From: Susan Von Struensee [redacted]
Sent: Saturday, June 19, 2021 12:20 PM
To: Comments
Subject: [EXTERNAL MESSAGE] RIN 3064-ZA24

COMMENTS OF SUSAN VON STRUENSEE, JD, MPH

to the

Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, Including Machine Learning

86 FR 16837-38 (March 31, 2021)

Agency/Docket Numbers:

Docket ID OCC-2020-0049

Docket No. OP-1743

Docket No. CFPB-2021-0004

Docket No. NCUA-2021-0023

AI has been found to be used by organizations around the world for the detection of anomalies. It is used to establish optimal investment strategies. The other use of AI in securities is algorithmic trading, programs that integrate information regarding changing market dynamics and price levels by using proprietary algorithms to making automated trading very rapidly.

However, given the financial consequences, companies should ensure a sufficient understanding of the AI and other technology used in business by the senior management and the board to ensure proper monitoring. This is particularly important in view of the growing expectations of Board members to monitor substantive issues affecting the long-term value of a company. The decision-making, deployment, and use of AI must be carried out within the context of risk management, in order to capture market improvements. It will include four main tasks, including risk recognition, risk assessment, prevention and risk control.

Operational risk is fundamentally different from all other risks taken on by an organization.

Operational risk management (ORM) refers to a wide range of possible failures in the operation

of the organization that are not directly related to market or credit risk. Operational risks are

associated with inadequate systems, management failure, faulty controls and human errors. It is complex to measure & model and therefore cannot be understood in a

simplistic manner. It is harder to measure and model, and not straightforwardly eliminated. While it varies considerably, operational risk tends to represent about 10–30 per cent of the total risk pie and has grown rapidly since the 2008– 2009 crisis.

Latest policy developments in digital era – challenges & impacts

Historically, approaches to risk management were mainly focused on financial reporting, compliance and legal risk. However, that approach had changed when organizations began to realize that the biggest losses came from strategic and operating risks. ORM has always been influenced by introduction of new technology, despite that the challenge is to develop rapidly (in line with other technological applications), fueled by growing computing power, emerging technology's diminishing cost and the data explosion. The technological ecosystem and digitalization create new risks with every new opportunity and vice versa.

In the recent years, we are witnessing two broader trends that are shaping up ORM. Firstly, the application of technology across the financial services industry has transformed many industry functions and outcomes e.g. integration of software, core banking systems, credit/debit cards, NEFT/RTGS, automation and internet-based services are only a few of those changes that the industry has adopted, setting the foundation for better and faster services now through the use of blockchain, machine learning, and artificial intelligence.

Secondly, the impact of the economic crisis led to stricter regulations that required better control and more focus on compliance and has further accentuated the issues of rising costs and low efficiency. New challenges of cybersecurity, financial sanctions etc. are testing the resilience and

relevance of financial institutions in a fiercely competitive and innovative environment where technology availability has considerably lowered barriers to entry. In the backdrop of these aspects, in my view, the most important challenges that affect policy are: -

Rapid evolution of Regulatory Technology (RegTech) with regulation and automation:

Regulatory and supervisory bodies are adopting more flexible approaches to develop policy (such as regulatory sandboxes, outcome-based regulation, risk-weighted regulation, and adaptive regulation), considering supervisory technologies to provide oversight, and publishing guidelines in emerging technology topics, such as data privacy, algorithmic decision making, autonomous vehicles, and initial coin offerings.

RegTech provides an opportunity to introduce new capabilities that are designed to leverage existing systems and data to generate data qualities on regulatory data and reporting in a cost- effective, flexibleand timely manner without taking the risk of replacing or updating legacy systems.

Achieving complete compliance in a dynamic and complex regulatory environment is challenging.

The complexity, frequency, intricacy of the current dynamic regulations is further intensified by efforts of regulators to streamline and create a robust system, in addition to its global implications and lengthy documentation. Over the last few years, a stream of regulations such as Second Payments Service Directive (PSD2), General Data Protection Regulation (GDPR), Markets in Financial Instruments Directive (MiFID) 2, and Alternative Investment Fund Managers Directive (AIFMD) have been launched in the developed world. In India, RBI and Government is focusing on digital financial inclusion and digital India.

Organizational resilience to digital change:

The focus on digitization also means that regulations designed for a digital-first environment are needed to enhance confidence in the new and innovative products and services. Organizational change comes in many forms. But whether prompted by regulation, technological change or a corporate restructuring, the result is always upheaval, and enforced changes to operational risk

frameworks to cope with new and often unusual sources of risk.

