-us/blog/new-azure-blueprint-simplifies-compliance-with-nist-sp-800-53/. Discussion: The fourteen (14) governance guiderails (security and privacy controls) are: account management, separation of duties, least privilege, remote access, audit review-analyses-reporting, least functionality, identification-authentication, vulnerability scanning, denial-of-service protection, boundary protection, transmission confidentiality-integrity, flaw remediation, malicious code protection, and; information system monitoring.

[409] With over 900 controls and enhancements for developing secure federal information systems, states like New York, Virginia, and Massachusetts are already pushing out mandatory security standards and regulations, choosing to align closely with NIST when customizing their frameworks. The Canadian federal government has done likewise. Source: https://www.auditboard.com/blog/nist-101-intro-to-cybersecurity-framework/.

thereby bolstering your internal security program. Security controls[410] their systems, systems architectures and systems infrastructures, require nothing less.[411]

Proceeding from this last discussion, a typical software development life cycle (SDLC) effort consists of specifying: requirements, design, development, quality assurance, and delivery. If you achieve all of this, in your implementation of the software development's life cycle (SDLC) deployment, security controls[412] fall naturally into place.

Transaction monitoring – whether a financial institution (FI) conducts their automation activities in – Capital Markets, Retail Banking, Real Estate, Risk and Compliance Departments (KYC/AML/CDD etc.), Trade Finance (Letters of credit / Letters of mortgage), Investment Banking, and Banking Admin Departments (HR and Digital Mailrooms, etc.) – it all leads back to adopting an aggressive stance with respect to Know Your Client (KYC) and anti-money laundering (AML) regulations.

Compliance touches all corners of a bank. Monitoring AI, therefore, is also touched by the importance of Know Your Client (KYC) and anti-money laundering (AML) regulations. Regulators will seek direct access to the (same) tools – either on an ongoing basis, or during supervisory

[410] Security controls, implemented by the Risk Executive Function, and the Enterprise Architecture systems development life cycle (SDLC), are standardized by NIST SP 800-39: Managing Information Security Risk – Organization, Mission, and Information System View(s) documentation. NIST risk assessment frameworks (RAFs) determine the criticality of the information and system according to potential worst-case, adverse impact (to the organization, mission/business functions, and the system) scenarios. See: https://www.nist.gov/system/files/documents/2018/03/28/vickie_nist_risk_management_framework_overview-hpc.pdf. FISMA Publications at sec-cert@nist.gov. Slide 5 of 36.
Discussion: In layman's language, the systems development life cycle (SDLC) captures Enterprise Architecture layers and views. As an enterprise architecture methodology, the systems development life cycle (SDLC) methodology describes Business Context, Conceptual, Logical and Implementation layers. Each Enterprise Architecture (EA) layer provides Business, Information, Technology, and Solution views. But can these views and layers be created independently without any order? The answer is No. For the systems development life cycle (SDLC) to reach its intended purpose, each layer is dependent on the preceding layers. Similarly, within each layer, each view is dependent on the preceding views. Why this is important: Business Architecture drives the Information Architecture, which essentially provides the information flow details, required for the business processes defined in the Business Architecture. The Technology layer provides the underlying infrastructure details, supporting the Business/Information architecture (layers). All three - Business/Information/Technology architecture 'layers' identify opportunities to create new solutions or upgrade existing solutions.
[411] Source: "At which place of the software development life cycle (SDLC) does Software Architecture take place?" [Quora blog] Ed Costello, Dated: May 21, 2016. See: https://www.quora.com/At-which-phase-of-the-SDLC-does-Software-Architecture-takes-place. See *also*: *Ibid*., [Foot Note # *407*, *412*]. Discussion: Among the more crucial elements of software architecture are technology choices, systems topology, object modeling and API definition. Some are necessary during the early software development life cycle (SDLC) *technology choice* phase, and/or when building the system overview. Others are needed shortly thereafter (high level APIs, high level object model, etc.).
[412] Source: "At which place of the software development life cycle (SDLC) does Software Architecture take place?" [Quora blog] Ed Costello.* Dated: May 21, 2016. See: https://www.quora.com/At-which-phase-of-the-SDLC-does-Software-Architecture-takes-place. See *also*: *Ibid*., [Foot Note # *406**] *a.k.a.* '(Joe Francis-Quora blogger - in answer to Ed Costello*-2016). See *also*: *Ibid*., [Foot Note # *411*] '(Costello and bloggers) security controls *a.k.a.* software development life cycle (SDLC) design issues and design parameters.'

reviews – as are deployed by their Financial Institution's (FI's) specific departments (listed above), and those departments IT support staff that maintain these tools in working order. As a result, firms will need to make data and control transparency their number one priority, as they implement these tools, and comply with data requests. It is shortsighted to focus solely on compliance with current regulations. Rather, firms – and their regulators supervising their activities – should develop a better understanding of where their data, and associated security controls, live.[413]

And then there are the new *financial* era technologies, with their regulatory hurdles yet to define. You can't improve the quality, security and immutability of, say, record-keeping across hundreds of participant nodes, by giving each node a better computer, or a newer version of Excel. The more complex the world, the more complex the technology. For example, for Sarbanes-Oxley (SOX) compliance efforts, undertaken by Financial Institutions (FIs) routinely every day, regulators attempt the near impossible: they exercise 'need to know' rights to access the corporations' systems. They want to know: who used a system, when they logged in and out, what accesses (or modifications) were made to what files, and what authorizations were in effect.[414]

These communications, in our present example describing Sarbanes-Oxley (SOX) compliance efforts, consist of commitments to the historical record, cataloguing 'legally material files and records' which typically require significant logging of change orders and incidence response data, to satisfy due diligence and regulatory compliance requests. Financial institutions (FIs) treat *all* regulatory requests with the deferential courtesy they deserve. Financial Institutions (FIs) essential service, or product commodity, is defending its pivotally important 'trust' relationship with all parties with which it transacts. Compliance is a given.

Keys (2018) has summed up the brittle challenge new financial era technologies face: "The Bitcoin protocol is the world's largest modern-day abacus; it only enables us to move a bead (or coin) from one side to the other. The ability to do this on a global *permissionless* substrate is not trivial. But I can't overemphasize the limited scope of this initial design, due to its use of a virtual machine which isn't Turing complete. To overcome the obstacle with the Bitcoin protocol, being neither 'private' nor 'scalable,' the new entrant Ethereum platform reimagined the Bitcoin 'use case – *store value'* as (in Ethereum's programming language *Solidify*)

[413] Source: PwC - We have discussed IT governance in greater detail in our Financial Services (FS) Viewpoint, "Great by Governance: Improve IT performance and value while managing risk." See: https:// www.pwc.com/us/en/financial-services/publications/ viewpoints/assets/information-technology-governanceimprovement-pwc.pdf. See *also*: *Ibid*., [Foot Note # *403*].

[414] Source: https://csrc.nist.gov/projects/role-based-access-control/rbac-and-sarbanes-oxley-compliance. Discussion: IT vendors responding to Sarbanes-Oxley (SOX) requirements have adopted RBAC, for evidentiary (rules) discovery, and FI monitoring actions / proceedings. NB: This text *appeared* once *before* in this Submission. It is repeated here - as it relates to the comment concerning - 'regulators (supervisors) seeking access to Financial Institutions (FIs) and FinTech's data pipeline toolkits and software development kits (SDKs). See Ibid., [Foot Note # *360*] '(Joan McGowan-Celent) *Quoting* a point made *earlier*: Sarbanes-Oxley (SOX) certification requirements *exceptions* reporting'.

reimagined to take the expression 'make *store value* into transacting assets that are natively digital, and *codify them*.' The codified result went from the Microsoft Word attorney-supplied documents and became a new transaction agreement – Internet commoditized i.e. covering the cost of communication while being digitally bound (commoditized) via Ethereum charges covering the codification process – which enabled the agreement to be bound by trust."[415]

What we have here is the whole wrap-around discussion of permissioned blockchains and their nemesis, smart contracts. These smart contracts enable parties to conduct transactions, and exchange value amongst themselves, possibly using the Ethereum blockchain platform. Ethereum's permissioned blockchains may also reconcile – through their respective adoption of constructed hierarchies – *permissioned* access to information systems. This does, however, require extensive work, as the case large financial institutions (FIs) have yet to constructively address or conceptualize their full approach to blockchain developments.

What has been blocking progress so far are hacks at exchanges – e.g. (for one) *ether* thefts on the Ethereum platform – which generates numerous headlines in the media. In the bank's case, smart contracts are still reaching for their stability, relevance and consistency. A lack of readily available rules and transaction history data from existing databases – which a bank would *need* for a loan recipient application process to proceed, to cite but one example – is contributing to the situation in which distributed ledger *smart contracts* are still viewed as nothing more than a drawing-board 'work-in-progress.' For smart contracts to be useful, and legally accepted, each Ethereum node must replicate information from source databases to verify, and validate, future transactions. This can only occur when several external factors come into play: **i**) network latency from the data source 'communicating to each node' becomes dependable **ii**) data integrity issues (whereby) – data being transmitted by the source 'to each node' is no longer considered 'causally at risk.' For example, delays due to network problems might result in incorrect computations. This results in the affected nodes being compromised, and may lead them to void transactions on the blockchain. And the third, and a very major factor, negatively impacting the future of Ethereum's *smart contracts* – from an external factor

[415] Source: "18 Blockchain Predictions for 2018," By Andrew Keys, (*now* Managing Partner, Digital Asset Risk Management Advisors/DARMA Capital). Quoted by Traders Magazine [online]. Dated: June 18, 2018. See *also*: *Ibid*., [Foot Note # *191*, *193*, *195-197*] '(Cardano-2020) Hoskinson's Cardano Project is totally ignored – in typical not-in-my-back-yard (NIMBY) fashion – by Andrew Keys. See *also*: https://new.consensys.net/. Discussion: ConsenSys serves as a venture capital company which incubates and accelerates Ethereum startups – launching products across industries – from finance to supply chain to law. ConsenSys claim to have deployed real-world Enterprise Ethereum solutions, assisting corporations, governments, and NGOs to: i) secure their IT infrastructure, ii) optimize workflows, and iii) unlock new blockchain-based business models. NB: Andrew Keys (2018) was employed by ConsenSys when the '18 Blockchain Predictions for 2018' article was written. Since that time, Andrew Keys has left to another crypto/blockchain venture capital entity, named DARMA Capital. This lengthy explanation, hopefully, conveys the insidiousness of blockchain industry stakeholders. They are solely focused on a messianic or religious defense of their platforms and worldviews, to the demise of any other blockchain platform or distributed ledger technology (DLT) advance that may be occurring around them. This is not particularly conducive to fostering a healthy, maturing industry, by a long shot.

perspective – coming into play: **iii**) governments around the world have yet to establish a regulatory framework for dealing with smart contracts. [416]

Keys (2018) offers an insight or two, regarding the future of the *new* financial era, looking at the 'next generation internet.' This will be a "stack" with: i) decentralized transaction layer (strongest – Ethereum); ii) decentralized file storage layer (IPFS/Filecoin and Swarm – early leaders); iii) decentralized messaging layer (Matrix or Whisper – candidates), and; iv) high throughput computing resource (Golem – attempting a prototype). If we compare Keys (2018) *next generation internet* to Julian Zawistowski, Founder/Golem Foundation, and his Web 3.0 vision, everything is predicated on the Ethereum network become more scalable. Or, Golem may have to launch its own Proof-of-Stake high throughput blockchain. The Mission Statement for Golem (may) ultimately prove to be the following: Golem will primarily serve as a platform for microservices, allowing users to run both small (e.g. ''note-taking app") and large (e.g. "streaming service app") in a completely decentralized way. Although ambitious, this vision seems to be the ultimate stake for Golem's long-term competitive potential.[417] In simple terms, Zawistowski's (2016) Web 3.0 will be a decentralized network allowing users to securely and directly exchange content without the permission of a middleman.

A more realistic assessment on the role of intermediaries in the distributed ledger technology (DLT) token-based model *space*, Advanced Systems Management Group (ASMG) would argue, is presented by the Central Bank of Sweden's Riksbank Report on central bank digital currencies (CBDCs).[418] Riksbank (2020): "Despite being bearer instruments, a token e-krona is digital and thus requires all transactions to be recorded in a register or a ledger, to avoid the risk of fraudulent use or double spending. The ledger is – in all relevant senses – also a form of account. This is a contrast to other bearer instruments, like cash which once withdrawn, can circulate from user to user outside the banking system with no records of what it has been used for or by whom. The risks associated with bearer instruments regarding double spending lies primarily on the payee in the absence of a register (e.g. checking security details like a watermark)."

[416] Source: "What Is the Enterprise Ethereum Alliance?" By Rakesh Sharma [online – Investopedia]. Dated: June 25, 2019. See: https://www.investopedia.com/tech/what-enterprise-ethereum-alliance/. Sharma: The third point is that governments around the world have not embraced a regulatory framework for dealing with smart contracts. If (when) these rules are put in place, Ethereum's community and developers will have a headache dealing with their implications, because they encompass multiple industries, including highly-regulated ones such as finance.
[417] Source: "The Golem Project: Crowdfunding Whitepaper (final version)," By to Julian Zawistowski, [online], Page 6. Dated: November 2016. See *also*: "Crypto 101: An Introduction to Golem (GNT)," By Matthew Howells-Barby, [online – thecoinoffering.com]. Dated: November 11, 2018. Discussion: The Golum working application in beta version can be downloaded on the main-net. (We'll pass).
[418] Source: "E-krona design models: pros, cons and trade-offs," By Hanna Armelius, Gabriela Guibourg, Stig Johansson and Johan Schmalholz. Riksbank Economic Review, Page 87. Dated: February 2020. See: https://www.riksbank.se/globalassets/media/rapporter/pov/engelska/2020/economic-review-2-2020.pdf. See *also*: https://www.coindesk.com/riksbank-worlds-oldest-central-bank-study-digital-currency-results.

Riksbank (2020) continuing: "The distinction between a token-based or account-based e-krona has no bearing on the potential implications of the e-krona on the monetary system by itself. There are, however, certain advantages of token-based models inherent in the 'distributed ledger technology (DLT)' technology used. Modern digital tokens are based on advanced cryptography, that allow for the use of 'smart money' and 'smart contracts through atomic swaps'. This makes it possible to have desired conditional requirements built into the tokens. With the use of so-called 'atomic swaps,' it is possible to automatize conditions for exchange and for the exchange to occur only when these conditions are fulfilled – notably for simultaneous exchange of currencies (payment vs payment) eliminating so-called Herstatt risk, and simultaneous exchange of the security and the liquidity leg in securities trading (delivery versus payment). Similar use can also be accommodated for transfers of ownership in the payment swap, when buying a car for example. However, due to the novelty of smart money technology, there are still challenges associated with alteration and revocation of smart contracts."

Advanced Systems Management Group (ASMG) favours the Riksbank characterization of token-based distributed ledger technology (DLT) conditions – over the Keys and Zawistowski proselytizing – sorry to say. And here's the kicker: "For account-based models, these important principles for secure exchanges require the existence of a trusted third party such as a continuous linked settlement (CLS) for currency exchange or central securities depository (CSD) for trade in securities." And in a foot note comment referencing this quote, the Riksbank state: "An open DLT network is associated to several disadvantages; every transaction must be verified by every participant (cf. blockchain) in a time and resource consuming manner. The responsibility for the Riksbank regarding anti-money laundering (AML), know-your-client (KYC) and counter-terrorist-financing (CTF) could be indefinite. Fraud and cyber-attacks are hard to prevent in an open network, an example being open source installations / implementations involving the Linux operating system.[419]"

These developments all lead in one direction – to examining the data.

Advanced Systems Management Group (ASMG) would be an excellent choice among the available options for OCC to consider retaining to address the creation of a data management strategy. Finding meaning in data, retrieving and/or accessing data, and connecting data to the business relationships affected by data, occurs billions of times each day. Application programming (product) interfaces (APIs) facilitate the contextual – and *ongoing* conceptual validation efforts – which occurs when data transfers between people and machines (systems). This is the fabric of what connects customers, suppliers, analysts and employees.

[419] Source: "E-krona design models: pros, cons and trade-offs," By Hanna Armelius, Gabriela Guibourg, Stig Johansson and Johan Schmalholz. Riksbank Economic Review, Page 87. Dated: February 2020. See *also: Ibid*., [Foot Note # *337*, *418*] '(Riksbank – 2020) justification for third party intermediary *for* continuous linked settlement (CLS) for currency exchange, and/or central securities depository (CSD) for trade in securities in a distributed ledger technology (DLT) open source *installation* / *implementation*.'

Raphael Auer (2019), at the Bank for International Settlements (BIS), dissected the advent of embedded regulation in technology to masterful effect. That, Advanced Systems Management Group (ASMG) borrowed from to *embed* in the title to this section. No better time than now, to explore it further!

Auer (BIS-2019) calls for embedded supervision whereby compliance is placed in the *tokenized* market segment, to be automatically monitored by reading the markets (distributed) ledger. By doing so, Auer (BIS-2019) believes, we reduce the need for firms to actively collect, verify, and deliver data. Auer (2019 Page 6: "In today's compliance process, data's trustworthiness is guaranteed by the legal system, regulatory authorities compliance interventions, and the threat of legal penalties. In a distributed ledger technology (DLT) based system, by contrast, data credibility is assured by economic incentives, i.e. supervisors of the distributed ledger need only examine the conditions under which the markets economic consensus is strong enough to guarantee the quality of the data contained in the distributed ledger."

Auer (BIS-2019) gives us three (3) preconditions to govern a (DLT-based) regulatory framework with an *embedded supervision* approach. Embedded supervision (DLT-based) regulation needs to: i) occur in a decentralised market, modelled to replace today's intermediary-based verification of legal data with blockchain-enabled data, credibly based on economic consensus; ii) the (decentralized) market's economic consensus should be strong enough to guarantee that transactions are economically final, so that supervisors can trust that the distributed ledger's data fully reflects the market's economic consensus, and; iii) legislative and operational requirements should be designed and followed that would promote low-cost supervision, and a level playing field for small and large firms alike. [420]

Advanced Systems Management Group (ASMG) disagree with point number two. Auer (BIS-2019) wishes us to believe that there is a way for the 'decentralized' market's economic consensus to be made strong enough to guarantee that transactions are economically final, and that they won't deceive supervisory efforts needed to monitor [those same] decentralized markets, to verify *governance* parameters are fully applied in every case. How is this possible? Advanced Systems Management Group (ASMG) do not feel this is possible, unless you can always know where data resides, how it is being treated, and who is the receiving and sending party involved in the transaction. We do this in-depth monitoring with the data-centric security (DCS) solution. Without this applied, there is simply no way to achieve what the author is calling for (point two above).

Advanced Systems Management Group (ASMG) would like to *also* point out that 'the market's economic consensus' is over-shadowed by forces at play in the Dark Web. Dark Web actors conduct their transactions, and lure in the unsuspecting, to places out of supervisory reach, nullifying any good which penalties to discourage malfeasance would do to deter bad actors

[420] Source: "Embedded supervision: how to build regulation into blockchain finance," By Raphael Auer, Bank for International Settlements (BIS) Working Paper # 811 [online]. Page 3 - statement in Introductory Abstract '*commentary*.' Dated: September 16, 2019. See *also*: *Ibid*., [Foot Note # *19*, *57*, *156, 185*]

and their inappropriate conduct. Auer (2019) is unaware of the power and fidelity of Advanced Systems Management Group's (ASMG's) data-centric security (DCS) solution, which is unfortunate. Instead Auer (2019) would like to institute 'something like' – land registries or rating agencies – to act as verifiers – *a.k.a.* intermediaries or *supporting* third-party-type of institutional 'players' – to ensure the decentralized transfer of funds or securities '*is*' (or has *become*) irrevocable. How can this be done, without tracing the origin of the data back to its source? ASMG feels the data-centric security (DCS) solution, fully applied on all data, irrespective of whether it falls under a centralized authority or the decentralized distributed ledger's control is immaterial. This point is *absolute*. Why?

Auer (2019) worries about creating a centralized party (supervisory entity?) to apply vouchers for "legally-binding signatures," possibly applying a different set of criteria for transaction finality confirmations. This analysis of Auer's (2019) emphasizes the point that once 'finality (of transactions)' is established, it is no longer possible to reverse the [said] event e.g. transaction. Why? ASMG's data-centric security (DCS) solution platform does this with redacted data, metadata etc., thoroughly (and) in an auditable fashion. Auer (2019) must not be aware of this.

In today's prospective 'zero-interest-rate' rent-seeking investment and depository environment, where the consumer may one day "pay" a financial institution (FI), or a FinTech to 'hold / clear' their transactions, this metric of Auer's (2019) – i.e. 'posting or applying vouchers for "legally-binding signatures" – makes no sense whatsoever. Auer (BIS-2019) states (Page 7) that: "The verifier (needs) total skin in the game." ASMG strongly agree. We would go even further, that to encourage a data-centric security (DCS) solution is, in fact, accomplishing just this – skin in the game. Create a premium offset – for this, that (and the other) – but audit the data!

Auer's (BIS-2019) analysis goes further, to try to broach 'broader societal goals' – e.g. establishing a level-playing field – the BIS author suggests public authorities can *digitally sign* and *time-stamp* relevant information, ensuring blockchain interoperability, which will keep costs low. Huh? Then Auer (BIS-2019) adds: 'open source suites of monitoring tools' may be made accessible to potential market (new? Or current?) *entrants*. This is 'sort of OK'.

Auer (BIS-2019) Page 9, suggests that a scheme for transferring ownership without central registry (is obtainable). Then Auer (BIS-2019) adds the following addendum that *auxillary frameworks* that govern distribution markets and their 'infrastructures' need be contemplated. Why are we making this so complicated? Advanced Systems Management Group (ASMG) would respond to this last point – *auxillary frameworks* that govern distribution markets and their 'infrastructures' need to be mandatory – as fully alleviated, and addressed, per the data-centric security (DCS) reference architecture's (RA's) specifications, published implementation directives and guidelines – an open standard, ratified at the Object Management Group (OMG) standards-setting organization.

In summing up, Auer (BIS-2019; Page 23 – 25) makes several additional points, and very specifically states that regulatory bodies and supervisory authorities need: i) to take an active role, regarding standardization of the database structure (by the available *open source* suite of monitoring tools) ii) to create *clarity* regarding how specific regulatory frameworks are applied in practice and; iii) adopt "Efficient guidance of market standards (which will) ensure contestability," but may also require "adequate definitions of what it means to be truly *decentralized* in (the supervisory authorities') regulatory decision-making capacity." Amplifying this a little further, Auer (BIS-2019) suggests: "regulatory bodies and supervisory authorities need a definition of what risk-taking and systems governance (Buterin 2017)[421] should look like – from the industry insiders' perspective – balanced by the critical reviews and appraisals by analytic experts (Walch - 2017).[422]"

Auer's (BIS-2019) final statement was, unfortunately, *too* weak (Page 23): "Regulators and supervisors can steer *some* design elements of the new *decentralized* market (offering), as they will set the market standards under which regulatory compliance can be automated." Change this to read: Regulators and supervisors can steer *ALL* design elements of the new *decentralized* market (offering), as they will set the market standards under which regulatory compliance can be automated. Advanced Systems Management Group (ASMG) can assist with this becoming a reality, *a.k.a.* the data-centric security (DCS) solution reference architecture's (RA's) implementation. The Information Exchange Framework (IEF) Reference Architecture (RA) – and all installation and implementation guidelines (OMG – omg.org)[423] – are available *now*, with the full knowledge-based technology discovery effort completed.

Q9. – Considering small institutions and research departments

For this question, 'Considering small institutions' – the first half of Q9) – we felt a little stuck. On the one hand, banking disruptors are now lining up to play havoc with the profitability of smaller financial institutions (FIs). The Federal Deposit Insurance Corporation (FDIC) in 2019 asked a very sensible question, worrying aloud: Where might the necessary funding come from,

[421] Source: "The Meaning of Decentralization," By Vitalik Butern, Ethereum. [online – Medium publication]. Dated: February 6, 2017. See *also*: *Ibid*., [Foot Note # *512*] '(Buterin Medium article-2017) advocates for decentralizing and centralizing (both) benefits, at the same time'. This is a rambling - basically incoherent - discussion on risk-taking and systems governance.'

[422] Source: "Open-source operational risk: should public blockchains serve as financial market infrastructures?" By A. Walch, (In) D. Lee, K. Chien and R. Deng (editors), Handbook of blockchain, digital finance, and inclusion, Vol. 2 publisher: Elsevier. Dated: 2017. See *also*: "Deconstructing *decentralization*; exploring the core claim of crypto systems," By A. Walch. (*appearing* in) C. Brummer (editor), "Crypto assets: legal and monetary perspectives," Oxford University Press. Dated: 2019.

[423] The Object Management Group® (OMG®) is an international, open membership, not-for-profit *technology standards* consortium, founded in 1989. OMG standards are driven by vendors, end-users, academic institutions and government agencies. OMG Task Forces develop enterprise integration standards for a wide range of technologies and an even wider range of industries.

for small community banks, to resume their normal operations? A FICO representative[424] reinforced this somewhat dismal view recently, stating: "Smaller community banks, attracting the most vulnerably profitable *small business* Clients, will undoubtedly take the largest of the financial institutions' (FIs') sector's economic fallout (*hit*), especially now that Covid-19 pandemic conditions are upon us." Or, do small banks turn to FinTechs (or Big Techs) to meet their financing requirements?

Before we can answer these questions, we need to backtrack a bit. As we reported in our answer to Q6) 'Payment technologies a.k.a. 'getting interoperability right,' depository bank account (DBA) providers, in the US – whether they be small community banks with holdings less than $10 billion in assets – or their larger brethren in the top tier of US banking, the too-big-to-fail financial institutions (FIs) and related parties, are all losing their deposit bank account (DBA) revenue base at an accelerating rate. This may be the issue to address first.

The traditional – or mainstream – banking sector was analyzed by Anthony Carfang, a respected banking analyst.[425] Carfang (2019) conducted a review of the financial status and overall economic standing of traditional banking, with his critical appraisal focused on several issues, e.g. five (5) potential banking sector disruptors:

i) asset managers (investment firms) overtaking banks *equivalent* products and services;
ii)technology disintermediating the [FinTech] intermediaries;
iii) Private liquidity funds emerging as a major asset class;
iv) currency takes on a new role, and;
v) alternative currencies gain traction / acceptance and economic viability.

Advanced Systems Management Group (ASMG) whittled down Carfang's list of topics to these five selections, as they nicely overlap with the intended subject matter the OCC has asked to be examined. Seeking expertise quickly, then moving to the technical issues which motivate a firm such as Advanced Systems Management Group (ASMG) to bring technology solutions to the table, has been our favoured *modus operandi* throughout this Submission. Here is an analysis of each of Anthony Carfang's (2019) issue areas identified and analyzed.

First – **i**) asset management activities for banking in general – commercial banks have traditionally acted as depositors (and borrowers), and operating in this 'channel,' they have enjoyed providing near exclusive service to their investors' capital via the secondary market.

[424] Source: "How Small Banks Can Respond to the Coronavirus Outbreak and Help Businesses Survive," By David Smith, FICO [online – news site]. Dated: April 6, 2020. Discussion: A measure of credit risk, FICO scores are available through all major consumer reporting agencies in the United States: Equifax, Experian, and TransUnion. FICO scores are also offered in other markets, including Mexico and Canada, as well as through the fourth U.S. credit reporting bureau, PRBC.
[425] Source: Megatrends in Treasury, Money and Banking," By Anthony Carfang, The Carfang Group [online]. Dated: May 2019. See: https://www.linkedin.com/in/carfang. See *also*: *Ibid*., [Foot Note # *427*].

– Plus, commercial banks have acted as the primary source of loan issuance to their Clients. This is no longer a day-to-day reality, as new players are entering this space. Asset management organizations, for one, are granting more and more loan underwriting, in both the retail and wholesale markets. This is explained due to systemically important financial institution (SIFI) supervision, and Basel III requirements, which Carfang (2019) suggests has flattened the bank's growth trajectory. The Big Three asset management firms have tripled in size, during the past decade, when the regulatory mix is examined. Today's regulatory milieu has effectively done next-to-nothing to stop the asset management firms' encroachment, in retail and wholesale banking, side-swipes.

Point two addresses – **ii**) technology a.k.a. "disintermediation" of the FinTech (and other) intermediaries. This was a find: banks on both side of the *separation* (or divide) between the suppliers of capital (depositors / investors) and the users of capital, relied solely, in the past on banks. Why? Banks – if they did not know the counter party in a transaction, could locate a correspondent bank that did know that counter party. Today, however, social networks (LinkedIn), P2P networks, intelligent robo-advisors, etc., are altering 'e.g. bypassing' the traditional banking channels. The upshot? Financial Institutions (FIs) are being displaced.

The third point – **iii**) private liquidity funds emerging as a new asset class – this lies outside the set of questions the OCC asked, but Advanced Systems Management Group (ASMG) feel challenged to include it as it has important financial disruptor technological ramifications we find intriguing. Carfang (2019) describes private equity funds – which a few decades ago provided an avenue to circumvent public markets *a.k.a.* for sourcing long-term capital – are now captured by private liquidity "Sweep" accounts. Private liquidity *sweep* accounts are now available at low cost, to most savers / investors. Thanks to FinTech technology-aided platform advances, *sweep* accounts can be drawn down precisely when they are needed. In 2016, US regulators implemented measures to reduce the viability of prime money market funds, which Carfang (2019) states had the unintended effect of causing providers (and issuers) of prime money market funds to push the bulk of these prime money market funding 'sources' into government and treasury funds, to avoid significant penalties if they stayed the course in their conventional money market lending activities. This caused a drying up in prime money market funding 'sources,' which were no longer widely available to businesses.

Carfang (2019) didn't say it directly – as when the article was written the Covid-19 pandemic had not yet occurred, but Advanced Systems Management Group (ASMG) will state the obvious: a massive chunk of the North American (and international) economy has been served a body-blow, and small businesses are in very disastrous straits. Carfang (2019) quite rightly states: "The conduit between providers and users of liquidity has been significantly curtailed." He adds: "Will the 2a-7 funds (limited to investors) be the answer? Or, will a new asset class appear? An asset class being dissimilar to money (-market) mutual funds (MMFs), special mention accounts (SMA), or Ultra Short Bond Funds, with the latter – SMAs for example – only investing in fixed-income instruments, with very short-term maturity horizons? And will these

new liquidity vehicles function, not coincidentally, to incorporate the "redefined" liquidity via a just-in-time cash [-like] feature?" Good questions, all.

'Considering small institutions' – the first half of Q9. – wasn't clear-cut by any means.
The approach Advanced Systems Management Group (ASMG) has chosen to adopt is to answer this question in a two-fold manner. First i) we have summarized the competitive and economic disruptors facing the larger banks. Secondly ii) we will turn our focus *next* to examine small community banks[426] – holding less than $ 10 billion in assets – specifically tasking ourselves to assess their perceived inability, in the middle of the Corona pandemic disruption, to survive the economic challenges unscathed.

As we have just reported in our answer to Q6. 'Payment technologies a.k.a. 'getting interoperability right,' the deposit bank accounts (DBAs) – no matter if they are held by community banks or their large-scale competitors, the too-big-to-fail megabanks – are losing their profitability ranking. Anthony Carfang (2019) states: "Issues that appear small or incremental – such as Deposit Banking and immediate payments ascension – [*plus*, adding in the other five (5) potential banking sector disruptors: **i)** asset manager investment firms; **ii**) technology disintermediation; **iii**) private liquidity competitors; **iv**) new role for currency, and; **v)** alternative currencies/coins] are cumulatively seismic in their disruptive influence, with the negative consequences being felt as we speak.[427]"

Carfang's (2019) article's fourth point: **iv**) currency taking a new role – falls squarely in the corner of a possible central bank digital currency (CBDC) development. This is not a question the OCC asked about directly. Central banks, and many others, are trying to figure out a way to create electronic (on-line) cash or currency depository options, particularly with respect to emergency payments to the dispossessed in society. Even before the pandemic, Anthony Carfang had noted that regulators have not really expressed any certitude about the route which central banks might take – nor the likelihood they will succeed – with a prospective roll-out of a central bank digital currency (CBDC). The same seems to be the case today.

Turning to the last of the five (5) banking disruptor topics – **v**) alternative currencies 'gain traction / acceptance and economic viability' (e.g. crypto currency / crypto assets), here again Carfang's (2019) advice is somewhat mundane. Anthony Carfang states: Crypto assets are not offered by governments' (*yet*); nor are they backed by the *trust* mechanisms endowed through central banks.

How instructive have Carfang's (2019) predictions proved to be, with respect to applying their message to the fate and/or providence which the smaller community banks in the US are

[426] Source: "What's Going to Happen to the Smaller Banks, the Community Banks," By John Mason [online] Seeking Alpha. Dated: March 31, 2020. See *also*: *Ibid*., [Foot Note # *428*].
[427] Source: Megatrends in Treasury, Money and Banking," By Anthony Carfang, The Carfang Group [online]. Dated: May 2019. See *also*: *Ibid*., [Foot Note # *425*] '(Carfang-2019) Deposit Banking and immediate payments ascension "losses," as the cumulative disruptor(s) to *break* small banking, and threaten their continued business survival.'

confronted with today? Partially useful. Anthony Carfang (2019) points out a whole slew of retail and wholesale service offerings, which may prove lucrative, if the community banks were permitted to operate in these financial service areas. We haven't itemized these service offerings, due to the sober realization that the smaller community banks are expressly excluded – in the main – from pursuing any but their current banking activities which follow a very narrowly prescribed services mandate. This has had negative consequences, as the next set of statistics will dramatically underscore.

The Federal Deposit Insurance Corporation (FDIC – 2019) tallied up the number of community banks – which the FDIC believe represent a count of approximately 4,750 in number – down from over 10,000 banks recorded in the early 1990s. Since the Great Financial Crisis (GFC) of 2008-2009, all three indices of community banking health have declined: i) loan growth, ii) interest earnings and, iii) size of (and number of) deposit bank accounts (DBAs) registered within the community banks asset mix in total. Community banks have no security trading to speak of, nor do they offer any significant proportion of investment banking services. This severely restricts their growth prospects, and imperils their 'fiscal' economic survival. Now, with Covid-19 pandemic conditions moving older Clients out of their branches and into online services offered by their Competitors, the small community banks have an almost insurmountable challenge they must overcome.[428] And, back to small businesses.

Returning to our earlier point – small business financing – in the post Covid-19 pandemic economic environment, who will bail them out? Where might they attract the necessary funds to resume their affairs? The FinTech lenders – e.g. Lending Club and Prosper – are not the panacea for them, as originators of small business lending.[429] Before the Covid-19 crisis manifested itself, FinTech's only assessed, and successfully granted, loans or issued credit lines to fifty-one (51) per cent of their small business loan applicants, in the mid- to -high risk portion of the small business credit-seeking portion of the (US) economy. This compares with twenty-one (21) per cent of the small businesses considered low-risk receiving FinTech industry lending ('issued credit lines') financial support. What's the danger here? Many consumer protections that cover loans issued for an online personal-loan requirement – i.e. granted a householder – are specifically *off-side* to an inquiring small business owner.[430] This squeeze is reflected in the drying up of the available number of credit-granting options which a small business owner might be able to turn to. FinTech companies also, are not covered under mandatory disclosure requirements, which means finding data on their lending practices is hard (if not impossible) to measure.

[428] Source: "What's Going to Happen to the Smaller Banks, the Community Banks," By John Mason [online] Seeking Alpha. Dated: March 31, 2020. See *also*: *Ibid*., [Foot Note # *426*] '(Mason-2020) elderly clientele moving out of small banks, and on-line during Covid-19 pandemic.'

[429] Source: "Another Risk for Small Business: Lightly Regulated FinTech Loans," By Lenore Palladino [online] Barron's. Dated: April 21, 2020.

[430] The 'Truth in Lending Act and Fair Debt Protection Practices Act' cover loans made to households from non-banking (FinTech-type) institutions, but exclude business loans issued to businesses from the same protection mechanisms.

The Consumer Financial Protection Bureau (CFPB) needs to apply for authorization to implement Dodd Frank section 1071, to fix this inequity, something which is even more urgent given FinTech's are now recipients of Paycheck Protection Program (PPP) funding, as well. This is even more grating to small business owners, whom are feeling 'shafted' by the US federal government bail-out regimes, which due to the haste in which they were awarded, have been noted to have excessively rewarded larger corporate enterprise, out of proportion to the number of smaller businesses which feel they have simply 'struck out'. This is not an issue which can be easily swept under the rug!

Is it any surprise when Brian Hamilton, Founder of the Company Sageworks, suggests "Consumers lose when small banks can't compete?[431]" Mr. Hamilton decries the fact that the Great Financial Crisis (2008-2009) was precipitated by a few huge US banks, which nearly toppled the economy. Brian Hamilton states that banks with fewer than 30 employees would sell themselves – in a minute – due to their non-competitive state of affairs. Plus, a regulatory regime which is, frankly, not friendly to their interests, and too expensive. That seems to be a good wrap-up statement to conclude our analysis of small banks in the US.

Now we have arrived at the second part of Q8. – 'Considering research departments.' Investment Banking Division's (IBD's) in banking institutions and their counterpart departments housed in the investment management firms, are responsible for working with corporations, institutions, and governments, to carry out capital raising activities – underwriting services with equity products, debt financing, and multiple service offerings for hybrid markets.[432] In addition, research departments also plan or assist with the delivery of research services targeted to mergers and acquisitions (M&As) activities pursued by Investment Banking Division's (IBD's) in banking institutions and their counterpart departments in the investment management firms.

The bank's *research departments* can be further sub-divided by their function: Equity Research (ER) versus Investment Banking (IB). Equity Research (ER) involves working with *publicly available* information. From this trove of publicly available information, databases, and so on, the *research departments'* analyst builds financial models, and pursues the performance tasks associated with 'knowing your industry'. Investment Banking (IB) groups advise Clients on underwriting, 'pitch (sales and prospectus investment trading) books,' ad hoc financial analysis, and prepare (and write) Prospectus / Letters-of-Intent / Memorandums of Understanding, etc. Investment Banking (IB) often deals with *non-public* information, and pursues deals and transactions with a *sales angle*. Among the sectors served by both Investment Banking (IB) and

[431] Source: "Consumers lose when small banks can't compete," By Brian Hamilton, Sageworks [online – interviewed by Mary Ellen Biery, Company Research Specialist]. Dated: March 29, 2018. Discussion: Mr. Brian Hamilton also suggested that the Volcker Rule, and certain capital leverage ratios under Dodd-Frank Act, only make sense for large financial institutions (FIs). Not sure how this applies to small banking institutions, but it is worth noting.
[432] A hybrid market is an exchange through which traders can use both automated trading systems and traditional floor brokers in order to execute transactions. In the United States, the most famous example of a hybrid market is the New York Stock Exchange (NYSE).

investment management firms' research departments are a few over-lapping industry or economic areas: Technology Media and Telecomm (TMT), Financial Institutions (FI), Energy, Mining, Healthcare; Industrials / Manufacturing and Real Estate.

There are two views regarding the *value-add* contribution made by research departments. A skeptic would say a bank's research *sell-side* 'product' is provided for internal use [not for public consumption], within the investment bank, where it is not nearly as valuable as it may have been in the past, due to new regulations. These regulations are the EU's SFTR – reviewed in Q8) 'Regtech and the OCC: Governance embedded in technology,' reviewed in that answer's introductory section – plus the European Commission (EC) Market's in Financial Instruments Directive II (MiFID II).[433] MiFID II clearly spells out dramatic compliance monitoring measures which are somewhat deleterious, and far-reaching, in the negative impact they have had on corporate research departments. The new regulations – particularly the EU's MiFID II 'pre- and post-trade' transparency requirements, implemented on January 3, 2018 – may be usefully viewed as comparable in their styling, if not their actual intent, to the US Security and Exchange Commission's (SEC's) "US Regulation of Investment Advisers (US) SEC"[434] documentation.

We will give a very short summary of the EC's Market's in Financial Instruments Directive II (MiFID II), but with the *proviso* that we are not experts in the field.

Callaghan (2017) suggested recently that one reason why Market's in Financial Instruments Directive II (MiFID II) came about was: "The idea – in MiFID II – *is* to bring about transparency in bond trading, by creating transparency obligations on a quote-by-quote basis. This has the effect of bringing *light* into the previously *un-lit* over-the-counter (OTC) trading practice (e.g. bond trading *a.k.a.* over-the-counter/OTC trades).[435]" The situation Callaghan (2017) – the corporate regulatory compliance *specialist* at the ICMA Group was describing – describes has to do with the MiFID II regulatory guidance directives, addressing Systematic Internaliser (SI)

[433] The European Commission (EC) Market's in Financial Instruments Directive II (MiFID II) banned the bundling of research reports and asked they be separated from their trade execution activities. MiFID II introduced a shift in trading towards more structured marketplaces, improved best execution, orderly trading behavior within markets and more explicit costs for both trading and investing. By uniting market and client data on the one hand, but with MiFID II demanding companies to separate transaction fees from research charges, the Company's local regulator must agree to the approved reporting mechanism (ARM) reports, no later than the close of the following working day. Organizations are required to determine if they have breached MiFID II systematic internaliser (SI) thresholds. The trading venues: Regulated Market (RM), Multilateral Trading Facility (MTF), or Organized Trading Facility (OTF) are all subject to SI thresholds. Large global or regional banks are the most likely candidates to take part in the SI regime. The perception in earlier trading enforcements monitored under MiFID I, was that in MiFID I, bond trading frequently experienced a "natural arbitrage" (pre-trade transparency could be circumvented by trading off-venue). The idea in MiFID II is to bring about transparency in bond trading by creating transparency obligations on a quote-by-quote basis. – bringing light into the previously un-lit over-the-counter (OTC) trading practice. Source: "MiFID II implementation: The Systematic Internaliser regime," By Elizabeth Callaghan, Published by Secondary Markets – Issue 45, Second Quarter 2017, Page 33. Dated: April 2017. See: lcmagroup.org.