Further, advances in digital technology such as Artificial Intelligence (AI) and Big Data have greatly increased the usability of advanced analytics in the financial services sector. This development can lead to better suited products and services, but it also poses the question whether a limit should be put on the profiling of individuals.

FinTech revolves around the risks of increasing financial discrimination through the extensive use of algorithms based on consumers' demographic and personal information available online (collected by big tech companies) and, as a result, having the potential to give rise to greater income inequality.

Unlike regulated banks, FinTech companies are not subject to strict rules on consumer protection, e.g. to compensate consumers, offer deposit insurance and meet standards in order to prevent misleading vulnerable consumers into buying unsuitable or harmful financial products. Therefore, those who trust FinTech products lacking such a safety net are currently relying on big FinTech providers to regulate themselves.

Cybersecurity, data security and data privacy: Today, cyberattacks have moved beyond identity theft and online account hacks. Adaptation of digital technologies such as AI, automated botnets, Internet of Things (IoT), and cloud computing both facilitate attacks and defend against them at a scale, speed, and level of sophistication never seen before. New types of malware such as automated phishing tools and crypto mining software combined with emerging technologies are expanding the cyber risk landscape.

While increased reliance on digital technology may heighten the risk of cybersecurity being

compromised, digital technology also presents numerous opportunities to improve security of digital financial services e.g. Data encryption to protect digitally stored data, Data analytics to detect irregular patterns and fraud. Distributed Ledger Technology (DLT) could increase the transparency of transactions, making them easier to track and control, improving Anti-Money Laundering (AML) regulations.

The world's most valuable resource is no longer oil, but data and AI. These have the capability to unlock and leverage data, transforming our lives. In this respect, the expanded availability and broader use of consumer data raises issues relating to data ownership and data usage and their implications for consumer privacy.

Global Sanctions and Personal Responsibility regime: - Under the European Union's General Data Protection Regulation (GDPR), which came into force in May 2018, financial organizations face penalties for non-compliance of up to 4% of their global annual turnover or €20 million (whichever is higher) for data privacy breaches. Similarly, proposed Indian Personal Data Protection Bill has stricter provisions of penalty for breach.

Tighter anti-money laundering (AML) controls and efforts to prevent transactions with internationally sanctioned entities have been a priority of regulators around the world in recent years, especially in the US.

The SMR's4 purpose is to ensure that individuals take full responsibility for their actions,in order to increase personal accountability for decision making.

Hence, Organizations should consider fostering stronger partnerships between the operational risk and technology functions, so that they understand how quickly the organization is adopting

new technologies and the impacts those technologies may have on business models and risk.

In the UK, the Senior Managers Regime (SMR), which came into force in March, seeks to codify a culture of personal responsibility for risk managers, with individuals who fulfil certain designated control functions now personally liable for various forms of misconduct profiles.

Conduct replaces capital as focus: - Work culture affects reputation, capital, morale, employees and customers. Good culture helps especially in customer retention. The Australian royal commission in a 14-month investigation into the financial services industry, found evidence of business models driven by greed, a focus on sales over service and a failure to reign in unethical business practices i.e. businesses had ripped off consumers by charging for services they had not delivered, lied to regulators and given their customers poor advice. Interestingly, this is not unique to Australia.

US retail bank Wells Fargo was fined by regulators for scandals, including opening false accounts and mis-selling products leading to a complete overhauling of its governance and management. Similarly, MetLife, an insurer, has hired investigators to track down pensioners that it failed to pay properly over several years.

Two other forms of conduct risk namely ‘financial crime’ particularly money laundering, for which authorities have a high level of intolerance and ‘data regulation’ i.e. the growing pace of regulation and different interpretations of standards are time-consuming, e.g. EU’s GDPR regime affects the way every company operating in the EU uses data, including possibility of fines for mishandling data.

However, diversity is important, and it avoids everyone having the same operating system. If

there's a drive to make everyone have the same structure then there's a worry that there is too much prescription in the rules, and that creates more risk.

Managing the regulatory change and incorporating to business as best practice

According to the London-based RegTech Council, between 2012-15, more than 50,000 regulations were published across the G20. Traditional compliance tools and methods are not equipped to deal with this surge in regulation. Data compilation from fragmented systems and business units is often handled by legacy systems and inadequate aggregation tools; this is then manually processed, adversely impacting the accuracy and quality of data and insights produced.

Any censure or sanction from the regulator would have a number of potential negative consequences, such as monetary penalty; suspensions for the business and individuals; bans for the business and individuals; personal liability for senior managers and compliance staff; stakeholder lawsuits; client lawsuits; remedial consulting; commitment to more resource to assist compliance; additional reporting; legal fees; and heightened scrutiny by auditors and examiners on future inspections.