[434] Source: https://www.sec.gov/about/offices/oia/oia_investman/rplaze-042012.pdf.

[435] Source: "MiFID II implementation: The Systematic Internaliser regime," By Elizabeth Callaghan, Published by Secondary Markets – Issue 45, Second Quarter 2017, Page 33. Dated: April 2017. See: lcmagroup.org.

treatments. Systematic Internalisers' (SI's) – traditionally called *market makers* by research department professionals – are investment firm players or Stakeholders whom match *buy* and *sell* orders *in house*. Instead of sending orders to a central exchange, the Systematic Internaliser (SI) entity or trader matches a batch of *in house* 'buy and sell' orders, with other orders on their own book. Systematic Internaliser's (SI's) compete directly with stock exchanges, and with automated dealing systems.[436]

Callaghan (2017) was zeroing in here on the following salient observation: "The increased scope in the EC's Market's in Financial Instruments Directive II (MiFID II) regulation is this: an investment firm which pursues, on an 'organized, frequent and systematic, and substantial basis,' *deals* on its *own account* (principal trading actions) by executing client orders outside trading venues – e.g. these trading venues are confined to recognizable Regulated Markets (RMs), Multilateral Trading Facilities (MTFs), or Organized Trading Facilities (OTFs) – MiFID II will clearly set out well-defined thresholds, circumscribing these entities (investment firms') Systematic Internaliser (SI) participation. Why? To become a Systematic Internaliser (SI) entity or trader, requires the prior authorization by Market's in Financial Instruments Directive II (MiFID II) supervisory authority to determine that the trading volumes *in respect of* a pre-defined clarification on their "frequent and systematic" and "substantial" [trades] or 'substantiating trade-making' status, are in good standing. Large global or regional banks are the most likely candidates to take part in the Systematic Internaliser (SI) regime.[437]"

Advanced Systems Management Group (ASMG) may have this annoying habit of opening a topic, getting a proportion of the way into analyzing the issue, then retreating in short order. True. Guilty as charged! But in this case, what we are most interested in is the use of *technology* and *software* in Market's in Financial Instruments Directive II (MiFID II) compliance programs. Firms are required to ramp-up their reporting requirements, which for MiFID II, may require automation advances to produce a vast amount of data tracking items relating to, for example the conduct of Systematic Internaliser (SI) actions and activities.

ASMG want to know where these data sets are registered, what these data sets contain, and to what designated data repositories they are destined to be delivered. Processes must be put in place where the conduct of Systematic Internaliser (SI) actions and activities can be monitored, i.e. in a data flow or data transmission monitoring sense of the issue, to allow regulators and affected third party or originating Stakeholder transactors', to know whether or not they can (or have) detected if an employee breaches a 'Chinese wall',[438] or misuses information gained

[436] Source: "MiFID II implications for US financial firms," By Bovill Insights [online]. Dated August 30, 2017. See: https://www.bovill.com/mifid-ii-implications-for-us-financial-firms/. MiFID II is to be implemented in the EU on January 3, 2018. NB: This appeared as Foot Note # 3 in this Bovill Insights article, *reproduced in full*.
[437] Source: "MiFID II implications for US financial firms," By Bovill Insights [online]. Dated August 30, 2017. See *also*: *Ibid*., [Foot Note # *436*] '(Bovill Insights-2017) clarification re: 'frequent and systematic' and 'substantiating trade-making' status for MiFID II trading.'
[438] The term Chinese wall, as it is used in the business world, describes a virtual barrier intended to block the exchange of information between departments if it might result in business activities that are ethically or legally questionable. See *also*: *Ibid*., [Foot Note # *441*] 'Expanded definition for investment banking professionals.'

via a Conflict of Interest (COI) and therefore requires a punishable compliance enforcement measure to be issued.

Advanced Systems Management Group (ASMG) will rely on several specialists in the investment software field for the next set of technological points we wish to raise, and critically evaluate and review. Almqvist (2015)[439] suggests that: "Compliance and Information Technology (IT) need to carry out a detailed risk analysis, mapping out the required processes and procedures required under the EC's Market's in Financial Instruments Directive II (MiFID II), and then determine *task by task* if their existing solutions will be adequate." Almqvist (2015) continuing: "This risk based analysis should be documented and kept as an audit trail of the decision process. And secondly, when a firm decides what part of the regulation applies to their business, and what organization, processes and tools are required to be effectively monitored, the firm must endeavour to comply with the relevant regulatory compliance stipulations and directives, to the regulatory sections of that regulatory regime, which applies." The risk, both Almqvist (2015) and ASMG would agree, lies buried in the 'data'.

Understanding your *data* is a must, in-order-for your compliance function to *stay-in-step* with the regulations. Staying in compliance is the name of the game, to dodge penalties, and/or relieve (e.g. the target organization's / Client organization's) impending stressors, which can overwhelm their organization's regulatory compliance departments even at the best of times. An enterprise's compliance department's challenge in banking is *always* to positively identify internal systems, and/or internal data process and data handling deficiencies, operational inconsistencies or outright malefactions or shortcomings, which the regulator may demand to see addressed.

Plus, for the first time, the EC's Market's in Financial Instruments Directive II (MiFID II) brings Direct Electronic Access (DEA) Clients into scope for regulatory compliance, and MiFID II mandates that Direct Electronic Access (DEA) Clients *must* have written agreements put in place, between the [said] firm and their [external party] Client. This will involve an annual due diligence review every 12 months, which in the case of Client lifecycle / Client onboarding situations, will force financial institutions (FIs) to identify and classify *all* Direct Electronic Access (DEA) Clients specifically, and this identification extends to cover software solutions as well.

Here is the list of the EC's Market's in Financial Instruments Directive II (MiFID II) Client dealings falling under MiFID II's regulatory compliance guidance coverage: 1) Due diligence assessment; 2) Assessment of suitability of Direct Electronic Access (DEA) Client determinations; 3) Any pre-set trading and/or credit thresholds, and; 4) Mandatory – e.g. legally binding – instructions *written into* Direct Electronic Access (DEA) agreement(s). Ms. Glynn (2017), representative for

[439] Source: "Use of technology and software in MiFID compliance programs," Interview with Magnus Almqvist, Sunguard Software - By Financier Worldwide [*anonymous* author]. Dated: May 2015. See: https://www.financierworldwide.com/use-of-technology-and-software-in-mifid-ii-compliance-programs#.XxobJ5NKhGM.

the financial services compliance products software firm Fenergo [440] suggests: "Managed correctly and automated appropriately, financial institutions (FIs) can create a common, centralized Client Life-cycle Management platform, that delivers a *unified* view of client data and documentation. Furthermore, this will encourage the re-use of these [client identity data sets and] attributes across multiple business units, jurisdictions (data privacy rules permitting) and regulations, which will increase operational efficiency and improve the overall client experience."

Returning to our 'two views' regarding the *value-add* made by research departments, our skeptic's viewpoint dismissed outright the *research department* as a superfluous entity. I think we can bury this crass, and unproven opinion very quickly. The skeptic's camp has tried to argue that research 'used to be' helpful in gaining Investment Banking Division (IBD) business. It was viewed favourably only (in the skeptic's assessment) when it allowed bankers to 'imply that a company would be given favorable reviews' by the bank's covering analyst, if [said] company did business with them. That model is not allowed anymore due to the Chinese Wall.[441] Advanced Systems Management Group (ASMG) dismiss this viewpoint as ineffectual, and unproven.

That leaves us with the viewpoint, we support, articulated by the optimist camp. An optimist embraces the generically-held theory which believes that the work of the research department helps *gain* trading business. It is unimportant, whether the research department primarily execute trades with *sell-side* traders they are friendly and familiar with, and/or who provide the cheapest fees. Again, who cares?

The optimist would suggest research is essential to a trading franchise. You would be correct to believe the *buy-side* initiates trades executed on a relationship basis. If you want to trade Procter & Gamble (PG), and you know a trader at a bank who covers Procter & Gamble (PG), and (you) have a good relationship with him/her, you will pursue the trade with this contact. There is more to this than meets the eye. This is where *effective* research comes into play. A good *research department* gives the traders/sales people an opportunity to *build* that

[440] Source: "MiFID II: 6 Key Changes for Client Lifecycle Management," By Laura Glynn, [online] – Fenergo. Dated: June 2017. See: https://www.fenergo.com/resources/blogs/mifid-ii-6-key-changes-for-client-lifecycle-management.html.

[441] Chinese Wall – in this case – involves investment bankers in possession of material, non-public information concerning a publicly-traded *company.* Investment bankers are strictly prohibited from discussing any such information with individuals who do not have a '*need to know*' [for) such information, for purposes of servicing 'the client' that provided the information to the bank. Restraint should always be exercised with respect to the transmission of information (such as long-term corporate projections) that is not likely to become public – during the natural course of an investment banking assignment's occurrence. Obviously, this may inhibit the ability of the recipient to engage in normal business activities. This, without a doubt, restricts personal trading, once the investment banking assignment has been completed. See *also*: *Ibid*., [Foot Note # *438*] 'Simplified definition for Chinese Wall.'

relationship. You can't be a trader and expect to have a relationship with a Procter & Gamble (PG) analyst, at a buy-side fund, without ever talking Procter & Gamble (PG) with him/her. Your relationship builds because you articulate positively about Procter & Gamble (PG), and then other factors play into the relationship. If you have no research franchise, your traders have no relationship with these fund managers, and you are not getting any trades. Simply put, an employee at the other bank may have a good research franchise behind them, which leads to fruitful discussions about the company with the trader on the *buy-side*.

It is also true that *buy-siders* don't depend on a bank's research to generate investment ideas. But they do use their internal bank's research to initiate a dialogue, and discuss their thesis with the traders and research analysts. The research doesn't go unread by the *buy-side*, it is used. Possibly used selectively – and electively *a.k.a.* not referred to all-the-time – the research department's analysis has considerable weight to it. Also, without research, very few *buy-siders* have access to corporate management, which is another reason why a good research franchise makes it easier for traders to establish those relationships (with senior corporate management in their own organization). When you are a consumer trader, and you can go to a consumer trader on the *buy-side*, and be equal in your knowledge base to that of the knowledge held by the *buy-side* consumer trader, results *tend* to follow.

Story long on details, but it's an important issue to address, and a discussion which financial institutions (FIs) need to have.

The story of the imminent decline of the banking sector's *research departments* flew, fast and furious, around the banking and investment management institutions' Equity Research (ER) and Investment Banking (IB) divisions, as the EC's Market's in Financial Instruments Directive II (MiFID II) regulatory compliance measures took hold. As MiFID II implementation deadlines were arriving,[442] Quinlan & Associates – a Hong Kong-based consultancy – estimated that research revenues may decline by forty (40) per cent, as fund managers cut the number of research providers they use, and the amount they spend on research department staffing and funding activities.

The Australian Securities and Investments Commission's (ASIC's) guidelines on *sell-side* research and material *non-public* information have also, again, chosen to highlight the vexed relationship at large banks, between their research and corporate divisions. While the EC's Market's in Financial Instruments Directive II (Mifid II) doesn't strictly apply in Australia, brokers that deal with international or European fund managers, the Australian Securities and Investments Commission (ASIC) suggests, need comply with Mifid II.

We've really exhausted this topic, without getting to what concerns us as data specialists. Perhaps, by turning to a different regulatory regime, will help us *focus*. The European Market Infrastructures (EMIR) registration and reporting of derivatives regulatory compliance regime,

[442] Source: "Why investment bank research analysts are leaving their jobs in droves," By Joyce Moullakis, Sr. Reporter Financial Review [online] Dated: April 27, 2018.

emanating out of Luxembourg, is an EU initiative which – from Advanced Systems Management Group's (ASMG's) perspective – is a particular eye-opener.

The European Market Infrastructures (EMIR) supervisory regime calls for very specific data handling requirements, handling all derivatives transactions and derivatives trading processes and procedures. The European Market Infrastructures (EMIR) derivatives tracking and reporting initiative[443] will require: 1) mass upload and download of XML files through secured internet access, and; 2) automatic transfer of XML files through a SWIFTNet FileAct file transfer connection and Secure File Transfer Protocol (SFTP)[444] (*under development*); 3) SOAP[445] API connection via web services; 4) Processing of CSV files[446] and data transfer via SWIFT MT[447] messaging (*under development*).[448]

The European Market Infrastructures (EMIR) registration and reporting of derivatives stipulations state four (4) main requirements:

- Mandatory central clearing of certain classes of over-the-counter (OTC_ derivatives (entered-*into*) between certain types of counterparty
- Collection of margin in respect of un-cleared over-the-counter (OTC) derivatives between certain types of counterparty

[443] Source: "EMIR: Are you prepared to report your derivatives transactions?" by Xavier Zaegel, Deloitte Luxembourg. Dated: June 17, 2013, Slide 22 of 39. See: https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/financial-services/Banking/lu_en_emirreportderivates_01062015.pdf.

[444] Secure File Transfer Protocol (SFTP) is a file protocol for transferring large files over the web. It builds on the File Transfer Protocol (FTP) and includes Secure Shell (SSH) security components. This term is also known as Secure Shell (SSH) File Transfer Protocol. Secure Shell is a cryptographic component of internet security.

[445] The Simple Object Access Protocol (SOAP) provides the Messaging Protocol layer of a web services protocol stack for web services. It is an XML-based protocol consisting of: i) an envelope, which defines the message structure and how to process it, and; ii) a set of encoding rules for expressing instances of application-defined datatypes. SOAP is a protocol specification for exchanging structured information for implementing web services, across computer network(s). SOAP's purpose is to induce extensibility, neutrality and independence. It uses the XML Information Set for its message format, and relies on application layer protocols, most often Hypertext Transfer Protocol (HTTP) or Simple Mail Transfer Protocol (SMTP), for message negotiation and transmission. SOAP allows processes running on disparate operating systems (such as Windows and Linux) to communicate using Extensible Markup Language (XML). Since Web protocols like HTTP are installed and running on all operating systems, SOAP allows clients to invoke web services and receive responses independent of language and platforms. See *also*: *Ibid*., [Foot Note # *277*].

[446] A comma-separated values (CSV) file is the delimited text file that uses a comma to separate values. A CSV file stores tabular data (numbers and text) in plain text. Each line of the file, in a CSV file, is a data record.

[447] MT 760 belongs to a category of SWIFT Message types for guaranteeing letters of credit. SWIFT stands for Society for Worldwide Interbank Financial Telecommunications. Essentially, it is used to securely transfer information and instructions through a system of codes.

[448] ASMG would like to learn more about these *under development* components – # 2) "Automatic transfer of XML files through a SWIFTNet FileAct file transfer connection and SFTP (*under development*)," and # 4) "Processing CSV files and data transfer via SWIFT MY messaging (*under development*) – *both* as of 2013? Should the OCC, or your sister regulatory organizations, be involved on this activity, we would like to be contacted directly to apply the data-centric security (DCS) advances to these EMIR solution requirements.

- Reporting of all eligible over-the-counter (OTC) derivatives to authorized trade repositories
- Certain other risk mitigation requirements for over-the-counter (OTC) derivatives.

For the European Market Infrastructures (EMIR) – *a.k.a.* clearing and margining requirements – over-the-counter (OTC) derivatives are derivative contracts not executed on a regulated market. A "regulated market," for this purpose, is a market authorized under EC's Market's in Financial Instruments Directive II (MiFID II), or a Third-Country market considered equivalent for the purposes of MiFID II. For the US, such markets are designated by the US Commodity Futures Trading Commission (CFTC), the US regulatory organization that governs the U.S. derivatives markets, which includes futures, swaps, and certain kinds of options.

Over-the-counter (OTC) derivatives market participants are required to agree in writing, with their counterparty, certain arrangements for reconciling portfolios. If a Reporting Obligation is triggered, over eighty (80) data items must be reported to a trade repository, split into two broad categories:

Counterparty Data – includes detailed information on the counterparties and other entities involved in the trade, such as brokers, clearing members, CCPs* and trade repositories. (*NB: CCPs provide central, established to shift risk from traders to the central counterparties, and in exchange the CCPs use the substantial collateral assets for their own investments. The main idea being to introduce CCPs – trustworthy financial institutions – to replace the bilateral relationships that prevailed between two counterparties, vis-à-vis their centralized multilateral relationships [involving CCPs], which may have contributed *greatly* to the Great Financial Crisis (GFC 2007-2008).

- Common Data – includes detailed information on the contract itself, such as the underlying, notional amount, maturity, price, rates and currency, amongst other items. Counterparties should ensure that the Common Data is agreed between both parties.[449]

The European Market Infrastructures (EMIR) regulatory compliance regime underwent a *Refit* on June 17, 2019: Financial counterparties (FCs), as well as non-financial counterparties (NFCs), need to *now* report derivative contracts (concluded, modified or terminated) to a Trade Repository (TR). A trade repository is an organization that is regulated under the European Market Infrastructures (EMIR) regime to manage data in a transparent and confidential manner. The information reported to trade repositories (TRs) is accessible to (non-) European Economic Area (EEA) regulators.

The substance of European Market Infrastructures [EMIR] *definitions* are borrowed from the EC's Market's in Financial Instruments Directive II (MiFID II) directives, and cover – by way of a

[449] Source: "EMIR: What you need to know," By James Coiley, K. Ball, J. Haines and K. Knight, [online] ashurst web site. Dated: June 2019. See: https://www.ashurst.com/en/news-and-insights/hubs/finance-hub/emir/what-you-need-to-know/.

few examples – foreign exchange (FX) forwards, interest rate swaps, cross-currency swaps, commodity futures transactions, credit default swaps, total return swaps, options trades, and several other derivative instruments that *non-financial* entities regularly use to manage risks, relating to their commercial activities and treasury transactions. The substance of these definitions does not, however, cover foreign exchange (FX) spot transactions, stock loans and repurchase agreements.[450]

On May 3, 2018, an article titled "How the GDPR will Impact the Banking Sector?" outlined the General Data Protection Regulations' (GDPRs') effect on the banking sector:

- On a periodic basis, we need to review and enhance our current IT architecture supporting data storage, transformation and processing of personal data to fulfil General Data Protection Regulations' (GDPRs') requirements
- We need to develop – and implement – a Meta Data Management system, and establish and/or expand data lineage, to comply with data protection requirements.
- We need to perform a personal data inventory, and map all personal data through a glossary
- Cross border data transfer will be prohibited
- Clear process and procedures will need to be established, put in place, and supervised so that they effectively manage all external vendors, handling our customer data.

The goal of this article: "How the GDPR will Impact the Banking Sector?" is, quite simply, to demonstrate how to protect the *needs* of data owners, and other data Stakeholders, who could affect, or be affected by the banks' data. There needs to be a specified means to – protect data by (and from) – *all* who create data, those who use data, and those who set rules and requirements for data.

Caroline Kimber (2018) [451] has provided an analysis of the GDPR applied to banking, finding: "One interesting suggestion in the General Data Protection Regulation (GDPR) contains the 'principle of *data minimization*.' Data minimization means that organizations shouldn't hold more personal data than is needed. For example, for a simple savings product with no fixed-

[450] https://www.lw.com/thoughtLeadership/EMIR--A-Primer-for-Non-Financial-Counterparties-Using-Derivatives. See: See Article 11(2) of European Market Infrastructures (EMIR), and Articles 16 and 17 of Commission Delegated Regulation (EU) No. 149/2013, passed on December 19, 2012 *now* supplementing Regulation (EU) No. 648/2012 of the European Parliament and of the European Council (EC). This European Market Infrastructures (EMIR) revision, or *Reset,* applies with regards to regulatory technical standards on: i) indirect clearing arrangements, ii) the clearing obligation, iii) the public register, iv) access to a trading venue, v) non-financial counterparties, and vi) risk mitigation techniques for over-the-counter (OTC) derivatives contracts *not cleared* by a 'buyer-to-every-seller' and 'seller-to-every-buyer' central counterparties (CCPs) arrangements. [As in: a *single* counterparty must analyze on a bi-annual basis – the possibility to conduct a *portfolio compression* – to reduce counterparty credit risk.]
[451] Source: "How GDPR will impact the banking sector?" By Caroline Kimber, [online] May 2018]. See: https://www.financedigest.com/how-gdpr-will-impact-the-banking-and-finance-sector.html. See *also*: *Ibid*., [Foot Note # *465*].

term tie-in, one might argue that the only variables needed are the customer's contact details, their (customer's closing) balance, and the interest rate of their (the customer's) account. However, to a marketer, other variables may be key in helping determine different products or services, that could be offered (for example a special rate on a child's savings account, could be offered to customers, whom are also parents)."

Kimber (2018) suggests any algorithms used for profiling need to be fair and unbiased and finally, it is important that profiling doesn't "significantly affect" the consumer in a negative way. For financial services organizations, this is a difficult issue, as profiling could be used to determine, say, a more favourable interest rate being given to one consumer over another.

Kimber (2018) continues by arguing that the consumer needs to know the organization(s) with whom their personal data will be shared, so this information should be clearly set out in the privacy policy. If data is sold on to third parties, then additional opt-in consent must be obtained and the third parties clearly named. In summary, GDPR is much more than an IT and data compliance issue. For the banking sector, and possibly even the *research departments* within banks, this is another hurdle which may yet be put in your way.

Q10. – What other changes need OCC address

Hedge fund companies – with their reliance on *prime* brokerage firms (Goldman Sachs, Morgan Stanley and JP Morgan, to site three examples) – require an extra vigilant review by the Securities Exchange Commission (SEC – supervising hedge funds) and the OIC (supervising investment banks).

Reviewing where we are today, post-The Volker Rule (2014 - passed as part of Dodd-Franks legislation), these regulatory instruments attempted to ban investment banks from trading with their own capital. This was implemented in recognition of the damages incurred with the Great Financial Crisis (GFC),[452] although Goldman Sachs, Bank of America, and JP Morgan posted comments expressing concerns about 'The Volker Rule.'[453]

An interesting observation about 'The Volker Rule' was made by the person it was named for: Paul Volker. Mr. Volker was quoted by a New York Times Reporter in October 2011, suggesting: "[Volcker himself stated that he would have preferred a simpler set of rules]. I'd write a much simpler bill. I'd love to see a four-page bill that bans proprietary trading and makes the board

[452] The Great Financial Crisis (GFC) of 2017-2018 was incurred when mortgage-backed securities held by investment banks declined in 2007–2008, causing several to collapse or be bailed out in September 2008.
[453] Source: "Derivatives, 'Volcker' Rules May Be House Republican Targets", By Phil Mattingly, Bloomberg.com, Dated: November 19, 2010.

and chief executive responsible for compliance. And I'd have strong regulators. If the banks didn't comply with the spirit of the bill, they'd go after them.[454]

As much as we would like that type of regulatory expediency and simplicity, this next issue raises far more complexities than existed in 2014.

Hedge funds, by their very constitution, tend to be highly unpredictable. The original hedge funds were structured to hold stocks, 'long and short' (hence *hedged*). They pursue specializations in just about anything – even owning *other* hedge funds. FINRA (2008) report: "There is no exact definition of the term "hedge fund" in federal or state securities laws. Hedge funds are basically private investment pools for wealthy, financially sophisticated investors. Traditionally, they have been organized as partnerships, with the general partner (or managing member) managing the fund's portfolio, making investment decisions, and normally having a significant personal investment in the fund."[455]

For our purposes, reviewing regulatory compliance matters as they may apply to hedge funds, and their counterparts the *prime* brokers (investment brokerage houses), becomes complicated. Hedge funds tend to only be open to limited numbers of wealthy, financially sophisticated investors, and do not advertise or publicly offer their securities. Private hedge funds are usually not required to register with the Security Exchange Commission (SEC). But there is more to this.

FINRA (2008): "Funds of hedge funds are pooled investments in several unregistered hedge funds. Unlike the underlying private hedge funds, the fund of funds itself can register with the SEC under the Investment Company Act of 1940. In addition, the fund of fund's securities also can be registered for sale to the public under the Securities Act of 1933. Registered funds of funds can have lower minimum investments than private hedge funds (some as low as $25,000). A registered fund of hedge funds can be offered to an unlimited number of investors. However, unlike an open-ended mutual fund, there is no investor right of redemption - shares cannot be redeemed directly with the fund unless the fund offers to redeem them. Nor are the shares usually listed on a securities exchange like exchange-traded funds (ETFs). With very limited exceptions, there is no secondary market available, so you won't be able to sell your investment readily."[456]

That lengthy explanation of hedge funds offered by FINRA (2008) suggests they often use speculative investment and trading strategies. Many hedge funds are honestly managed, and

[454] Source: "Volcker Rule, Once Simple, Now Boggles," By James Stewart, [reporter] New York Times. Dated: October 21, 2011.
[455] Source: "Funds of Hedge Funds – Higher Costs and Risks for Higher Potential Returns," By FINRA Organization [website]. Dated: October 6, 2008. See: https://www.finra.org/investors/alerts/funds-hedge-funds-higher-costs-and-risks-higher-potential-returns. See *also*: *Ibid*., [Foot Note # *456*].
[456] Source: "Funds of Hedge Funds – Higher Costs and Risks for Higher Potential Returns," By FINRA Organization [website]. Dated: October 6, 2008. See *also*: *Ibid*., [Foot Note # *455*] '(FINRA 2008) - general provisions for prohibitions against security fraud *do apply*'.

balance a high risk of capital loss with a high potential for capital growth. The fund of (hedge) funds /FOF-hedge, is a fund of funds that invests in a portfolio of different hedge funds to provide broad exposure to the hedge fund industry, and to diversify the risks associated with a single investment fund. Collectively hedge funds' value of assets managed approached US$3.11 T in 2019. Let's continue with this story.

Danielsson *et. al*., (2005) studied the regulatory conundrum re: Hedge Funds. They state "Traditional regulatory techniques, such as activity restrictions and disclosure, are likely to be ineffective (for hedge funds). Hedge funds circumvent such regulations by moving operations offshore, and they also specialize in the most advanced uses of proprietary financial technology. Hedge funds outsource most activities except trading decisions (for example, execution, settlements, clearing, leverage, risk management, etc.) to prime brokers which generally are major investment banks."[457] Since *prime* brokers are regulated, in the US by the OCC, their hedge fund business indirectly falls under supervisory oversight. This does contain a degree of intra-party (counter-party) risk. If the hedge fund fails, the prime broker will detrimentally suffer.

Anecdotal evidence (Danielsson *et. al*., 2005) suggests that *prime* brokers do sometimes inform some of their hedge fund clients about selective trades made by others. For a hedge fund to develop costly proprietary trading models, and then ignore the model in favor of herding, puts the hedge fund at a distinct disadvantage, to a lower cost copycat fund. The latter informational requirement – following proprietary trading models – would insinuate that herding, in the hedge fund's case, would be an inefficient (uneconomic) activity to pursue.[458]

The academic notion of herding refers to the phenomenon by which funds mimic other funds, despite their own private information, or proprietary model, suggesting different strategies. The latter informational requirement implies that herding is inefficient, as it prevents the release of valuable information. For a hedge fund to develop costly proprietary trading models, and then ignore the model in favor of herding, puts it at a distinct disadvantage to a lower cost copycat fund. Since herding requires that trades are observable either directly or indirectly through prices, the secrecy of hedge fund trades makes wide ranging copy-cat herding unlikely. This does not prevent sharing of information to occur between groups of hedge fund managers, or among selected managers and their prime brokers.

But let's not forget that so much of what hedge funds 'do' is highly secretive. The flexibility of hedge fund investment strategies, which is their great investment advantage over other

[457] Source: "Highwaymen or Heroes: Should hedge funds be regulated?" by Jon Danielsson, Ashley Taylor and Jean-Pierre Zigrand, London School of Economics and FMG. Dated: September 2005. Page 3, 6. See: http://www.regattapress.com/ShouldHedgeFundsbeRegulated.pdf. Discussion: Most hedge funds only deal with one prime broker, while some might use more. These may include: Morgan Stanley, JP Morgan or Goldman Sachs, to name three. See *also*: *Ibid*., [Foot Note # *455--461, 464*].

[458] Source: "Highwaymen or Heroes: Should hedge funds be regulated?" by Jon Danielsson, Ashley Taylor and Jean-Pierre Zigrand, London School of Economics and FMG. Dated: September 2005. See *also*: *Ibid*., [Foot Note # *455--461, 464*] '(Danielsson *et. al*.,) prime broker/ hedge fund herding - lack thereof'.

investment classes, fundamentally depends upon confidentiality of (their) trading positions. Remember, though, that *prime* brokers (investment banks) observe the whole trading activity of client hedge funds, and often run its risk engines. Given their involvement in counterparty risk, they have a strong incentive to monitor fund exposures closely. Such continuous monitoring can provide early warning signs for systemic risk.[459]

Supervisors that regulate *prime* brokers could require that prime brokers fulfill the function of 'monitoring fund exposures closely'. Danielsson *et. al.,* (2005) state: "The regulatory framework of hedge funds needs to comprise credible and clear *ex-ante* cost-sharing mechanisms, as well as crisis management procedures." Danielsson *et. al*., (2005) *continuing*: "a formal mechanism is adopted, which party or parties have the ability or duty to trigger the resolution process – the regulator, the prime brokers (which at present are locally regulated entities for the most part), the creditor banks (including the subordinated debt holders) or the hedge funds themselves? What are the informational requirements for this party? Under what jurisdiction does the resolution mechanism proceed? These are issues which require further consideration to provide the correct incentives for the various parties."[460]

Danielsson *et. al*., (2005) next state: "[the resolution process] should start as early as possible, both because the extent of the problem and the related costs grow significantly with time and because it does take some time to understand the exact nature of the hedge funds' positions. A carefully thought through contingency plan would contribute to minimal disruption. (And then,

[459] Source: "Highwaymen or Heroes: Should hedge funds be regulated?" by Jon Danielsson, Ashley Taylor and Jean-Pierre Zigrand, London School of Economics and FMG. Dated: September 2005. See: *Ibid*., [Foot Note # *456-461, 464*] '(Danielsson *et. al*.,) prime broker(s) run the hedge funds' *risk engines'*. Discussion: The September 17, 2019 US Federal Reserve emergency repo loan bail-out springs to mind. The repo loan 'go direct' bail-out program made hundreds of billions a week in loans, to a list including one foreign bank and 23 stock brokerage houses and investment banks, or whom the New York Federal Reserve refer to as the 24 *primary* dealers. There is nothing in the history of the Federal Reserve Act to suggest that elected members of Congress ever intended that the Federal Reserve would become the lender-of-last-resort to bail out the reckless trading floors on Wall Street – and yet that appears to be what happened in 2008, and what is happening today (November 11, 2019). See *also*: https://wallstreetonparade.com/2019/11/the-feds-repo-bailout-and-jpmorgans-38-trading-floors/.
Discussion (*contd*.): Rates in the $2.2 trillion market for repurchase agreements rose as high as 10% on September 17 (2019) as demand for overnight cash from companies, banks and other borrowers exceeded supply. Analysts and bank rivals said big changes JPMorgan made in its balance sheet played a role in the spike in the repo market, which is an important adjunct to the Fed Funds market and used by the Fed to influence interest rates. Without reliable sources of loans through the repo market, the financial system risks losing a valuable source of liquidity. Hedge funds, for example, use it to finance investments in U.S. Treasury securities and banks turn to it as option for raising suddenly-needed cash for clients. Publicly-filed data shows JPMorgan reduced the cash it has on deposit at the Federal Reserve, from which it might have lent, by $158 billion in the year through June, a 57% decline. JPMorgan's moves appear to have been logical responses to interest rate trends and post-crisis banking regulations, which have limited it more than other banks. The data shows JP Morgan's switch accounted for about a third of the drop, in all banking reserves, at the Fed during the period. (Risk engines, anyone?). See *also*: https://www.reuters.com/article/us-usa-repo-jpmorgan-analysis/too-big-to-lend-jpmorgan-cash-hit-fed-limits-roiling-us-repos-idUSKBN1WG439.

[460] Source: "Highwaymen or Heroes: Should hedge funds be regulated?" by Jon Danielsson, Ashley Taylor and Jean-Pierre Zigrand, London School of Economics and FMG. Dated: September 2005. See *also*: *Ibid*., [Foot Note # *456-461, 464*] '(Danielsson *et. al*.,) Page 26-27.

very prophetically, it is stated: other client banks, to the extent that they also have this knowledge, should have the same reporting obligation. Furthermore, the banks should have an obligation to participate in the resolution process. Enforcement of the necessary actions should be a part of the process and may require a special arbitration body. However, the unwinding, reorganizing or refinancing of the portfolio of a hedge fund may be profitable, certainly if the trigger for the resolution mechanism is a temporary lack of liquidity by the hedge fund."
The corollary to all of this? "Non-enforcement of regulatory compliance "might hasten the introduction of a more intrusive regulatory regime for hedge funds, and banks might suffer considerable costs if the failure of a hedge fund had systemic consequences prompting overbearing financial legislation, as happened following the 1929 crash." [461]

Let's bring this narrative up to the present day. BlackRock, an investment manager of (pre-pandemic) $7 Trillion in stock and bond funds, has been hired by the US Federal Reserve, the Bank of Canada, and Sweden's central bank - the Riksbank,[462] to coordinate monetary and fiscal policy to provide pre- and -post coronavirus pandemic stimulus counsel. This is follow-on activity from the US Congress handing over $454 billion to the Fed to forego the losses on toxic assets produced by the Wall Street banks it supervises. As it proceeds, the Fed may leverage the $454 billion into a $4.5 Trillion bailout package, 'going direct' with bailouts to the commercial paper market, money market funds and a host of other markets.

BlackRock have been tasked by the Fed to 'go direct' and buy up to $750 billion in both primary and secondary corporate bonds, and bond ETFs (Exchange Traded Funds), a product of which BlackRock – through its iShares brand, plus a giant roster of holdings in stock-based ETFs – is one of the largest purveyors in the world. Estimates suggest BlackRock will get $75 billion to cover losses on corporate bond purchases, including its own ETFs, which the Fed is allowing BlackRock to buy, including its own ETFs, in the 'go direct' program.

A BlackRock statement at the G7 Summit of central bankers, convened in Jackson hole, Wyoming in August 2019, reported: "Any additional measures to stimulate economic growth (given a financial crisis of a global scale) will have to go beyond the interest rate channel. And 'go direct' [with] a central bank crediting private or public sector accounts directly with money. One way or another, this will mean subsidizing spending – and such a measure would be fiscal rather than monetary – by design. This can be done directly through fiscal policy or by expanding the monetary policy toolkit with an instrument that will be fiscal in nature, such as credit easing by way of buying equities. This implies that an effective stimulus would require

[461] Source: "Highwaymen or Heroes: Should hedge funds be regulated?" by Jon Danielsson, Ashley Taylor and Jean-Pierre Zigrand, London School of Economics and FMG. Dated: September 2005. See: *Ibid*., [Foot Note # *456-460, 464*] '(Danielsson *et. al*.,) Page 28. Discussion: Such profits highlight the need for effective Chinese walls between the prime broker and other divisions of the investment bank. Otherwise, the investment bank might have an incentive to hasten the demise of a hedge fund, or exploit its inside information in the resolution process.
[462] The Bank of Canada announced in April 2020 that BlackRock will offer the Canadian central bank advice on commercial paper, provincial bonds and corporate bond buying programs. A press release on May 15, 2020 by the Riksbank, announced that Blackrock will advise the Swedish central bank on possible design options for a potential corporate bank asset purchase program.

coordination between monetary and fiscal policy – be it implicitly – or explicitly."[463]

And quite explicit it is! The Fed has granted BlackRock a no-bid contract to manage all its corporate bond programs. Danielsson *et. al*., (2005) grabbed the bull by the horns decades ago! They wrote: "Prime brokers may have the belief that if worse comes to worst, public funds will bail out the bank. Are the informational restrictions for investment banks likely to hold in practice?"[464]

The answer to that last question? Advanced Systems Management Group (ASMG): The systemic failure reporting obligation, outlined so succinctly above, should have an audited, secure information sharing (and information exchange) tagging and labeling audit trail, between the Federal Reserve, SEC, OCC (and the hedge funds or investment banking entities in difficulty). This can be demo'ed now, and should, ASMG believes, occur haste-post-haste. Not to proceed in this fashion would be highly unusual, to say the least.

Q11. – Changes to banking (post Covid-19)

11-1 Cyberthreats

As many enterprises become more reliant on integrating customer-sourced data into their processing activities, the emphasis shifts dramatically towards protecting and securing data. Organizations simply cannot risk exposing detailed data from customers when any change to the way data is handled can have unintended consequences. Maintaining confidentiality across more and varied input sources brings new levels of complexity to data governance, security, and privacy.[465]

[463] Source: "BlackRock Authored the Bailout Plan Before There Was a Crisis – Now It's Been Hired by three Central Banks to Implement the Plan," By Pam Martens and Russ Martens, Wall Street on Parade [online]. Dated: June 5, 2020. See *also*: Ibid., [Foot Note # *294*].
https://wallstreetonparade.com/2020/06/blackrock-authored-the-bailout-plan-before-there-was-a-crisis-now-its-been-hired-by-three-central-banks-to-implement-the-plan/.

[464] Source: "Highwaymen or Heroes: Should hedge funds be regulated?" by Jon Danielsson, Ashley Taylor and Jean-Pierre Zigrand, London School of Economics and FMG. Dated: September 2005. See *also*: *Ibid*., [Foot Note # *456-461*] '(Danielsson *et. al*.,) Page 28.

[465] Every product, sensor and edge device is a potential attack point that must be safeguarded, which means that resource allocation to cybersecurity, data privacy, and compliance issues will need to keep pace. As attack surfaces expand, threats like advanced malware, worms and advanced persistent threats, coupled with GDPR compliance issues, will require immediate attention. Source: "Top 10 operational impacts of the GDPR: Part 1 – data security and breach notification," by Rita Heimes, Critical Infrastructure Protection Program -CIPP / US. Dated Jan. 6, 2016. '(EU-US Working Group on Cybersecurity and Cybercrime has been working on a global response for data protection and data privacy.' See *also*: "How GDPR will impact the banking sector?" By Caroline Kimber, [online] May 2018] *a.k.a.* [Foot Note # *451*] '(Kimber – 2018) GDPR Compliance overview (as good an overview as any)'.

The risk quotient generated by top cyberthreat dark web actors[466] is at a dangerous level. Cybercrime damage costs will more than double during the global pandemic of COVID-19. Here are some recent reports on how consumers in the US have been adversely affected. Social Catfish, the identity verification non-profit in the US, has reported five (5) states – California, Florida, New York, Texas and Pennsylvania combined account for one--third of the 150,000 instances of everything from fake stimulus check offers, to shopping scams and fake Covid-19 cures. Maine, a smaller state, has reported a surge in consumer-related identity theft complaints and scams due to Covid-19 related fraud, which are quadruple the number received in the past, over just the March to July (2020) timeframe. Victims, in total, have been swindled of a number as high as approximately $97.5 million, the US Federal Trade Commission (FTC) reports. Other types of fraud being perpetrated, according to the FTC, include: robo-calls, texts or emails seeking personal information to "deposit benefits scams promising to deposit non-existent funds into victims' accounts[467].

Hackers leveraging on the COVID-19 pandemic are motivated by a combination of personal financial gain, as well as political espionage, to cause social upheavals.[468] This will be caused by not only phishing scams, but an uptick in ransomware attacks, insecure remote access to corporate networks and, employees exposing login credentials and confidential data to members at home. In the financial sector, a UK research report (Cybersecurity Ventures) claims that around 70 per cent of financial firms in the U.K. reported security incidents in 2019. This UK Report (2019) highlighted that most of the attacks have originated due to employees who failed to follow proper data protection policies. As well, employees made erroneous downloads of malware or viruses from third-party devices like USBs, and file transfers to unsecured sources.[469]

---

[466] Source: "How coronavirus is impacting Cyberspace," By cisomag [online]. Dated: 2020. See: https://www.cisomag.com/cybercrime-will-cost-the-world-us6-trillion-by-the-end-of-the-year-study/. See *also*: *Ibid*., [Foot Note # *468*, *473*]. Discussion: On dark web forums: 1) a group from Hong Kong hatched a plan to create a new phishing campaign targeting the population from mainland China. The group aimed to create distrust and incite social unrest by assigning blame to the Chinese Communist Party. 2) CYFIRMA (March 18, 2020) report that Korean-speaking hackers were planning to make financial gains using sophisticated phishing campaigns, loaded with sensitive data exfiltration malware and creating a new variant of EMOTET virus (EMOTET is a malware strain that was first detected in 2015 and is one of the most prevalent threats in 2019). These hackers were planning to target Japan, Australia, Singapore, and the United States. Thirdly, 3) A Russian hacking community developing a new malware called CoronaVP was being discussed, which could lead to a new ransomware or EMOTET strain, designed to steal personal information. See *also*: *Ibid.,* [Foot Note # *468, 473*] 'How coronavirus is impacting Cyberspace.'

[467] Source: "Study: Covid-19 Fraud Reaches $100 Million," By Richard Neil, attributed spokesperson for Social Catfish.com, [online]. Dated: Thursday July 8, 2020.

[468] Source: "How coronavirus is impacting Cyberspace," By cisomag [online]. Dated: 2020. See: https://cisomag.eccouncil.org/cybercrime-will-cost-the-world-us6-trillion-by-the-end-of-the-year-study/. See *also*: *Ibid*., [Foot Note # *466, 472*].