Currently, the main drivers which appear to be shaping regulation and business practice are A.) the reduction of information asymmetry (i.e. the ability of new technology to capture and process a high amount of data in real time) is improving the price discovery mechanism in several areas of the financial system thereby improving borrower's behavior through competition and resilience. B.) improvement of Communication Efficacy, C.) increasingly integrated economy i.e. sharing economy through digital platforms that enable the matching of buyers and sellers, and D.) financial inclusion.

Moreover, the Financial Services Ecosystem is undergoing a Systemic Transformation with RegTech and FinTech. The impact of these solutions will extend beyond regulatory compliance, initiating a fundamental change in banks' core business operations.

In this connection, enhanced data governance and operating models will improve the quality of the data, make risk and business decisions more consistent, and ensure responsiveness to data

needs of risk management.

An integrated sequence process automation performed by groups of humans and machines and

sophisticated risk models (by machine-learning algorithms) can find complex patterns (indicative

of fraud) and make more accurate predictions of default and other risk events.

The risk infrastructure will evolve to support new innovative interfaces, data security and to

deliver risk insights in more intuitive, interactive ways through risk dashboards, augmented-reality platforms for customers etc.

Further risk infrastructure will utilize external service providers to vastly improve customer

onboarding, fraud detection, regulatory reporting etc. and will have more tech-savvy personnel,

with inhouse grooming, with fluency in the language of both risk and the business.

Ensuring an adequate regulatory level playing field for all participants is fundamental to achieve

appropriate competition. Any difference in regulation and supervision should be based on the

risks posed by different products and services. Again, there should not be unnecessary barriers

to competition in the market beyond those justified by risk considerations.

Considering the inherent nature of interconnectedness and global dimension of most

technological innovations in the financial system, regulatory frameworks need to be

internationally co-ordinated and upgraded.

Recent developments in AML & KYC policies

These developments will further shape evolution of AML and KYC policies, namely:

Evolution of crypto-businesses and virtual assets setting AML & KYC rules standardization:

crypto businesses themselves are encouraging regulation, simply to increase the addressable

market for adoption. Also, FATF's 'FinTech & RegTech initiative' to support financial innovation that is resilient to money laundering and terrorist financing is a great step in this direction.

After debating the AML risk crypto poses for years, Japan and Switzerland, are adopting a

considered approach allowing for trade and investment, and China and South Korea, is opting for

tight restrictions on exchanges and data mining.

The unevenness of the cryptocurrency landscape has prompted efforts by governments to

develop a global regulatory framework. The FATF released a set of international AML standards

in June 2019. https://www.fatf-gafi.org/publications/fatfrecommendations/?hf=10&b=0&s=desc(fatf_releasedate)

Also, Monetary Authority of Singapore (MAS) ramped up their engagement with

the sector in 2018.

The EU's Fifth Anti-Money Laundering Directive (5AMLD) introduced AML

obligations for cryptocurrency exchanges operating within member states which will have to be

complied with by 2020. https://www.mayerbrown.com/en/perspectives-events/publications/2020/01/the-fifth-eu-anti-money-laundering-directive-takes-effect

AML 5 further strengthens the EU's anti-money laundering and combatting the financing of terrorism ("AML-CFT") regime in multiple ways, including: increasing transparency regarding the beneficial ownership of companies; enhancing cooperation and information sharing between financial supervisory authorities; introducing stricter controls of transactions with customers located in high-risk third countries; restricting the

anonymous use of virtual currencies; allowing for better identification of politically exposed persons ("PEPs") and extending the scope of sectors and firms subject to AML-CFT obligations.

FinTechs will further propel demand for automated AML & KYC: High-quality data is the driving force of AI and machine learning tools and is the key to effective automation of AML risk management, which will be critical for FinTech to be successful.

Requirement of Transaction Monitoring solutions: The availability of new transaction monitoring software platforms which can help financial institutions configure a range of monitoring scenarios, analyze data more efficiently, and better separate genuine suspicious activities from false positives, will become essential.

Regulators will increasingly expect firms to be able to show not only that they have a system in

place to monitor transactions but also will be able to prove that it is effective and auditable.

Anticipation of Ultimate Beneficial Ownership (UBO) legislation: There are many creative ways in which criminals use entities such as shell companies and offshore structures (Panama Papers) to hide their cash from becoming public knowledge. To increase transparency, policymakers are

considering 'ultimate beneficial ownership legislation'. In 2018 G20 Summit, where leaders made clear a desire to implement 'international standards and the availability of ultimate beneficial ownership information'.