[469] Source: https://www.cisomag.com/finastra-hit-by-ransomware-attack-shuts-down-servers/. See *also*: *Ibid*., [Foot Note # *36*, *471, 472*].

In the case of London-based Finastra, they warned their financial sector customers that "we are anticipating some disruption to certain services, particularly in North America," said Finastra Chief Operating Officer, Tom Kilroy. (Kilroy): "We would like to reassure our stakeholders that, to the best of our knowledge, we do not believe that any customer or employee data was accessed or exfiltrated, nor do we believe our clients' networks were impacted."[470]

Organizations that fail to provide good data governance, the cornerstone to RegTech, will lose and lose big.[471] Financial establishments, as they wrestle with regulatory compliance issues, experience threats from a variety of sources, and led by mobile application and web portal proliferation, are under increasing duress. Cyber criminals may steal or manipulate valuable user data and or "clone" banking apps, and use them for nefarious purposes.[472]

So how are we doing so far, in the middle-of-the-year (2020) time-frame? Could be better. It is estimated that cybercrime will be more profitable than the global trade of all major illegal drugs combined. What researchers have seen and heard, regarding this rapidly expanding list of threat indicators, are made up of conversations observed and uncovered in the dark web, hackers' forums, and closed communities. These hackers' communities span far and wide, communicating in Cantonese, Mandarin, Russian, English, and Korean, unleashing campaigns one after another, to wreak havoc on unsuspecting nations and enterprises.

And if we want one seminal example, we couldn't do better than to examine the hack of Capital One. A software engineer in Seattle, Washington, and ex-Amazon employee that hosts the Capital One corporate financial records on Amazon's Web Service (AWS) hosting platform, found configuration vulnerabilities in Capital One's security software. The hacker, Paige Thompson (identified publicly in official records of the incident) used a gap in firewall systems, approximating a *gate* or window left open, to gain security credentials and download credit card and social security numbers. This led to Capital One's experiencing losses in the range of $400 million, after cybersecurity insurance policies were administered.

Capital One spent close to $100 million in corrective remediation measures, to ensure this would not happen again. Capital One were tipped off three months after the incident occurred,

---

[470] Source: https://www.finextra.com/newsarticle/35499/finastra-brings-servers-back-online. Discussion: Finastra public relations announcement – March 23, 2020. See *also*: *Ibid*., [Foot Note # *36*, *471, 472*].

[471] Source: https://www.talend.com/blog/2016/08/08/cio-3-questions-to-ask-about-your-enterprise-data-lake/. Discussion: Since the Global Finance Crisis (GFS), financial institutions are under far greater government scrutiny. As a result, the bar has been raised in terms of the IT and data governance measures required to meet these regulations. For example, a US bank recently settled a multi-million-dollar penalty with SEC, due to its failure to enforce policies and procedures to prevent and detect false securities transactions (involving the misuse of material and non-public information). See also: Ibid., [Foot Note # *35, 344, 365-367*].

[472] Source: TokenEx [security services third party player] Report – "As many as 20 million card details potentially revealed in breach". Email dated Friday, April 3, 2002 at 9:45 am. [to: J. Carter, ASMG]. Discussion: Global fintech firm, London-based Finastra, takes multiple servers offline after suffering breach. A ransomware attack on Finastra has resulted in a disruption to the services it provides North American customers, including two U.S. financial institutions. Details of the breach, which customers were affected, and what records were exposed have not yet been made available. See *also*: *Ibid*., [Foot Note # *36*, *470, 471*].

by an email posted on the coding platform GitHub. While it is pure speculation if anyone else had access to the back-door '*in*' to Capital One's financial records, the damage was certainly felt to the core of the organization.

The tasks which regulatory compliance professionals address may be even more difficult than what would have been thought possible, just a few months ago.[473] Most prototyped analytic algorithms and models, serving any big data engine and/or the overall regulatory compliance ecosystem itself, have struggled to reach production in even the best of times. Under global pandemic conditions, the security threat has grown even more astronomically.

Before we can move to address the challenges that lie ahead, we need to summarize and review the subject of inconsequential web-based apps. Web-based apps, e.g. apps on mobile devices or Internet-of-Things (IoT) appliances (sensors) and mobility devices (smart phones) may all have been improving somewhat, but on security matters, they register a great big fail.

We alluded just now to Web-based apps improving. Google designers in 2015 coined the term progressive web apps (PWAs). PWAs describe apps which take advantage of new features, supported by modern web browsers. PWAs are easier and cheaper to develop, and they can be coded for use in a browser. Examples of these are Slack (chat, messaging and files) Trello (collaboration tool or electronic whiteboard), Google Docs (free alternative to Microsoft Word, acting as a word processor on Google's online office suite), Gmail (the ubiquitous email service) and the social media's Twitter.[474]

Google designers would have us believe that progressive web apps (PWAs) behave very much like native apps, downloaded onto our smart phones, with the only difference being they do not control our smart phone's hardware. Progressive web apps (PWAs) are reputed to be more censorship resistant, and touted for their greater decentralization, the ethos of the *new* Web 3.0. Compare these observations with the more in-depth review of web apps, offered by the Open Web Application Security Project (OWASP).

The Open Web Application Security Project (OWASP) foundation state that the top five most critical web application and web site, and mobile device, application security risks[475] are:

i) Broken access controls
Broken Access Control: This means that restrictions on authenticated users are not properly enforced, leading to one user able to see other users' files or modify other users' data.

[473] Source: "How coronavirus is impacting Cyberspace," By cisomag [online]. Dated: 2020. See *also*: *Ibid.,* [Foot Note # *466, 468*] '(cisomag-2020) How coronavirus is impacting Cyberspace.'
[474] Source: "Four things you need to know about mobile dapps," By Adriana Hamacher, article on Decrypt [online], Dated: Feb 14, 2019. See: https://decrypt.co/5181/four-things-mobile-dapps-apps-crypto. See *also*: *Ibid*., [# *155*, *163*, *164*).
[475] Source: "Top 5: Security risks associated with web apps," By Tom Merritt, article in Security / published at TechRepublic [online]. Dated: March 16, 2018.
See: https://www.techrepublic.com/article/top-5-security-risks-associated-with-web-apps/.

ii) XML external entity (failures)
XML External Entities: This occurs when older (or badly configured) XML processors evaluate external entity references within XML docs. This step can expose internal files, and allow for internal port scanning, remote code execution, and denial of service attacks.

iii) Sensitive data exposure
Sensitive Data Exposure: This is where sensitive data is not encrypted, in transit or at rest, leaving it exposed for attackers to steal or modify.

Iv) Broken architecture
Broken Authentication: If authentication - and session management - is implemented wrong, attackers can compromise passwords, keys or session tokens and assume other users' identities.

v) Injection (with untrusted communications / data / authorizations)
Injection: Whether it's SQL, NoSQL, OS, or LDAP, an untrusted dataset gets sent to an interpreter, tacked on to a command or query, tricking the interpreter into executing unintended commands, or accessing data without authorization.

Advanced Systems Management Group (ASMG) cannot sit idly by. Web and Internet-of-Things (IoT) application security shortcomings – expressed via mobile network, and web site data transport failings 'at the application interface level' and even deeper into data holdings – are, in a word, appalling. So here is an in-depth look at this issue.

Visitors to Web sites or application Users – citing a routine, everyday bill payment example, at a check-out register in a retail store – expect organizations to retain secure socket layer (SSL) certificates, use compliant payment systems, and to protect their data and information from getting leaked to hackers. What we generally know, and accept as the unfortunate state-of-affairs in eCommerce today, is that the user experience via an on-line transaction, and the security in-place to protect our user experience, is a balancing act.[476]

'Secure By Design,' is a term which means software and software systems, or applications supported by software and software systems, need to be secure from initiation with no compromising with security parameters while heading toward a [task] completion.

The UK's National Cyber Security Centre (NCSC) characterize a lower profile threat actor as involved with commodity threats. A commodity threat agent makes use of tools and techniques that are openly available, cheap and simple to apply. Regardless of their technical capability and motivation, attackers will often turn to commodity tools and techniques first. Next higher on

[476] Source: "Secure by Design: A Web Development Essential," By Shilpi [online – opensenselabs.com]. Dated: September 3, 2019. See *also*: *Ibid*., [Foot Note # *486, 497*].

the threat intelligence scale, are elevated threats. Elevated threat agents are well-funded groups, maybe high-end organized crime cartels or state-sponsored groups.[477]

The organization that monitors and applies solutions to commodity threat actors and agents is called the Open Web Application Security Project (OWASP), a foundation which we are going to draw from next. OWASP have listed their top five most critical web application or web site and mobility device application security vulnerabilities. Let's begin with broken access controls first.

11.1.1 Broken access controls

The main purpose of an authentication system is to assure that any entity attempting to access a resource is genuine. A weak authentication system will lead to a system breach, allowing an attacker *entry*. In a situation with a broken access control, an unauthorized user bypasses the authorization and performs the tasks of a trusted privileged user. For instance, an employee from outside of the financial department can access or check the finance or transaction records, which may be occurring within the finance department.

In another scenario, it is the physical records which set up the cause for a breach to occur. Old and obsolete pages can be a major source of broken access vulnerabilities. To get a clear picture of where the attack has (or *will have*) happened, one solution may be to involve the user experience (UX) staff in fully sketching out (data logs, etc.) user flows related to access permissions and get rid of the pages which are no longer needed by taking all the 'uses e.g. use-cases' into consideration. Additionally, the focus should be given to responsible parties to address weak uniform resource locators (URLs), while creating the information architecture or search engine optimization (SEO) such that by keeping track on the ways by which outsiders/attackers might *manipulate* URLs, to grant their access through malfeasance intent, can be monitored, and remediated and/or restricted.

Conclusion here: An application is viable to security attacks at every level of that app's development. This is reason enough to take restrictive and tight-monitoring-timetabling on malicious events. A few common commodity threat precautions to take include, two factor authentication (2FA), which can be used to restrict repetitive log-in attempts. Secondly, password safes may be used to create unique (and strong) passwords otherwise impossible to remember. The UK's National Cyber Security Centre (NCSC -2020) warn that if you forget the master password for your password manager / password safe, you will not be able to get back in. A standalone password manager requires you to remember a long master paraphrase (unlike a browser-based paraphrase). They also may have more advanced security such as: i) notifications about compromised websites; ii) flagging *up* used or weak passwords; iii) prompts for you to change old passwords; iv) assistance with changing passwords for *some* web sites by integrating with your (web or application) browser, and; v) multi-factor authentication installation. The UK's National Cyber Security Centre (NCSC -2020) have stated that *password*

[477] Source: "Design guidelines for high assurance products," By Duncan A. [online – ncsc.gov.uk]. Dated: February 6, 2020.

manager / *password safe* may have outstayed their welcome, although they do not prescriptively tell us what we should use next.

Web access controls were not, it is true, deliberately designed when web apps started to proliferate, with any real developer concern about security of the content the app was delivering. They simply, web apps that is, just grew and become more prevalent all over the place. An *ad hoc* set of rules justifying (or assigning to whom) access rights to web content perplexes, even today, the most competent web site systems administrator. In a nutshell, the problem lies with the web interfaces, the site where applications process their copious traffic flows. And, the site where outsider and insider threat attacks enter a web app or the web address and web data repositories with an unneeded regularity.

11.1.2 XML external entity (failures)

The Open Web Application Security Project (OWASP) foundation describes this next topic as a type of attack against an application that pares XML input.[478] This attack occurs when XML input containing a reference to an external entity is: processed by a weakly configured XML parser. This attack may lead to the disclosure of confidential data, denial-of-service server side request forgery, port scanning from the perspective of the machine – where the parser is located – and other system impacts.

There are a few types of entities under the XML 1.0 standard – one example being the term 'external general -parameter parsed entity', which is *shortened* to just 'external entity (XXE)' – that can access local or remote content, via a declared 'system identifier.' A system identifier is assumed to be a uniform resource identifier (URI) that can be dereferenced (accessed) by the XML parser, when processing the *entity*. Let's jump forward. If the system identifier contains tainted data, the XML processor may disclose confidential information normally not accessible by the application. Similar attack vectors might freely apply the usage of external 'document type declarations' (DTDs), external stylesheets, external schemas, etc. which – when included, as part of an attack vector – may allow similar, external resources. to offer 'inclusive-style' attacks.

Since the attack occurs relative to the application processing the XML document, an attacker may use this trusted application to pivot to other internal systems, possibly disclosing other internal content via http(s) requests. Or, the attacking party may launch a 'cross-site request forgery' (CSRF)[479] attack, to any unprotected internal services. Note that the application does not need to explicitly disclose *type information* for exfiltration of data through the sub-domain,

[478] Source: "XML External Entity (XXE) Processing," By Open Web Application Security Project (OWASP) foundation [online]. No Date.

[479] JavaScript wasn't invented until `1995. Cross-site request forgery (CSRF) attacks generally require session cookies, and cookies weren't introduced until 1995. See: "Security Briefs – XML Devoid of Service Attacks and Defenses," By Bryan Sullivan, Vol. 24, No. 11/Microsoft documentation library [online]. Dated: November 2009. See: docs.microsoft.com. See *also*: *Ibid*., [Foot Note # *478, 480*, *481*].

for exposure of *type information* to occur, i.e. the 'names to a DNS server that they possessed controls for' can be subject to exfiltration.

Sullivan (2009) reviews XML denial-of-service (DoS) attacks and suggests that are extremely asymmetric in their delivery. Denial-of-service (DoS) vulnerabilities in code that processes XML are extremely widespread.[480] Sullivan (2009) suggests denying attack surface (e.g. denying service to your application) by disabling entity expression, if you don't require the entities expression in the first place, may work.

Morgan (2014) wrote the definitive study on this topic. The core of eXtensible Markup Language (XML) is the ability to define and validate document structure using schemas and document type definitions (DTDs). However, Morgan (2014) reviews their incorrect usage: a straight path to security vulnerabilities. Certain featured built into the design of XML, namely inline schemas and DTDs, are a well-known attack vector. This stems from the overall fact that overall awareness within the development community remains low, while the behavior of many XML parsers is to expose risky features by default.

Morgan (2014) calls on the vendors supplying / developing XML libraries to try to disable the most dangerous of features by default and improve API documentation[481] to mitigate any remaining risks. Here are several more of Morgan's suggestion(s): i) conduct research on the default XML parsers provided by mobile platforms, such as the - iOS NSXML Parser and Android's Xml Pull Parser – to better understand the risks associated with the [XML] libraries; ii) develop a better understanding of what XML parser configurations – if *ever* would allow the schemaLocation and the noNamespace SchemaLocation attributes [can be] used in Server-Side Request Forgery (SSRF) attacks, and; iii) test additional XML parsers commonly used in Java and

[480] Source: "Security Briefs – XML Devoid of Service Attacks and Defenses," By Bryan Sullivan, Vol. 24, No. 11/Microsoft documentation library [online]. Dated: November 2009. See *also*: *Ibid*., [Foot Note # *478, 479, 481*] '(Sullivan 2009) denying attack surface by denying entity expression'.
[481] Source: "Security Briefs – XML Devoid of Service Attacks and Defenses," By Bryan Sullivan, Vol. 24, No. 11/Microsoft documentation library [online]. Dated: November 2009. See *also*: *Ibid*., [Foot Note # *478 - 480*] '(Sullivan 2009) call to fix XML libraries'.

Ruby.[482]

11.1.3 Sensitive data exposure

Sensitive data like passwords, information related to finances (credit card numbers, passwords, personally identifiable/PID information) must be protected as it can be re-engineered to allow an attack on an unsuspecting victim/user. For example, a Man-in-the-Middle (MIIM) scenario, in which the offender either eavesdrops, or impersonates, the victim/user, or steals the valuable information making it appear to be a normal information exchange. A solution may be to use data encryption, and secondly – don't allow data storage on the web account – *two* measures offering *some* degree of relevancy to fend off data breaches.

As this topic's name suggests, the security threat that occurs when the web application doesn't adequately protect sensitive information, like session tokens, passwords, *banking information*, location, health data or any other similar critical data – whose leak can be critical for the user –

[482] The Trusted Information Exchange Service (TIES) / IEF technology demonstrator project (TDP), funded by the Government of Canada (GoC), addressed Secure Messaging services. The TIES / IEF technology demonstrator focused on Policy-driven, Data-centric access and release policy management issues and services, for Structured Messaging. This was analyzed *with* deployment of this capability in a cloud environment. ASMG – the project implementer– adopted the computer platform / infrastructure integration configuration which used open-source applications: They include:

• Open Slice DDS was used to provide the basic ISMB, with the intent to move to a DDS Security Implementation;
• Balana open-source XACML 3.0 implementation was used to provide the PDP and PEP function. The PEP was extended to:
  o provides the integration to the ISMB;
  o provides an integration to OpenSplice DDS – (which) – provides an integration platform for the integration of the client environment;
  o provides an integration to Apache Tomcat – (which) – provides basic web service communications; and
  o implements the core element of the Messaging-PEP capabilities.
• NASA World Wind development toolkit was used to provide a GIS for geospatial information.
• Apache Cloud Stack was used to provide the Cloud Services for the deployment of virtual Windows and Linux implementations of the Information Exchange Framework (IEF) Reference Architecture (RA). The IEF reference architecture was also deployed on stand-alone Windows and Linux machines.
• Simple Logging Facade for Java (SLF4J) for basic application level logging. Logging will be enhanced in the next version provide the TLS capability to incorporate hash log files or blockchain features.

Beyond the custom integration (using JAVA 8), only the ASMG implementations of the Packaging and Processing Service (PPS) and partial implementation of the PAP represented a custom service implementation. This implementation executed policy models for standard messages including:

• STANAG 5525 – NATO Multilateral Interoperability Programme (MIP) Protocol Data Units (PDU) and MIL XML. This included the use of the Shared Operational Picture Exchange Services (SOPES) Information Exchange Data Model (IEDM) V1.0 policy model. • OASIS Common Alerting Protocol (CAP) v1.2.
• Maritime Information Exchange Model, Maritime domain model for the National Information Exchange Model (NIEM) canonical model.

Messaging on the IEF Secure Message Bus (ISMB) represented a subset of the XML messages provided in Annex A, issued as a simple string over Distributed Data Services (DDS).

The Trusted Information Exchange Service (TIES) / IEF demonstrator project features structured messages which contain embedded elements (e.g., Digest, multiple information package, and multiple information payloads). Source: Information Exchange Framework (IEF) Final Revised Submission (FRS) See: OMG Document Number: MARS/2017-02-21; pp.8, 327.

are situations which the Open Web Applications Security project (OWASP)[483] foundation are concerned about. OWASP describe any threat that causes financial loss, access to the victim's accounts, blackmailing and / or depletes trust in the *brand* the user has vested their reputation and confidence in, or unacceptable threats to allow to go unpunished.

Data transmitted over a network is considered *data in transit*. For example, when you browse the web, you generate HTTP traffic which carries data between you and the target server. Because it is in motion, this type of data can be targeted. For example, if you land on a website which asks for your credentials without using HTTPS, your credentials will transit in clear-text. If a vulnerable server returns more information than it should. For example, JavaScript files can contain production API keys, passwords, etc., the server can return verbose errors which disclose passwords of highly sensitive assets. It's even possible that a vulnerability may occur which generates an error contained the admin password of a critical marketing asset.

All data which doesn't move in the network is at rest. *Data at rest* includes archives, backup files, databases, etc. an attacker can access it through a lack of authentication, poor access control on a repository, etc.

Remediation efforts all involve classifying data. This ensures that you clearly distinguish your sensitive data. There are many data classification policies available, for instance to stem the manipulation of Credit Cards, there is the PCI DSS standard. There are specific encryption requirements for PCI DSS. The general rule is to use strong encryption algorithms and protocols. As well, by applying the least privilege principle on the way you access your data, to reduce the attacker's abilities to read sensitive data, provides one deterrence. Another is to employ unprivileged database users with specific permissions, in-line with the acceptable level of risk your business can afford.

11.1.4 Broken architecture

We are in an environment of constant creation, but application development generally seems to have a general lack of awareness about security.[484] To build an application on expediency (of result) rather than longevity (product responsiveness) is simply wrong. Here are a few tips:

1) Separated storage – this follows the simple observation 'store files that serve different purposes in different places. Store all app images in image directories. Core application files and assets should not mix with other data, e.g. especially not with *user input*. Keep user-uploaded files and activity logs (which can be vulnerable or sought after in injection attacks) separate from the main application. Achieve separation via a different server, different *instance*, separate IP range or separate domain.

[483] Source: "Sensitive Data Exposure explained – Open Web Application Security Project (OWASP) Top 10," By OWASP foundation [online]. No Date.
[484] Source: How to make your app's architecture secure right now: separation, configuration and access," By Victoria Dale [online – feeCodeCamp]. Dated: October 1, 2019. See *also*: "Open Web Application Security Project (OWSAP) App Security Verification Standard," By OWASP foundation [online]. No Date.

2) Customized configurations[485] – examine architecture components for unattended areas:
a) default accounts, default passwords, or sample date 'left' in the application (e.g. web pages, tutorials' text, sample *test case* data, etc.);
b) unnecessary 'ports' left in service; ports left open to the internet;
c) unrestricted permitted HTTP methods;
d) sensitive information stored in automated logs;
e) default configured permissions in unmapped service;
f) director listings or sensitive file types; left accessible by default.

3) Controlled access and user scope – automated testing tools struggle with an application in a misconfigured access control. Consider this a pressing vulnerability early in software development e.g. be extra careful at the 'design in' stage with: sensitive tokens; keys passed as URL parameters, or; asses (in advance) any/all security controls 'suitability to prove to be functioning' securely or 'suitability to prove to be functioning' insecurely.

4) Security misconfigurations[486] – show an excessive display of text describing "verbose errors" (messaging). By displaying way too definitive an 'error message' the attacker / threat agent can learn a system vulnerability at a very high-level. Secondly, security misconfigurations may be caused by the failure to remove unused features from 'code', and / or displaying 'generalized error messages' which may be too instructive. Thirdly, a regular review of account permissions or back-up authentication credentials – should they lag far behind the norm, are all susceptible to an outsider / attacker gaining unwanted access.

A computer system is a dynamic system and operating system configurations continuously change. Installing or updating software and hardware drivers happens frequently and installing different versions of an application affects the system's internal structure, the registry and

[485] Customized and Configured. The problem is that these terms are not always well defined. Here's an attempt: Customize: "To write new code (i.e. programs, class files, scripts) to put in the software that meets specific requirements." Configure: "To use tools in the application to meet specific requirements without the use of code." Which is better? Custom code is working outside the application, but may become brittle (won't work). Configured code uses tools within the application, in a way that the application was expressly design to have [those] changes made. Configuration is inherently better because it is working within the application. Source: "Configuration vs Customization – What's the Difference and Why Does It Matter?" By Brad Baldauf [online - Miratech]. Dated: June 20, 2017. See: https://mitratech.com/resource-hub/blog/configuration-vs-customization-whats-difference-matter/. NB: With the introduction of cloud computing, the purposes of software configuration management (SCM) have become merged, i.e. the SCM tools themselves have become virtual appliances that can be instantiated as virtual machines and saved with state and version. The tools can model and manage cloud-based virtual resources, including virtual appliances, storage units, and software bundles. The roles and responsibilities of the actors have become merged as well with developers now being able to dynamically instantiate virtual servers and related resources. See: "Develop cloud applications with Rational tools", By A. Amies, A, S. Peddle, T M Pan and P X Zou; IBM developerWorks. IBM. Dated: June 5, 2012.
[486] Source: "Secure by Design: A Web Development Essential," By Shilpi [online – opensenselabs.com]. Dated: September 3, 2019. See *also*: *Ibid*., [Foot Note # *476, 497*].

other crucial components that persuade testing results.[487] Then, if we look at something like an Android (mobile device), 'Users' interact with the app to: i) fetch data from a server, ii) interact with the device's sensors, iii) access local storage, or iv) render complex user interfaces. To make your code easier to test, develop your code in terms of modules, where each module represents a specific task that users complete within your app.

For example, a "task list" app might have modules for creating tasks, viewing statistics about completed tasks, and taking photographs to associate with photos (from a set list of) task(s). Such a modular architecture also helps you keep unrelated classes decoupled and provides a natural structure for assigning ownership within your development team. Each module should have only one area of focus, and the APIs that allow for inter-module communication should be consistent.[488]

According to Forbes, the current mobile market share of Android lies between eighty (80) and (almost) ninety (90) per cent. iOS (Apple), in comparison, dominates the other ten (10) to twenty (20) per cent of the market, which basically leaves an extremely low percentage to other operating systems. Apps that are running on Android are programmed in Java, currently the most popular programming language in the world. Android may also be written with Kotlin, or C#. Apple's native mobile app development language Objective-C has given way to Swift, with advanced error checking and a streamlined language set. The back-end development – the integrated developmental environment (IDE) is, for Android – Eclipse, Android Studio and IntelliJ. For Apple, the IDE is (usually) Xcode8, although Appcode is also used.

A year ago, it was reported in the 'tech press' that Facebook was distributing a data-siphoning Virtual Private Network (VPN) – a simple software that was created to protect your online privacy and make life harder for hackers by anonymizing your traffic and location – that was doing anything but what it was designed to do! Facebook's VPN app was allowing adults and teens that were the acquirers of the VPN app (where the VPN was installed), a gifting to the receiving party (hackers!) near-complete access to their iPhone data. The hackers offered the unsuspecting victims – the acquirers of the VPN app (where the VPN was installed) – an exchange of $20 a month in gift cards. Facebook could do this due to its access to an Apple-made developer tool, that was explicitly designed to let apps bypass the Apple App Store – and

[487] Source: "Automated Testing in Virtual machines," By Smartbear staff [online – smartbear.com]. Dated: 2020. See: https://smartbear.com/learn/automated-testing/testing-on-virtual-machines/.
[488] Source: "Fundamentals of [Android] testing," By 'developers' [online]. Dated: March 19, 2020. Discussion: Be forewarned! Android suffers from fragmentation – many versions of the OS and Devices are on the market. If you need to provide offline access to content or perform functions, without a network/wireless connection, then an app makes sense. Two more tips (Vaghela 2010): Memory usage is limited, so code wisely. Secondly, understand the synchronous and asynchronous way of interacting with the remote services. How will you handle push messages? How will you sync the local data store with the remote store? Do not just build applications, build solutions? Source: "Introduction to Mobile Development," By Pragnesh Vaghela, Technology Three [online]. Dated: March 2010. See: https://www.slideshare.net/technologythree/introduction-to-mobiledevelopment.

that, until now – has largely escaped the Apple App Store's scrutiny.[489] Another analyst has claimed that Google Android Marketplace possesses mobility device management (MDM) apps designed to phish banking credentials from unsuspecting customers[490].

And now for something completely different … a good example! Mobile device management (MDM) software solutions can assist financial institutions' (FIs') with client *transaction monitoring* but more specifically, defuse the abusiveness of broken architectures. DeviceAssure is one example of mobile device management MDM at work. DeviceAssure enables organizations to reliably identify counterfeit and non-standard devices with a real-time check on a device's authenticity.[491]

There are two critical issues mobile device management (MDM) solution software addresses: 1) falsified identities – HTTP headers, brand and model spoofing, and IMEI,[492] and; 2) Incorrect specifications – OS skins, custom ROMs and below specification hardware.

The first, *falsified identities*, are shown to be affected by: Botnets, emulators and non-standard devices. *Incorrect specifications*, the second mobile device management (MDM) software corrective factor addressed, identifies the things that *spook* the mobile device, the spooking consisting of planned (and programmed) 'mixing-up' of: non-authentic devices and non-standard devices. Both *Falsified identities* and *Incorrect specifications* are subject to: i) device fraud (dFraud) and click fraud; ii) fraudulent access to services; iii) malware distribution events; iv) non-standard bring-your-own-device (BYOD) device corruptions, and; v) duplicate Type Allocation Codes (TACs)[493] entered on networks targeted for specific mobile devices, to confuse, or disrupt, the mobility device's normal operations.

The approach DeviceAssure (Afilias Tech) software takes is to provide an embeddable app and web library, which examines non-(PII) personal identifier information, and assesses typed characters while texting, and compares them to 'good' configs stored in the product's DeviceAtlas. DeviceAssure software for mobile device transaction monitoring integrates into existing apps, software development kits (SDKs), and websites to build device verification *in* to your own personalized profile. DeviceAssure protects 1) brands 2) networks and 3) consumers.

---

[489] Source: "How Apple's Enterprise App Program became the new wild west of Mobile Apps," By Nick Statt [online – The Verge]. Dated February 20, 2019. See: https://www.theverge.com/2019/2/20/18232583/apple-ios-developer-enterprise-program-store-mobile-apps. See *also*: *Ibid*., [Foot Note # *499*].

[490] See: "Financial Institutions must address security concerns in mobile banking and payments," By Dan Butcher, Assoc. Editor, Mobile Commerce Daily [online - retaildive]. Dated: 2017. See: retaildive.com.

[491] Source: https://www.cybersecurityintelligence.com/deviceassure-5034.html.

[492] International Mobile Equipment Identity (IMEI) issues the 15-digit unique number for identifying a device on a mobile network**.** You can think of it as your phone's social security number.

[493] A Type Allocation Code (TAC) is made up by the first 8 digits of the so-called International Mobile Station Equipment Identity (IMEI) number, associated with mobile devices. GSM networks use the IMEI number to identify valid devices, and can stop a stolen phone from accessing the network. For example, if a mobile phone is stolen, the owner can have their network provider use the IMEI number to block-list the phone. This renders the phone useless on that network and sometimes other networks, even if the thief changes the phone's subscriber identity module (SIM).

The company claims their credence applies to the workload of government regulatory bodies, as well.

Now here is an example of something totally off the beaten path!

Open API GPT-3 is a text generating neural network, released in June 2020 after $14 million spent on testing. Its creator – the AI Research Agency Open AI – created a language based on 175 million parameters. Parameters are network calculations that apply particularized weights to different aspects of data. Since the language behind GPT-3 is capable of meta-learning, it performs tasks without training. Out in a request and GPT-3's text predictor provides an answer.[494]

Currently GPT-3 is available as an API in a private beta version. DevOps designer Jordan Singer built a Figma plugin[495] which can produce the app design. As the world's first collaborative interface design tool, the Figma API is based on the REST structure. The Figma API supports authentication via Access tokens and OAuth2. The Figma API can 'Request / Broker' via HTTP endpoints, with clear functions and appropriate response codes. Endpoints allow you to request Files, Images, File versions, Users, Comments, Team Projects and Project Files. With that impressive sales pitch, what's the 'con' to all of this?

.

GPT-3 lacks accuracy in adversarial natural language inference (NLI) tasks. This can cause embarrassing failure cases from simple prompts. What do we get with GPT-3 now? "We're closer to building big compressed knowledge bases than systems with reasoning ability.[496]" Then again, if you are one of Sam Altman, Marc Benioff, Elon Musk or Reid Hoffman, what's a few million here, a few million there, for yet another of your vanity projects?

Do these examples really fit into the exposition of *broken architectures*? Good question! Perplexing, all the same, when the real problem is, and remains, how to secure the data.

11.1.5 Injection (with untrusted communications / data / authorizations)

In injection attacks, untrusted data is supplied to a 'code' sample interpreter through a form submission document or data set, or any other input source to a web application. The input is

[494] Source: "Open AI GPT-3: how it works and why it matters," By Jordan Singer, [online – Byteant.com]. Dated: August 5, 2020.

[495] In Figma, plugins are written in JavaScript and their UI is created with HTML. A Figma plugin is built on top of the most popular open-source tools in the web development community, rather than being rolled out on the Figma developer community's own proprietary solutions. Some things that go along with this approach are: i) TypeScript - to make navigating the API easier and write robust plugins; ii) Webpack – to bundle large multi-file projects and import libraries, and; iii) React, Vue, etc. to create complex user interfaces. Figma is the only design tool of its type that performs in such multiple ways, and can 'shop' and use hardware running different operating systems. Source: https://www.figma.com/plugin-docs/prerequisites/.

[496] Source: Denny Britz [blogger on GPT-3 blog *feed-back* board]. Dated: August 3, 2020.

processed by the 'code' sample interpreter as part of a command or query, altering the execution of a program or application.[497]

Here is a specific example Shilpi (2019) cites: "Cross-site scripting (XSS) is a type of injection attack, allowing attackers to inject client-side script into web pages that are being viewed by other users. Cross-site scripting (XSS) is used by the attackers to breach access controls, such as 'Same-origin' policy. To prevent Cross-site scripting (XSS), take extreme precautions downloading *things* which need to be taken while rendering user input in the (web or application) browser.

To prevent injection, Shilpi (2019) recommends you limit the *length* and *type* of the text to be 'entered' into an input field. Also, this may ensure the escape, and declining actions, restricting to a few acceptable, i.e. trustworthy characters by entry fields, which may work in minimizing any attack vectors.

In the wider arena, database tools and resources (SQL, NoSQL) and tools or toolkit processes (OS, or LDAP) – all *employ* standardized languages used to access and manipulate databases, and to build customizable data views, for each user. Sure. It's one thing to inject poisoned data into – for example – an SQL database. But quite another circumstance altogether when a threat vector poisons a web application. Depending on your application logic and use of output encoding, you are inviting the possibility of unexpected behavior, leaking data, and even providing an attacker with a way of breaking the boundaries of input data into executable code.[498]

Google, Facebook, and countless other app makers all use the 'Apple Developer Enterprise Program' to distribute their iOS-based apps, after receiving an Apple certificate license. This program does not involve Apple in reviewing the software or checking which permissions it might be tapping into, meaning the potential is always there for 'violators' to occur.to test internal versions of iOS software, like Instagram and Google Maps, before those versions become official updates, a process many companies say is a necessary part of large-scale development to avoid bugs, security flaws, and to improve overall quality of the software.

In this same the *tech press* article, it is reported (this time by Reuters) that numerous companies operate illicit app stores that utilize the enterprise program to sidestep Apple's screening processes. Not only must the storefronts be side-loaded, but nearly every piece of software available in those storefronts must also be independently side-loaded, revealing confusing webs of what appear to be fake companies, with access to Apple's enterprise certificates. What is clear is that each one of these apps has independent permissions, and perhaps the independent ability to access unwanted parts of your phone; installing a version

[497] Source: "Secure by Design: A Web Development Essential," By Shilpi [online – opensenselabs.com]. Dated: September 3, 2019. See *also*: *Ibid*., [Foot Note # *476, 486*].
[498] Source: "The Basics of Web Application Security," By Cade Cairns and Daniel Somerfield [online – MartinFowler.com]. Dated: January 5, 2017. See *also*: *Ibid*., [Foot Note # *501*].

of *Pokémon New World* on your phone, may install an entirely new enterprise certificate, with permissions that are not easily decipherable. There's no telling what type of data these apps can access, or what any one developer's primary business model *is*.

For years, Apple's App Store has been viewed as one of the leakiest pipes in Apple's platform infrastructure.[499] Apple fought back. When Apple began wholesale revoking Facebook and Google's certificates in response to the virtual private network (VPN) apps postings, in what some view as a kind of warning shot, employees at those companies were unable to get work done, check what meals were being served in the cafeteria, or even figure out how to get home.

This tit-for-tat exercise is self-defeating. For Apple, the Apple App Store requirements to distribute everything from beta versions of public software to apps designed only for contract workers in the on-demand economy, may have once made perfect sense[500]. But for both Google and Facebook, to think they could get away with distributing VPN apps to research participants in ways that blatantly violated Apple's policies, what gives?

Let's turn this around, and go back to 'the data'. If we uncover malformed data treatments as a security concern, what are we to do? Cairns / Somerfield (2017) address this with input validation. Input validation suggests that if an expected set of data values falls outside of an expected set of 'sought after' values, assume your application will get unexpected – and therefore unwanted and unwarranted – results. Input treated in this way, such as database query, or data / database commands executed on then client as HTML, or JavaScript – treat with caution! A simple example is whitelisting. A user won't request transferring a negative sum or money, or request several thousand items being added to their shopping cart! Or, a contract form 'handling' the code – reflecting how you deal with a customer – if at any point this code is violated, rejects the result. Even if this rejection serves to override a customer-satisfaction "poll," or a customer feedback "score," just *let it go*. Otherwise, this "score" or "poll" result may host a cyber threat attack.

Rejecting inputs which have dangerous *potential* values embedded in them is called blacklisting. Maintaining blacklists is time consuming and costly. Also, even though your blacklists caught the attack by 'fixing' it, you just may have inadvertently reintroduced your vulnerability. Filtering something 'out' doesn't mean the attacker can't (or won't) filter it right back in again. Any code that handles input from an untrusted source can be validated in much the same way,

[499]Source: "How Apple's Enterprise App Program became the new wild west of Mobile Apps," By Nick Statt [online – The Verge]. Dated February 20, 2019. See *also*: *Ibid*., [Foot Note # *489*] '(Statt-2019) - Apple App Store a leaky proposition.'

[500] An Apple spokesperson – off-the-record–] has stated that "There is the possibility that several companies in China maintain robust enterprise program subscriptions for the sole purpose of selling access to independent app makers, that *they then use* to distribute software outside the App Store." [unattributed].

whether JSON, XML, or any other format (or even if it is a cookie, a header, or URL parameter string). If you can't control it, don't trust it![501]

There are so many tools and frameworks, and encoding contexts (e.g. HTML, XML, JavaScript, PDF, CSS, SQL, etc.) these days, that Cairns / Somerfield (2017) provide a shortened guide here. What to use, and what to avoid:
i) output encode all app data on output with an appropriate codec
ii) use your framework's output encoding capability, if available
iii) avoid nested rendering contexts as much as possible
iv) store your data in raw form and encode at rendering time
v) avoid unsafe framework and JavaScript calls that avoid encoding.

A final thought, on *use policy* to *authorize behaviour* is offered by Cairns / Somerfield (2017): "Use policy to authorize behavior" is Policy which determines whether an action can be taken, by that principal, against a resource. Or, with role-based access controls (RBAC), users are assigned roles and roles are assigned permissions. Food for thought.

Here's a few more examples, good and bad, of how 'broken access controls' through to 'XML external entity (failures)' through to 'sensitive data exposures' through to 'broken architectures' through to 'injection (with untrusted communications / data / authorizations) can all lead to disaster. This disaster is the waiting-in-stealth of elevated threat actors, organized crime syndicates, malfeasance cartels or even state-sponsored attack groups, with the latest and most sophisticated – maladroit – services and products.

Here are a few examples. The Company Checkpoint Security (2020) recently reported that attackers using public (web) pages are taking it a step further. The attack Search Security are referring to, commissioned a PDF file, hosted on Google Drive – Google Drive being a Microsoft SharePoint document that asked the users to login with their Office 365 credentials on the organization's emails – which would raise no suspicion in the user. The user would think that Google Cloud Storage has 'all our security covered'. The expert at Search Security weighing in on this situation, Loten Finkelstein, Manager of threat intelligence at Checkpoint – the Company reporting the breach – states: "The typical warning signs in a phishing attack include suspicious-looking domains or websites without a HTTPS certificate.[502]"

Well known public cloud services such as Google Cloud or Microsoft Azure host these pages, which attackers use to snare victims. Recently, Checkpoint's Finkelstein has observed that Google *Functions* – 'Functions' being the *code* in the *cloud* whereby Google Functions 'instances' were deemed unable to detect / see malicious domains – which served,

[501] Source: "The Basics of Web Application Security," By Cade Cairns and Daniel Somerfield [online – MartinFowler.com]. Dated: January 5, 2017. See also: *Ibid*., [Foot Note # *498*] '(Cairns/Somerfield-2017) identifying injection attacks and typologies'.
[502] Source: "Evasive phishing company hid inside Google Cloud Services," By Arielle Waldman [online – Search Security]. Dated: July 23, 2020.

unreservedly, in granting the attacker the 'edge'. The attacker bypassed many security protections, such as reputation checks for URL. The only way Google could have stopped (or even detected) this breach would have been to analyze the affected phishing page's source code, which is how Checkpoint's researchers discovered this particularly malicious and pernicious URL attack campaign.

And this isn't just about Microsoft OS, Linux is affected in many breach attacks, as well. Here is one example involving Linux OS. This next breach example involved malware which communicates freely with command and control (C2) servers through a firewall that should, under normal circumstances, prevent precisely this kind of communication from reaching this kind of communication from the *infected* server. Shevchenko / Easton (2020) call this the 'Cloud Snooper' malware attack or malware Trojan. It is a method of piggybacking C2 traffic on legitimate traffic, such that normal web traffic with the attached infected malware can bypass many if not most firewalls.[503]

Cloud Snooper [the Trojan] uses a *bespoke* Advanced Persistent Threat (APT) toolset, which may even be nation-state-sponsored. It compromised systems running both Linux and Windows EC2 *instances*, and the site where the attack occurred had been set up to only allow inbound HTTP or HTTPS traffic, and in the former case (on Linux OS) the Linux System was still listening for inbound connections on port 2080/TCP and port 2053/TCP.

We'll drop this back a notch (or forward with more depth, as you prefer!) for the completists! A toolkit was discovered that granted the malware operators the ability to remotely control the server through the AWS Security Groups (SGs).[504] This rootbit is not limited to just the Amazon Cloud: It also could be used to communicate with and remotely control, malware on any server behind any Boundary Firewalls, even on on-premises servers. This became especially troubling as other Linux 'hosts' connected with a similar C2 as the one found were also discovered to be compromised Linux hosts. The Windows EC2 backdoor is apparently based on source code of the infamous Ghost RAT malware. This infection involves a toolkit that inspects network traffic, and a backdoor that the attackers leverage to send commands to, and receive data from, the backdoor, *so engaged*.

Firewalls typically prevent machines behind the firewall from receiving traffic sent to arbitrary destination ports, but they don't pay attention to the source points, due to these ports being normally treated as ephemeral, i.e. not relevant to the server or the services it is hosting. Shevchenko / Easton (2020) conclude their analysis by stating that: "Cloud Snooper (their

[503] Source: "*Cloud Snooper* malware attack bypasses Firewall Security Measures," By Sergei Shevchenko and Timothy Easton [online – Sophos News]. Dated: March 24, 2020. See *also*: *Ibid*., [Foot Note # *504*, *505*]. Discussion: AWS- Security Groups (SGs) are a set of firewall rules that provide security at the protocol and port access level, mating inbound network traffic at the perimeter. *'Cloud Snooper'* malware remotely controls the Amazon Web Services (AWS) Security Groups (SGs). The attack is a multi-platform phenomena - bypassing Firewall Security Measures.

[504] Source: "*Cloud Snooper* malware attack bypasses Firewall Security Measures," By Sergei Shevchenko and Timothy Easton [online – Sophos News]. Dated: March 24, 2020. See *also*: *Ibid*., [Foot Note # *503, 505*].

colorful name for the offending malware Trojan) is extremely interesting as it demonstrates the true multi-platform nature of a modern attack. A well-financed, competent, determined attacker will unlikely ever be restricted by the boundaries imposed by different platforms.[505]"

This observation by Shevchenko / Easton (2020) on the depth of attacks involving multi-platform agency was echoed recently by Israel's Cyber Chief Yigal Unna, who recently commented that a cyber winter is coming. Unna (2020): "Rapid is not something that describes how fast and how crazy and how hectic things are moving in cyberspace and I think we will look back at May 2020 as the changing point in the history in cyber warfare."[506]

11-2 Apps - Dapps not secure (IoT/mobile) *and* 'What DLT Data Center?'

This final topic is, admittedly, getting-a-bit-*ahead*-of-the-game. The financial services industry is moving – massively – to mobile devices. Half the world's internet traffic is now moving through mobile phones. Since the *Covid-19 pandemic*, it would not be surprising if this number hasn't grown even more. What this means is that mobile-related security issues are a *be-all* and not just a *nice-to-do* bucket list item for the Information Technology (IT) / Information Management (IM) security establishment to address. So how are we doing in terms of mobile-related security? Lagging.

Researchers and developers have widely embraced decentralized apps (dapps) that run in a distributed fashion on your personal device, as opposed to in the cloud. Distributed apps (Dapps) need to attract enough people that are using browsers and tokens, to want to download a *specific* Dapp onto their mobile device. This would lead, fortuitously the DevOps professionals hope, to a critical mass of users propelling that "new dapp" to wide-spread adoption. But that success is proving harder and harder to come by. Followers of blockchain worry that – in the same way that the Internet promised a collaborative, decentralized and democratized place for doing business and sharing information – blockchain may itself eventually get hijacked, by large Third Party Players (TPPs) like Google, Facebook and Amazon, who dominate the internet landscape.[507] These players, or entities in their category, will force a similar level of subjugation over the economic interests contained in the distributed ledger / blockchain.

[505] Source: "*Cloud Snooper* malware attack bypasses Firewall Security Measures," By Sergei Shevchenko and Timothy Easton [online – Sophos News]. Dated: March 24, 2020. See *also*: *Ibid*., [Foot Note # *503, 504*].
[506] Source: "Israeli Cyber Chief Warns Cyber Winter is Coming after Israel thwarts Attackers on Water Grid," by the Times of Israel (reporter not attributed]. May 28, 2020. See: timesofisrael.com.
[507] Source: "Blockchain Watchers Say Decentralized Apps Are Around the Corner," By Rubaia Islam (online – Money in Crypto). Dated: 2018. See: https://moneyincrypto.com/2018/06/26/blockchain-watchers-say-decentralized-apps-are-around-the-corner/. See *also*: *Ibid*., [Foot Note # *168*].

Another facet of blockchain that makes it difficult to fathom is that it is run amok by developers.[508] Most of the blockchain industry consists of high-end developers. Right now, all the tech you hear concerning blockchain – be it smart contracts or private keys, or the latest crypto asset to spring on consumers, for example – are still super complicated. But when you talk about mass audiences, you need to make blockchain (and crypto resources in general) very simple.**[509]** Following up on that point, *keeping-things-simple*, let's drill down a bit into decentralized finance (DeFi).

We are nearing the end of this Submission. If pressed to state what is the most unsettling issue we have come across up until this point, it is the fact that distributed ledger technology (DLT) protagonists, driving this whole economic endeavor – and in this grouping we would include developers, technologists, and infrastructure specialists (crypto engineers?) – fail to be consistently accurate. Here's a case in point.

It's a tad hypothetical, but here goes. 'The blockchain crypto asset infrastructure owners and operators are pleased to announce' (made up example): "The whole approach with Peer-to-Peer (P2P) network '*interoperable* [sic!] communications' is that if your Dapp is financially sustainable, and you want to provide your users with *access* – without requiring them to maintain a *shard*[510] of the system, there will be an opportunity for Dapp maintainers to run nodes/servers." Notice the obvious point here. They whom *own the servers*, command all power relationships in the traditional Client-server network model. In the decentralized blockchain network environment, to the contrary, "each connected machine, and even every mobility device" – blockchain crypto asset infrastructure owners and operators will (and do) argue – "has the same rights as its peers on the blockchain network, and each can use that right

[508] These developers are oftentimes not very good at their jobs. One developer, responsible for launching two (2) large initial coin offering (ICO) projects on blockchain, made the rather incredulous admission: "Had I adopted Open Web Security Application Security Project (OWASP) frameworks early-on (which I missed), OWASP security frameworks would have successfully assessed the severity of vulnerabilities afflicting *both* ICO projects. For example - the need for: bug bounties; correcting bad lines of code, and; checking and verifying that communications / configurations were supporting smart contracts correctly, etc. This would have saved hours in pointless discussions about each issue, with Team members. Long emails going back and forth, and so on." Source: "What I Learned Working for 'Two (2) ICOs' as a Blockchain Engineer," By Merunas Grincalaitis [online – Medium publication – *with advertorial* for *self-published book*]. Dated: June 18, 2018. NB: Maybe take a pass on purchasing that book!

[509] Source: "OKEx's Lennix Lai: Passive Income in Crypto Is the New Way to Earn," By Lennix Lai, OKEx Director of Financial markets, [interviewed by Cointelegraph's Erhan Kahraman]. Dated: March 22, 2020. See: https://cointelegraph.com/news/okexs-lennix-lai-passive-income-in-crypto-is-the-new-way-to-earn. See *also*: *Ibid*., [Foot Note # *189*, *347*].

[510] Shard, in the sense of the term used *here*, refers to 'each app consisting of a series of shards, distributed across the user-base, sharing the server-load, comparable to torrent functionality.' See: https://www.reddit.com/r/Elastos/comments/8r9x5b/elastos_vs_holochain/. See as [*specific* comments by]: Blogger post – "level 7 - C00mbsie" - 2 points: 'Elastos vs. Holochain P2P network comparisons' and 'Elastos / Holochain (P2P) blockchain component [blog discussion].'

as they see fit.[511]" No less an authority than Vitalik Buterin (Ethereum) weighs in by stating: "if (you) *shard* at a node (A, B or C), instead of verifying all data sets or data 'shards' individually, the *whole point* is that these systems should not act like *self-interested* unitary monopolies. Hence, you can certainly make a case that the blockchain would be more secure, if they were more *discoordinated.*"

Buterin (2017) goes on to say – and this is a stretch of epic proportion – "Maybe we need to make the blockchain more *discoordinated*, for its own benefit.[512]"

Let's get back on track. The distributed ledger technology (DLT) and mobile technology *supply chain* consists of: a) the device b) the network and c) the data center.[513] The third leg of the mobile technology ecosystem, supply chain, or *whatever* we wish to call it – *is* the data center – and we have punted wide of the goal post, by several football fields, by being negligent in raising this idea sooner, as a key, foundational distributed ledger technology (DLT) and mobile technology supply chain infrastructure and enterprise architecture issue. Mea culpa.

To redress this, Advanced Systems Management Group (ASMG) are faced with the dubious distinction of trying to figure out what *is* the crypto data center. For a traditional financial institution (FI), the data center is their internal private data infrastructure (front-end and back-end) stacks, or may even be complimented by a cloud service provider (CSP) service offering, for certain elements they that outsource to that channel. For crypto players, it is *what*? And *where* do we find it? Is it the Virtual Asset Service Provider (VSAP)? Virtual Asset Service Provider (VSAPs) offer: i) exchange (services) between virtual asset stakes and fiat currencies; ii) exchange, transfer or safekeeping (services) for virtual assets, or, even; iii) participate as mini-financial service players related to the virtual asset accumulation effort, in an advisory or sales capacity.

---

[511] This is a very troubling issue. Blockchain adherents' present a very fractured view of the world. On the one hand, advocating 'democracy at all costs,' via their statements and actions, in support of 'the defense of the distributed ledger's peer-to-peer (P2P) networks'. This is at variance with their equally obvious actions, earning them untold economic reward, as they defend their decentralizing (in *name* but not in organizational / empirical fact) 'crypto asset infrastructures.' Blockchain adherents' own and operate the distributed ledger's services, and its infrastructure delivery capacity (and networks). Having it both ways – at the same time – are we?

[512] Source: "The Meaning of Decentralization," By Vitalik Butern, Ethereum. [online – Medium publication]. Dated: February 6, 2017. See: https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274. See *also*: *Ibid*., [Foot Note # *510*] '(Buterin – 2017) data 'shards' (not allowed) as *self-interested* unitary monopolies – *a.k.a.* (however) keep-them-as '*discoordinated* – for the benefit of the blockchain.' In this same article, Vitaly Buterin (Ethereum 2017) made an extemporaneous address as to the meaning of decentralization – stating three things: i) don't mitigate undesired coordination building protocols to be resisted; ii) allow enough room for protocols to evolve, but not enough to enable crypto chain adherents' attacks, and; iii) make distinctions between the 'beneficial' and the 'harmful.' Give it up, Vitaly!

[513] Source: "Mobile Banking Applications: Security Challenges for Banks," By Chris Thompson and Roshani Bhatt, Accenture New York [online]. Dated: 2016. See *also*: *Ibid*., [Foot Note # *515*]. See *also*: "Secure Mobile Development Best Practices," By NowSecure [online]. Dated: 2016. See: https://www.nowsecure.com/ebooks/secure-mobile-development-best-pratices/.

Luxembourg, in the European Union, put their foot down recently, and on March 25, 2020, *a.k.a.* amendments to the Principality's anti-money laundering (AML) regulations. These (regulatory) supervisory amendments established a direct, centralized electronic data research system. This anti-money laundering (AML) supervision addresses (crypto and regular banking) depository accounts, and bank accounts identified by an IBAN number[514] – as well as safe deposit boxes – held by credit institutions in Luxembourg. It also, very specifically defined custodian wallet service providers, defining 'custodian wallet service providers' as being "a service consisting of the safekeeping of private crypto graphic keys – on behalf of [crypto] clients – for (the) purposes of 'holding, safekeeping and transferring' virtual currencies.[515]"

A Virtual Asset Service Provider (VASP) must now register with the Luxembourg financial regulator – the Commission de Surveillance du Secteur Financier (CSSF). This legislation process documents 'in-depth' the following provisions or directives: i) a description of Virtual Asset Service Provider (VSAP's - and their service offerings); ii) provides a registration process for financial institutions (FIs) to actively describe their anti-money laundering (AML) and combatting financing of terrorism (CFT) *risks* that they (the FI) or their Registrants' – [crypto asset holder or; their custodian wallet service providers' or; their Virtual Asset Service Providers' (VASPs')] – verify and authenticate; iii) these registration procedures apply to all Financial Institutions (FIs) dealing with virtual assets, but most particularly address the Virtual Asset Service Provider (VASP) community, and the custodian wallet service providers alike.[516]

That, in an unsatisfactory (to this author) round-about manner, brings two new players to the table: Virtual Asset Service Providers (VASPs) and Custodian Service Providers. The first type of organization, Virtual Asset Service Providers (VASPs), conduct the exchange between virtual assets and fiat currencies, or between one (or more) virtual assets, perform d=safekeeping or administration of virtual assets, participate in an issuers' offer (of that virtual asset) or sell virtual assets.[517] The second organization mentioned, a digital asset custodian, or Custodian Service Provider, is any organization that has custody of digital assets. Again, the SEC offers a definition for the term "custody": (1) "Custody" means holding, directly or indirectly, client funds or securities, or having any authority to obtain possession of them.

[514] International bank transactions use either an IBAN, or the ISO 9362 Business Identifier Code (BIC) system, or SWIFT (codes), in conjunction with the Basic Bank Account Number (BBAN). The banks of most countries in Europe publish account numbers using both the IBAN format and their own nationally recognized identifiers, this being mandatory, within the European Economic Area (EEA).
[515] Source: "Mobile Banking Applications: Security Challenges for Banks," By Chris Thompson and Roshani Bhatt, Accenture New York [online]. Dated: 2016. See *also: Ibid*., [Foot Note # *513*] '(Thompson/Bhatt-2016) centralized depository accounts - *a.k.a*. VASPs, custodian wallet (crypto) service providers, etc. - regulations and tracking for AML - for *all* applicable credit institutions in Luxembourg.'
[516] Source: "New registration and governance requirements, for virtual asset service providers in Luxembourg," By Anne-Marie Nicolas, Loyens-Loeff Law Firm [online]. Dated: April 12, 2020. See: loyensloeff.com. Discussion: An exception is made for any entity already adequately covered by Luxembourg's Payment Services Law, but this grouping is very small, in relation to Virtual Asset Service Provider (VSAP) sector's activities overall.
[517] Source: https://aml-cft.net/library/virtual-asset-service-provider-vasp/.

That description of digital asset custodians is still not clear to us. Are they: i) crypto asset exchange providers – firms which exchange, arrange [or make] the arrangements (whether automated or otherwise) for the exchange of money (i.e. fiat currency) and crypto assets; or, of one crypto asset for another? Or might they be: ii) custodian wallet providers – firms that provide services to safeguard, or to safeguard and administer – crypto assets, or private crypto graphic keys – on behalf of [their] customers; or which hold, store and transfer crypto assets?[518]

What Advanced Systems Management Group (ASMG) fall back on, when we experience definitional inconsistencies – jurisdiction to jurisdiction – is to revert to the technology itself, and proceed from there. A noted financial analyst, Kentouris (2020) suggests: "A qualified custodian will receive deposits, and exercise genuine discretionary fiduciary powers, approximating those permitted by national banks. What will determine how a custodian service is selected may be: i) the technology platform they use ii) cybersecurity procedures implemented iii) asset segregation tasks performed iv) cold wallets or multi-signature authentication used v) cybersecurity insurance held, and vi) the global instant settlement network installed.[519]

That last point really caught our eye! Investigating this point further, Trepanier (2020) states: "Global instant settlement networks are now emerging that empower banks to settle with maximum transparency, speed and security, while making the transfer of digital assets between institutions far more cost-effective.[520]" Advanced Systems Management Group (ASMG) particularly found the observation that "many essential custody services applications are not latency-sensitive or super high-throughput and run on cloud services (but do have) proven security and robust data analysis, such as Snowflake Amazon Web Services (AWS).[521]

Advanced Systems Management Group (ASMG) jumped on this last point fast. Who is the high-latency, high-throughput provider? Found not one, but two!

Fireblocks are a Tel Aviv-New York City global instant settlement network, offering a multi-party computation (MPC) Hot Vault, a workflow authorization engine – which is SOC 2 Type II certified, and RegTech pen-tested by the NCC Group and ComSec – offering crypto settlement network services to: i) twenty-six (26) crypto exchanges ii) over-the-counter (OTC) clients iii)

[518] Source: https://talkingtech.cliffordchance.com/en/industries/fintech/-crypto-exchange-providers--and--custodian-wallet-providers--bec.html.
[519] Source: "National Banks as Digital Asset Custodians: Big Deal or Not?" By Chris Kentouris, Editor [online – FinOps report]. Dated: August 14, 2020. See: *Ibid*., [Foot Note # *84*] '{Kentouris-2020) Avanti Bank and Trust (Wyoming) – example of *hybrid* (crypto) custodian service; and crypto exchange service provider and depository (crypto) asset banking institution.'
[520] Source: "How US Banks Can Start Planning to Deliver Crypto Custody Services," By Thomas Trepanier, Banking Journal [online]. Dated: August 20, 2020. See: bankingjournal.aba.com. See *also*: Ibid., [Foot Note # *521*].
[521] Source: "How US Banks Can Start Planning to Deliver Crypto Custody Services," By Thomas Trepanier, Banking Journal [online]. Dated: August 20, 2020. See *also*: *Ibid*., [Foot Note # *520*] '(Trepanier-2020) custody applications not latency-sensitive or high-throughput.'

wallets and hot (crypto) wallets (clients) and iv) counterparties *e.g.* other custodian service provider clients.

Advanced Systems Management Group (ASMG) found Curv, another Tel Aviv-New York City Company, next. Curv calls their offering an institutional cloud-hosted blockchain-agnostic digital wallet service. Curv boasts scalable software, also multi-party computation (MPC) compliant, resolving interoperability issues between digital wallets. The Company's private cloud holds shares, so that the private key is never located on any device at any time.

When an organization wants to send funds, it sends the request to the Curv Tech Platform, that is validated and authenticated, triggering an MPC-event – via a computation protocol – which signs and completes the transaction. No private key is ever revealed, therefore there is no 'single-point-of failure.' Curv has unprecedented (up to $50 million underwritten by Munich RE) levels of liability insurance, covering all their services. Curv provides: i) [in-house] decentralized exchange (DEX) ii) ICO Investing iii) ICO Staking iv) Portfolio Tracking v) ICO Porting vi) NUKE (conversion – BTC to ETH – (back to) BTC etc. and, viii) Fiat Gateway Service. Are we starting to see something happening here? This is the beginning of a crypto dynasty, to rival a Facebook, Amazon or Google. These various innovation-driven, technologically-significant players are beginning to lay claim to the 'how' process determining digital crypto asset movements, storage, exfiltration and all manner of related exchange services.

Might we be moving towards a Distributed Ledger Technology (DLT) Data Center conglomerate-in-the-making, once all these pieces fall together, and merge into one organizational strata to control things? To Advanced Systems Management Group (ASMG) that answer is overly obvious!

We have sailed over crypto miners, and for good reason. Crypto mining is what Advanced Systems Management Group (ASMG) view as boiler-plate operations, a subset of cypto data center activities overall. In 2017, China declared crypto mining centers illegal, forcing all (mainland) Chinese crypto currency mining exchanges to close. In May 2018, the Province of Quebec (Canada) said 'not interested' (to crypto mining operations) being allowed to locate their operations in that Canadian Province. This same 'not interested' stance (to crypto mining operations) was issued from the State of Washington, on the US's west coast. The State of Washington, home to five hydro-electric dams, and the Province of Quebec, home to several of North America's largest hydro-electric dams, made clear they were uninterested in sponsoring crypto mining centers within their boundaries, and both did this the same year.[522] What could cause such reticence? Easy. These are not well-regulated, nor perceived to be 'ethically-acceptable' operations. Plus, crypto mining centers fail to take the security of their product stewardship at a significantly pronounced level to justify, and overcome, the business risk they attract from cyberattacks.

[522] Source: 'The Challenges of Site Selection for Crypto Currency Data Centers in North America," By Michael Rareshide, Site Selection Group [online]. Dated: June 8, 2018.

And that is Advanced Systems Management Group's (ASMG's) problem with trying to delineate a distributed ledger technology (DLT) Data Center for crypto asset service delivery. It absolutely is under construction, but we just don't have a clear idea as to what it will look like.

The traditional banking data center is very explicitly defined (unlike the case with *prospective* crypto distributed ledger technology/DLT data centers). A traditional *mainstream* financial data center is either resident within the organization's own walls, or is a hybrid configuration, with some services inside, and some hosted by a cloud service provider (CSP).

Accenture (2016) very specifically lists the attack service threats to a traditional banking *on-premise* or 'with a cloud-service provider (CSP) *add-on*' data center, by first delineating the data center's Web Server, as one attack target of note. The Web Server – a venerable cornerstone asset of an organization's data centre – has vulnerabilities to attack which include: i) platform (vulnerability) issues; ii) server misconfiguration issues iii) Cross-site scripting (XSS) weaknesses iv) Cross-site request forgery (XSRF) lapses iv) weak input validation efforts and; v) brute force attack susceptibilities. Accenture (2016) *next* very thoroughly lists the attack service threats to a traditional banking *on-premise* or 'with a cloud-service provider (CSP) *add-on*' data center with four (4) more critical weaknesses, or vulnerable areas, which an organization struggles to protect. They include issues on the organization's data center Database side (a.k.a. databases held by the data centre) which are: i) SQL injection ii) Privilege escalation iii) data dumping and iv) OS command execution.

These data center vulnerabilities – grouped into two sets of issues, and assigned as Web Server vulnerability prone issues, and/or Database-side vulnerability issues, have numerous, well-tested solutions to address and mitigate their failings and shortcomings. These failures and shortcomings include seeking out (and applying) defensive measures which will mitigate against one specific, troubling threat vector attack: data exfiltration or *holding data for ransom*. Many vendors and security providers have adapted their product suites and consulting services to 'fix' (and curb the negative impacts) of these threats / vulnerabilities. That's the story for the traditional, *mainstream* financial data center segment.

The same situation is simply not the case for the newer decentralized, blockchain organizational data center model. As elusive, and hard-to-define as the newer decentralized, blockchain organizational data center model might be, it still exists today, or is starting to take shape.

A distributed ledger technology (DLT) Data Center for crypto asset service delivery will serve to provide crypto asset exchange services across the sector's installed base, however in getting there, Advanced Systems Management Group (ASMG) hold no grounds for optimism, that the reparations or mitigations to address and defeat security lapses, or data center vector attacks, have been 'designed in' to the moment. Specifically, the crypto asset exchange services – and

we have identified several micro niche service providers in the crypto space so far,[523] plus, the entity which Advanced Systems Management Group (ASMG) predicts will grow out of this listing of entities, and will coalesce into one, or at most two or three, oligopolistic distributed ledger technology (DLT) crypto data centers, face an insurmountable problem.

At some point in time, data needs to be protected over the full course of its lifecycle. And protected conclusively. If not, a poor situation, which is getting worse-for-wear, day-by-day, will continue to plague our economy and society. And here is one more pronounced event, which is extremely troubling, the repeated occurrence of cryptojacking.

Cryptojacking (Arsene, 2019) has so far been reported as: "Flying under the radar. A mining installation for crypto has rigged GPU farms, arrayed to adopt a brute-force type of structure / infrastructure. New demands for graphic cards, increased alongside the complexity of generating new crypto currency units, swamp the Virtual Asset Service Provider's (VSAP's) / crypto asset exchange services operational functioning, and subject them to attacks they are ill-prepared to defend against. Threat actors have focused on browser-based crypto currency mining scripts, such as CoinHive, to inject these 'infected' script processing information-targeting *malware components* 'straight-in and unopposed' into the Virtual Asset Service Provider's (VASP's) / crypto asset exchange services operations. These operations are now severely compromised, at the web site entry point.[524]"

And this is only the first volley of the attack! Next, cyberthreat actors continue their attacks by – i.e. removing and repurposing – the usable computing power of the unsuspecting crypto mining site's installation (and/or the Virtual Asset Service Provider's (VASP's) / crypto asset exchange services operational infrastructure. Then, they move on to manipulate and co-manage the full suite of service offerings they uncover, and these threat actors can now perform their own mining activities, with the power they have leached away, from the unsuspecting host entity. Cyberthreat actors now possess – and know full well they possess – their data center target(s) fully accessible operational workloads, since these workloads always operate at a *virtual* or 'always-on' capacity, rarely pausing or rebooting. Since the target is always in the 'uptime' mode, this – effectively – allows threat actors to go about their nefarious activities undetected.

Here's what organizations need to do to defend themselves:

[523] The micro niche - crypto asset and crypto exchange - service providers / players we are referring to are: Virtual Asset Service Provider (VSAP); Custodian Service Provider; Crypto Asset Exchange; Decentralized (Crypto) Asset Exchange (DEX); Global Instant Settlement Network, and; Cloud-hosted Crypto Asset - Crypto Wallet Service Provider. For starters – those are just the crypto service providers uncovered in this section of the Report.
[524] Source: "Double Jeopardy: Data Center Security and the Threat of Crypto Currency Mining," By Liviu Arsene [online – Bitdefender]. Dated January 24, 2019. See *also*: I*bid*., [Foot Note # *525*]

1) Deploy security on workloads, analyze attacks at the hypervisor level, and even run cloud baselining to spot anomalies;
2) Implement next-generation, layered security defense advances;
3) Adopt memory introspection technology *a.k.a.* for software-defined data centre installations;
4) Monitor all scripting for defects: look for PowerShell, VisualBasic, WMI threads or dose traces that are embedded in email attachments (or inside web sites, however they got there);
5) Monitor network communications, with command and control (C&C) servers.

Arsene (2019) concludes by stating: "Whether the crypto mining data centers are implemented as 'virtualization' facilities, as software-defined infrastructures' organizationally, or are hyper-converged facilities – all crypto data centers need to know about these threat solutions, and must act proactively.[525]"

This brings up the second point we raised, when mentioning that the mobile technology chain consists of: a) the device b) the network and c) the data center. The *network* is highly regulated, has very intensive technological advances occurring fairly routinely, benefiting all stations in the traditional financial institutions' (FIs') networking infrastructure. FinTechs (and other) financial sector stakeholders, report the same positive results, in terms of protecting their critical networking infrastructures from cyberattack, as well.

The mobility network extends quite comprehensively into the communications and networking firmament of traditional banking. The Internet of Things (IoT) is, however, causing the ingestion of data from IoT devices – including a significant number of smart phones and tablets etc. – which has seen a rapid spread across all mainstream financial institution verticals. This massive data expansion has caused a planned and deliberate uptake of Message Queuing Telemetry Transport (MQTT) advances. MQTT is a lightweight, publish-subscribe network protocol that transports messages between devices. The protocol usually runs over TCP/IP; however, any network protocol that provides ordered, lossless, bi-directional connections can support MQTT. It is designed for connections with remote locations where a "small code footprint" is required or the network bandwidth is limited.

The Message Queuing Telemetry Transport (MQTT) protocol defines two types of entities in the network: a message broker and numerous clients. The broker is a server that receives all messages from the clients and then routes those messages to relevant destination clients. A client is anything that can interact with the broker to send and receive messages. A client could be an IoT sensor in the field, a smart phone, or an application in a data center that processes IoT data.[526] Since Message Queuing Telemetry Transport (MQTT) messages are

[525] Source: "Double Jeopardy: Data Center Security and the Threat of Crypto Currency Mining," By Liviu Arsene [online – Bitdefender]. Dated January 24, 2019. See *also*: I*bid*., [Foot Note # *524*] '(Arsene-2019) hyper-converged or virtualization organizational models for data mining operations – susceptibility to cyberthreats'. See *also*: I*bid*., [Foot Note # *524*].
[526] Source: "Getting to know MQTT," By Michael Yuan [online – IBM Developer]. Dated: January 7, 2020. See: *Ibid*., [Foot Note # *527*].

organized by topics, the application developer has the flexibility to specify that certain clients can only interact with certain messages.

And if your question is: 'How do I secure the communications?' The client-to-broker connection can be an encrypted transport layer security (TLS) connection to protect the data in transit. In addition, since the Message Queuing Telemetry Transport (MQTT) protocol imposes no constraints on the payload data format, the system could have an agreed upon encryption method and key update mechanism. After that, all content in the payload could be encrypted binary data of the actual JSON or XML messages.[527]

Many would lead us to believe we need – more than anything else – a user-owned, decentralized alternative, to store and allocate our resources, by giving the end user a way to generate a self-sovereign identity, or at least one means to store and allocate our resources, so they may be used across multiple applications. This may endorse using, and leveraging, an encryption service to secure the user's data by default, via that application. This would – a.k.a. as the *new Internet* some have hoped for – transform the Internet as we know it. Until then, we have what we have.

In a peer-to-peer (P2P) decentralized networking connotation, files are often transferred between two non-trusting peers. This presents an opportunity for hackers to spread malware, as there is no central monitoring authority. This lack of oversight is what allows the proliferation of Dark Web or black-market practitioners full sway over the blockchain, to pursue their nefarious and illegal activities with impunity.

This issue – a central thesis of Advanced Systems Management Group's (ASMG's) position in this Submission to the OCC – has a familiar ring to it. Our odyssey as a Company, has been to provide a catalyst for provisioning and addressing the need for new intelligence – an information genesis – to alert decision-makers to the hindsight, insight and foresight of the data and information resources they require to make informed decisions.[528]

ASMG believe protection needs to be applied, either as security attribution attached to the information objects in the files and data sets which users depend upon, and / or there needs to be a protective layer to apply such attribution, and afford the protection required when the information is accessed. At the outset, this invariably means that the solution must be applied with knowledge of the content and context of the information asset itself.

The standards setting exercise which led to the Object Management Group's (OMG's) July 2017

[527] Source: "Getting to know MQTT," By Michael Yuan [online – IBM Developer]. Dated: January 7, 2020.
See: *Ibid*., [Foot Note # *526*] '[IBM-2020] MQTT protocol's encryption method and key update mechanism.'
[528] ASMG has contributed for a 20+ year period to solidifying the technical architecture *underpinnings* required to accomplish information *assurance* / information *interoperability* and information *exchange* in this standards-body approved manner.

ratification of the Information Exchange Framework (IEF)[529] has been predicated on that approach, i.e. security attribution attached to information objects, allowing tailoring of the data content / information message in the actual information exchange itself. This is based on the same rules that would be applied by a knowledge worker if he were asked to classify the data within the context of its intended use.

Key to this approach is the separation of the application programming (product) interfaces (API) software and the Policies (rulesets) used by the API, thereby allowing Cloud services to implement the Infrastructure Services, but retaining control of the Security Policies by the Bank and / or government entity, its Business/Policy analysts or government sector Information Technology / Information Management (IT/IM) staffers.

This is a fundamentally different security paradigm than what is recommended by the *status quo*. The current reality is that businesses (and government) secure their networks, or their applications, but not their data *per se*. A grass roots movement called the "data-centric manifesto" has – as of Friday June 19, 2020 – produced 837 signatories subscribing to the concept that data needs to be protected and secured.[530]

Networks provide a road of travel, but do not provide sign posts along the way pointing out exactly where a data asset 'sits' at any point in time. The Advanced Systems Management Group's (ASMG's) data-centric security (DCS) solution formally maps and proscribes the provenance of data.

ASMG's DCS solution has:
-supported enterprise architecture which retains institutional memory
-separates rules about data from data in the system itself, and;
-partners / builds the community-of-interest (C-o-I) wishing to share information [agreements]

[529] The Object Management Group® (OMG®) is an international, open membership, not-for-profit *technology standards* consortium, founded in 1989. OMG standards are driven by vendors, end-users, academic institutions and government agencies. OMG Task Forces develop enterprise integration standards for a wide range of technologies and an even wider range of industries.
[530] Source: http://www.datacentricmanifesto.org/signatories/. Discussion: Michael Abramson, ASMG - signatory # 763 of 837 – and ASMG colleagues, have made a career of seeking out a Data- Centric Security (DCS) Paradigm *shift*, where security enforced data policy that is independent of the infrastructure and application, are used to share and process data. This has resulted in the publication of the Information Exchange Framework (IEF) Reference Architecture (RA) at the Object Management Group (OMG). The IEF RA is a policy-driven, data-centric security (DCS) solution to information sharing and safeguarding, and an open standard!" See *also*: *Ibid*., [Foot Note # *28*].

via an architecture-driven, platform-based sharing of reusable patterns in UML.[531]

In the pre-2013 time-frame, data subject-matter-experts realized that to properly secure the data lake, data assembly functions governing 'secure data stores' required their own specialized vocabulary. This vocabulary, based on Model Driven Architecture (MDA) design principles, possessed the inherent strength to support the serialization of packaging and processing (data) models. These Model Driven Architecture (MDA) –derived constructs are termed the Information Exchange Packaging Policy Vocabulary (IEPPV).[532]

To sum this up, the standardized Information Exchange Framework (IEF) Reference Architecture (RA)[533] on which ASMG's DCS solution is anchored, provides users (/owners) of data with a secure, safeguarded methodology to perform analytic tasks,[534] via open application programming (product) interfaces (APIs). Data is created by applications (thick or thin, rich or basic), either using the application itself, or by using an agent (client-side), that profiles the data

[531] *Responsible Information Sharing* – what these three points are describing – seeks to introduce a systematic process for translating information sharing and safeguarding via policy instruments (e.g. legislation, regulation, policy and service level agreements) into a machine consumable form, that can be automated in the operational (/runtime) environment. This specification (IEPPV) offers one option to model users, a model -based transformation using the UML Profile (See: IEPPV OMG Document Number: MARS/2013-12-05; Annex C) [which] modeled user policy in a manner that aligns the policy to the specification data environment. The IEPPV UML profile is used to define permissible patterns for assembling data and information elements into releasable datasets that conform to the originating policy. These policy models can then be transformed into a serialized form that is machine consumable and automated by platform specific implementations of policy decision and enforcement points linked to user data stores (e.g. RDBMS) or other data repositories (data warehouse, data lake etc.) or in the Cloud.

[532] Model Driven Architecture (MDA) provides the transformational ability to serialize [data] models as interface code or policy / rules languages, that can be executed by multiple services (i.e. decision and enforcement points) or platforms. Source: Information Exchange Framework (IEF) – Information Exchange Policy Packaging Vocabulary (IEPPV), See: MARS/2013/12-05-IEPPV 6th Rev. Submission, OMG Document Number: MARS/2013-12-05; Page 6. See *also*: *Ibid*., [Foot Note # *279*, *283*].

[533] The Information Exchange Framework (IEF) Reference Architecture (RA) codifies the commonly understood vocabularies underpinning the ASMG-led data-centric security (DCS) solution, as ratified by Object Management Group (OMG – see omg.org) – an international standards-setting organization. The Information Exchange Framework (IEF) Reference Architecture (RA) provides a full unmasking of structured policy-based information exchange(s) – highlighting its importance to Machine Learning models and AI – constituting a fully implementable, policy-driven, data-centric solution to 'information sharing and information safeguarding,' and an open standard.

[534] Next step forward? Create a data-centric security (DCS) environment, package *up* the DCS as a virtual machine (VM), put in SELinux (or suitable OS), close doors to reduce vectors of attack, and now you have a solution to deploy in the Cloud. This achieves defense-in-depth data protection, is fully auditable, employs the latest in Identity Management advances, and even *transitions* structured Information Elements (e.g., NIEM, EDXL, and HL7 or financial industry ontologies) from data stores, and assigns information exchange services, in accordance with local information sharing and safeguarding (ISS) policies conforming to the Information Exchange Framework's [Policy- based] Packaging Policy Vocabulary (IEPPV). Working as an integral part in all of this, the Policy-based Packaging and Processing Services (PPSs) provide the ability to selectively package (aggregate, transform, mark, filter, structure and format) Information Elements for publication to authorized recipients. The Policy-based Packaging and Processing Service (PPS) is the only tagging and labelling service (TLS) available today to achieve this, with (as we mentioned) a full audit trail, and may be conducted at machine speeds.

prior to storage or transmission. The extent of that implementation, and the products used to implement it, we are absolving from an IT governance issue, into an implementation issue. This Report is intended to show that the means to implement this at the Enterprise level can be achieved based on existing and evolving Open Standards.

The range of choice is broad, offering widespread access – including the entire world population on one far end of the spectrum – and at the other end, all the problems, trials and tribulations which are growing by the day – as the policy ramifications of not acting, to secure our data, inflicts the untold damage on the unsuspecting population, as they click on their cellular device, surf the web, or engage with IoT devices across the globe, at this other 'unsecure' end of the spectrum.

The OCC should take heart. There is a secure solution in the offing. This is the *bona fide* message which Advanced Systems Management Group (ASMG) has been delivering throughout this Submission. We can demonstrate *now* the data-centric security (DCS) solution to fix many of the security failings we all wish to see an end to.

Advanced Systems Management Group (ASMG), in the final section of our Submission to the OCC, will reproduce an accurate representation of the data-centric security (DCS) solution and data-centric-security (DCS) transformational paradigm. This is reproduced as it first appeared in a document submitted to the Big Five (5) Canadian Banks. Should any of the information contained in the next section of this Submission prove to be repetitive or redundant, and bears more than a passing resemblance to any ideas already expressed, our apologies in advance.

Appendix A

The Solution -

Data-Centric Security (DCS) – a.k.a. – ASMG and the IEF

The solution Advanced Systems Management Group (ASMG) envision for banking, and the government sector clientele, starts from a very basic premise. If the enterprise adopts a policy that all data holdings will be placed behind a layer of protection, then the IT approach can be globally prescribed as one of inserting a protective data interface layer everywhere data is accessed, or at least everywhere there is an Open application programming (product) interface (API) requirement. We could do this as the data is created by applications (thick or thin, rich or basic), either using the application itself, or by using an agent (client-side), that profiles the data prior to storage or transmission. The extent of that implementation, and the products used to implement it, we are absolving from an IT governance issue, into an implementation issue. This Report is intended to show that the means to implement this at the Enterprise level can be achieved based on existing and evolving Open Standards.

Protection needs to be applied, either as security attribution attached to the information objects in the files and data sets which users depend upon, and / or there needs to be a protective layer to apply such attribution, and afford the protection required when the information is accessed. At the outset, this invariably means that the solution must be applied with knowledge of the content and context of the information asset itself.

The Information Exchange Framework (IEF) Use-Case

The standards setting exercise which led to the Object Management Group's (OMG's) July 2017 ratification of the Information Exchange Framework (IEF)[1] has been predicated on that approach, i.e. security attribution attached to information objects, allowing tailoring of the data content / information message in the actual information exchange itself. This is based on the same rules that would be applied by a knowledge worker if he were asked to classify the data within the context of its intended use.

Key to this approach is the separation of the API software and the Policies (rulesets) used by the

[1] The Object Management Group® (OMG®) is an international, open membership, not-for-profit *technology standards* consortium, founded in 1989. OMG standards are driven by vendors, end-users, academic institutions and government agencies. OMG Task Forces develop enterprise integration standards for a wide range of technologies and an even wider range of industries.

API, thereby allowing Cloud services to implement the Infrastructure Services, but retaining control of the Security Policies by the Bank and/ or government entity, its Business/Policy analysts or government sector IT/IM staffers.

Advanced Systems Management Group (ASMG)[2] has contributed for a 20+ year period to solidifying the technical architecture *underpinnings* required to accomplish *information assurance* / *information interoperability* and *information exchange* in this standards-body approved manner.[3]

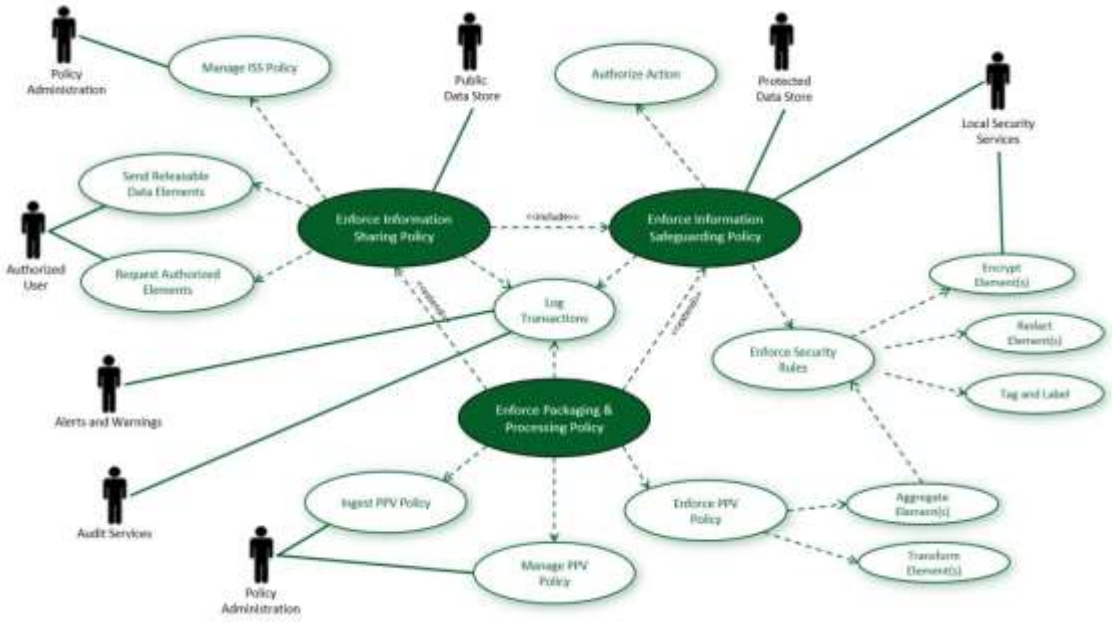

Figure 1: The Information Exchange Framework (IEF) Use-Case

The Information Sharing and Safeguarding (ISS) Solution – data-centric security (DCS) solution *a.k.a.* the two descriptions may be used interchangeably – is a comprehensive term to describe the application of the Information Exchange Framework (IEF) Reference Architecture (RA) to address these requirements – adopting a unified security policy, and data-centric security profile enterprise-wide. The data-centric security (DCS) Solution also incorporates: a) the provision of protective security layers (called defense-in-depth), and; b) encryption, key management, tagging and logging services (TLS) and, trusted audit services; as part of its overall

[2] ASMG-Ltd is a Canadian technology company based in Ottawa, Canada**.** The company delivers policy based data-centric security (DCS) for information sharing and safeguarding solutions. ASMG software can be integrated into client environments, compliant to the OMG Information Exchange Framework (IEF). We provide policy based software services for the challenges of information access and protection (security, confidentiality and privacy). The software can be integrated into existing environments as a standards compliant data access service, gateway, or API. We support secure structured data and other files, videos, and sensor data through commercially available networks including web, VPN or other network interfaces. Encryption and attribution tagging is supported based on information sensitivity analysis based on policies defined by the organization.