In this context, the US continued its pioneering work around Geographic Targeting Orders (GTO). https://www.fincen.gov/news/news-releases/fincen-reissues-real-estate-geographic-targeting-orders-12-metropolitan-areas-3

The implementation also of the FinCEN Final Rule on Customer Due Diligence showed that the US is committed to increasing transparency of ownership. In the UK, steps were taken to introduce ultimate beneficial ownership registers for companies in overseas territories by the end of 2020.

Geographic targeting orders are a tool used by the Financial Crimes Enforcement Network (FinCEN) to detect and prevent money laundering. Geographic targeting orders impose AML requirements on obligated firms, in addition to standard Bank Secrecy Act (BSA) AML/CFT obligations, when they deal with certain transactions over a specified value.

Geographic targeting orders are often used by FinCEN to prevent money laundering on the high-value real estate market. Given their scope, financial institutions in the United States should understand the regulatory requirements that will be imposed upon them under a geographic targeting order and how their AML responsibilities will be affected.

A geographic targeting order (GTO) affects financial institutions within specific areas of the United States, imposing additional record-keeping and reporting requirements for transactions over a certain value. FinCEN issues GTOs under the authority of the BSA (31 USC 310).

Increased Information sharing: The success of information sharing between regulators and banks will extend further to include smaller financial institutions. The inconsistency of territorial regulation and privacy legislation need to be resolved for this trend to emerge.

Information sharing is of crucial importance to combat financial crime effectively. We have traditionally seen challenges in being able to share and obtain information with financial institutions due to the fear of tipping off and privacy related issues. FinTech and emerging technologies will play a vital role in shaping the sharing of information.

How will Indian BFSI sector prepare for GDPR regime?

The Indian BFSI sector has been the pioneering sector when it comes to adoption of technological innovations. However, risk miscalculation, financial discrimination and cyber security remains some of the big challenges for the sector, all these with ensuring regulatory compliance to ensure data privacy.

Protection of customer's sensitive information in India has traditionally been under various regulators such as the Reserve Bank of India (RBI) and Insurance Regulator and Development Authority of India (IRDAI). Data privacy in the BFSI sector is largely controlled as per the

Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) rules where BFSI enterprises need the consent of a customer before releasing any associated customer data.

Improper operational risk management systems and practices, inadequate controlling, monitoring of logical and physical access of customer sensitive data leads to misuse, and abuse of data for commercial reasons or creates serious safety and privacy concerns.

RBI's various master circulars, Guidelines on Cyber Security Framework in Banks, directives etc. requires banks to take appropriate steps in preserving the confidentiality of customer information, and to ensure that such confidentiality is not compromised at any cost, in any situation.

However, there is a clear lack of enforcement of data privacy often differing from case to case, and organizations to organization and the contract in question. Unfortunately, such enforcement is not guaranteed by law. However, recent draft Personal Data Protection Bill is a great step in that direction.

Strong customer data privacy protection norms and stringent penalties for infringement have been the main drivers of robust cyber security arrangements by banks in most OECD countries. The General Data Protection Regulations (GDPR) in the EU imposes a penalty of up to €20 million, or up to 4% of the annual worldwide turnover, for violation of norms.

Moreover, there might be challenges over resolution of number of breach of personal data issues initially as both the industry players and customers are not aware of the issue fully. Further, how to maintain accurate copies of personal data in different locations at all times constitutes another challenge.

Some thoughts regarding robust data protection for BFSI sector: India had a 55% share of the US$185-190 billion global outsourcing business in FY18. With the advent of the General Data

Protection Regulation in the EU w.e.f. May 25, 2018, transfer of data from the EU to another nonEU country will need to pass either (i) the adequacy test (i.e. India has adequate level of data

protection framework in place), or (ii) be in accordance with standard contractual clauses offering enough safeguards in relation with the data.

For adequacy test, the European Commission will examine the data protection rules in place in

India, data protection rights and their effective administration, data protection

authority, powers vested with such authority, international commitments with regard to data

protection and a periodic review of the aforesaid criteria. In the present list of countries

determined to be 'adequate', India does not figure, however, countries like Argentina, Canada,

Israel, Isle of Man, New Zealand and the United States have been determined as 'adequate'.

Accordingly, the challenge for India is to bring its own regulatory framework on data protection in line with the EU or other developed economies.

Further, building applications that can identify the relevant data points and correct partner APIs,

will entail data sharing/enabling for different businesses. The BFSI sector can also design the

core applications in such a way that they themselves have information, the inbuilt logic on what

amount of data is being shared.