[3] Source: "Information Exchange Framework (IEF) Final Revised Submission (FRS)," Version: 1.0 [online]. Dated: October 2019. See: https://www.omg.org/spec/IEF-RA/.

reference architecture and implementation solution. ASMG has evolved this concept and can demonstrate an implementation of the structured data information exchange Packaging and Processing Service (PPS), which has been documented as a draft open specification in the IEF Packaging Service.[4]

As we move forwards in the digital era, cloud computing (and cloud data storage and cloud data management) will increasingly need to accommodate the *need-to-know* requirement to track down the origination of *all* data for security confirmation purposes. The owners of the data, or the third parties entrusted to handle data on a Clients' bequest and behalf, may increasingly be asked to adapt to more stringent privacy and security regulations [5]and this will directly affect the requirement for added vigor in protecting an enterprise's information assets.

The goal of the Information Sharing and Safeguarding (ISS) Solution, as delivered by structured data information exchange Packaging and Processing Services (PPS), is to provide information protection services to unmodified client applications and back-end data services. This is intended to occur with minimum impact on existing operations. Current operations will run as they are designed to do. The added value is that defense-in-depth security will be achieved across the organization.

[4] Source: "Information Exchange Framework Information Exchange Packaging and Processing Service (IEPPS)," Version: 2017-12-12, [online]. Dated December 17, 2012. See: https://www.omg.org/cgi-bin/doc.cgi?mars/2017-12-12

[5] Source: "Top 10 operational impacts of the GDPR: Part 1 – data security and breach notification," by Rita Heimes, Critical Infrastructure Protection Program -CIPP / US, dated Jan. 6, 2016, Page 2. Discussion:
One example of more stringent data regulations is the General Data Protection Regulation (GDPR) of the European Commission. GDPR specifies suggestions for what kinds of security actions might be considered "appropriate to the risk," including: i) The pseudonymization and encryption of personal data; ii) The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems / services; iii) The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, and; iv) A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the [data] handling/processing/reporting. NB: The EU' s objective is to embed cybersecurity in the future EU data policy initiatives from the start. This is particularly the case for new technologies and emerging sectors, such as connected vehicles, smart grids, the Internet of Things (IoT) and Open banking, the latter via the adoption of the Payment Services Directive 2 (PSD2).

All forms of data and information exchange - be they: File share supported by a file server;[6] Email (with Web objects) supported by an e-mail server; Instant Messaging / IM or 'chat rooms,' and – in the special case accorded to Open banking – Secure (e.g. Structured) Messaging, are covered by ASMG's Information Sharing and Safeguarding (ISS) methodology.

What the Policy Packaging Services (PPS) methodology / component of the Information Sharing and Safeguarding (ISS) Solution delivers, specifically, is a single, holistic and unified security orientation to handle *all* data, via modular design techniques and with layered security defenses. This holistic security solution utilizes mandate-level, mission-level and departmental-level policies[7] treating all information assets as critically important.

In the pre-2013 time-frame, data subject-matter-experts realized that to properly secure the data lake, data assembly functions governing 'secure data stores' required their own specialized vocabulary. This vocabulary, based on Model Driven Architecture (MDA) design principles, possessed the inherent strength to support the serialization of packaging and processing (data) models. These Model Driven Architecture (MDA)[8] constructs are termed the Information Exchange Packaging Policy Vocabulary (IEPPV).

---

[6] The protected file-share is a designated location on the user's own infrastructure. A file share authorization event consists of a file share sequence in which a representative interaction between Information Exchange Framework (IEF) components conducting file access actions (e.g., Create, Copy, Cut, Delete, Move, Open, Paste and Save) occurs. There are a number (i.e. a multiple) group of paths through which authorizations occur, depending on: i) the number of files being requested simultaneously ii) the source and target for the requested InformationElements (i.e. "file") iii) the capabilities of each of the selected IEF components iv) the availability and fidelity of the user's (e.g., network, devices, systems, services and users) authorizations, privileges and attributes v) the complexity and fidelity of the user's own policies. Many of the preceding items will be addressed in the individual component specification section(s). The preceding list of items outlines the process for accessing a single file located in the IEF protected file share. If the file resides in a protected IEF file share location: a) The file is or will be encrypted using a symmetric key b) The file is or will be appropriately marked c) The file will be maintained in a Secure Access Container (SAC). Source: "Information Exchange Framework (IEF) Final Revised Submission (FRS)," Version: 1.0 [online]. Dated: October 2019. See: OMG Document Number: MARS/2017- 02-21; Page 282-283. See: http://www.omg.org/spec/IEFRA/.

[7] A policy is a definitive course or method of action selected from among alternatives and follows given conditions to guide and determine present and future decisions. Source: "Information Exchange Framework (IEF) Final Revised Submission (FRS)," Version: 1.0 [online]. Dated: October 2019. See *also*: OMG Document Number: MARS/2017-02-21; Page 315). Policy Driven refers to a process involving formal documents describing a plan of action (Policy_Instrument) translated into machine readable rules (/instructions) and enforced by software services and systems. This process results in full traceability from Policy_Instrument to instrumentation (policy decisions and enforcement points). See *also*: *Ibid.*, [previous Foot Note # 3] Page 316. Note to Reader: We will drop the IEPPV insignia, when identifying ISS components (/units) – indicating the IEF RA's "elements" throughout the remainder of this Appendix A. This naming convention will imply [i.e. reference to] simply 'the IEPPV' *in all cases*.

[8] Model Driven Architecture (MDA) provides the transformational ability to serialize [data] models as interface code or policy / rules languages, that can be executed by multiple services (i.e. decision and enforcement points) or platforms. Source: "Information Exchange Framework (IEF) – Information Exchange Policy Packaging Vocabulary (IEPPV)," 2017-12-12, [online]. Dated December 17, 2012. See *also*: MARS/2013/12-05-IEPPV 6th Revised Submission, OMG Document Number: MARS/2013-12-05; Page 6.

Operational Analysis for Semantic Interoperability

Here is the graphical illustration of our grand view - Figure 2: IEPPV in the Information Sharing and Safeguarding Methodology Policy Life-Cycle.*

**Note*: Governance is informed by the information derived from Architecture / Operational Analysis. These *information flows* illustrated, serve as connectors 1 & 2 (enclosed in the green ovals) shown in the previous diagram (Figure 1).

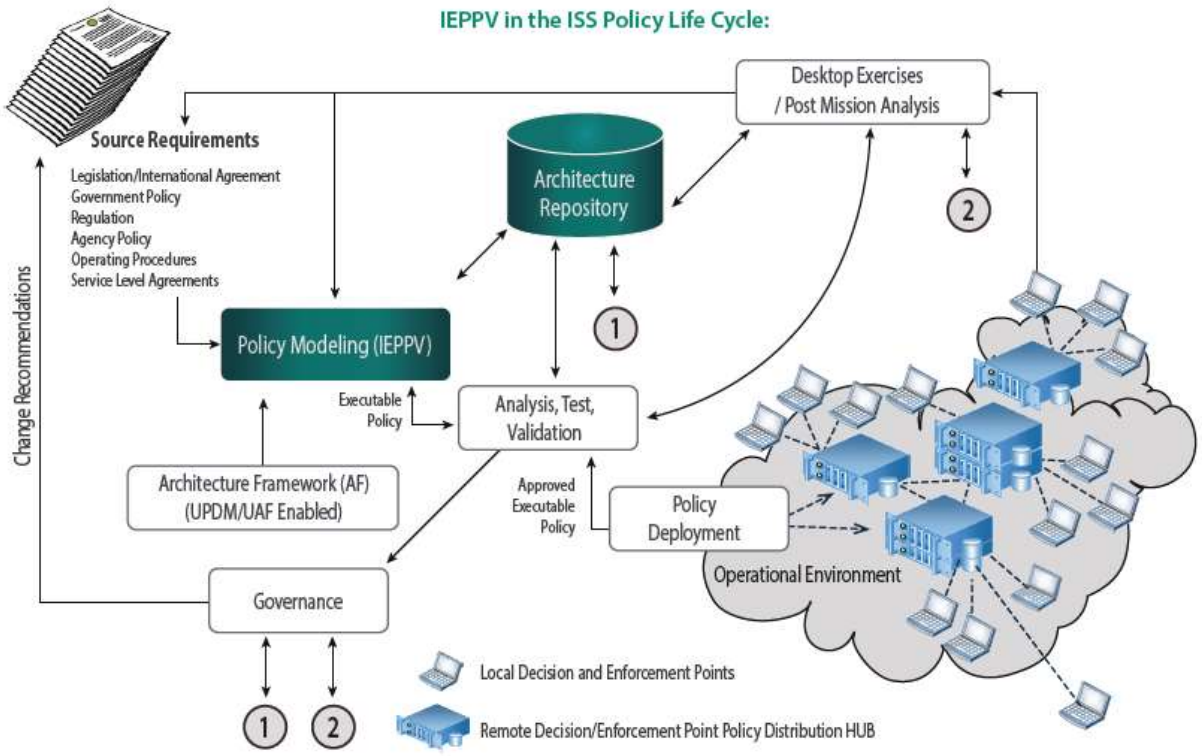

Figure 2: Information Sharing Policy Life-Cycle
Source: ASMG

Conceptually, what the Information Sharing Policy Life-Cycle *figure* illustrates is semantic interoperability. Semantic interoperability allows information exchange to occur, in such a manner that the meaning and intent [of that information], and its usage, is always understood. Semantic interoperability, in the context in which we are examining it, is the requirement to enable information integration, machine analytics, inferencing, knowledge discovery, and data federation to *all* be comprehensively, and resolutely – if not routinely – addressed. Semantic interoperability[9] is not only concerned with the packaging of data (structure and syntax) but also addresses the simultaneous provision of intent and meaning (semantics) attached to data.

[9] This is not to be confused with Technical Interoperability, a term which defines an agreed communication protocol which exists between established communications infrastructure, allowing systems to exchange bits and bytes, and which dictates how the underlying network and protocols are unambiguously defined.

At the heart of the Information Exchange Framework (IEF) Use Case (Figure 1) is the Information Exchange Policy-based Packaging Vocabulary (IEPPV). The IEPPV is shown in the green square at centre left in Figure 2. The objective of the IEPPV specification is to provide vocabulary that will be tool agnostic, and provide the expression of Rules governing:

1. Information Packaging (aggregating, transforming, tagging / marking and redacting / filtering) data and information, and;

2. Information Processing (parsing, validation, transformation and marshalling) data and information *guided* to - and from - data stores (e.g. RDBMS).

Traditional data and information exchange practices have allowed data 'extract-transfer (-transport) -and-load' (ETL) tools to function as a non-intuitive, non-intelligent manifestation. Information has, accordingly, been left siloed in stove pipes, with their brutal inefficiency, integrity, and inaccessibility virtues left unattended. In the timeframe up until *now*, legacy vendor architecture and infrastructure interest(s) have remained inviolable – and resistant to all possible reform efforts – and accordingly, the situation has never changed, nor been comprehensively addressed. Until *now*. Separating information according to their data streams' inherent sensitivity attributes (e.g. data's classification, confidentiality and privacy, and legal significance and caveat) debunks, once and for all, the long-held view that proprietary channels are the only way to operate the global, holistic IT / IM environment.

Today, stove-pipes with an ever-increasing number of partitioned systems, failing to communicate information with one another, are the clear-cut legacy architecture holdover 'failing' from the past. In this environment, subsets of concepts contained in information vocabularies are managed by ETL (Extract, Transfer and Load) tools, further depriving and / or distancing the end-user from accessing the data and information they require. ETL tools[10] fail to do what a cross-domain, or cross-silo information sharing capability asks to be done. Information sharing and safeguarding in a secure, data-centric environment, requests the packaging (assembly and formatting) of information elements, and the inverse processing of received messages and data sets, to be the base mandatory minimum requirement always.[11]

[10] Extract, Transform and Load (ETL) tools can be very applicable in micro-assembly applications. One example of this is the US Navy's use of an ETL with a filtered semantic (Navy_SA) which executes the subtended rules for the assembly (aggregation, transformation, tagging / labeling and filtering of data and information elements used to describe a Navy Unit Status [(NavyUnit_SA)]. Source: Ibid., [previous Foot Note] Page E-4 to E-7. Generalizations will not suffice in this Report. The Navy Unit Status (NavyUnit_SA) example uses Distributed Data Services (DDS), Web service and User Application definitions enable (the user) to accomplish the rapid generation of 'information exchange patterns for new operations.' Source: "Information Exchange Framework (IEF) – Information Exchange Policy-based Packaging Vocabulary (IEPPV),"2017-12-12, [online]. Dated December 17, 2012. See *also*: MARS/2013/12-05-IEPPV 6th Revised Submission, OMG Document Number: MARS/2013-12-05; Page E-5.

[11] Source: "Information Exchange Framework (IEF) – Information Exchange Policy-based Packaging Vocabulary (IEPPV)," 2017-12-12, [online]. Dated December 17, 2012. See *also*: MARS/2013/12-05-IEPPV 6th Revised Submission, OMG Document Number: MARS/2013-12-05; Page 6.

There is more to the story. The data-centric security environment utilizes UML[12] and OWL[13] specifications, the former (UML Profile) enables Information Packaging specifications to align to other architecture models (i.e. open architecture) while the latter, (Web Ontology Language/OWL) enables users to analyze the serialization of the data and data models at the granularity they require. This new approach to securing information as we share it – indeed before we share it – requires a new vocabulary to proceed. This vocabulary *is* the Information Exchange Packaging-Policy Vocabulary (IEPPV).

Returning to Figure 2, the data sharing environment we are now articulating replaces the shortcomings of the previous data sharing, legacy-based ETL environment, in which "Traditional" data and information exchange practices (and their assigned vocabularies) singularly failed to adapt to the increases in operational tempo and the dynamics of real-world events. Today's fast-paced information exchange environment demands **Responsible Information Sharing**. *Responsible Information Sharing* is a term which means having the maximum allowable data awareness and data management capabilities at your disposal.

It is all-encompassing, in that: law, regulation and policy 'e.g. *policy as-a-community'* and agency 'e.g. *policy-execution strategy* and *direction,*' are captured at the level of granularity required to empower real-world information access / information exchange, in real-time - a.k.a. in a virtual mode – for *all* information exchange conditions that may arise. Responsible

[12] Source: "Information Exchange Framework (IEF) – Information Exchange Policy-based Packaging Vocabulary (IEPPV)," 2017-12-12 [online]. Dated December 17, 2012. See *also*: MARS/2013/12-05-IEPPV 6th Revised Submission, OMG Document Number: MARS/2013-12-05; Page 6. See: *Ibid*., [Foot Note # 11] Page A-10. Unified Modeling Language (UML), in this instance, refers to a profile in the Unified Modeling Language (UML) which provides a generic extension mechanism for customizing UML models for user domains and platforms. Extension mechanisms allow refining standard semantics in a strictly additive manner, preventing them from contradicting standard semantics.

[13] Source: "Information Exchange Framework (IEF) – Information Exchange Policy-based Packaging Vocabulary (IEPPV)," 2017-12-12 [online]. Dated December 17, 2012. Page A-8. The combination of Ontology Definition Metamodel (ODM) -based visualization and OWL2 reasoning support, solidified the high-quality, logically consistent ontology product which the IEPPV represents. See: www/pmg.org/spec/ODM/1.0. The Ontology Definition Metamodel (ODM) is cited as an integral part of the MDA transformation used to generate the OWL Language implementation of the Information Exchange Policy-based Packaging Vocabulary (IEPPV). It is provided as a separate machine readable file – See specification Manifest, Policy.

Information Sharing,[14] by its very definition, *must* prove to be fully accessible and accountable, to all users and partners.[15]

Term [Data]	Definition [A fact]
Information	1) Data in context; and/or 2) Collection of data that informs a decision
Responsible Information Sharing	The ability to maximize the information available to authorized users while simultaneously protecting sensitive (Private, Confidential, Legally-significant or Classified information from unauthorized access, release or tampering.
Data Centric Security	The ability to deliver applied security/protection directly to the Data.

Table 1: A few definitions
Source: ASMG (2019)

Key elements in the Information Sharing Policy Life-Cycle

So much for the 64,000-foot elevation picture. Let's turn now to specifics. Key elements in the Information Sharing Policy Life-Cycle (Figure 2) include:

•Policy Instruments: typically, unstructured textual documents, that express information sharing and safeguarding policy.
•Policy modeling and serialization: implements the IEPPV profile and other Architecture Views to develop policy models that align information sharing policy with operational need and data domains. Using UML to develop the user policy models will enable the use of QVT (Query/View/Transformation) or other Model Driven Architecture (MDA) approaches to serialize the policy model to one or more machine readable and enforceable languages (e.g., XACML).
•Testing, Validation and certification: testing, modeling and simulation and analysis tools that enable users to validate and verify that policy models and machine readable serialization conforms to the originating policies.
•Policy/Rules Management: the deployment, management and administration of policies/rules in the operational domain.

[14] *Responsible Information Sharing* seeks to introduce a systematic process for translating information sharing and safeguarding via policy instruments (e.g. legislation, regulation, policy and service level agreements) into a machine consumable form, that can be automated in the operational (/runtime) environment. This specification (IEPPV) offers one option to model users, a model -based transformation using the UML Profile (See: IEPPV OMG Document Number: MARS/2013-12-05; Annex C) [which] modeled user policy in a manner that aligns the policy to the specification data environment. The IEPPV UML profile is used to define permissible patterns for assembling data and information elements into releasable datasets that conform to the originating policy. These policy models can then be transformed into a serialized form that is machine consumable and automated by platform specific implementations of policy decision and enforcement points linked to user data stores (e.g. RDBMS).
[15] Source: Information Exchange Framework (IEF) – Information Exchange Policy Packaging Vocabulary (IEPPV), See: MARS/2013/12-05-IEPPV 6th Revised Submission, OMG Document Number: MARS/2013-12-05; Page G-5.

•Operational Analysis: procedure(s) and tools used to determine the effectiveness and efficiency of information sharing and safeguarding (ISS) policy applied in the operational domain.
•Governance: the system of rules, practices, processes by which ISS policies are controlled.
•Decision and Enforcement Points: applications and services that combine to enforce ISS policy.
OWL tools allow users and data administrators to employ the reasoning application to analyze and validate the rules (composite policies) instantiating messages within the operational environment[16]. The operational environment is multi-focal, but allows data management to be reviewed via an audit trail. This tamper-proof audit trail includes the capability to identify conflicting rules, or combinations of rule sets, that may have been developed separately from one another, in which case privacy or security considerations may have been breached.

Overall effect of IEF and IEPPV adoption

The overall effect of Information Exchange Framework (IEF) and Information Exchange Packaging Policy Vocabulary (IEPPV) adoption[17] produces the development of analytical and business intelligence tools and services that enable:

- Governance and Stewardship
- Certification & Accreditation (C&A)
- Threat Risk Assessment (TRA)
- Statement of Sensitivity (SoS)
- Modeling & Simulation (M&S)
- Pre – and Post – Mission Scenario Analysis, and;
- Design and Operational Audits (e.g. Security)

The Logical Entity Exchange Specification (LEXS) defines the XML message structure, which includes the following: InformationPackage, StructuredPayload (e.g. NIEM messages), metadata, Digest, and Linkages[18]. The Logical Entity Exchange Specification (LEXS) was created by the legal community to minimize the impact of changing requirements and varied demands

[16] Source: "Information Exchange Framework (IEF) – Information Exchange Policy-based Packaging Vocabulary (IEPPV)," 2017-12-12 [online]. Dated December 17, 2012. See *also*: MARS/2013/12-05-IEPPV 6th Revised Submission, OMG Document Number: MARS/2013-12-05; Page 8.
[17] The IEPPV is organized to capture compliance points which build on contracts (renamed InformationExchangeSpecifications), transactionals (renamed TransactionalElement) and Wrappers (WrapperElement). The IEPPV extends rules to cover transformations (of data elements), plus manages the addition of tags and markings (labelling), and filtering / redaction processes. The IEPPV does not specify the technology components that must be used to capture the compliance points.
[18] Source: "Information Exchange Framework (IEF) – Information Exchange Policy-based Packaging Vocabulary (IEPPV)," 2017-12-12 [online]. Dated December 17, 2012. See *also*: MARS/2013/12-05-IEPPV 6th Revised Submission, OMG Document Number: MARS/2013-12-05; Page 8.

for information sharing of the sources, and consumer citations, in their field. The Logical Entity Exchange Specification (LEXS) provides a protocol for structuring and formatting a complex XML message structure. While LEXS was originally developed to address law enforcement needs, its basic construction extends to a broader audience. The Logical Entity Exchange Specification (LEXS) defines a means to consistently describe units of information to be shared and the interfaces and protocols to publish information, search / retrieve, and conduct / subscribe functions, and to receive notification regarding the data handled.[19]

For the technically astute, the Information Exchange Packaging Policy Vocabulary (IEPPV) components and elements are dedicated to reusing existing specifications: the IEPPV is intended to provide a path for tool vendors to develop a model-based information packaging and protection solution. The Information Exchange Packaging Policy Vocabulary (IEPPV) is also seeking to provide a vocabulary that frames many of the community-derived Extensible Mark-up Language (XML) -based exchange standards / specifications (e.g. NIEM and EDXL) and messaging specifications (e.g., LEXS, ATOM and EDXL/DE). [20]

In addition, the Information Exchange Packaging Policy Vocabulary (IEPPV) seeks to support transformation to multiple standardized policy languages, including (references in Annex F - MARS/2013/12-05-IEPPV 6th Revised Submission/OMG):

- Security Assertion Markup Language 2.0 (SAML 2.0),
- eXtensible Access Control Markup Language (XACML 1.0), and
- Ponder.

IEPPV Architecture –

The Information Exchange Packaging Policy Vocabulary (IEPPV) will be directly tied into architecture frameworks through the Unified Architecture Framework (UAF).[21] Unified modeling language (UML) provides for the integration of policy models into enterprise architecture constructs (e.g., platform and system views [interfaces], operational deployment

[19] Source: "Information Exchange Framework (IEF) – Information Exchange Policy Packaging Vocabulary (IEPPV)," 2017-12-12 [online]. Dated December 17, 2012. See *also*: MARS/2013/12-05-IEPPV 6th Revised Submission, OMG Document Number: MARS/2013-12-05; Page 9.

[20] Source: "Information Exchange Framework (IEF) – Information Exchange Policy Packaging Vocabulary (IEPPV)," 2017-12-12 [online]. Dated December 17, 2012. See *also*: MARS/2013/12-05-IEPPV 6th Revised Submission, OMG Document Number: MARS/2013-12-05; Page 9.

[21] Source: "Information Exchange Framework (IEF) – Information Exchange Policy Packaging Vocabulary (IEPPV)," 2017-12-12 [online]. Dated December 17, 2012. See *also*: MARS/2013/12-05-IEPPV 6th Revised Submission, OMG Document Number: MARS/2013-12-05; Page 17 – 18. UAF stands for The Unified Architecture Framework. The core purpose of UAF is to document a strategic coordination of a process (a task) and ensuring the underlying groups or entities involved are not only able to interact cooperatively, but are able to interact effectively, with clear definitions for interoperability ranging from the protocols used, through to hardware connectivity, ensuring all are following the guidelines laid out to achieve a combined forces goal. (By forces, we mean military personnel pursuing an activity in a defense or warfare theatre of operations). See: community.sparxsystems.com/white.../119_b5ebd190fd92233b5ed23e82fc28748f.

views, information and data views, and security views). The Information Exchange Packaging Policy Vocabulary (IEPPV) Partitioning are the package(s) which serve as the basic unit of partitioning in the IEPPV specification. The packages partition the model elements into logical groupings that minimize circular dependencies among individual partitions.

Enumerations extend the Information Exchange Framework (IEF) Reference Architecture (RA). The Information Exchange Framework (IEF) does not pick or choose which specific enumerations the user community should adopt. This allows for customization where the situation warrants, and in reaction to real-time events. [22] Component Enumerations offer the alert(s) notification within the IEF Reference Architecture (RA) specification. This puts the Information Exchange Framework (IEF) administrator in the driver's seat, in a situational awareness context, allowing them to monitor all data traffic activities in which they have a stakeholders' interest.[23]

The Policy-based Packaging and Processing Service (PPS) shown in the centre / bottom green oval contained in Figure 1, acts as an Open application programming (product) interface (API) and *transitions* structured Information Elements (e.g., NIEM, EDXL, and HL7) from data stores, and assigns information exchange services, in accordance with local information sharing and safeguarding (ISS) policies conforming to the Information Exchange Framework's [Policy- based] Packaging Policy Vocabulary (IEPPV). Working as an integral part in all of this, the Policy-based Packaging and Processing Services (PPSs) provide the ability to selectively package (aggregate, transform, mark, filter, structure and format) Information Elements for publication to authorized recipients. It also provides the ability to process (parse, transform, and marshal) Structured Messages, and integrate the data element for structured messages into the user's

[22] See: Information Exchange Framework (IEF) Final Revised Submission (FRS), OMG Document Number: MARS/2017-02-21) has a section devoted to extending the information sharing and safeguarding (ISS) model's functionality, called enumerations. See Page 232 for Alert Component Enumeration.

[23] This component or unit – AlertWarningType – monitors unauthorized or persistent attempts to perform unauthorized activities. The IEFComponentType unit ties in with Policy Enforcement Points (PEPs), Policy Administration Points (PAPs), Policy Decision Points (PDPs), and Policy-based Packaging and Processing Services (PPSs). The SAMSON demonstrator had a full Certification & Accreditation review carried out on the various enterprise and product security control catalogues, namely the ITSG-33, NIST SP800-53, and the Common Criteria, Evaluation Assurance Levels. It was determined that, using a product based approach; the most effective security assurance coverage would be obtained by using the Common Criteria at the EAL3 level. A SAMSON Security Target was developed based on the NSA Labeled Security Protection Profile (version 1b). The Samson Security Target provided a listing of Security Functional Requirements for Audit, User Data Protection, Identification and Authentication, Security Management, Protection of the **TOE****, and Cryptographic Support for the SAMSON product. Source: "Secure Access Management for a Secure Operational Network (SAMSON): Scientific Paper," by Daniel Charlebois et. al., Defence R&D Canada – Centre for Security Sciences (CSS). Technical Report (Document # TR 2013-037 – unclassified), Date: December 2013, Page 62. Although unit and system testing was part of the RAD approach for the creation of SAMSON, a formal test cycle was performed against the architectural baseline. This test cycle was performed against a SAMSON deployment to the Classified Test and Development Center (CTDC), a representation of the Consolidated SECRET Network Infrastructure (CSNI). See: *Ibid*, [*footnote # 83*], Page 61.Note: ** **TOE** is defined as "Target of Evaluation (TOE)" In accordance with Common Criteria, an information system, part of a system or product, and all associated documentation, that is the subject of a security evaluation. See: https://www.ncsc.gov/nittf/docs/CNSSI-4009_National_Information_Assurance.pdf).

data stores (e.g., RDBMS).[24]

The Policy-based Packaging and Processing Service (PPS) is the only tagging and labelling service (TLS) available today to achieve this, with a full audit trail, and may be conducted at machine speeds. An instantiation exists today.

In summary, the Policy-based Packaging and Processing Services (PPS) ingests information sharing and safeguarding (ISS) policy inputs conforming to the Information Exchange Packaging Policy Vocabulary (IEPPV), and *next* executes the packaging and processing rules and constraints defined by its semantics.[25]

Based as it is on Object Management Group (OMG) standards ratification efforts, specifically the Information Exchange Framework (IEF) Reference Architecture (RA), the Policy -based Packaging and Processing Services (PPS) is – therefore – not tied to any specific vendor solution. An organization can replace a vendor solution with another product that provides similar capabilities.[26] For instance, ASMG uses either distributed data services (DDS) services or REST services, to implement our internal and external messaging services. Both implementations are compliant with Information Exchange Framework (IEF) Reference Architecture (RA).

Policy Enforcement Points (PEPs) operate via proxy – called J2EE[27]– serving the Community of Interest (C-o-I). A second Policy Enforcement Point (PEP) Proxy is called the distributed data service (DDS).[28] Since the communication protocols and data formats vary, depending on the type of application that is to be protected, the proxy portion of the application Policy Enforcement Point (PEP) will vary in its implementation. However, the general application proxy

[24] Source: "Information Exchange Framework (IEF) Final Revised Submission (FRS)," Version: 1.0 [online]. Dated: October 2019. See: https://www.omg.org/spec/IEF-RA/. See *also*: OMG Document Number: MARS/2017-02- 21; Page 32 – 34.

[25] Source: "Information Exchange Framework (IEF) Final Revised Submission (FRS)," Version: 1.0 [online]. Dated: October 2019. See *also*: OMG Document Number: MARS/2017-02- 21; Page 92.

[26] Paragraph adapted from [Source]: Secure Access Management for a Secure Operational Network: A Scientific Paper, By Charlebois, Daniel -DRDC CSS et. al., Defence R&D Canada – CSS. Technical Report (Document # TR 2013-037 – unclassified), Date: December 2013, Page 14.

[27] J2EE (or "JEE") consists of core Java with a powerful set of libraries. With "JEE", obviously, you make websites, via Java beans and more powerful server applications. The J2EE is located within the client tier, and is a web component, acting with servlets and Java Server pages (JSPs), or standalone Java applications providing a dynamic interface to the middle tier. In the server tier (or middle tier) enterprise beans and Web services encapsulate reusable distributable business logic for the business application. The J2EE platform is a platform-independent, Java-centric environment, and the MARS IEF deploys the version offered by the vendor /

[28] Distributed Data Service (DDS) is a non-repudiation capability of an installed, functioning ISMB infrastructure. DDS is middleware. DDS is also a specification and a standard called a Platform Specific Standard, which assigns components in the IEF their data dissemination tasks and assignments. J2EE (or "JEE") consists of core Java with a powerful set of libraries. With "JEE", obviously, you make websites, via Java beans and more powerful server applications See [DDS] - Source: "Information Exchange Framework (IEF) Final Revised Submission (FRS)," Version: 1.0 [online]. Dated: October 2019. See *also*: OMG Document Number: MARS/2017-02-21; See [J2EE] - Page 265, and; Appendix D - Page 1.

architecture for intercepting data will leverage the Information Exchange Framework's (IEF's) defined core security services, and information protection logic. Taken together – the Information Exchange Framework's (IEF's) *defined* core security 'services' and information protection 'logic' – specifies "how" the Information Exchange Framework (IEF) processes data requests, and performs its functionality (e.g. read *here* that this "completes" *all-in-one* tasks and requirements) in its day-to-day operational picture.[29]

What we have described [herein] is a policy engine, with specific mention of the critical components or units which make it work. When the user sends their information request through the Information Exchange Framework (IEF) Secure Service Gateway (ISSG),[30] this policy engine will, in turn, process all access requests, evaluate these requests against domain security policies, and return Policy Decision Point (PDP) recommendations for enforcement.
The Policy-based Packaging and Processing Service (PPS) is a powerful, adaptable and comprehensive means to track and trace data, all the way through to where that data resides in its data stores (e.g., RDBMS or the Cloud). Plus, it ensures that user security caveats are always in full force and effect, and those caveats are rigorously enforced by the sponsoring (or hosting) organization. The sponsoring organization has the means at its disposal to conduct detailed information sharing and safeguarding (ISS) guidance activities.

Overall ISS Solution

One very frequent challenge facing the private sector is the situation in which the erosion of institutional memory and institutional knowledge is compounded by organizations having lost sufficient institutional knowledge and memory so that they become unable to properly manage

[29] The IEF Security Service Gateway (ISSG) intercepts all communication between IEF components and the user's security services (e.g., Identity Management, Privilege Management, and Key Management) infrastructure and the ISS supporting services *e.g., situational awareness*). The ISSG: i) Provides messaging interfaces for both 1a) the ISMB; and 1b) the Users messaging infrastructure; ii) Authorizes each request (gains authorization from the PDP); and iii) translates the requests and responses between IEF protocols and user networking protocols. The ISSG identifies the IEF Security Services Gateway interfaces that provide the integration point between IEF components and user specified security services, including: Identity Management, Privilege/Attribute Management, Cryptographic, Trustmark Provider, and Policy Development and Management Environments. Source: "Information Exchange Framework (IEF) Final Revised Submission (FRS)," Version: 1.0 [online]. Dated: October 2019.
See *also*: OMG Document Number: MARS/2017- 02-21; Page 100.

[30] The IEF Security Service Gateway (ISSG) intercepts all communication between IEF components and the user's security services (e.g., Identity Management, Privilege Management, and Key Management) infrastructure and the ISS supporting services *e.g., situational awareness*). The ISSG: i) Provides messaging interfaces for both 1a) the ISMB; and 1b) the Users messaging infrastructure; ii) Authorizes each request (gains authorization from the PDP); and iii) translates the requests and responses between IEF protocols and user networking protocols. The ISSG identifies the IEF Security Services Gateway interfaces that provide the integration point between IEF components and user specified security services, including: Identity Management, Privilege/Attribute Management, Cryptographic, Trustmark Provider, and Policy Development and Management Environments. Source: "Information Exchange Framework (IEF) Final Revised Submission (FRS)," Version: 1.0 [online]. Dated: October 2019. See *also*: OMG Document Number: MARS/2017- 02-21; Page 100.

and maintain Business Rules,[31] specifically the business rules related to information usage and information exchange actions or activities. This is particularly critical for the handling of Structured Messaging. Structured Messages are required to overcome three internal obstacles: a) Multiple (Structured Messaging) formats may be in use by stakeholders – e.g., JSON,[32] and Binary[33] – spread across [messaging] format domains; b) canonical information exchanges may have business "problem –specific issues" such as: canonicals are difficult to integrate, and canonical data may come from multiple canonical model sources, and; c) support for the inherent business rules upon which an organization relies, may be *absent* in an operational sense, and the information safeguards to protect business rules may be *underdeveloped*, or even *missing*.

The ISS Solution is a comprehensive solution, covering any/all operations affecting "files" (e.g. storing files, deleting files, redacting files etc.) and equally, this solution covers any kind of data object (e.g., e-mail, Instant messaging / IM or 'chat', file transfers and a special case, Secure Messaging. Secure Messaging was addressed outside the MARS / IEF demonstrator, as 'The Trusted Information Exchange Service (TIES) / IEF technology demonstrator project (TDP)', funded by the Government of Canada (GoC), addressed Secure Messaging services. The TIES / IEF technology demonstrator focused on Policy- driven, Data-centric access and release policy management issues and services, for Structured Messaging. This was analyzed for deployment of this capability in a cloud environment. ASMG – the project implementer– adopted the computer platform / infrastructure integration configuration which used open-source

[31] The Semantics of Business Vocabulary and Business Rules (SBVR) is an adopted standard of the Object Management Group (OMG) intended to be the basis for formal and detailed natural language (speech, signing and writing) declarative description of a complex entity, such as a business. SBVR encompasses business vocabularies, business facts, and business rules so that 'vocabulary plus rules' constitute a shared domain. The focus of SBVR is on semantic aspects and shared meanings, while syntax is thought in a perspective based on formal logic mapping. Information technology experts convert business rules into implementation rules to run automated systems. SBVR uses OMG's Meta-Object Facility (MOF). ASMG supports multiple environments, including a CORBA type system interface environments for entities in the architecture. Common Object Request Broker Architecture / CORBA bridges between systems on different operating systems, programming languages, and computing hardware. In short, CORBA is a set of schemas by which the structure, meaning and behaviour of objects are defined. OMG's Meta-Object Facility (MOF) creates its meta-models as UML class diagrams. A supporting standard of MOF is XMI, which defines an XML-based exchange format. MOF/XMI mapping rules, enable generating MOF-compliant models and define an XML schema. The SBVR is well suited for describing business domains and requirements, for business processes and information systems to implement business models.

[32] JavaScript Object Notation (JSON) emerged as a standard for easily exchanging JavaScript object data between systems. JSON's biggest weakness is its lack of defined data structures. NB: JSON was examined with the examination of 'Partners,' which refers to the owner of each individual application which may be in the process of 'transforming' that application to move "application content" in and out of a canonical format.

[33] Binary data, involving XML, in and of itself is not a data serialization language, but many data serialization formats have been derived from it. Data serialization formats offer various ways to convert complex objects to sequences of bits. It does not include markup languages used exclusively as document file formats. There are many ways to serialize programming data structures into XML. It should be noted that any XML based representation can be compressed, or generated – using Efficient XML Interchange (EXI) – which is a "Schema Informed" (as opposed to schema-required, or schema-less) binary compression standard for XML. Further discussion of binary, though interesting, is beyond the scope of this Report.

applications.[34]

There are two stakeholder groups, each with their own interests to look-out for, when it comes to implementing a need-to-know information sharing and safeguarding (ISS) solution in the way we have described.

- The **first Stakeholder group** are Security and Privacy Officers, representing data owners, data stewards, and data custodians. This group have the stated goal of needing to apply defense-in-depth data protection, to verify and institute a trust paradigm, with the appropriate credentials and authorization points well endowed. This Stakeholder Group, undoubtedly, view multiple self-contained enclaves or Communities-of-Interest (C-o-I's), defined by their security caveats or security designation clearances, as the constituency they serve.

- The **second Stakeholder Group**, Operational Users of the enterprise's data, require

[34] The IEF reference architecture was deployed on internal virtual machines and on stand-alone Windows and Linux machines. The Trusted Information Exchange Service (TIES) / IEF demonstrator project features structured messages which contain embedded elements (e.g., Digest, multiple information package, and multiple information payloads). Additional PEP elements or components were implemented to provide the integration to the ISMB, to Open Splice DDS, and to Apache Tomcat to provide basic web service communications; and;
• a NASA World Wind development toolkit was used to provide a GIS for geospatial information.
• Apache Cloud Stack was used to provide the Cloud Services in Windows and Linux.
• Open Slice DDS was used to provide the basic ISMB, with the intent to move to a DDS Security Implementation;
• Balana open-source XACML 3.0 implementation to implement the core element of the Messaging-PEP capabilities
• NASA World Wind development toolkit was used to provide a GIS for geospatial information.
• Apache Cloud Stack was deployed to provide the Cloud Services for the deployment of virtual Windows and Linux implementations of the Information Exchange Framework (IEF) Reference Architecture (RA). The IEF reference architecture was also deployed on stand-alone Windows and Linux machines.
• Simple Logging Facade for Java (SLF4J) for basic application level logging. Logging will be enhanced in the next version provide the TLS capability to incorporate hash log files or blockchain features.
Beyond the custom integration (using JAVA 8), only the ASMG implementations of the Packaging and Processing Service (PPS) and partial implementation of the PAP represented a custom service implementation. This implementation executed policy models for standard messages including:
• STANAG 5525 – NATO Multilateral Interoperability Programme (MIP) Protocol Data Units (PDU) and MIL XML. This included the use of the Shared Operational Picture Exchange Services (SOPES) Information Exchange Data Model (IEDM) V1.0 policy model. • OASIS Common Alerting Protocol (CAP) v1.2.
• Maritime Information Exchange Model, Maritime domain model for the National Information Exchange Model (NIEM) canonical model.
Messaging on the IEF Secure Message Bus (ISMB) represented a subset of the XML messages provided in Annex A, issued as a simple string over Distributed Data Services (DDS).
The Trusted Information Exchange Service (TIES) / IEF demonstrator project features structured messages which contain embedded elements (e.g., Digest, multiple information package, and multiple information payloads).
Source: Information Exchange Framework (IEF) Final Revised Submission (FRS), See: OMG Document Number: MARS/2017-02-21; pp.8, 327.

> information and data in an immediately accessible form and format. This stakeholder group- *inclusive* of their operational information usage, and usage information assets and data/metadata and/or raw data, have their stated goal of needing defense-in-depth protected data to efficiently (and quickly) exchange and receive the data elements they need to perform their assigned work. Operational Users are steadfast in their determination to have access to full data discovery, unhindered by any accessibility issues affecting them or their membership enclave, or Community-of-Interest (CoI). They expect to have this accomplished with a minimum of fuss, and may only be peripherally aware of their certification and authorization (C&A) data access requirements, as per any training on such matters that they may have voluntarily received.

Both Stakeholder Groups are addressed by the IEF Reference Architecture's (RA's) IEPPV policy and semantics vocabulary instructions, since that was the whole purpose in designing and defining the IEPPV capabilities in the first place.[35] It is important to point out that for this canonical data transport application, the IEPPV serves as a very practical, and robust Information-as-a Service (I-a-a-S).[36]

What we have just presented is the ability to process (parse, transform and marshal) structured messages. Next, we have reviewed how to integrate the structured messages' data element into the user's data store (e.g. RDBMS or the Cloud). Marshalling and persisting data elements to the specified data store is optional. The user *may* direct the Policy-based Packaging and Processing Services (PPSs) to operate only in volatile memory and not persist the information. The IEPPV component to handle this (saving volatile memory and not persisting the information

[35] Treating all parties to an information exchange democratically, while maintaining security on information communications, is the goal of the Information Exchange Framework (IEF) reference architecture (RA) which the TIES / IEF demonstrator deployed. Many workshops have taken place under the Object Management Group's (OMG's) jurisdictions to establish this as a solid information exchange framework and solution. For the purposes of elaborating on this point, the capabilities and solutions applicable to address data protection and Quality of Service (QoS) issues, requires most organizations to also adopt a set of standards for message structure and content, called Message Payload. Message Payload is constructed from XML schema, and the method for using XML schema – in web services situations – may lend itself to tools from such specialist companies as: Sparx, iGnite XML, Altova Schema Agent, and Progress DataXtend. Source: "Canonical Modeling: NIEM and Beyond," By Priscilla Walmsley, slide deck presentation, Dated September 19, 2012, [slide #'s] Page 36-37.

[36] Information-as-a-Service (I-a-a-S) provides access to data in real-time. In this context, the Information Exchange Policy and Packaging Vocabulary's (IEPPV's) capabilities extends to allowing: i) distribution of data across the enterprise as a shared service, allowing business intelligence tools, mashups, and portals to interact with identical data in real-time; ii) the creation of a single source of data "truth" for major data domains, i.e., provides the ability to establish and maintain one trusted source of data for specific work flows, getting everyone on the same page; iii) reduces the operational problems that may stem from 'batch' data updates between systems. Even minor discrepancies in data between out-of-synch batches, in enterprise systems, can cause serious problems, especially in financial transactions [See: previous Foot Note # 150], and; iv) I-a-a-S allows the simplifying and streamlining of data exchanges between enterprise systems, reducing many of the cost factors that have inhibited the thorough sharing of back-end data with (/between) consuming systems in the past. By establishing a single, trusted source of data as a shared service, it is possible to set up separate consumers of that data in number(s) of separate applications, with comparatively little effort.

is Process Structured Message Elements which issues instructions required by the Policy-based Packaging and Processing Services (PPSs). All policies required by the IEPPV and its components are set with and through the Policy Administration Point (PAP) authorization service, issuing instructions (policies) to the environment using the component "PAP-Command message."

Another powerful feature of the IEPPV – (currently implemented / currently configured a.k.a. the Trusted Information Exchange Service [TIES]) / IEF demonstrator) – is the capability of the Policy-based Packaging and Processing Services (PPSs) to trigger the packaging and publication of messages to all recipients, in a Community-of-Interest (CoI) or user enclave, by monitoring data state or events based on watchpoints, set via modelling in the PAP. This is achieved by the specific issue to all participants in these entities, according to issued authorizations these entities (/enclaves or /communities) are assigned,[37] deliberated by the Policy-based Packaging and Processing Services (PPSs) mediation and brokerage service, for the authorized updates in question.

The Policy-based Packaging and Processing Services' (PPSs') mediation and brokerage service calls up the IEPPV –appropriate component as follows: the IEPPV component Process Structured Message Elements issues the *request*, which is required by the Policy-based Packaging and Processing Services (PPSs), in accordance with Policy Administration Point (PAP) authorization – falling under the control of the message command component "PAP-Command." The "PAP- Command" message component *next* actions: Multi-party updates (or /alerts), occurring via component 'Trigger_Watchpoints.' This is a machine-to-machine example of real- time information sharing and information exchange safeguarding in action.[38]

And on one final note, taking a slight digression in our discussion, XML Schema can be supported, especially in Web services situations, by deploying resources such as the Sparx Schema Composer. Sparx Schema Composer greatly simplifies the process of creating

[37] This is very different from a more traditional Email alert. Just to review an Email alert, if an IEF Security Service Gateway (ISSG) issues a request via the component "ISSG-Response (sender attributes)," this requests the user's Identity and Credentials Access Management (ICAM) service, to retrieve the user's identity, information and authorizations. The sequence (above – ICAM request action) would occur as follows: the IEPPV component or unit ISSG retrieves the user's (/sender's) identity information and distributes, packages these identity authorizations as an ISSG-Response, and issues the response to the Email-Policy Enforcement Point (Email-PEP). Source: "Information Exchange Framework (IEF) Final Revised Submission (FRS)," Version: 1.0 [online]. Dated: October 2019. See *also*: OMG Document Number: MARS/2017-02-21; Appendix E - Page 278, and; Appendix E.

[38] Source: "Information Exchange Framework (IEF) Final Revised Submission (FRS)," Version: 1.0 [online]. Dated: October 2019. See *also*: OMG Document Number: MARS/2017-02-21; Page 98-99. Discussion: The full InformationElement component, or /unit (original source code) appears at: IEF Reference Architecture - Final Revised Submission (FRS), OMG Document Number: MARS/2017-02-21; Page 227-231.

standards- compliant schema in a reusable and accessible manner.[39]

Applicability to a Banking Context

In a banking context, networks provide a road of travel, but do not provide sign posts along the way pointing out exactly where a data asset 'sits' at any point in time. The Distributed Ledger (conceptually) corrects this deficiency. However, internal issues and practices related to the location of data, and how it is managed in that location within the bank, can be addressed by the Information Exchange Framework and the Policy-based Packaging and Processing Service (PPS), and should no longer simply be swept under the rug. We can do better.

As this Report has pointed out, the Object Management Group's (OMG's) leadership position formally mapping and prescribing the provenance of data, and developing the restrictions on its location, movement and use, is an asset the banking community – and our government sector Clients – have yet to fully appreciate. It is worth mentioning here that ASMG has defined these requirements due to its' exposure to Government and Industry information storage and access, and information security related projects over the years. The requirements have come from the Government and Banking sectors over the years, and the solution was devised to enable information exchanges that are secure, traceable, and can be managed during operations.

Enterprises tend to outsource security management to a third party, and that third party may host the Client's Information Technology / Information Management (IT / IM) assets through complicated agreements, tied in with other Clients' IT / IM services and agreements, as well. These complicated series of tenant assignment rights, called multi-tenancy assignments, creates the condition in which multiple customers, all as different tenants on the same Cloud service or Cloud platform, may share assets in one Cloud, although they may not know what actual security management protects them in their own Cloud. Many companies or institutions are uncertain about hosting their internal data on a computer that is external to their own company/institution, in great part due to this condition of multi-tenancy, whereby charting or mapping the exact path that enterprise data travels consumes more and more of a company's (or an institution's) resources.

[39] Many industries have worked hard over the last decade to define shared meta-models specific to their industry, and it is these models that now form the basis for contractual information sharing across organizations and across geographic borders. A typical usage scenario of the [Sparx] Schema Composer is in the creation of message definitions (/schema) to exchange information between organizations, ensuring that such messages comply with the underlying meta-model that has been adopted by the involved parties. When information is shared between organizations, it is frequently the case that only a subset of the full meta-model is required, but it is essential that what is shared conforms precisely to the agreed meta-model. This converts a UML class model to a W3C XML Schema (XSD), This [Sparx – Schema Composer] toolkit also allows Data Modellers to start working at a conceptual level in UML. Source: Sparx Systems Enterprise Architect User Guide Series – Schema Model 6 Version: 1.0. Dated: June 3, 2017 online, Page 4-6. All interesting stuff, but slightly beyond the scope of this Report.

In Summary

When all is summed up – the relative placement of the data, the subjects sending and / or receiving the data, the applications and the users' experiential knowledge of data assembly and data management – *all* these points are key in determining what an enterprise's overall data management plan truly '*is*'. Whether the Information Exchange Framework (IEF) Reference Architecture (RA) and the Information Exchange Framework's (IEF's) Information Exchange Policy and Packaging Vocabulary (IEPPV) are instrumental in contributing to finding solutions to your enterprise's data management challenges, remains to be seen.

We have much more information we wish to share with the Canadian banking community leaders, including Chief Technology and Operations Officers' (CTOO's) and their hand-picked Teams. For example, Unified Modeling Language (UML) – is indeed a graphical language for visualizing, specifying, constructing and documenting artifacts of a software-intensive system. UML captures business processes and systems functions; makes 'concrete' things such as programming language statements, database schemas, and; *specifies* reusable software components. We have used basic subsets of UML, but it is regarded as part of the toolset, not the purpose or an absolute prerequisite for the environment.

The capture and retention of information about the rules governing the operation of transactional interface(s) in a manner that enables certification and accreditation[40] may be one issue the bank's Technology Team may find extremely relevant.

It is virtually impossible to cover everything, and many real-life data use cases, and/or specific taxonomy clarification issues have yet to be defined or explored. ASMG and the bank's Technology Team may have several issues of data taxonomy clarification to discuss, some of which may include topics such as the following:

- Conceptual data models [41]typically do not supply semantic information about the concepts behind the [data] classes, i.e. they do not compromise characteristics.[42] Definitions or explanations are sometimes given in combination with a conceptual data model, but very often

[40] Source: "Information Exchange Framework (IEF) – Information Exchange Policy-based Packaging Vocabulary (IEPPV)," Version: 1.0 [online]. Dated: October 2019. See *also*: MARS/2013/12-05-IEPPV 6th Revised Submission, OMG Document Number: MARS/2013-12-05; Page 5-6.

[41] Conceptual data models benefit from IEPPV modelling conventions, which certify and categorize information exchange rules. The IEPPV promotes the information exchange environment and is, therefore, the additional certitude bridge or layer of clarity to conduct information exchanges. By definition, Conceptual data models are typically represented by means of diagrams in UML, Unified Modelling Language (OMG 2015), which is a standardized general-purpose modelling language used in object-oriented software engineering. The conventions for using UML concepts and convention is something which, standards- body organizations,' such as the Object Management Group (OMG), are dedicated to maintaining.

[42] Source: "Establishing a solid foundation for data modelling," By Bodil N. Madsen and Hanne E. Thomsen [online – terminfo]. Dated: 2015. http://www.terminfo.fi/sisalto/establishing-a-solid-foundation-for-data-modelling-332.html.

these may not be actual or 'explicit' definitions, but rather bland recordings or registering of facts as a *bookmark* to indicate the presence of 'some information'.

- A data 'class' represents number(s) of similar objects, or instances in the database. Associations link classes to each other and thus resemble concept relations in terminology terms. When moving from a terminological ontology to a conceptual data model, concepts will typically be mapped into classes. However, when a subdivision is mapped into a class, the subordinate concepts under the relevant subdivision criterion will then be mapped into attribute values. These will then eventually become 'options re: pick-list' in the data base user interface (UI).

- The data model – in a banking application and/or in a regulatory agency or governmental example –- may be defined using the entity-relationship "data model." For example, it may refer to an abstract formalization of the objects and relationships found in a specific application *domain*, e.g. 'customers', 'products' and/or 'orders/services'. At other times, (possibly) it refers to a set of concepts used in defining formalizations, examples being concepts such as: 'entities', 'attributes' 'relations' or 'tables'. In programming languages, data models may be synonymous with data structure.

- A data model represents classes of entities (kinds of things) about which a company wishes to hold information. In short, the entities represented by a data model can be tangible entities, but models that include such concrete entity classes tend to change over time. Robust data models might include an entity class often identified as an abstraction of (such and such) an entity. Just to review, an object model, in computer science, is a collection of objects or classes through which a program can examine and manipulate some specific parts (of its world).

And there are many more data practice and taxonomy issues [43] which, no doubt, are waiting to be comprehensively, and collectively, addressed.

For instance, Advanced Systems Management Group (ASMG) have created our Administration Point which functions as our Human-to-Machine application programming (product) interface (API) software component for the Policy Packaging Service (PPS). We are excited about the generators we possess, which allow us to capture a relational model from target databases and/or HTML Schema. These benefits will translate into allowing analysts the ability to concentrate on information exchange policies, not the complexities of extracting and conducting the storage of 'data elements *per se*,' in what can be a vast and/or rapidly evolving RDBMS environment. Additionally, this will save the depletion of critical resources in pursuing the production of a message (or messages) *compatible* with a complex schema, or set of data schemas.

In short, Advanced Systems Management Group (ASMG) have created our Administration Point as a totally effective Human-to-Machine application programming (product) interface (API) software component for the Policy Packaging Service (PPS) –to support complex messaging at

machine speeds – and to automate that *messaging* process feeding *directly* into an operational data store. Advanced Systems Management Group (ASMG) – of course – are searching for (and will find) new challenges with every implementation, but we have significantly simplified the *rote processing* of relational data significantly, to date. Advanced Systems Management Group (ASMG) are discovering that the database itself is becoming more and more transparent to the information exchange policy definitions, as they are implemented, over time. Whether this is a goal which is feasible, or desirable, in a big data environment, is certainly open to question. At least, however, we start from a well-documented approach, that has withstood the test of intensive peer review in a *critical* standards body review exercise and standards-deliberating effort, plus we have fully tested this approach with Canadian Government factions and participants and in defense sector NATO environments.

What can ASMG Offer?

The Information Exchange Framework (IEF) works without logical models and target database documentation, and without metadata generators. Each message – and its persistence logic – entering into the database environment needs a lot of modeling by analysts, which is still better than case-by-case parsing of messages, using an antiquated extract-transfer-load (ETL) environment to or toolkit item to *feed* an operational data store. As effective as that may have been for a limited set of information exchanges, we believe it still can be improved upon significantly. The opportunity Advanced Systems Management Group (ASMG) wishes to address maintains that a situation exists in which the opportunity for programmer error and ad-hoc policy definition may occur, and these occurrences may be buried in application programming (product) interfaces (APIs) that are then hard to decipher – and modify – over time. Advanced Systems Management Group (ASMG) can, however, use the generators we have built to get *in minutes* what would take days / weeks / or months to do for “foundation class” formulations, governing their representative database interfaces.

These, and other examples, are best addressed via a ‘live DEMO’:

i) examination of the hosting situation, in which the “Policy Packaging-based Packaging Service (PPS)” have no inherent policies, it does what it is told, and logs the results of its actions;

ii) the PAS can be used to define and provide a defined set of policies as defined by the IEF; and provides the logic <rules> of the Information Exchange Package-based Policy Vocabulary (IEPPV),

iii) The PPS can accept, marshal, store, received messages and can generate messages and implement the interfaces specified via the “Information Exchange Policy-based Packaging System (IEPPS)’, consistently, and lastly;

iii) The approach is easily scaled since the installation of the open API is devoid of the data policies, a.k.a. ‘data policies’ are added ‘in’, as an operational component, over time.

Appendix B

NB: European Parliament of the European Union (EU) *Horizon 2020 Programme 2016-2017* 'call for proposals / technology demonstrators' to fulfill the mandate of the GDPR.

DS-08-2017: Cybersecurity PPP: Privacy, Data Protection, Digital Identities

Citation: HORIZON 2020 - Work Programme 2016 – 2017 "Secure societies – Protecting freedom and security of Europe" [/at p.76]

Specific Challenge: The use of modern telecommunications and on-line services involve users' personal information. For example, using search engines exposes the query terms used, which can be both sensitive and identifying, as illustrated by the exposure of search terms; social networking services expect users to reveal their social connections, messages and preferences, that could lead to direct privacy violation if exposed. Browsing the web also leaves traces of where users have gone, their interests, and their actions - meta-data that can be used to profile individuals. The implementation the draft General Data Protection Regulation (GDPR - currently in the law-making process) presents both technological as well as organizational challenges for organizations [to] implement novelties such as the right to data portability, the right to be forgotten, data protection impact assessments and the various implementations of the principle of accountability. Many services on the Internet depend on the availability of secure digital identities which play a crucial role in safeguarding the data and privacy of citizens as well as protecting them and other actors such as private companies or public services form various online threats. At the same time, many European countries already have or are in the process of developing an electronic identity (eID) scheme. Most of these projects are built to be at a very high security level, which makes them very suitable for diverse eGovernment processes. But in turn they may lack usability for commercial applications.

Scope: Innovation Actions: Proposals may cover one of the strands identified below.

Privacy-enhancing Technologies (PET)

Novel designs and tools to provide users with the functionality they require without exposing any more information than necessary, and without losing control over their data, to any third parties. PET should be available in a broad spectrum of products and services, with usable, friendly and accessible safeguards options. PET should be developed having also cost effective solutions. Comprehensive and consistent Privacy Risk Management Framework(s) should be available,

[to] allow people to understand their privacy exposure (i.e. helping people to understand what happens to their data when they go online, use social networks etc.). Open source and externally auditable solutions are encouraged [to] maximize uptake and increase the trustworthiness of proposed solutions.

General Data Protection Regulation in practice

Tools and methods to assist organizations to implement the GDPR [*addressing*] the final provisions of GDPR and guidance from relevant authorities (Data Protection Authorities, Art 29 WP or its successor). Proposals may also address the need to provide support (procedures, tools) for entities to understand how to operate without requiring unnecessary information ([to] promote privacy respecting practices), *particularly* [when] the issue is mainly related to the fact that organizations (businesses, service providers, and government agencies) often require too much information from their target customer/user.

Secure digital identities
With a view to reducing identity fraud while protecting the privacy of citizens, proposals should develop innovative, secure and privacy enhancing digital identity platforms beyond national eID systems. Activities may leverage existing European electronic identification and authentication platforms with clearly defined interfaces based on the General Data Protection Regulation (GDPR).

Proposals may:
• Leverage evidence-based identities (using adequate correlation of multiple soft proofs of identity, as opposed to the usage of a central register);
• Provide a function for so called "qualified anonymity," which means, that the online service does not have any information about the user but a pseudonym. The real identity of the user can only be revealed under specific conditions such as at the request of legal authorities;
• Consider cost-effective and user-friendly verification methods for mobile identity documents. For all strands, proposals should identify and address the societal and ethical dimensions of the strand they choose to cover taking into consideration the possibly divergent perspectives of pertinent stakeholders. Proposals [to] address the specific needs of the end-user, private and public security end users alike. Proposals are encouraged to include public security end-users and/or private end users. The Commission considers that proposals requesting a contribution from the EU between EUR 2 and 3 million would allow these areas to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts. The outcome of the proposals is expected to lead to development up to Technology Readiness Level (TRL) 6 to 7; please see part G of the General Annexes.

Expected Impact:
• Support for Fundamental Rights in Digital Society. • Increased Trust and Confidence in the Digital Single Market • Increase in the use of privacy-by-design principles in ICT systems and services

Type of Action: Innovation action
The conditions related to this topic are provided at the end of this call and in the General Annexes.

2020

ACPR

SUBMISSION FROM ADVANCED SYSTEMS MANAGEMENT GROUP (ASMG)

JIM CARTER

Table of Contents

Overview 2
Over-reliance on Network Security 3
Interconnectedness / Handling information security risks 6
Trusted Architecture base 10
The EU's General Data Protection Regulation (GDPR) 19
1)– privacy violations caused by search engine identity exposures. 21
2)– responsible information sharing. 22
3)– protecting *online* identities from malevolent cyberthreat actors, both in the public and private sphere. 23
4)– PET (Privacy-enhancing Technologies) – ASMG's data-centric security (DCS) solution – [be] available with usability, accessibility and safeguarding features 'designed-in' 25
5)– Open source and externally auditable. 25
6)– leverage identity-based solutions. 26
7)– reduce identity fraud / protecting citizen's privacy 27
8)– Extended impacts (3): i) support for fundamental rights in a Digital Society; ii) increased 'trust' (in EU's Digital Single market), and; iii) increased use of 'privacy-by-design'. 28
9)– The Following Topic did not appear in the call-up documentation, but ASMG would have addressed it (regardless): data protection embedded or rooted in data governance. 28
Data-Centric Security (DCS) 29
Summary 36
Appendix A 40

Overview

This reply to the ACPR (Banque de France) discussion document, titled "Governance of Artificial Intelligence in Finance (Dated June 2020)," by authors Dupont, Fliche and Yang, will address the ACPR's Report from the perspective of an entity which operates with information security as our primary objective and mission.

The ACPR "Governance of AI in Finance" paper summarizes the results of a comprehensive review – via workshops and participatory interview(s) – of a wide segment of industry participants. Our goal in this reply will be to point out areas in which the ACPR authors have come to conclusions with which Advanced Systems Management Group (ASMG) would agree. Plus, point out areas in need of further reflection and study.

Since we were not a part of the process itself, as an actual participant (part-and-parcel) contributing to the report, and we do not have access to the enterprise architecture 'first principles' to which ACPR themselves are privy, *a.k.a.* the hardware / software environment, communications establishment, and skills sets applied to your enterprise – at an enterprise architecture level – the best we at Advanced Systems Management Group (ASMG) can offer *herein* is to point out benchmarks which would apply, specifically, in the case where the implementation of security (solutions) might be applied to '(ML) machine learning' *contextually*.

Two different problems exist today, in the environment in which a financial regulatory body operates. The first is the heavy (we would say over-reliance) on network security as the be-all and-end-all layered defense, which is installed and counted on to protect regulatory data, wherever it manifests itself. The ACPR paper cites, and rightly so, that "Setting up a proper data governance for an AI algorithm will not work if data sources fed to it are inappropriately managed, for example, if they are fragmentary, anecdotal, insufficiently durable, can be tampered with, or if the organization does not control their lifecycle"[1].

The second problem regulatory organizations face was articulated by Germany's Federal Financial Supervisory Authority last year, listing ten implications of the proliferation of big data and AI[2] which are key issues for regulators and supervisors. From this list two are critical to the

[1] Source: Wei Dai, Isaac Wardlaw. Data Profiling Technology of Data Governance Regarding Big Data: Review and Rethinking. Information Technology, New Generations. Advances in Intelligent Systems and Computing. 448. pp. 439–450. ISBN 978-3-319-32466-1 (2016).

[2] Source: https://www.european-microfinance.org/sites/default/files/document/file/risks_of_AI.pdf. The complete list Germany's Federal Financial Supervisory Authority laid out includes:

1. Emergence of new business models and companies.
2. Connecting markets and market participants (e.g. risks from increased interconnectedness).

topic addressed in this ACPR Report, and Advanced Systems Management Group's (ASMG's) response to your document: a) Connecting markets and market participants (e.g. risks from increased interconnectedness) and; b) Handling information security risks.

The first of these topics, the '(speed of) networks and interconnectedness'[3] is amplified by ML models optimizing themselves in real time (rather than following pre-programmed rules), introducing an extra degree of opacity and uncertainty, which is magnified by the lightning speed at which algorithms make decisions. And the second point, 'handling information security risks', the Center for the Study of Financial Innovation (CSFI)[4] authors state: "problems that arise ultimately come down to a lack of care and due diligence – for example, failing to pay attention to monitoring, logging, audits and testing of models. It's the boring stuff which is critical". And this boring stuff, if you do not provide a sufficient ML security solution, is exacerbated quickly by a lack of human understanding, as well as obliviousness to cyber threats and cyber incident preparedness.

Over-reliance on Network Security

When a financial institution is tasked with the job of assembling different learning systems, the risk of ML security will arise with respect to protecting test and training data, and data outputs being rendered by ML algorithms. These data sets are far from assured the sufficient levels of protection they warrant, in today's network-centric security environment. What's even more alarming, is the sense that all-things-security-related somehow fall under the rubric of 'securing the (data) packet', since if the (data) *packet* is secured, then the job is done.

ASMG fundamentally disagree with the above assertion. Learning systems, and machine language models and AI, attempting as they do to share testing information with partners, often multiple partners, some of that data being structured, unstructured or even constituting

metadata, must be communicated across a wide swath of Information Technology /

3. technology to limit undesirable developments (e.g. via technological safeguards). Redefining and addressing systemic importance.
4. Governance.
5. Fighting financial crime and preventing conduct violations.
6. Subjecting internal models to supervisory approval.
7. Handling information security risks. *
8. Risk of discrimination.
9. Ensuring trust in the financial market. [*NB: denotes – addressed in this Submission].

[3] Source: "Artificial intelligence and machine learning in financial services," Financial Stability Board. https://www.fsb.org/wp-content/uploads/ P011117.pdf; Page 31 – 'networks and interconnectedness'.

[4] See: "It's not magic: Weighing the risks of AI in financial services," By Keyur Patel and Marshall Lincoln. Center for the Study of Financial Innovation (CSFI), Dated: (*unattributed*) ISBN: # 978-1-9997174-7-6; Page 36

Information Management (IT / IM) infrastructures. This is problematic, unless we focus on a data-centric security perspective. When data is shared across different computer architectures, each with their own enterprise architecture configurations, this introduces complexity which may be generally harmful to traditional (network-centric) security solutions. Network-centric security falls short in its efforts to protect (and manage) data. There may be different operating systems (OS), or different versions of operating systems, spread across one (or several) computer network(s). This might lead us to believe that by simply having a 'bolted down' computing base, all is well.[5] If this were true, data traversing the Cloud, or finding its way to the "edge-of-the Cloud", which is where networks send data, should – ultimately – be secure, as well. This is something which multiple cyberthreat attacks on critical data assets proves, over-and-over-again, to be a patently false security supposition to make!

In your paper, ACPR authors ask the right set of questions (page 40 / Question 20):
"What is the impact of using ML on IT security? [Follow-up question]: Which types of attack against ML models (causative attacks, surrogate model attacks, adversarial attacks, etc.) appear the most important to you, both in terms of occurrence likelihood and in terms of damage inflicted in case of [attack] success?"[6].

Papernot (2018) addresses some of this concern for you – i.e. 'security of ML models'? – stating that "the security of a system deploying ML can (also) depend on the security of the ML model itself. For instance, some security properties such as *availability* only make sense in the context of the entire system, but may depend on security properties of the ML component itself (e.g., *integrity*).[7] Take the example of a software defined network (SDN) controller, that integrates an ML model for intrusion detection. If the integrity of that intrusion detection model cannot be guaranteed, the availability of the SDN controller, and of the entire network it manages, may be affected as well."[8]

Software defined networks (SDNs), possibly deploying the Rapid Spanning Tree Protocol (RSTP) method to *switch* (move) data packets across a network – or data pipe – obviously determines the *path* [over which] data transverses. Let's just think about this: if decision-making functions are removed from the *switch*, and (instead) handled by the 'software' (the SDN), the physical forwarding of [data] *packets* – once an attacker takes control of their target's 'controller' – now presents itself as a greatly expanded threat vector within which the cyberthreat actor can stage their attack. The cyberthreat vector actor's malicious intent, once they crack your controller,

[5] Source: Nicolas Papernot, "A Marauder's Map of Security and Privacy in ML: an overview of current and future research directions for making ML secure and private." Proceedings of the 11th ACM Workshop on AI and Security (2018). See: https://arxiv.org/pdf/1811.01134.pdf. See *also*: *Ibid*., [Foot Note # *34*], alternative (but *identical*) citation.

[6] Source: ACPR (Banque de France) discussion document titled "Governance of Artificial Intelligence in Finance (Dated June 2020)" by authors Dupont, Fliche and Yang, Page 40.

[7] *Ibid*., [foot note # *5*], Page 4 – 'security properties of the ML component itself (e.g., availability vs. integrity)'.

[8] *Ibid*., [foot note # *5*]: Page 4 – 'security of the Software Defined Networks (SDNs) *a.k.a.* intrusion detection.'

may progress unimpeded, since *they* (the cyberthreat actors) have – essentially – cracked and *fully* hijacked your network.

If I could refer ACPR authors to re-examine this SDN *compromise* issue a little more closely, an article posted by the company Bitdefender (2018)[9] suggests that when SDN network and security policies are maintained and managed 'in' the controller, it becomes relatively less difficult to *both* get the policy evenly distributed throughout the network, and it becomes relatively easier to enforce those 'security' policies. SDN also abstracts control away from the hardware devices, so it becomes easier to sidestep proprietary controls, and develop tools that will simplify security across the network. This comprehensive network view will make it more transparent for analysis and event response. The comprehensive view (which SDN provides) also makes it easier to identify something malicious, and then respond, accordingly. All good.

But what happens when things progress to a deteriorating state of affairs? Here is an example: when placing all the centralized control in the SDN controller, this action comes at huge risk. If the antagonist cracks the controller, these attackers have cracked your network! This situation begs a defender to have previously instituted several defensive measures to shore-up (network) *controllers*. These may include such controller best-practice defensive measures as: including traffic monitoring capability in the SDN toolkit; system patching efforts, tools and measures; aggressive access control monitoring efforts, and; adopting *other* high availability protections, such as having ready-to-go solutions for potential denial-of-service attacks.

This still requires network operators to be responsible for creating security and authentication policies, to ensure that only the *right* people have access to the information the SDN is attempting to protect. Is this feasible today?

There are numerous private companies offering proprietary controllers. There are many 'open controller' companies – Floodlight, Open Daylight, Open Contrail and Open Network (Operating System) controller – to name a few. However, when the Open Networking Foundation attempted to standardize *northbound* APIs' they failed.[10]

[9] Source: https://businessinsights.bitdefender.com/security-benefits-software-defined-network.

[10] Source: https://www.computerworld.com/article/2496832/clarifying-the-role-of-software-defined-networking-northbound-apis.html. The oft-mentioned northbound API - that will let applications tell the controller what they need from the network, which may be one set of instructions for Hadoop, or one set for Oracle server, or another set of instructions for OpenStack's Nova - the Open Network Foundation's argument is that the northbound API is "how the business talks to the controller". If the buyer is buying a business application, you buy one (specific) implementation; and this will continue to be the case. The efforts the Open Networking Foundation are pursuing is 'categorizing / documenting' what exists. That's it.

Interconnectedness / Handling information security risks

A very succinct analysis of how the greater AI *interconnectedness* condition is manifesting itself in the financial services system today has been chronicled by the Financial Stability Board (FSB), whereby they suggest "this state of increased interconnectedness may help to share risks, and act as a shock absorber up to a point." Yet, the FSB state, "the same factors could spread the impact of extreme shocks."[11]

If critical segments of financial institutions rely on the same data sources and AI (and ML) algorithmic solutions / strategies, then under certain market conditions, a shock to those data sources – or a new strategy exploiting a widely-adopted algorithmic strategy – could affect that financial services industry segment, as if it were a single node. This may occur even if, on the surface, the segment is made up of tens, hundreds, or even thousands of legally independent financial institutions. As a result, collective adoption of AI and machine learning tools may introduce new risks.

The opposite – or positive – condition which this *interconnectedness* might contribute to would be for financial institutions experimenting (or experiencing) AI and ML-enabled algorithm-generated data sets, to benefit from new things. These new advances may allow financial services sector participants to predict, in a more accurate sense, vastly uncorrelated profits or economic returns, which no doubt will please the modeling industry as their potential for growth will expand, accordingly. But it doesn't remove one important point: there is a risk remaining that these AI and ML-enabled algorithms will be exploited on a sufficiently wide scale, even as banking correlations increase (for the better). The banking sectors' attack surface has, effectively, grown alongside the proliferation of AI and ML advances. Cyberthreat adversaries' activities will, and have grown, precipitously. This condition of *positive trade-offs* versus *negative trade-offs* – as tallied by the Financial Stability Board (FSB) – suggests that as (potentially) unforeseen *interconnections* in the financial services sector become clear, as AI and ML-enabled technologies are fully, or more widely, adopted and made more publically available, we cannot be sure how to protect ML and AI advances appropriately.

Moving to the topic of 'handling information security risks,' let's turn to a brief examination of the European Union's (EU's) recently enacted General Data Protection Regulation (GDPR), due to come into force in 2018. ACPR authors partially address GDPR Articles at page 62 of your Report. Your discussion – *explainability* versus *interpretability* – states that there is a tension

[11] See: *Ibid*., [Foot Note # *3*], Page 31. See: [original *citation*] "Rethinking the financial network," speech by Andrew Haldane/FSB, at the Financial Student Association, Dated: April 2009.

between the GDPR's *right to access personal information* collected (articles 13-15),[12] and

GDPR's *right to* collect *data* (article 22)[13]. I'm sorry. This explanation wasn't focused enough on the citizen's privacy rights, and I would refer you to address this from the exploratory (and explanatory) analysis of the GDPR made by your associates at the Financial Stability Board (FSB).

The FSB believe that the GDPR will become especially relevant with respect to the use of AI and machine learning *as per* Article 11, which provides a right to "an explanation of the decision reached after [algorithmic] assessment, and allied articles providing for similar disclosures[14]" have been (more) fully met. Other key articles relating to AI and Machine learning are found at (GDPR) Article 9, which prohibits the processing of "special [sensitive] categories of personal data" as defined; (GDPR) Article 22, which provides for a data subject's qualified "right not to be subject to a decision" with legal or significant consequences based solely on *automated processing*; and at (GDPR) Article 24, which provides that "decisions shall not be based on *special* categories of personal data."

Staying with this for a moment, the FSB discussion skirts the topic of whether (or not) GDPR Article 22 grants a disproportionate weight to data collection actions and activities. Both the Financial Stability Board's (FSB's) and ACPR's analysis converges, or agrees, to the threat – prospective or real – which may lie in wait, e.g. the development of a "black-box" society

[12] Source: "European Union regulations on algorithmic decision-making and a *right to explanation,*" By Bryce Goodman and Seth Flaxman, Dated: 2016. Published: ICML Workshop on Human Interpretability in Machine Learning (WHI 2016). Page 3. See: https://arxiv.org/pdf/1606.08813v2.pdf.

[13] See: *Ibid*., [Foot Note # *12*], Page 1 (Introduction-Goldman and Flaxman/2016). NB: Right to data versus right to collect data are two different things. The first assumes the privacy of the User/Client is paramount, while the second condition – Right to collect data – is a more loaded term. See: *Ibid*., [Foot Note # *36*, *37*] GDPR – 'privacy violations caused by search engine identity exposures' and other points raised in this section of ASMG's Submission titled: "The EU's General Data Protection Regulation (GDPR)."

[14] See: *Ibid*., [Foot Note #*3*], Page 38. See: [*citation*]: Sandra Wachter, Brent Mittelstadt, and Luciano Floridi (2017), "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation," International Data Privacy Law, (*Forthcoming*). NB: GDPR Articles 9, 22 and 24 are all subject to exceptions. Wachter et. al. argue that these provisions confer no right to an ex-post explanation of decisions, though ex-post explanations may be crafted through jurisprudence or EDPB work. On the other hand, Goodman and Flaxman (2016) argue the law will also effectively create a "right to explanation," whereby a user can ask for an explanation of an algorithmic decision that was made about them. ASMG tend to award Wachter et. al. with the more compelling position of the two.

(Pasquale, 2015)[15] seeking control over information, data and/or *our* identities. I will not weigh in on the GDPR policy proclamations further here[16], as in a previous working relationship,

Advanced Systems Management Group (ASMG) were unsuccessful in our efforts to have the European Union (EU) Parliament address data-centric security (as opposed to the network-centric security *orthodoxy* prevalent today)[17]. But it is important to state (*herein*) that protecting 'personal information' and 'the right to collect data' are both business process governance issues, without question.

In your paper, ACPR authors state (page 67) "the detailed code analysis suggested for level-4 explanations (replication) should also focus on the use of (such as are available *off-the-shelf* libraries," but as Papernot (2018) points out (under the point 'complete mediation' e.g. *every access to every* (ML model) *object must be checked for authority*: "a data provenance question [to be addressed by *complete mediation*] occurs 'if the defender is unable to verify the integrity of its training or test data.' Or, more pointedly, is the ML model defender potentially exposing (their) algorithmic model's testing and training inputs, and/or ML algorithmic-generated outputs, to poisoning, evasion or privacy attacks?[18]"

ACPR authors (page 28) reference this fact, stating "A comprehensive description of the potential flaws of an ML model – 'ML security' I believe you meant to *add*, or this was implied by this statement – and of the means to *remedy* 'the flaws of an ML model / ML security' [*then*] – is beyond the scope of this document."[19] Just prior to this statement, the ACPR authors' reference ML security by suggesting the way to make an ML model safe is different from the way in which a web service exposed through a (set of) REST APIs is made safe. It is inferred, in your ACPR paper, that this data is captured on three (3) potential architectural layers: the model layer, the application layer and the data layer.

---

[15] Source: "The Black Box Society: The Secret Algorithms That Control Money and Information," By Frank Pasquale (2015). Harvard University Press (ISBN 9780674368279). NB: Pasquale: (The opposite to the black box] "(Is) an intelligible society, which would assure that key decisions of its most important firms are fair, nondiscriminatory, and open to criticism. Silicon Valley and Wall Street need to accept as much accountability as they impose on others." *See* also*:* https://dl.acm.org/doi/pdf/10.1145/3086512.3086513.

[16] Technology issues relative to the implementation of the GDPR are a totally different matter, and cry-out for definitive technological solutions. This condition in which a paucity of technology exists today, which would also allow or enable AI and ML modeling algorithmic analysis to proceed apace, is a topic which concerns ASMG to no end. This topic will be examined much more definitively at a later section of ASMG's Submission titled: "The EU's General Data Protection Regulation (GDPR)." See: *Ibid*., [Foot Note #*3*], Page 38 [and the *later* section in this Submission].

[17] See: Appendix A "Cybersecurity *privacy-protection-pilots* (PPP): Privacy, Data Protection, Digital identities (DS-08-2017) / re: European Union (EU) call for submissions [tendered via citation 'Horizon 2020 – Work Programme 2017- 2017 – "Secure Societies-Protecting freedom and security of Europe /at p. 76.' NB: The original call-up is issued at Appendix A. Briefly, what ASMG *had intended* to submit - updated to todays' 2020 IT/IM environment - will be summarized [*See* section titled]: "The EU's General Data Protection Regulation (GDPR)," [Foot Note # *27*].

[18] See: *Ibid*., [foot note # *5*], Page 8, 9 – 'complete mediation' (a.k.a. training points to predict data poisoning).

[19] See: *Ibid*., [foot note # *41*] 'ASMG reply to ACPR's ML security reservations'.

ACPR report authors reinforce your testimonial to AI governance stability by stating (page 9-10) "the relative lack of maturity of AI in the (financial services) industry, which has been introduced primarily into the less-critical business processes (and those which bear little by way of *ethics* and *fairness* risks)," has led to a situation in which (page 10 – the text describing 'Appropriate data management'): "All data processing should be as thoroughly documented as the other design stages of an AI algorithm (source code, performance of the resulting model, etc.). This documentation enables risk assessment in the areas of regulatory compliance and ethics."

Agreed.

And that also should mean that any time data assets are introduced from 'outside' the financial institutions' own walls, or from sources on the Internet (or in the cloud) which the financial institution did not author themselves, then these extraneous (non-originating within the financial institution's *in-house* data stores and/or data repositories) information sources poses a real threat of losing control over that data set's pedigree of *origination*, accuracy and *explainability*, at-all-times when non-originating data is admitted *in-house.*

Returning to your analysis on page 28 (under your heading 'ML security') "the attack surface in finance is narrower than in other sectors: IT security in finance is usually a well-funded and mature area, furthermore, exposure from things like open source code and *use of public data* has, thus far, tended to be more limited than elsewhere." You state in the foot note [#14] that "many actors rely heavily (and sometimes exclusively) on open-source libraries and products implementing ML functionality to avoid 're-inventing the wheel', and [cite the fact that] … the use of so-called alternative data (collected from the web or from other publically available sources) *should it* become widespread [among data-driven systems in finance]," would – Advanced Systems Management Group (ASMG) believes – constitute new avenues for threat vectors to originate, something your organization should be worried about!

Papernot (2018) addresses this *above* point – obliquely – stating that "As machine learning (ML) is increasingly applied to domains involving security or privacy considerations (e.g., intrusion detection) "[In practice]: adversaries may attempt to find attack variants that evade intrusion detection, e.g. manipulate the inputs of high-frequency trading – to cause them to issue disadvantageous transaction orders – (as one example)."[20] *Contd.*: "potential misuses of learning-based systems are not limited to the ML model itself, but also the computer system hosting this model. In other words, the security of an ML model can: (1) be impacted by, but (2) can also *itself* impact – the security of the system that is deploying this very ML model."

[20] See: *Ibid*., [foot note # *5*], Page 3.

This is the entire ML security challenge you face! Or, as Papernot (2018) colorfully describes it: "ML models can only be as secure as the system that hosts it. This situation demands – boils down to – establishing a trusted computing base."[21] Papernot (2018) then addresses areas which may introduce further data compromise, incurred when a side-channel on the accelerator (e.g., FPGA, GPU, TPU, etc...) that runs the (ML) model, is itself 'compromised'. Not speaking to hardware issues directly (herein), at least since ASMG do not consider ourselves hardware authorities, nonetheless, Papernot's (2018) points are well taken.

Papernot (2018) states: "while combining computer systems with different architectures or configurations (certainly) introduces complexity, [complexity] that is generally harmful to traditional computer security (e.g., running different operating system versions in a computer network)."

Trusted Architecture base

What ails privacy and data protection today begins with the architecture. Advanced Systems Management Group (ASMG) strongly believes that by *designing* - *sourcing* (and installing) a trusted architecture base, via an entirely different paradigm, we may significantly correct the deficiencies of the current enterprise architecture model, following religiously as it does, the Network-centric security, and Application-centric security enterprise architecture design parameters which are observable, and prevalent today. Let's examine the current *status quo* enterprise architecture elements and components, at work today, before we address the *new* enterprise architecture design which ASMG believes is required.

The Information Communications Technology (ICT) industry casts a huge shadow over the prevailing delivery of Information Technology / Information Management (IT/IM) services globally. They have vested huge amounts of resources to defend their technological edifices and services delivery *beach-heads*. But their beach-heads – if they are not living up to the needs and requirements expressed by the Exercise of Users' Rights over user-defined privacy and data protection efforts – is fundamentally at odds with what the world desires.

First, let's take a close look at the Network-centric enterprise architecture platform. The ICT community approach the securing of data – in the data governance context – from a network-centric perspective. Network-centric (the *status quo* conditions) stress the paramountcy of: publicly co-funded infrastructure projects, privacy-supporting components (many, and hard to count or keep track of, including: data controllers, key servers and anonymizing tools and services, storage, CPUs and innumerable network tools and add-ons). Network-centric security

[21] See: *Ibid*., [foot note # *5*], Page 4.

proponents, generally-speaking, view privacy/data protection standardization efforts as placing extraneous demands on stakeholders.[22]

Let's look at this situation from the perspective of an industry major, the European Union Agency for Network and Information Security (ENISA/2014), a major voice for advocating on behalf of network-centric enterprise architecture solutions. ENISA respond to user rights with respect to *data privacy* and *data protection* in a manner which is ripe for unpleasant data monitoring, and data access *breach* conditions to occur. ENISA membership resources are contributing to the creation of a condition which is identifiable, and defined as, network-centric data *gating*.