Deeper data analytics and modern technology can help keep the financial records secure. Big

data, machine learning and Artificial Intelligence are the key to prevent financial crimes and stay

protected. Understanding the high potential of financial crime and infringement, Reserve Bank of

India (RBI) has asked all the payment services firms to provide an in- depth record of effort taken

by them towards data localization i.e. to keep the customer records safe and secure in the

servers within the nation.

Again, the requirement to store a copy of all personal data in India will affect both foreign and Indian companies. The RBI had mandated payment systems and platforms that data pertaining to financial transactions data occurring in India, should be stored only in India and obligated concerned companies to submit an audit report on adherence with the directive.

The payment platforms, such as card payment networks, not based in India, employ a different payment processing framework which extends beyond territorial boundaries of India thereby, the transaction data that these companies process and generate, is not entirely stored in India. This issue needs a conciliatory, amicable solution with focus on data security.

Another area of focus should be automated threat detection system, with the use of machine learning to analyze threats at impeccable speed. This ensures that as new threats are developed to target mobile payments, security defenses are aware of them and can work in real time to detect and mitigate them. In this connection behavior analytics, which leverages machine learning to recognize regular user habits and behavior, such as common times of use and location will be very helpful.

The BFSI sector must leverage proactive solutions and look at ways to create interoperability between different security systems so that information on an event identified on one device is automatically shared across the entire distributed security architecture.

In this regard, to leverage a common operating system or management interface is of utmost importance and this can be achieved through reduction of complexity by further integrating solutions, focusing on interoperability as devices are purchased or replaced and consolidating existing security devices.

Organizations need to commit to safeguard privacy and confidentiality of customer's personal information through appropriate risk management practices, use of technology and employee awareness with innovative new approaches to address data protection, fast identification of data breach and quick recovery challenges.

Today we are facing the challenge that technology possesses such as having legitimate concerns about competition, about the market power of technology giants, and the cyber- risks and social disruptions that may accompany rapid technological change. Also, there are concerns about how data is collected and used; and how IT firms are taxed.

In this context, we need to strike the right balance in our policy choices between promoting innovation while preserving financial stability, and between acting in the national interest while avoiding adverse spillovers to other sectors. We need to act together to design new policy frameworks to meet these challenges, or we run the risk of exacerbating our common vulnerabilities and threats.

With the evolution of risk and its sophistication with technology and increasing regulatory demand to comply, the challenge remains for institutions to understand the latest threats and to change according to the demands of evolving operational risk to ensure they limit future penalties and potential reputational damage.

Every enterprise has specific needs and will take a unique path to achieve its vision of the operational risk management. The organization need to move from a primarily compliance-based and value-protection approach to an approach that also embraces risk- taking for value creation. In my view data analytics, risk controls and risk culture must be strengthened if operational risk management is to prosper.

By acknowledging and recognizing all expected outcomes of policy changes and thereby

potential outcomes, we can more effectively communicate the goals of supervisory

policy, increase accountability and transparency, and better fulfill our mission.

Citation:

Mishra, Rabi N., Dynamics of Operational Risk Management in Digital Arena Regulatory Panacea or Overkill? (April 11, 2019). Available at SSRN: https://ssrn.com/abstract=3407160 or http://dx.doi.org/10.2139/ssrn.3407160

Applications of Artificial Intelligence in Financial Management Decisions: A Mini-Review

Artificial Intelligence (AI) has, during the past few years, made many signs of progress which have enabled the creation of professional financing applications, which would, perhaps, disrupt the finance industry. Thus, it is assumed that the AI could not only replace human capital in full or in part but also enhance its performance beyond human benchmarks. For companies around the world, there are a variety of programs.

A systemic content analysis methodology was used to evaluate related literature publications in this study. A selection of papers, including posts, has been collected. This research focuses on broad publications peer-reviewed, including Scopus and SSRN, which are listed in quality and impact rankings. This selection of the highest-ranking papers not only guaranteed the quality of papers that were most reviewed and validated but also provided the most up-to-date research state during their publication periods. Some keywords are used to scan for artificial intelligence papers, such as artificial intelligence and financial articles such as corporate finance, artificial intelligence, digital finance, financial and artificial intelligence, etc.

CITATION:

Al-Blooshi, Laila and Nobanee, Haitham, Applications of Artificial Intelligence in Financial Management Decisions: A Mini-Review (February 18, 2020). Available at SSRN: https://ssrn.com/abstract=3540140 or http://dx.doi.org/10.2139/ssrn.3540140

Respectfully Submitted,

Susan von Struensee, JD, MPH