Network-level security resources '*gate*' access to data (repositories), but do not have any inherent visibility on the assets being protected. Owners of information are just that: owners of data. This is not a rhetorical statement. Third parties, whether they are computer integrators, telecommunications providers or application vendors (i.e. hardware / middleware or software products / service suppliers), all too commonly insert themselves into the data management process wherein their presence is not always advised.[23] Historically, allowing third parties to handle data may have occurred out of a recognition that the third party possesses a means (or tools) to assist in data management, or likewise have the tools/expertise to assist with data collection, data transformation and / or data storage services. In today's knowledge-based economy, corporate success can only be attained when the information and technology used for business, is mandated to be secure, accurate and reliable. Data communication, transport, and retention services should be community – and consensus building – in their focus. We almost fool ourselves into thinking this is happening in an innocuous manner today. This is simply not so.

[22] Source: "Privacy Data Protection by Design – from policy to engineering," By George Danezis, *et. al.,* Dated: December 2014, authored by the European Union Agency for Network and Information Security (ENISA), Page iv, 7, and 60. ENISA believe that standardized policy and languages that express descriptions of data processing and data safeguarding, as well as assign notification of risks and/or 'how to' mechanisms for users to exercise control over their data, would raise comprehension levels beyond the 'fix' that rest (interfaces) have usefully provided. ENISA would examine PETs (privacy-enhancing technologies) addressing; i) protocols for anonymous communications; ii) attribute-based credentials; iii) privacy –enforcing database search solutions, and; iv) encryption. Only the last PET is widely used (encryption), which means the beach-head installation of ICT service(s) and product offerings is, largely at present, undisturbed.

[23] This point was emphasized in the James Carter prepared "Water Made Smart: The Arcadis Digital Conveyance Solution" Report (dated December 2016). Reproducing that *text*: GE Chief Executive Jeffrey Immelt says he wants his digital business line to grow to $5 billion a year by 2020, up from roughly $6 billion now (20a6). GE's software centre in San Ramon, California now employs 1,400 people. Among other things, the San Ramon (near San Francisco) Software Centre developed a cloud based operating system, called *Predix,* a sort of Windows for industrial applications. See: The Globe and mail – Toronto, Canada: "Manufacturing hasn't vanished – it's just smarter," Report on Business, Page B-1, by Barrie McKenna, reporter-Washington, D.C. See *also*: https://www.bloomberg.com/opinion/articles/2018-07-31/ge-needs-digital-just-not-the-jeff-immelt-version. (For an update from Bloomberg News on this story).

From a definitional standpoint, Advanced Systems Management Group (ASMG) take exception with organizations such as the European Union Agency for Network and Information Security (ENISA) whom state that when we approach what ails *data privacy* and *data protection* today, data *interoperability* (which underpins the issue) has not been sufficiently addressed in a standardized context, by *standardization* bodies.[24] The requirement to address information *interoperability* – in the substantive manner that ACPR authors believe it should be addressed – should be all-encompassing in its design and implementation, as an *architected* solution. It requires meeting the requirements to enable information integration, handling machine learning (ML), analytics and algorithmic test data, training data and data 'outputs', *plus*; process data supplied from inference engines, through search efforts (knowledge discovery) and/or handle or accommodate data compiled from federated information libraries or 'other' source materials.

These *other* data sources – and types of data – whether structured, unstructured, or sourced as *new* data – be they passive or active, subject to flat and/or horizontally scalable database structures, or be data processed by real-time query tools (as opposed to delineated snapshots), and/or other more advanced data analytic processing techniques, all serve to enhance our physical, cognitive, and decision-making capabilities.

As well, *new* powerful queries' libraries (often called NoSQL) are changing the dynamics of business. We now think of data volumes in petabytes (or exabytes/EBs), large SQL infrastructures have *sharded* their existing database resources to create more flexible, horizontally scaled environments, to leverage big data tools and capabilities. The challenge addressing big data is time-consuming, and requires conscientious "persisting and uniting" of disparate data sets, some of which may even be hosted by third party systems. These rapidly proliferating data resources – crossing borders (and organizational boundaries) constantly – are beyond human attention spans, at times.

This is the whole purpose as to why ACPR are approaching the analysis of AI in Financial innovation in the first place!

Advanced Systems Management Group (ASMG) would argue that network-centric security advocates, such as the European Union Agency for Network and Information Security (ENISA), are misguided when they state that data interoperability has not been sufficiently addressed in a standardized context. Why? ENISA (and their membership e.g. exercised via their advocacy on behalf of their memberships' sphere-of-influence) are defining *interoperability* as 'technical interoperability'. Technical interoperability is a term which defines an agreed communication protocol which exists between established communication infrastructure(s), allowing systems to exchange bits and bytes of information, as defined by that communications infrastructure's underlying network and protocols, which are unambiguously defined.[25]

[24] See: *Ibid*., [Foot Note # *22*], Page iv.

[25] Source: Information Exchange Framework (IEF) – Information Exchange Policy Packaging Vocabulary (IEPPV), See: MARS/2013/12-05-IEPPV 6th Revised Submission, OMG Document Number: MARS/2013-12-05; Page G-6.

If challenged on the *narrowness* of their definition of information interoperability, ENISA might defer to a second definitional portrait encapsulated by Application-centric interoperability. Not coincidentally, ENISA also champions the interests of application vendors (i.e. hardware, middleware or software products/services suppliers). Application-centric security vendors and suppliers also run up against their own set of interoperability *gating* issues. Application-centric level security, applied in the information interoperability context, '*gates*' access to data (repositories), but do not have any inherent visibility on the assets being protected. (This is the same condition, as we just stated, which we just encountered with data *gating* by network-centric security interoperability activities). Application-level security models *gate* access to a specific type of information resource (e.g. one example being */files*) but do not provide a comprehensive access model across the enterprise's information architecture.[26]

Here is a specific example of Application-centric security shortcomings: a data asset (and/or its receipt generated) tends to be poorly handled, or is read as 'incomplete' by current information transport systems. This condition, application-centric security model *gating*, falls short in its

efforts to deliver comprehensive protection of identities, and citizen privacy, since it fails to accommodate: 1) data tracking 2) data versatility (monitoring), and; 3) specified parameters [for data tagging / labeling] which, if they are lacking, fails to distinguish – definitively – where data resides.

An example may be found in several Application-centric platforms visible *vis-à-vis* Machine learning (ML), which involve a huge number of sensors and data-generating devices. These sensors and data-generating devices are increasingly being applied to domains involving, or asking for, security or privacy solutions. This is obviously a reaction to more and more mobile devices, sensors and actuators (within physical devices) sending and receiving increasing amounts of data. The physical network, where sensors reside, have demand for data processing and data analytics located on Internet-of-Things (IoT) platforms, whether they be located on-premise, or at the edge and/or on-the Cloud. Some service providers – Forescout, Semantic and Trend Micro – provide firmware to address these demands. Other integration components are designed to fit ERP platforms, such as Oracle Fusion Middleware, Link Smart, Apache Kafka or the Open Source IoT platform, Dynthings. Each general purpose IoT framework receives 'customized' treatment, oftentimes deploying application analytics via AI, ML and visualization.

The financial services sector has been particularly affected by growing communications channels, and the logarithmic increase in applications (*microservices*). Larger financial institutions are developing *microservices* rapidly, sweeping through 'Products', 'Channels', 'Functions', and 'Infrastructure' capabilities. These microservices are solidly anchored by a

[26] Source: Secure Access Management for a Secure Operational Network: A Scientific Paper," by Daniel Charlebois – Defence Research Development Canada (DRDC) Centre for Security Science (CSS) *et*. *al*., Defence R&D Canada-CSS. Technical Report [Document # TR 2013-037 – unclassified]. Dated: December 2013, Page 1.

connector grid and services grid, and empowered by the appropriate (application) real-time call-up procedures, for any application linked to that bank's Smart Core. *Microservices,* in the banking sector's service-oriented architecture (SOA) implementation model, feature services which are: independently deployable (from one another) and; are scalable, and; tailored to fit business implementations by operating on the business process itself. This builds a matrix of multiple service sets, adapting differing programs, language and database management (e.g. storage technology) solutions. The Customer-centric focus practiced by all of today's modern banks adds domains of knowledge, from the core outwards (concentrically), which specifically demands that the bank must hold *all* data stewards, data holders, data owners, and data custodians – and their upper Business Line executives – accountable to *owning* the information they use.

Obviously, Employees have an incredibly deep understanding of their transactions history, which they create every day. This is accompanied by the empowered Customer, whom approaches their interactions with a Financial Institution (FI) as an *affinity* group, well-read on topics that are of interest to them, overtly-plugged with information from their social networks, computers and smart devices, and rarely wrong!

To keep the Customer placated involves immediate information accessibility, and real-time insights to protect the bank's bottom-line. A general decline in Customer *stickiness*, in which the younger generation – one in three millennials surveyed in the United States – report they

would be open to switching banks, in the next ninety (90) days. Or, even more drastically, believe they will not even need a bank in the future.[27]

Organizational efforts to stay abreast, particularly with mobility-escalating trends, which feature torrential data feeds, growing by the day, places even more stressors on architectural domains, and impinges on front-office (and back-office) performance. The modern bank is transforming to: 1) connect / integrate services, using an enterprise service bus (ESB). This process enables the banking domain *Business Rules* (e.g. rules governing a service, delivered by an application) to be put in the banking *core*, as opposed to leaving these business rules as residing in *all* the distributed applications.

Secondly, the *new* transformational era in banking can achieve: 2) the placement of *Business Rules* in the enterprise's *core* (not placed within the apps, or within distributed applications), since application-based *Business Rules* are not likely to be abstracted properly or conveniently. The benefit to *data abstraction* which the bank's Lines-of-Business management greatly appreciate, is for their Channels (and their Channels' services) to deploy *abstracted* data, which they strive to do even more productively and efficiently, since *abstracted* data sets – built with a single code base – are ideal. This ensures that banks can have an infinitely easier time of it, as

[27] Source: Viacom Media Networks – The Millennial Disruption Index. See also: https://marketmatchblog.wordpress.com/category/millennial-disruption-index/. Multiple sources of information on Millennials, are available in the popular press.

they seek to dissipate *Business Rules* across *all* banking channels, at a much faster rate.

Getting into the thick of things, Business Analysts' employ the tools called the Semantics of Business Vocabulary and Business Rules (SBVR)[28] as they process their workloads, conduct their data management and data analytic tasks, and integrate ML model algorithms' *interpretive* outputs into their *decisioning* process. This situation in which the bank's business analysts' find themselves, is being confronted daily by advances in cyber (internet, mobile communications, etc.) and other technologies, operating without the limitation of state borders, which adds business process and data management *complexity* to the crowded data processing environment in which financial sector employees operate. Communications (and Application-centric) customer-facing 'data handling / data monitoring' customer-service *touch-points* push even more complex data processing environments to the foreground! With Clients (banking Customers) wanting instantaneous service delivery, in as close to real-time conditions as possible, if we feed into this workplace (and workload) dynamic the network-centric data interoperability shortcomings – and Application-centric data interoperability failings – these two conditions contribute to data accessibility issues, via the creation of Information

technology / Information Management (IT / IM) data stove pipe *dead-ends*. Something needs to give!

The presence of these inaccessible data repositories frustrates cross-domain (and cross-platform, and cross-enterprise architecture) secure information exchange functions. The goal for an *ideal* or 'optimal' information exchange environment is for information to be separated according to that data set's sensitivity attributes – e.g., classification, confidentiality and privacy, legal significance and (security) caveats – which the current IT/IM environment has no clue how to address.

The information *stove-pipes* are conflicted with an ever-increasing number of partitioned systems, failing to communicate with one another. This is the essential information exchange conundrum! In this environment, subsets of concepts contained in information vocabulary are managed by ETL (Extract, Transfer and Load) tools, further depriving (and/or distancing) the end-user from accessing the data and information they require. We need something to transcend this! That is a *secure* data-centric environment requesting the packaging (assembling and formatting) of information element(s), and the inverse processing of received messages and data sets, as a *mandatory* minimum requirement, always.[29]

[28] SBVR is the first specification under the Object Management Group's (OMG's) *new* stream of Model-Driven Business specifications). It is a Vocabulary – special purpose natural language *ontology* – and a Behavioral Guidance tool – specifying *business policies, operative business rules, and advices of permission* – which governs business actions of an organization. In effect, SBVR creates documents for an organization to build a bridge from business to IT and back.

[29] Source: *Ibid*., [Foot Note # *21*]; Page 6. ACPR's statement of 'data processing risk and specific algorithmic risk (in terms of *availability* and *integrity*)'. ACPR goes further that the FSB citation, suggesting "An additional

The Internet Privacy and Engineering Network (IPEN), founded by the European Data Protection Supervisor – together with other data protection authorities[30] – are cited by the European Union Agency for Network and Information Security (ENISA) as an ICT Internet-related sector organization calling for the provision of "free" open source software tools for all systems developers (DevOps professionals). Plus, IPEN wish public grants to be made to maintain the expertise contained in application (and communications) code base, as the penultimate *ask* to ensure user privacy and security safeguards are properly protected, by voluntarist industry protection societies and regulatory bodies alike. (What?).

Furthermore, ENISA state that Privacy-enhancing Technologies (PETs) in four (4) areas will cover (and protect) the exercise of User Rights for identities and data protection security. They are: 1) encryption; 2) protocols for anonymous communications; 3) attribute-based credentials, and; 4) private search (tools) for databases. Of these, *encryption* is widely used, and in fact, Advanced Systems Management Group's (ASMG's) data-centric security solution accommodates encryption. The other three (3) PETs are, however, specific to the technology interoperability paradigm, or world-view, which supports network-centric (and Application-centric) exigencies, but not as appropriately or conclusively as ASMG's data-centric security (DCS) solution would accomplish.

What should be especially troubling for financial sector participants to be made aware of is that financial institutions (and the regulators which serve the industry) cannot perform real-time analysis across all data stores, which causes them to suffer from a potentially devastating knowledge gap. To overcome this knowledge gap, organizations must tailor and customize their *Search* and *Query* results, and not have these efforts always simply parrot what they think (or guess) as the status-quo conditions at work. Although knowing what is 'in' your corporate data repositories may be an efficient use of an Employee's time, and may stem data processing downtimes, if the data you are looking at is immaterial to your business (or regulatory activities or proclivities?), what have you gained? What may be needed is the pairing of instantaneous *Search* and *Query* alerts, critical, boundary-pushing searches, and then – maybe even receiving – relevant information on your desk, exactly when you need it.

It is entirely possible that the user of data could be from two opposing data stakeholder constituencies, each addressing completely different business tasks and technical-administrative scenarios. The first might be Security and Privacy Officers. These Security and Privacy Officers represent data owners, data stewards and data custodians. This group have the stated goal of needing to apply *defense-in-depth* solutions to protect their data, which will efficiently (and quickly) exchange and receive the *specific* data elements they need, to perform their assigned work.

---

consideration is the potential outsourcing of the design, implementation or exploitation of those solutions, which bears ML-specific *security risks*." (Point taken).

[30] Source: *Ibid*., [Foot Note # *22*] - ENISA *citation* - Page 53. See *also*: [*original* citation] "On syntactic anonymity and differential privacy" By Chris Clifton and Tamir Tassa. Transactions on Data Privacy, 6(2):161–183, 2013.

Their opposite counterpart(s) are the Operational users of data. This group are steadfast in their determination to have data via full data discovery, unhindered by any accessibility issues affecting them or their membership enclave, or Community-of-Interest (C-o-I). They expect to have this accomplished with a minimum of fuss, and may only be peripherally aware of their certification and authorization (C&A) data access requirements, as per any training on such matters that they may have voluntarily received.

The ACPR Report (Page 26) examines these users in your section devoted to 'technical validation,' which addresses the human agency (or human operator). In point form, these human operators include:
-Data Owner and Data Steward are respectively responsible for the governance and for the quality of data used by algorithms.
-Data Engineers and Data Scientists are tasked with ensuring proper operational behaviour of software components which implement the algorithms.
-Lastly, in this context data Analysts perform initial ongoing validation of the algorithms' output.

(*Continuing*/Page 27): This technical (validation) expertise should span the Data Science spectrum (from data engineering to state-of-the-art ML technique) and may be multi-tiered: generalist skills, financial sector specialization, and deep knowledge of business process specific applications or domain knowledge necessary to 'run' the organization.

This should lead us to consider a point made by the Financial Stability Board (FSB). The FSB asks us to consider "Where financial institutions rely on third-party providers of AI and machine learning services for critical functions, specified instructions or directives on dealing with *outsourcing* (Third Party relationships and contracts) may not be in place, or not be understood. These outsourcing services / providers may *not* be subject to supervision and oversight. Similarly, if providers of such tools begin providing financial services to institutional or retail clients, this could entail financial activities taking place outside of the regulatory perimeter.[31]"

Advanced Systems Management Group (ASMG) believe that a set of follow-up questions to this topic should be to ask: When employing Third Party / Outsourcing options, how do financial institutions exercise the removal (where possible) of incorrect data handling and data monitoring? What are the appropriate evaluations of risk associated with internal control malfunctions? And, thirdly, how is ML model validation – through audit operations discovery efforts – to be ensured to exercise the 'precise' context (/understanding) of (an) algorithm? For example, has the ML algorithm tool / toolkit been extensively documented, a.k.a. – How was it pre-designed / -designed / tested? – What are its operational parameters, functions, effectiveness? And; – What Q&A *follow-up* is *designed-in* (to the ML algorithm tool / toolkit),

[31] See: *Ibid*., [Foot Note # *3*], Page 33 – 'Third Party AI suppliers/providers outside regulatory perimeter'.

and is this monitored and reported on to all parties involved? Foremost to all three of these issues, as well, should be the question answered: How does the financial institution evaluate the business processes into which it (the ML model algorithm) is integrated, or which are impacted by it (the ML model algorithm) in-*one-way-or-another*?

This entire discussion is aided and abetted by what Papernot (2018) reviews as 'complete mediation' (taken from Saltzer and Schroeder's cryptographic research classification taxonomies)[32]. Complete mediation requires every access to every object must be checked for authority.[33] This is relevant to ML security in several ways. Papernot (2018): "First, a model that is originally a black-box may become a white-box later in the future. That is, an insider could leak the model, or an adversary with access to a device deploying the model, could reverse-engineer the device' software to recover the model.[34] Secondly, an adversary can adapt by considering the model whose gradients were masked as a black-box, and transfer adversarial examples found on a different model whose gradients are not masked.[35]

First from a confidentiality and privacy standpoint, it is key to enforce access control to the model and its predictions. The model itself may constitute a *channel* for more elaborate attacks, that recover sensitive information analyzed by the model during training. Or, the

defender may be unable to verify test data (provenance), as an attacker may have exposed the model (test or training data sets) to poisoning, evasion or privacy attacks.

Papernot (2018) states: "Indeed, just like a program can be policy-compliant yet still have buffer overflows, one could imagine that a ML model may still exhibit undesired behavior despite passing model assurance.[36]" This has led Papernot (2018) to ask: Should the framework encompass training and test time adversaries? Papernot's answer to this is: "One argument in favor of including both (test data and training data) in a unified framework is that it would allow us to consider dynamics between training-time attacks and test-time attacks: for instance, how does defending against adversarial examples impact robustness to poisoning attacks? These dynamics have been unexplored, by our, community so far.[37]"

[32] See: *Ibid*., [Foot Note # *5*], Page 4. See also: [original *citation*]: "The protection of information in computer systems," By Jerome H. Saltzer and Michael D. Schroeder. Proceedings of the IEEE, 63(9):1278–1308, (1975).

[33] See: *Ibid*., [Foot Note # *5*], Page 9 – 'complete mediation.' NB: If the defender is unable to verify the integrity of its training or test data, it potentially exposes the model to poisoning, evasion or privacy attacks. It could also make it difficult to implement the failsafe defaults.

[34] See: *Ibid*., [Foot Note # *5*], Page 5 'black box turning to white box later [with adversary code loaded]'.

[35] See: *Ibid*., [Foot Note # *5*], Page 6 - 'open design/security mechanisms not secret'.

[36] See: *Ibid*., [Foot Note # *5*], Page 12 – 'test admission / input-output pairs'. NB: 'If' the security policy does not apply to a zero-day attack. Hence, given an input and an output, we'd like to be able to know whether we admit the input-output pair into our pool of answers. This is difficult in ML because the underlying distribution is unknown.

[37] See: *Ibid*., [Foot Note # *5*], Page 16 – 'Towards a similar framework for security.'

Advanced Systems Management Group (ASMG) might suggest: This *may* lead to data that is *compromised*, or may even be *substituted*, and may not originate from the 'distribution of interest' which the defender believes it to be sourced from.

This is an important issue: knowing (and trusting) the data your financial industry ML models use. It is even more important when you reflect on the fact that, as significant an effort as the General Data Protection Regulation (GDPR) of the European Commission (EC) has legislatively stated it wishes to see enacted, the technologies required to allow users to *know* and *trust* data *always*, via hardened and proscribed technologies, and their accompanying solution strategies, in actual *bona fide* technology implementations, is something that the General Data Protection Regulation (GDPR) of the European Commission (EC) has left 'somewhat' muddy and *unclear*. But as unclear as GDPR implementations may be at present, they still go a considerable distance beyond the narrow strictures which the ACPR authors assigned in your efforts to analyze ML security.

In short, the GDPR is attempting to address, in a much more in-depth manner, what kinds of security actions might be considered "appropriate to the risk," including: i) The pseudonymization and encryption of personal data; ii) The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems / services; iii) The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, and; iv) A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the [data] handling/processing/reporting.[38]

The EU's General Data Protection Regulation (GDPR)

(NB: See Appendix A[39])

One specific technology demonstrator *call-up* released by the GDPR – issued via an *expression of interest* document circulated to *all* prospective technology solutions, computer integration and product and service vendors and suppliers – which caught the interest of Advanced Systems Management Group (ASMG) – addressed the European Union (EU) Parliament's need for a *data security* and *breach notification* Privacy-enhancing technology (PET). This topic,

[38] Source: "Top 10 operational impacts of the GDPR: Part 1 – data security and breach notification," by Rita Heimes, Critical Infrastructure Protection Program -CIPP / US, dated Jan. 6, 2016, p. 2.

[39] This section relies upon a *call-up* from the European Parliament of the European Union (EU) *Horizon 2020 Programme 2016-2017* 'call for proposals / technology demonstrators' to fulfill the mandate of the GDPR. Citation: HORIZON 2020 - Work Programme 2016 – 2017 "Secure societies – Protecting freedom and security of Europe" [/Page 76]. Call-up #: DS-08-2017: Cybersecurity *privacy-protection-pilots* PPP: Privacy, Data Protection, Digital Identities. See: *Ibid*., [Foot Note # *40, 42*].

ASMG determined, was something which was situated explicitly within ASMG's wheelhouse. We set out to find a corporate partner at a critical juncture, in which an ASMG senior staff member was on assignment as an employee with a Netherlands-based design engineering consultancy major.

ASMG, and this EU-domiciled design/engineering consultancy major, hoped to jointly submit the Technology Demonstrator Project Proposal for Privacy-enhancing technologies (PETs) to address *data security and breach notification* specifically. To successfully acquire funding under the EU Parliament's Horizon 2020 / GDPR Privacy-enabling technology (PET) enhancements[40] programme, ASMG authored the solution *design document*, called "ABCs of the ISS: A Technical Deep Drill (Dated April 2017)," answering all *mandatory* requirements (and then some). ASMG were enthusiastic to proceed, as the Netherlands-based design/engineering consultancy major, an EU-domiciled Company, were a prerequisite participant to substantiate our European content, to match the EU Parliament's rigorous screening process.

The Netherlands-based design/engineering consultancy major – provided with this comprehensive design document, "ABCs of the ISS: A Technical Deep Drill (Dated April 2017)," authored by ASMG – answered all *mandatory* requirements (and then some). Unfortunately, the design/engineering consultancy major pulled out at the last minute. When this Netherlands-based design/engineering consultancy major *demurred* in their participation, this left ASMG adrift, without a major EU-based corporate champion to join us in this pursuit, and subsequently ASMG were *disqualified* from proceeding.

This section of our Submission to the ACPR Team will summarize – in a *hypothetical* or prospective manner – what the EU Parliament's Horizon 2020 funding programme *missed out* evaluating, by not being in receipt of ASMG's data-centric security (DCS) solution. Not coincidentally, much of the technical merits of ASMG's data-centric security (DCS) solution –

profiled in the section of this document which appears *next* – meets in *totality*, the three directions requiring further ML modeling / AI attention identified by Papernot (2018): a) ML model assurance / admission control; b) audit ML (via 'open platform / secure platform') solutions, and; c) the "need" for formal identities / security / privacy protections (*a.k.a.* for – i) /Users; ii) /citizens; and/or iii) /banking Service Customers.[41]

[40] See: DS-08-2017 "Privacy, Data Protection and Digital Identities," Horizon 2020 Work Programme 2016-2017 'Secure societies – protecting freedom and security of Europe' [/Page 76]. NB: This Document appears as Appendix A.

[41] ACPR (Page 28) state that ML security – and the flows of an ML model, and the means to remedy (secure) those ML model flows – are "beyond the scope of our (ACPR) Report." ASMG find this observation wanting. The data-centric security (DCS) paradigm alleviates AI risk and offers mitigations (risk and compliance) assurance techniques which address: ML model susceptibility; underlying data contextual issues (semantics), and: provides *predictive* "decisioning" sought by ML modeling *predictive* outputs, collected (/collated) from multiple *decisioning* points across the enterprise.

The "Privacy, Data Protection and Digital Identities" funding opportunity or call-up (*hypothetically* responded to) presented *herein* – [Dated: April 2017 'Horizon 2020' proposal] – covered a big wish-list of items, identified as project "mandatories." They include (in point form – with [ASMG's prospective] response to each mandatory – with a few mandatories skipped in this discussion, as non-compliant with the stated purpose of achieving ML security (at the heart of this Submission)[42]:

1)– privacy violations caused by search engine identity exposures.

Search engine identity exposure is something which is so ubiquitous. It is almost impossible to get a handle on. Web 2.0 – the participative social web – involves Google, Facebook (and others) harvesting our information simply by the fact we deploy their search engines.

When we use a web search engine "tool", our information is harvested via such topics as:

1. Podcasting
2. Blogging
3. Tagging (our downloading information)
4. Curating with RSS (*really-simple-syndication* [a.k.a.] the converters data harvesters deploy)
5. Social bookmarking (Facebook, Google etc.)
6. Social networking (Facebook, Google etc.)
7. Social media
8. Web content voting

[42] ASMG met all mandatories in our 'hypothetical/prospective' proposal. To streamline this discussion, the following *mandatories* are deemed, today, less relevant (/irrelevant) for the purposes of concisely addressing the 'issue' of privacy, data protection, and digital identities covered by our Privacy-Enhancing Technology (PET), the DCS solution. They are: i) public eIDs (electronic identities); ii) 'not exposing user information any-more-than-necessary' (irrelevant, as the DCS IEPPV does not expose user information to the wrong/unauthorized parties, period; iii) the PET proposed solution should be cost-effective (this is set aside, for now. How do you cost the full (/radical) elimination of cyberthreats, in an economic sense?); iv) deploy comprehensive/consistent [privacy] risk management frameworks/RMFs – an issue of importance to network-centric security solution providers, protecting data at the level of the [data] *packet* – less consequential (but may still be deployed) since ASMG's data-centric security (DCS) offering addresses the entire data element securely; v) leverage existing eID / authentication platform(s) and/or services, with clearly defined interfaces. NB: ASMG DCS secures the data in a defense-in-depth manner [meaning] sure – secure the interfaces – (/non-essential, given DCS is a more comprehensive security solution); vi) offer "qualified anonymity/pseudonymization (/not required, given the IEPPV's comprehensive reach), and; vii) demonstrate *up to* Tech Readiness Level (TRL) 6 to 7: ASMG's data-centric security (DCS) solution meets an even higher securitization / accreditation standard. This is the certification and authorization (C&A) security assurance coverage at Common Criteria EAL 3 level, via NSA Labeled Security, protection Profile (version 1b). This EAL3 standing covers secure Functional Requirements for Audit, User data Protection, Identification and Authentication, Security management and Protection-of-the-Target (TOE) *plus* Cryptographic Support. See: https://www.ncsc.gov.nittf/docs/CNSSI-4009_National_Information_Assurance.pdf.

These (listed) activities are where Google, Facebook *etc.* are prolific in their pursuit of web content mining, and poaching of our private identities. Merely by our action (/or activity) of logging onto their web platform, we have acted in a consensual manner, acknowledging that these search engine web players are entitled to profit from the harvesting of our personal identifiers, and our social (network) footprints.

With Web 3.0 – the semantic web – Web 3.0 necessitates using a declarative ontological language, like OWL, to produce domain-specific ontologies that [Google, Facebook *etc*.] machines use to reason about information, and make *new* conclusions, adding a more massive sophistication and analytic complexity that surpasses the social web's narrowly defined keyword searching / matching efforts. The cloud service providers (CSPs – Amazon, Google and Microsoft Azure, to name the 'big three' players in the data hosting space – the first two firms *identified* also occupying coveted real-estate in the search engine *space*) *hold* user status over Customer data, called "state."

By holding the rights to data and information *state*, these monolithic information and technology industry giants hold the value that is/(was) created on the web, by the billions of subscribers which search web content daily. *State* tracking is an essential element of a system. In a cloud implementation of services, you require 'state' to become a system. That is the definition of a *stateful* system. Advanced Systems Management Group (ASMG) would argue you need the Information Exchange Framework (IEF) Reference Architecture's (RA's) full complement of resources (or an equivalent set of infrastructure resources) to make *stateful* systems work to their information security advantage, across disparate software environments, which argues favourably for deploying the data-centric security (DCS) solution.

A more recent development at the Object Management Group (OMG) is the creation of a Working Group (WG) to address the Digital Twins *domain* (OMG Quarterly on-line meeting, streamed June 21- 2x, 2020). This effort, from ASMG's perspective, is re-inventing the 'systems-of-systems' approach, which will link objects to keep track of 'states'. This is, of course, an effort to tie the objects so they are not independent objects anymore. Since the interpretation of a digital twin object's 'message' is dependent on the *state* of its source, if you get the wrong result, it could lead to unintended (not bargained for) results. For example, Is the 'state' object friendly (or hostile?)? Is the plane landing (or attacking?) etc. etc. Advanced Systems Management Group's (ASMG's) coverage of this topic – addressing search engine identity exposures caused by search engine identity exposures – would have been historically-rooted, in its answer to this mandatory requirement. ASMG's *prospective* (GDPR) PET submission would suggest that had a data-centric security platform existed (or had it been introduced 'at any time' during the Web's gestation (/genesis) developmental period), data would be tracked. Sounds obvious in retrospect, but this point is still not registering widely enough, across the Internet, or within the ICT community today.

2)– responsible information sharing.

In the pre-2013 time-frame, data subject-matter-experts realized that to properly secure the data lake, data assembly functions governing 'secure data stores' required their own specialized vocabulary. This vocabulary, based on Model Driven Architecture (MDA) design principles, possessed the inherent strength to support the serialization of packaging and processing (data) models. These Model Driven

Architecture (MDA)-derived constructs are termed the Information Exchange Packaging Policy Vocabulary (IEPPV).[43]

The data sharing environment we are now articulating replaces the shortcomings of the previous data sharing, legacy-based ETL environment, in which "Traditional" data and information exchange practices (and their assigned vocabularies) singularly failed to adapt to the increases in operational tempo and the dynamics of real-world events. Today's fast-paced information exchange environment demands Responsible Information Sharing. Responsible Information Sharing is a term which means having the maximum allowable data awareness and data management capabilities at your disposal. It is all-encompassing, in that: law, regulation and policy e.g. '*policy as-a-community'* and agency e.g. 'policy-execution *strategy and direction*' are captured at the level of granularity required to empower real-world information access / exchange in real-time – a.k.a. virtual – information exchange conditions. Responsible Information Sharing[44], also, must prove to be fully accessible and accountable to all users and partners.[45]

3)– protecting *online* identities from malevolent cyberthreat actors, both in the public and private sphere.

The ACPR workshop titled 'Probability of Default' (Page 54 / *text* reproduced in full) states: "The solution offered by the consulting firm is not an off-the-shelf product operating as a black box, but a toolbox which enables to design and build a model while maintaining a constant interaction between the solution provider and the customer. In practice, the resulting model is a hybrid one, partly based on advanced ML algorithms during the design phase but then translated into simple and explainable algorithms for the deployment phase. This choice appears to have been motivated by the necessity to

deliver a well-documented model, along with an audit track." Continuing, "The solution as currently available is designed to support credit scoring and probability of default models, however the solution provider is working on applying a similar approach to internal risk models, namely leveraging ML to yield corrections and improvements to currently used models in the form of business rules."

[43] Model Driven Architecture (MDA) provides the transformational ability to serialize [data] models as interface code or policy / rules languages, that can be executed by multiple services (i.e. decision and enforcement points) or platforms. See *Ibid*., [Foot Note # *25*]. Page 6. See *also*: "ABC's of the ISS Solution: A Technical Deep Drill," by James Carter, ASMG Dated April 2017, Page 8. (This publication is available upon *request*).

[44] Responsible Information Sharing seeks to introduce a systematic process for translating information sharing and safeguarding via policy instruments (e.g. legislation, regulation, policy and service level agreements) into a machine consumable form, that can be automated in the operational (/runtime) environment. This specification (IEPPV) offers one option to model users, a model -based transformation using the UML Profile (See: IEPPV OMG Document Number: MARS/2013-12-05; Annex C) [which] model's user policy in a manner that aligns the policy to the specification data environment. The IEPPV UML profile is used to define permissible patterns for assembling data and information elements into releasable datasets that conform to the originating policy. These policy models can then be transformed into a serialized form that is machine consumable and automated by platform specific implementations of policy decision and enforcement points and accountable to all users and partners. See *also*: *Ibid*., [Foot Note # *25* – full *citation*].

[45] Source: *Ibid*., [Foot Note # *25* – *original* ASMG IEPPV *citation*]; Page G-5.

ASMG finds this workshop summary could be potentially setting up ACPR to bear witness to a theatre ripe for cyberthreat attacks. Why? Papernot (2018) reviews *federated learning*, which section 8.4 is touching upon, as (Papernot / 2019 states), more ideally suited for a more specific solution to cryptographic research classification research (Saltzer and Schroeder's taxonomies), under the guise of the 'separation of privilege'. The *separation of privilege* is very applicable to ML, in the case of distributed settings for ML. One prominent framework implementing this 'separation of privilege' is *federated learning*, where rather than collecting data centrally, the ML modeling is built by having client compute model updates (performed) individually, on their own data, and then aggregating these local updates *only*.[46] Papernot (2018) continues by stating: "One can possibly involve multiple parties to separate privileges (e.g., by having more than one entity responsible for shuffling data, before it is analyzed by a third party). In a completely different threat model, one could also envision using an ensemble of models trained on independent data pipelines (in order) to reduce one's exposure to (cyberthreat) poisoning attacks."[47]

NB: This *next* section of ASMG's *hypothetical* (GDPR) PET programme submission, reproduces (in its entirety) *earlier* text (appearing in this ASMG Submission to the ACPR). This text answers the (GDPR) PET programme *mandatory* requirement, (that the PET demonstrator technology) 'protect *online* identities from malevolent cyberthreat actors, both in the public and private sphere,' as follows:

One point Papernot (2018) addresses is very important to this discussion "re: protecting *online* identities from malevolent cyberthreat actors, both public and private sphere"[48] This should lead us to consider a point made by the Financial Stability Board (FSB). The FSB asks us to consider "Where financial institutions rely on third-party providers of AI and machine learning services for critical functions, specified instructions or directives on dealing with *outsourcing* (Third Party relationships and contracts) may not be in place, or not be understood. These outsourcing services / providers may *not* be subject to supervision and oversight. Similarly, if providers of such tools begin providing financial services to institutional or retail clients, this could entail financial activities taking place outside of the regulatory perimeter.[49]"

Advanced Systems Management Group (ASMG) believe the follow-up questions to this should be to ask: When employing Third Party / Outsourcing options, how do financial institutions exercise the removal (where possible) of incorrect data handling and data monitoring? What are the appropriate evaluations of risk associated with internal control malfunctions? And, thirdly, how is ML model validation – through audit operations discovery efforts – to be ensured to exercise the 'precise' context (/understanding) of (an) algorithm? For example, has the ML algorithm tool / toolkit been extensively documented, a.k.a. –

How was it pre-designed / -designed / tested? – What are its operational parameters, functions, effectiveness? And; – What Q&A *follow-up* is *designed-in* (to the ML algorithm tool / toolkit), and is this monitored and reported on to all parties involved? Foremost to all three of these issues, as well, should be to question answered: How does (the financial institution) evaluate the business processes into

[46] Source: H. Brendan McMahan, E. Moore et. al. "Communication-efficient learning of deep networks from decentralized data." See: arXiv:1602.05629, (2016). Quoted in (See): https://www.groundai.com/project/a-marauders-map-of-security-and-privacy-in-machine-learning/1.

[47] See: *Ibid*., [Foot Note # *5*], Page 6-7 – 'separation of privilege.'

[48] See: *Ibid*., [Foot Note # *3, 31*] Page 33 – 'Third Party AI suppliers/providers outside regulatory perimeter'.

[49] See: *Ibid*., [Foot Note # *48*].

which it (the ML model algorithm) is integrated, or which are impacted by it (the ML model algorithm) in-*one-way-or-another*?

This entire discussion is aided and abetted by what Papernot (2018) reviews as 'complete mediation' (taken from Saltzer and Schroeder's cryptographic research classification taxonomies). Complete mediation' requires every access to every object must be checked for authority. This is relevant to ML security in several ways. Papernot (2018): "First from a confidentiality and privacy standpoint, it is key to enforce access control to the model and its predictions. The model itself may constitute a *channel* for more elaborate attacks that recover sensitive information analyzed by the model during training. Or, the defender may be unable to verify test data (provenance), as an attacker may have exposed the model (test or training data sets) to poisoning, evasion or privacy attacks. This may lead to data that is *compromised*, or may even be *substituted*, and may not originate from the 'distribution of interest' which the defender believes it to be sourced from.

4)– PET (Privacy-enhancing Technologies) – ASMG's data-centric security (DCS) solution – [be] available with usability, accessibility and safeguarding features 'designed-in'.

This section of the *hypothetical* PET Technology Demonstrator proposal would summarize *all* features of the ASMG data-centric solution (DCS).[50]

Bringing this topic to a greater level of non-compromise (i.e. covering all ML modeling data), Papernot (2018) reviews ML modeling in the vein of its addressing *useable, accessible* and *safeguarding '*designed-in' features – via his assessment of ML security – under the topic 'psychological acceptability.' In short, it is particularly relevant for ML security (especially with deep neural network models) to employ *ease-of-use* human interfaces, to allow users to routinely – i.e. *accessibly* – and automatically, apply protection mechanisms correctly. ASMG's data-centric security's (DCS's) IEPPV takes the guess work out of this equation, since the IEPPV *always* presents data as a 'one-source-version-of-truthiness.' This directly translates into pronounced 'psychological acceptability' of security and privacy associated with 'data' – exchanged and safeguarded via the Information Exchange Framework (IEF) Reference Architecture's (RA's)] IEPPV – in a significantly enhanced manner, then any/all methods which have been used up until now. This does not mean the ML algorithm *creates* outputs any more accurately, but at least the data it (the ML model algorithm) is working with can withstand the test of rejecting inputs manipulated by adversaries, as the modeler can 'see' in advance that the data audit did not signify the presence of a confirmed IEPPV- generated data store / data set *relic* in the first place.

5)– Open source and externally auditable.

[50] Profiled in the *next* section of this Submission.

Papernot (2018) reviews this topic under 'open design.' Papernot (2018) states: "the design of security mechanisms should not be secret." This more than adequately summarizes the goal of Advanced Systems Management Group's (ASMG's) data-centric security (DCS) IEPPV. Although with one important

distinction. ASMG believes all data should be fully auditable (and recoverable) while access to data modeling outputs, training sets and test data sets should absolutely remain secret, or furtively protected! The ASMG data-centric security (DCS) solution maximizes data uptake, and instills 'trust' in data, *always*. It also proves that no unnecessary information is being collected, as determined by a very precise data audit trail.

Owners of information are just that: owners of data. This is not a rhetorical statement. Third parties, as we stated once before[51], whether they are computer integrators, telecommunications providers or application vendors (i.e. hardware / middleware or software products / service suppliers), all too commonly insert themselves into the data management process wherein their presence is not always advised. Historically, allowing third parties to handle data may have occurred out of a recognition that the third party possesses a means (or tools) to assist in data management, or likewise for data collections, data transformation and / or data storage services. In today's knowledge-based economy, corporate success can only be attained when information and technology, used for business, is mandated to be secure, accurate and reliable.[52] Data communication, transport, and retention services should be community –and consensus– building in their focus. We almost fool ourselves into thinking this is happening in an innocuous manner today. This is simply not so.

6)– leverage identity-based solutions.

ASMG proposed to answer this section by first highlighting the shortcomings of network-centric (and Application-centric) *gating*, which has been profiled once already.[53]

Now for data residency. The ASMG DCS solution, at its very core, maps the complete data life-cycle. In other words, networks (and Applications) provide a road of travel, but do not provide sign posts along the way, pointing out exactly where a data asset 'sits' at any point in time, unless and/or until the receiver of the data asset signals having received the data asset in question. In the pre-information sharing and safeguarding (ISS – what data-centric security/DCS was called pre-2013) era, the data incidence tracking report was oftentimes a mystery. In the case of ASMG's data-centric security (DCS)

[51] See: *Ibid*., [Foot Note # *23*]. The example of GE was made an explanation of a major corporation seeking to deny third party software providers from 'ruling-their-roost'. GE may not have fared too well, economically, in the meantime, but their *Predix* software product is still surviving, albeit only for internal corporate use.

[52] Regarding legal liability, there may be questions on the allocation of responsibility among suppliers, operators and users of AI and machine learning systems – for example the responsibility of a manufacturer or distributor of a financial product that is based on third party data input devices or algorithms. See [several *citations*]: U.S. Federal Trade Commission Report, January (2016), "Big Data: A tool for Inclusion or Exclusion?" January, Page 1; EBA, EIOPA and ESMA (2016), "European Joint Committee Discussion Paper on the Use of Big Data by Financial Institutions," JC 2016 86, Page 7.

[53] See: *Ibid*., [Foot Note # *23*], Page 1 – 'network-centric security paradigm [data *gating*]'. See *also*: *Ibid*., [Foot Note # *26*], paragraph on Page 7 of this submission – *a.k.a.* providing ASMG's analysis of 'Application-centric security paradigm [data *gating*]'.

solution environment, incidence tracking reports – *a.k.a.* monitoring data / metadata resources in real-time (or near real-time) – are not 'known unknowns', ever.

This does lead, invariably, to an examination of issues and practices related to the location of data – e.g. data residency – wherein data may move, or be transported, across physical and geographical

jurisdictions. This may cause some to reflect on the *sovereignty* of that data, claimed by which jurisdictional authority, a topic partially (but significantly) addressed by XACML (eXtensible Access Control Markup Language). XACML is a standard that addresses access control, including (by its provisioning of): a policy language, and an innate "architectural" ability, through its taxonomically-mapped reference terminology, to define (/reflect) 'data/metadata' *processing* behavior. The Information Exchange Framework's (IEF's) IEPPV ontology and taxonomy directives *leverage* XACML. For more on this topic – XACML architecturally leveraging identity-based solutions – *see* these foot note citations.[54]

7)– reduce identity fraud / protecting citizen's privacy.

The Object Management Group's (OMG's) Command, Control, Communication, Computers and Intelligence (C4I) Task Force started an effort in 2007 towards drafting a specification for Data Tagging and Labelling for Security and Privacy. A Request for Information (RFI) was issued in 2007, and a Request for Proposals (RFP) in 2010.[55] The effort was suspended, but is now being revived (circa 2017) due to strong interest from several military organizations. This data tagging and labeling for security and privacy specification is now fully developed, in today's *current* IEPPV data-centric security (DCS) solution (2020).

In short, the Data Tagging and Labelling for Security and Privacy *functionality* is as comprehensive a protection for identities, and citizen privacy, as could be deemed a necessary, or an essential necessity. This approach allows: 1) data tracking ii) data versatility (monitoring), and; iii) specified parameters for tagging / labeling data *semantically*, wherever that data resides. More and more, ASMG's Clients are

[54] Data residency is the set of issues and practices related to the location of data and metadata, the movement of data (/metadata) across geographies and jurisdictions, and the protection of that data (/metadata) against unintended access and other location- related issues. Source: "Data Residency Challenges and Opportunities for Standardization." By Claude Baudoin, (Editor) et. al. OMG Document Number; MARS/2017-03-22; published by OMG Middleware And Related Services (MARS) Platform Task Multiple experts are addressing the data residency issue: 1) *Ibid*., [previous Foot Note] Page 4. Source: 2) "Data residency and the Public Cloud: Why We care and Techniques to Think About," By Evelyn De Souza, Wired Innovation Insights publication, August 2014. See: http://insights.wired.com/profiles/blogs/data-residency-and-public-cloud-why-we-care-and-techniques-to#axzz4KFEadsGr. Source: 3) Meeting Data Residency and Compliance Challenges [Company spokesperson unattributed], Hewlett Packard Enterprises. See: www.hpe.com/h20195/V2/getpdf.aspx/4AA6-0217ENN.pdf. Source: 4) "Data Residency and Legal Questions," By B. K. Winstead, ITPro Windows, Dated July 2011. See: http://windowsitpro.com/blog/data-residency- and-legal-questions-about-cloud. Dated: March 3, 2017; Page 4.

[55] Source: 1) Object Management Group: "Data Tagging and Labeling for Security and Privacy RFI." OMG document omg/07- 09-04, September 2007. Secondly, 2) Object Management Group: "Data Tagging and Labeling for Security and Privacy RFI." OMG document omg/07-09-04, September 2007. www.omg.org/cgi-bin/doc?omg/07-09-04.pdf.

requiring data security / data compliance and accreditation (C&A) letters *be issued* (to them) before they respond with a Standing Offer Agreement (SOA) and/or Project purchase order.[56]

8)– Extended impacts (3): i) support for fundamental rights in a Digital Society; ii) increased 'trust' (in EU's Digital Single market), and; iii) increased use of 'privacy-by-design'.

The first two points are self-evident. The third *privacy-by-design* is a vastly over-hyped, and fundamentally over-rated concept, and essentially, is a prescriptive which serves in name – more than in practice – to be largely ineffectual to properly assess. Personal Identity (pID) management, and the protection of security and privacy, is already fully *baked-in* to ASMG's data-centric security (DCS) solution. Plus, big tech titans (Amazon, Google and Microsoft Azure as CSP's, and Facebook and Google – the latter two being [also] – web search conglomerates), and their peers, are already in possession of advanced filtering to capture private user data. If their data sources had encountered DCS decisioning, "before they drew data into – e.g. populated – their massive data libraries / data repositories / data lakes," their cartelization of data may have been resisted, or at least significantly monitored, for the benefit of public and private users and constituencies alike.

9)– The Following Topic did not appear in the call-up documentation, but ASMG would have addressed it (regardless): data protection embedded or rooted in data governance.

This is an important issue, and significant more-so, since the GDPR leaves technology solutions strategies, and technology implementations, somewhat muddy and *unclear*. If data governance is described (or defined) from a network-centric 'technical interoperability' paradigm /perspective, as advocated by the *status quo* thinking of the global IT/IM community – the Information Communications Technology (ICT) sector at present – then our use and adaptation of technology to clear-up failings in *data security* and *breach notification* Privacy-enhancing technologies (PETs) will always come up short. On the other hand, if GDPR installations or implementations address *data security* and *breach notification* Privacy-enhancing technologies (PETs) from the data-centric security (DCS) perspective / paradigm,[57] it is probable, not just possible, that data protection will be fully embedded, or *rooted*, in data governance.

---

[56] Issues which may trouble us further, may include the specter that data retrieval actions and activities may involve: a) industrial spying by a foreign company or a foreign government, or; b) may expose data resources to have their sensitive details *exposed*, and may cause unintended consequences, both financial and legal / regulatory, and; c) may precipitate a pre-emptive strike by a foreign government – a.k.a. 'Country B' may demand they have (supplied to their border policing authorities) secret keys to decrypt the data resource *in question*, and this may even happen while the Enterprise's "data custodian / consultant" sits haplessly by, in an airport lounge in 'Country B', waiting to border a plane to leave the country, while this whole *scenario* unfolds. See also: *Ibid*., [Foot Note # *4, 24*], Papernot's (2018) discussion 'separation of privilege'.

[57] Source: http://www.datacentricmanifesto.org/signatories/.

A grass roots movement called the "data-centric manifesto" has – as of Friday June 19, 2020 – produced 807 signatories subscribing to the concept that data needs to be protected and secured.[58] One of the clearest statements in the *data centric manifesto* participants' testimonials' posted at the data-centric manifesto.org site – pertinent to our examination of automation (ML) – is expressed by Peter Winstanley, Director (Semantechs Consulting Ltd., [*signatory* # 556 of 807 signatories] whom stated: "For automation instances, data is centralized, and it's *meaning* and/or *context* must be known. That *context* is self-described, by the data itself. The data-centric approach is particularly essential when it comes to automation. Data without context is meaningless. Data that is inaccessible creates lost opportunity, and an economic hardship."

Data-Centric Security (DCS)

The accurate explanation for the content appearing in this *final* section of our Submission, might more accurately be titled: "Data-Centric Security (DCS) by ASMG: Exercising User Rights via an Architected Solution."

An *executive summary*, capturing this in one paragraph, is presented here:

Advanced Systems Management Group (ASMG) have worked diligently to create a commonly understood vocabulary to underscore information sharing via decision-level 'rules-sets' based on UML[59] (however, other rules engines would also suffice) which, in the spirit of recent international cooperation and sponsorship at the standards body level, have created the

[58] See: *Ibid.,* [Foot Note # *43*] – 'signatory [# 763 of 807] "Discussion: Michael Abramson, President - Advanced Systems Management Group (ASMG) [*signatory* # 763 of 807] Made a career of seeking out a Data Centric Security Paradigm where security enforced data policy that is/was independent of the infrastructure and application, are used to share and process data. This has resulted in the publication of the Information Exchange Framework (IEF) at the Object Management Group (OMG). A policy-driven data-centric solution to information sharing and safeguarding, and an open standard!"

[59] Unified Modeling Language (UML) is a graphical language for visualizing, specifying, constructing and documenting data and information artifacts for a software-intensive system. UML captures business processes and systems functions. UML makes 'concrete' things such as: programming language statements, database schemas, and specifies reusable software components.

Information Exchange Framework (IEF) Reference Architecture (RA).[60] The IEF RA, championed by the Object Management Group (OMG), is exploring this reference architecture as a very effective means to support structured information exchange in the coordinated, non-proprietary environment, supportive of (all) previous standardization efforts and, providing an optimal path to integrate multiple domain standardization efforts, Also, The IEF RA provides a common approach to specifying information interaction in a structured policy-based approach.

This approach, providing as it does a holistic framework for *policy*[61] definition, addresses effectively and concisely an open, yet fully integrated, use of AI capabilities. ASMG can demonstrate that data centric security, via decision-level rules-sets, will deter the onset of cyber security attacks, by significantly abating cybersecurity threat vectors, stopping them (or at least frustrating their planned release) before nefarious damage can be accomplished.[62]

This Executive Summary (*above* paragraph) contains the *crux* of what ails privacy and data protection today. As we have just learned, by reviewing the presentation by the European Union Agency for Network and Information Security (ENISA/2014), interoperability [ENISA would have us believe] has not been sufficiently addressed in a *standardization* context.[63] This is an *incorrect* conclusion. More importantly, as the more accurate title for this section of our Submission alleges, "Data-Centric Security (DCS) by ASMG: Exercising User Rights via an Architected Solution," requires an entirely different paradigm to achieve the Exercise of Users' Rights over their *privacy* and *data protection* efforts. This protection is encapsulated in the architected solution we will unpack here.

---

[60] The Information Exchange Framework (IEF) Reference Architecture (RA) presents (/codifies) the commonly understood vocabularies underpinning the ASMG-led data-centric solution (DCS), as ratified by the international standards body the Object Management Group (OMG – see omg.org). The Reference Architecture (RA) provides a full unmasking of structured policy-based information exchange(s) – highlighting its importance to Machine Learning models and AI – constituting a fully implemented policy-driven, data-centric solution to information sharing and safeguarding, and an open standard.

[61] A *policy* is a definitive course or method of action selected from among alternatives and follows given conditions to guide and determine present and future decisions. (Source: Information Exchange Framework (IEF) Final Revised Submission (FRS), See: OMG Document Number: MARS/2017-02-21; p. 315). Policy Driven refers to a process involving formal documents describing a plan of action (Policy_Instrument) translated into machine readable rules (/instructions) and enforced by software services and systems. This process results in full traceability from Policy_Instrument to instrumentation (policy decisions and enforcement points). (Source: Ibid., [*above* Foot Note] p. 316). Note to Reader: We will drop the Information Exchange Policy-based Packaging Vocabulary (IEPPV) *insignia* or *acronym*, when identifying ISS [and/or DCS] components (/units) – to spell-out the IEF RA's "elements", throughout the remainder of this Report. This naming convention will imply referral to the IEPPV, in all cases. See: [Foot Note # 43], Page 7. (This publication is available upon *request*).

[62] This is proven today via NATO Coalition Warrior Interoperability eXchange (CWIX) initiatives, and contracted activities sponsored by Department of National Defence (DND) Canada. Source: Michael Abramson, Special Advisor on Public Safety/ Security - Open Interoperability Standards to the Centre for Security Sciences (CSS – Department of National Defence/DND Canada); Co-Chair C4I Domain Task Force at OMG; Chair Emergency, Crisis and Major Event Management SIG, Chair Information Exchange Framework (IEF) WG (OMG); and Information Sharing and Protection Standards Development Principal *author*.

[63] See: *Ibid*., [Foot Note # *24*], Page iv. See *also*: *Ibid*., [Foot Note 22 – original ENISA *citation*].

What we are examining (herein) is the solution capability which falls under Advanced Systems Management Group's (ASMG's) data centric security (DCS) umbrella. For over two decades – now entering a fifth generation of product conceptualization / product refinement – ASMG's data centric security (DCS) solution has now reached a commercialization footprint. That commercialization footprint has been dramatically reduced in size, to a compact one (1) Mega-byte of operational code, which may now be inserted wherever the need for industrial strength, defense-in-depth information sharing and safeguarding is required.

Advanced Systems Management Group (ASMG) have remained true to the open standards ratification effort journey the Company has undertaken, fully documented at omg.org.

Advanced Systems Management Group's (ASMG's) data centric solution (DCS) employs reusable patterns in unified modelling language (UML)[64], globally prescribed to insert a protective data interface layer everywhere data is accessed, or at least everywhere there is an Open API requirement. We could do this as the data is created by applications (thick or thin, rich or basic), either using the application itself, or by using an agent (client-side), that profiles the data prior to storage or transmission. The extent of that implementation, and the products used to implement it, we are absolving from an IT governance issue, into an implementation issue. This Report is intended to show that the means to implement this at the Enterprise level can be achieved based on existing and evolving Open Standards.

Protection needs to be applied, either as security attribution attached to the information objects in the files and data sets which Users depend upon, and / or there needs to be a protective layer to apply such attribution, and afford the protection required, when the information is accessed. At the outset, this invariably means that User(s) understand the specified content and context of the information asset itself.

ASMG offers, via information sharing and safeguarding (ISS) – now commonly referred to as the data-centric security (DCS) solution – what we call a specific 'commonly understood vocabulary' for decisioning, which would inclusively cover AI and machine learning (ML). This *decisioning* capability is offered via UML modeling, with many advanced features which secure data assets at their source. This information sharing and safeguarding vocabulary – or toolkit – is called the Information Exchange Policy-based Packaging Vocabulary (IEPPV). The IEPPV was modeled using UML, coupled with a profile that implements the Ontology Definition Metamodel (ODM)

[64] Unified Modeling Language (UML) is, indeed, a graphical language for visualizing, specifying, constructing and documenting data and information artifacts of a software-intensive system. UML captures business processes and systems functions: makes 'concrete' things such as programming language statements, database schemas, and specifies reusable software components. See: *Ibid*., [Foot Note # *25*], Page A-10. See *also*: "ABC's of the ISS Solution: A Technical Deep Drill," by James Carter, ASMG Dated April 2017, Page 10, 8. (This publication is available upon *request*).

profiles for the Resource Description Framework (RDF) and OWL,[65] and generates the RDF/XML artifacts as OWL 2.0 -compliant documents.

OWL tools – and their resulting ontologies[66] – allow users and data administrators to employ the reasoning application to analyze and validate the rules (composite policies) initiating messages within the Operational environment. The operational environment is multi-focal, but allows data management to be reviewed via an audit trail. This tamper-proof audit trail includes the capability to identify conflicting rules, or combinations of rule sets that may have been developed separately from one another. In these situations, privacy or security considerations may have been breached. The overall effect of the Information Exchange Framework (IEF) and IEPPV adoption may be to spawn the development of analytical and business intelligence tools and services with depth and breadth, including (but not limited to):

-Governance and Stewardship
-Certification & Accreditation (C&A)
-Threat Risk Assessment (TRA)
-Statement of Sensitivity (SoS)
-Modeling & Simulation (M&S)
-Pre – and Post –Mission Scenario Analysis, and;
-Design and Operational Audits (e.g. Security).[67]

Model Driven Architecture (MDA) provides the transformational ability to serialize [data] models as either interface code, or policy/rules languages, that can be executed by multiple services "decision" and "enforcement" points (and/or platforms).[68]

[65] The combination of Ontology Definition Metamodel (ODM) –based visualization, and OWL 2.0 reasoning support, solidified by the high-quality, logically consistent ontology product which the IEPPV represents, is *key*. The Ontology Definition Metamodel (ODM) is cited as an integral part of Model Driven Architecture (MDA) advances / transformations used to generate the OWL language implementation of the IEPPV. The ODM is provided as a separate machine readable file – See specification manifest. See: *Ibid*., [Foot Note # *25 – original* ASMG IEPPV *citation*]. Plus, [all published *specification* manifests]; Annex C – UML Profile; Page A-6 and Page A-8. See *also*: "ABC's of the ISS Solution: A Technical Deep Drill," by James Carter, ASMG Dated April 2017, Page 10 (*plus* Foot Note # *26* in the 'ABC's Report,' Page 8. [NB: This publication is available upon *request*].

[66] The resulting ontologies have been tested using the W3C RDF Validators, and several OWL-DL compliant reasoning tools. Metadata developed for the IEPPV utilizes OMG Architecture Board *metadata* specification(s) available at: http://www.omg.org/techprocess/AB/SM/20120614/SpecificationMetadata.owl.

[67] See: *Ibid*., [Foot Note # *25 – original* ASMG IEPPV *citation*], Page 8.

[68] See: *Ibid*., [Foot Note # *25*], Page 6.

What we are describing, essentially a repeat of what we have stated once already,[69] is the interoperability condition *per se.* Information interoperability, in the data-centric security *paradigm* sense of the term. This meets the requirement to enable information integration, handle machine learning (ML) algorithm analytics *outputs* as decisioning information data sets, *plus* addresses algorithmic test data, training data and data 'outputs' supplied from inference engines, through search efforts (knowledge discovery), and/or for data extraction compiled from federated information libraries or 'other' source materials.

All types of data, whether structured, unstructured, or sourced as *new* data, whether it is passive or active, subject to flat, horizontally scalable database structures, and processed by real-time query tools (as opposed to delineated snapshots), or other more advanced data analytic processing techniques, serves to enhance our physical, cognitive, and decision-making capabilities.

Data is transmitted in a huge number of packaging formats, including: diverse, maybe schema-less formats, unstructured, distributed (in an architected context), aggregated (from a variety of content sources), structured, geospatially-oriented, and even in unstructured data formats. Unstructured data includes: news feeds, marketing and 'markets', shipping information, to name but a few data feeds and data sources, causing all manner of data processing head-aches, in corporations, and governments, alike.

As was mentioned earlier, we covered the topic of data *gating* – 'gated' data is data left orphaned in inaccessible data repositories (and application) stove-pipes. Secondly, we have already mentioned the problem arising when information vocabulary *instances* –micro-managed by ETL (Extract, Transfer and Load) tools – are left in partitioned (or segregated) fashion, leaving an incomplete picture of what a data set or data element constitutes. Both these data management occurrences further deprive (and/or distance) the end-user from accessing the data and information they require. Static state data repositories serve no useful purpose! Something needs to be done to relieve the IT/IM community of these woefully inflexible data storage conditions, and needs to be done now, not at some distant point in the future. Why? As cyberthreats continue to advance, unabated and/or undetected, data is left in an increasingly vulnerable state, and is largely unprotected! What Advanced Systems Management Group (ASMG) argues we need is a '*secure*' data-centric environment, requesting the packaging (assembling and formatting) of information element(s), and the inverse processing of received messages (and data sets), as a *mandatory* minimum requirement, always.[70]

This is achieved with Unified Modeling Language (UML) specifications which, in this instance, refers to a profile in the Unified Modeling Language (UML) providing a generic extension

[69] See: *Ibid*., [foot note # *5*] Page 8, 9 – 'complete mediation' (a.k.a. training points to predict data poisoning). And, re-quoted [Foot Note # 18] – plus text appearing *below* this [Foot Note # 18] *citation*.
[70] See: *Ibid*., [Foot Note # *25* – *original* ASMG IEPPV *citation*], Page 6.

mechanism for customizing UML models, for user domains and platforms, alike. Extension mechanisms allow IT/IM practitioners to refine standard semantics in a strictly additive manner, preventing (standardized data semantics and identifiable data resources) from contradicting standard semantics. Let's drill into this more deeply.

Many industries have worked hard over the last decade or two, to define shared meta-models specific to their industry, and it is these models that now from the basis for contractual information sharing across organizations and across geographic borders. A typical usage scenario of the (Sparx) Schema Composer is in the creation of message definitions (/schema) to exchange information between organizations, ensuring that such messages comply with the underlying meta-model that has been adopted by the involved parties. When information is shared between organizations, it is frequently the case that only a subset of the full meta-model is required, but it is essential that what is shared conforms precisely to the agreed meta-model. This converts a UML class to a W3C XML Schema (XSD). This [Sparx – Schema Composer] toolkit also allows Data Modelers to start working at a conceptual level in UML.[71]

A core guiding principle of the Information Exchange Policy-based Packaging Vocabulary (IEPPV) is that since it is a commonly understood vocabulary to underscore information sharing via decision-level 'rules-sets' (which the IEPPV provides), this standards-body ratified set of ontologies/vocabularies allows users to systematically express and align business policy to individual business (/operational) domains. To aid in this effort, the Object Management Group (OMG) provides the Semantics of Business Vocabulary and Business Rules (SBVR) addressing the semantic aspects and shared meanings of terms in the business domain. The syntax for this is approached via formal logical mapping. SBVR uses OMG's Meta-Object Facility (MOF) which is a 'type' system processed by the OMG's Common Object Request Broker Architecture (CORBA), which develops a set of schemas by which the structure, meaning and behaviours of objects are defined. OMG's Meta-Object Facility (MOF) creates its meta-models as UML class diagrams. A supporting standard of MOF is XMI, which defines an XML-based exchange format/ MOF/XMI mapping rules, enable generating MOF-compliant models and can be defined by XML schema. The SBVR is well suited for describing business domains and requirements, for business processes and information systems to implement business models.

We earlier mentioned[72] two critical Stakeholders (/data owners or stewards) and Operational users of data. Let's review this point once again:

[71] Source: Sparx Systems Enterprise Architect User Guide series – Schema Model 6 Version: 1.0. Dated: June 3, 2017 *online* Page 4-6.

[72] See: Text – Section titled 'Trusted Architecture base' – Page 11-12 (of this Submission).

It is entirely possible that the user of data could be from two opposing data stakeholder constituencies. The first might be Security and Privacy Officers. These Security and Privacy Officers represent data owners, data stewards and data custodians. This group have the stated goal of needing to apply defense-in-depth solutions to protect their data, which will efficiently (and quickly) exchange and receive data elements they need to perform their assigned work.

Their opposite counterpart(s) are the Operational users of data. This group are steadfast in their determination to have data via full data discovery, unhindered by any accessibility issues affecting them or their membership enclave, or Community-of-Interest (C-o-I). They expect to have this accomplished with a minimum of fuss, and may only be peripherally aware of certification and authorization (C&A) data access requirements, as per any training on such matters that they may have voluntarily received.

Both parties (Stakeholder groups) are addressed by the Information Exchange Framework (IEF) Reference Architecture's (RA's) Information Exchange Policy-based Packaging Vocabulary (IEPPV) policy and semantics vocabulary instructions, since that was the whole purpose in designing and defining the IEPPV capabilities in the first place. To get to a more granular

description of what is going on, the capabilities and solutions applicable to address data protection and Quality-of-Service (QoS) issues, requires most organizations also adopting a set of standards for message structure and content, called (in the IEF RA) Message Payload. Message Payload is constructed from XML schema, and the method for using XML schema – in web service situations – may lend itself to tools from such companies as: Sparx, iGnite XML, Altova Schema Agent, and Progress DataXtend.[73] Although this is beyond our immediate attention – excepting (accepting?) the very important function of canonical data transport applications in financial institutions – the IEPPV serves as a very practical, and robust, Information-as-a-Service (I-a-a-S)[74] enabler.

Given that canonical data models (CDMs) always feature a one-way, unambiguous translation of data from the CDM to the connecting data model, and vice versa, for data translation to work in CDM environments, the translation is *not* restricted to the way the data is modeled, but will also be a translation of the values of the data itself. Most likely this features the XML type data model. However, JavaScript Object Notation (JSON) is increasingly supported by integration software and is becoming more popular because of its reduced size and the fact that it is used in front-end technology, especially for mobile devices. JSON emerged as a

[73] Source: "Canonical Modeling: NIEM and Beyond," by Priscilla Walmsely, slide deck presentation, Dated: September 19, 2013 [slide #'s] page 36-37. Discussion: Why did ACPR *not* address canonical data and canonical data models (CDM)? This is an essential data categorization / data transport activity, pursued by financial institutions, and third party services providers participating in the banking industry's delivery of their *core* banking services. (Curious).

[74] I-a-a-S allows the simplifying and streamlining of data exchanges between enterprise systems, reducing many of the cost factors that have inhibited the thorough sharing of back-end data with (/between) consuming systems in the past. By establishing a single, trusted source of data as a shared service, it is possible to set up separate consumers of that data in number(s) of separate applications, with comparatively little effort.

competing standard to XML, for the ease with which it can exchange JavaScript object data between systems. JSON's biggest weakness is its lack of defined data structures.

Canonical Data Models (CDMs) feature data-model design (canonical or not) which implies certain business rules and constraints. Thus, when a canonical data-model needs to be created, along with the vocabulary / terms defining the two (CDM and application) data-models, the implicit business rules need to be reconciled. This requires extensive business process analysis.[75] Creating a data model that represents both the interactions between systems, but also the internals of those systems, and then implementing such a model, can only be done as part of an enterprise-wide project involving conversations with stakeholders from across the business to understand how the business works.[76]

There is a solution, something which ASMG studied with the Trusted Information Exchange Service (TIES) / Information Exchange Framework (IEF) Technology Demonstrator Project (TDP).

In short, this involved tailoring the packaging of data and information element(s) into a message, based on the individual user's authorizations, and then directing that information to designated channels based upon the IEPPV's policy semantics. We may conclude, at this point, with the following statement: many workshops have taken place at the Object Management Group (OMG) over many years, with consultations involving governments, the private sector and academia. This has brought together capabilities and solutions applicable to address data protection and Quality-of-Service (QoS) issues, and these solutions are needed – even more *urgently* today – with so much information and data found resident in the cloud's data lake.

Summary

This Submission's author is a great believer in the power and practicality of public policy. Therefore, a quick review of some policy analysts' viewpoints may be in order. Before turning to their perspectives, a few items appearing in the ACPR Report are still pressing for further clarification.

The closest ACPR Report authors came to addressing *combining* computer systems with different architectures or configurations appeared at (page 6): "The workshops involved two actors: a banking group which designs and implements its credit scoring models internally, and a consulting firm which provides a development platform for hybrid (ML- and rule-based) models, tested in this case on the computation of the probability of default. Both application

[75] Source: "SOA, Cloud, Integration and Web 2.0 technologies," By Sarat Buddhiraj online blog, Dated: October 24, 2010. See: https://buddhiraj.wordpress.com/2010/10/24/challenges-with-the-canonical-schema-design-pattern/.
[76] Source: "The Canonical Data Model," By Steve Miller, Gresham Technologies plc. Dated: October 23, 2015 *online* web blog.

scenarios demonstrated how introducing ML impacts governance." ACPR provide a mention of hybrid model 'workflows discussion' (page 58 point 8.4.7); and, (at Page 55) review: 'managed services' behind the *hybrid model*. At page 52 – section 8.4 – you address the topic of a 'toolbox approach' to 'hybrid models,' a topic which ASMG found fascinating, if a little short on further analysis. ASMG would have also liked to have a more in-depth presentation of data scientists 'web scraping' [8.3.3.] activities, and would be fascinated to learn more about your viewpoints expressed (page 48) regarding business rule 'alert' engine mechanisms (functioning?) of 'filters,' and your very *cursory* discussion of alerting functions with respect to suspicious activity reporting (SARs).

On page 22 of the ACPR Report, the authors state "Best practices" adopted in the software industry need to be applied to assessing ML models. These best practices include: i) build automation rigor; ii) reproducibility of releases; iii) quality assurance (QA) procedures, and; iv) '*modeling in production'* monitored for state, stability and over-time issues. ACPR Report authors also identify **information sharing platforms** as vital to allow customer access to model and algorithm *outputs*. ACPR calls this the 'middle ground' involving audit tracks independent from the execution of the algorithm's processing tasks.[77] This may involve notifying multiple parties across a Group Level Risk Committee according to their need-to-know 'caveats to receive notification, and at what depth of knowledge the need reported. A caveat for

comprehensive notification may be issued by the IEPPV (ASMG data-centric security solution). The Information Exchange Policy-based Packaging Vocabulary (IEPPV)[78] is the perfect alerting tool for this purpose – reaching: Tech Team members responsible for build/validation tasks and responsibilities (governing the configuration / security parameter update(s) required/requested – *plus*; a different notification / alert caveat can be created (pre-designed) and automatically generated once the alert is triggered. This automatic alert triggering may be to notify: a) compliance and/or risk management departments; b) 'other' system administrator/technical staff, and; c) domain (or business analyst) specialists. This will address all the software best practices, cohesively and thoroughly, in the same manner.

This capability is extremely important with financial transactions, where Basel Models (in finance) automatically trigger reporting to regulatory authorities, something which ASMG believes is, in large part, driving this ACPR Report.

ACPR delve more deeply into this set of issues in section 8.4 – Workshop on Probability of Default' results. The ACPR Report authors suggest outsourcing to third parties may *up-end* the business process affecting: i) in-house validation of the (3rd party's) code base; ii) in-house supervision of design documentation reflecting the modeling being deployed; iii) audit steps in place, at design, and in the post-design/ -delivery phase, and; iv) integration 'to-be-fully-

[77] See: ACPR – Workshop on Probability of Default' results; section 8.4; Page 22 –ACPR Report (*titled*): "Governance of Artificial Intelligence in Finance: A Discussion Document" Dated: June 2020.
[78] See: *Ibid*., [Foot Note # *25* – *original* ASMG IEPPV *citation*], Page G-6.

explainable' by third party providers for in-house teams to monitor system security configurations.

The next observation is a repeat of what we have stated earlier: the ACPR Report seems to be very narrow in its description of ML security, something which the General Data Protection Regulation (GDPR) of the European Commission (EC) rectifies. The GDPR is attempting to address, in a much more in-depth manner, what kinds of security actions might be considered "appropriate to the risk," including: i) The pseudonymization and encryption of personal data; ii) The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems / services; iii) The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, and; iv) A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the [data] handling/processing/reporting.[79]
This situation the GDPR is addressing – an expression of need for *data security* and *breach notification* – led ASMG to find a corporate partner to seek funding to provide our solution, a solution which still eludes the world community at present.

Reviewing a few prominent policy analysts from the IT / IM community, and from institutional circles, let's start by examining a few succinct observations made by the World Economic Forum

(WEF). One of the key findings of the World Economic Forum's recent horizon-scanning study of AI in financial services[80] suggested – there are data network effects – which can arise because ML models automatically improve as they gain access to more data. The idea is that the more widely a product is used, the more data it will have access to and be able to train on. This, in turn, will make it more valuable to customers, which will increase its usage, in a virtuous feedback loop. In theory, with every cycle, its predictions will become more accurate and error rates lower.

ASMG do not believe the World Economic Forum's (WEF's) argument – e.g. AI predictions in financial services will become more accurate and error rates lower, due to increased volume and adoption rates – are convincing, something which the ACPR Report underscores.
On a positive note, an industry insider suggests: "There is potential for more and better data, combined with AI, to transform finance for the better – for consumers, for risk managers, for financial inclusion – and many other goals. Used alongside cell phones and new distribution

[79] Source: "Top 10 operational impacts of the GDPR: Part 1 – data security and breach notification," by Rita Heimes, Critical Infrastructure Protection Program -CIPP / US, dated Jan. 6, 2016, p. 2.
[80] Source: "It's not magic: Weighing the risks of AI in financial services," By Keyur Patel and Marshall Lincoln. Center for the Study of Financial Innovation (CSFI), Dated: ISBN: # 978-1-9997174-7-6; Page 34; 'data network effects'. See [original *citation*]: "The New Physics of Financial Services – How artificial intelligence is transforming the financial ecosystem," Dated: 2019 - World Economic Forum (WEF). https://www.weforum.org/reports/the-new-physicsof-financial-services-how-artificial-intelligence-istransforming-the-financial-ecosystem.
See [*citation*]: https://www.european-microfinance.org/sites/default/files/document/file/risks_of_AI.pdf.

systems, we can democratize finance, make it accessible, make it affordable, make it fair. It's like no technology in the financial industry that has ever existed before… it can be the most democratizing force."[81]

(World Economic Forum/WEF): "There are clear benefits to the users of financial products that continuously improve. The risk is that data network effects may create barriers to entry which are difficult to overcome, making effective competition in certain markets increasingly implausible. A difficult question for regulators here is how to police monopolies that may have arisen as a natural consequence of the technologies being used, rather than from anti-competitive behaviours such as (prospective) predatory pricing".[82]

The best take-away from the World Economic Forum's document is, possibly, the observation that more *interconnectedness* is afoot. This may involve ML algorithms implemented by many different firms, becoming increasingly interconnected over time – the output of one being used as the input into another – many times over, in a mesh of interdependencies. Many parties the WEF spoke to expressed concerns that as such interdependencies grow, an isolated failure at one third party institution might become magnified and quickly spread through the system. This might lead to problems with AI solution implementations, if improperly tested. This was flagged by the WEF as the chief risk that AI poses to the financial services industry, reported by many data scientists. These data scientists suggested: "A lot of the problems that arise ultimately

come down to a lack of care and due diligence – for example, failing to pay attention to monitoring, logging, audits and testing of models – It's the boring stuff which is critical."[83]

At many financial institutions, it isn't overregulation that is causing the most anxiety, the WEF argues, but the potential for an uneven playing field and a lack of clarity in the rules (a.k.a. financial regulators' understanding of AI technologies and ML practices). This further reinforces the keen support the financial sector will be investing in digesting the contents of this, the ACPR Report.

On the other hand, there's a feeling that financial regulators often aren't supportive enough of experimentation. The experimentation that has the potential to offer benefits to the industry. For example, Jane Jee, Barrister and CEO of Kompli-Global, an AI-driven regtech provider, said: "A bank thinks: why experiment when the regulator will give us no credit for it, and in the process, we may risk being fined or sanctioned? Indeed, why take the risk even if we can see that the new technology would reduce financial crime? Regulators should issue praise where a bank adopts an effective new technology and issue examples of good practice – provide some carrots for combatting financial crime."[84] Continuing with one other observation – cited by the

[81] See: *Ibid*., [foot note # *4*] - *first* citation "CSFI- Patel and Lincoln," at Chapter 2: Weighing the Benefits, Page 13.
[82] See: *Ibid*., [foot note # *4*] *citation* "CSFI- Patel and Lincoln," Page 34.
[83] See: *Ibid*., [foot note # *4*] Page 34-36.
[84] See: *Ibid*., [foot note # *4*] Page 38.

WEF document – one practitioner states: "I would emphasize that regulators and firms together need to develop standards for best practice on the design of safe and fair AI systems. We need to create the ability to audit an AI / ML system: is it using enough data to be statistically valid? Is the *training data biased*, and/or is the data accurate? We need to be able to audit outcomes in areas like discrimination. You can run those tests in parallel, test the AI against traditional underwriting systems, and analyze it to see whether it was more fair and inclusive."[85]

And last (but not least) a cautionary note is offered by a recent publication by the Bank of England (BoE), which argued that while the connection is not self-evident, there is a credible case to link cyber risk to systemic risk in the financial sector. The Band of England (BoE) authors said: "We are seeing a further growing gap between the technology environment we operate in and our ability to understand and secure it. As we build automated processes and artificial intelligence into its services, this will, by definition, compound the problem; making the mitigation of attacks significantly more challenging."[86]

When all is summed up, the relative placement of the data, the subjects sending and / or receiving the data, the applications and the users' experiential knowledge of data assembly and data management, all these points are key in determining the governance of artificial intelligence (AI) in Finance. Let us choose wisely.

Appendix A

NB: European Parliament of the European Union (EU) *Horizon 2020 Programme 2016-2017* 'call for proposals / technology demonstrators' to fulfill the mandate of the GDPR.

DS-08-2017: Cybersecurity PPP: Privacy, Data Protection, Digital Identities

Citation: HORIZON 2020 - Work Programme 2016 – 2017 "Secure societies – Protecting freedom and security of Europe" [/at p.76]

Specific Challenge: The use of modern telecommunications and on-line services involve users' personal information. For example, using search engines exposes the query terms used, which can be both sensitive and identifying, as illustrated by the exposure of search terms; social networking services expect users to reveal their social connections, messages and preferences, that could lead to direct privacy violation if exposed. Browsing the web also leaves traces of where users have gone, their interests, and their actions - meta-data that can be used to profile individuals. The implementation the draft General Data Protection Regulation (GDPR - currently in the law-making process) presents both technological as well as organizational challenges for organizations [to] implement novelties such as the right to data portability,

[85] See: *Ibid*., [foot note # *65*] - *first* citation "CSFI- Patel and Lincoln," Page 38. *Quoting* – text appearing in the box "Implementing rigorous regulation without stifling innovation" – public advocacy spokesperson Jo Ann Barefoot, CEO and Founder of the Alliance for Innovative Regulation (AIR).

[86] Source: "Artificial intelligence, financial risk management and systemic risk," London School of Economics. Systemicrisk.ac.uk. See: http://www.systemicrisk.ac.uk/sites/default/files/ downloads/publications/SP13.pdf.

the right to be forgotten, data protection impact assessments and the various implementations of the principle of accountability. Many services on the Internet depend on the availability of secure digital identities which play a crucial role in safeguarding the data and privacy of citizens as well as protecting them and other actors such as private companies or public services form various online threats. At the same time, many European countries already have or are in the process of developing an electronic identity (eID) scheme. Most of these projects are built to be at a very high security level, which makes them very suitable for diverse eGovernment processes. But in turn they may lack usability for commercial applications.

Scope: Innovation Actions: Proposals may cover one of the strands identified below.

Privacy-enhancing Technologies (PET)

Novel designs and tools to provide users with the functionality they require without exposing any more information than necessary, and without losing control over their data, to any third parties. PET should be available in a broad spectrum of products and services, with usable, friendly and accessible safeguards options. PET should be developed having also cost effective solutions. Comprehensive and consistent Privacy Risk Management Framework(s) should be available,

[to] allow people to understand their privacy exposure (i.e. helping people to understand what happens to their data when they go online, use social networks etc.). Open source and externally auditable solutions are encouraged [to] maximize uptake and increase the trustworthiness of proposed solutions.

General Data Protection Regulation in practice

Tools and methods to assist organizations to implement the GDPR [*addressing*] the final provisions of GDPR and guidance from relevant authorities (Data Protection Authorities, Art 29 WP or its successor). Proposals may also address the need to provide support (procedures, tools) for entities to understand how to operate without requiring unnecessary information ([to] promote privacy respecting practices), *particularly* [when] the issue is mainly related to the fact that organizations (businesses, service providers, and government agencies) often require too much information from their target customer/user.

Appendix A (*Contd.)*

NB: European Parliament of the European Union (EU) *Horizon 2020 Programme 2016-2017* 'call for proposals / technology demonstrators' to fulfill the mandate of the GDPR.

DS-08-2017: Cybersecurity PPP: Privacy, Data Protection, Digital Identities

Citation: HORIZON 2020 - Work Programme 2016 – 2017 "Secure societies – Protecting freedom and security of Europe" [/at p.76]

Contd.

Secure digital identities

With a view to reducing identity fraud while protecting the privacy of citizens, proposals should develop

innovative, secure and privacy enhancing digital identity platforms beyond national eID systems. Activities may leverage existing European electronic identification and authentication platforms with clearly defined interfaces based on the General Data Protection Regulation (GDPR).

Proposals may:
• Leverage evidence-based identities (using adequate correlation of multiple soft proofs of identity, as opposed to the usage of a central register);
• Provide a function for so called "qualified anonymity", which means, that the online service does not have any information about the user but a pseudonym. The real identity of the user can only be revealed under specific conditions such as at the request of legal authorities;
• Consider cost-effective and user-friendly verification methods for mobile identity documents. For all strands, proposals should identify and address the societal and ethical dimensions of the strand they choose to cover taking into consideration the possibly divergent perspectives of pertinent stakeholders. Proposals [to] address the specific needs of the end-user, private and public security end users alike. Proposals are encouraged to include public security end-users and/or private end users. The Commission considers that proposals requesting a contribution from the EU between EUR 2 and 3 million would allow these areas to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts. The outcome of the proposals is expected to lead to development up to Technology Readiness Level (TRL) 6 to 7; please see part G of the General Annexes.

Expected Impact:
• Support for Fundamental Rights in Digital Society. • Increased Trust and Confidence in the Digital Single Market • Increase in the use of privacy-by-design principles in ICT systems and services

Type of Action: Innovation action
The conditions related to this topic are provided at the end of this call and in the General Annexes.