From:	Katherine Hartley
To:	Comments
Subject:	[EXTERNAL MESSAGE] AIR Comment Letter: FDIC RIN 3064- ZA26
Date:	Monday, October 18, 2021 4:13:56 PM
Attachments:	AIR Comment Letter on Interagency RFI on Third Party Risk (9_21) (1).pdf

To whom it may concern,

The Alliance for Innovative Regulation, AIR, appreciates the opportunity to submit comments in response to the Interagency Proposed Guidance on Third Party Risk.

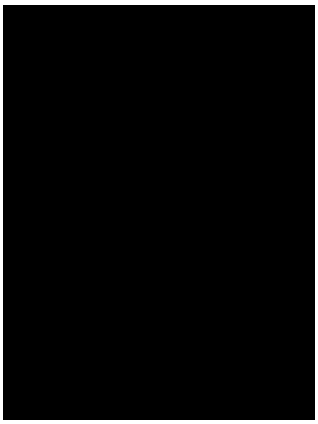
AIR is a nonprofit organization co-founded in 2019 by Jo Ann Barefoot, former Deputy Comptroller of the Currency, to help catalyze and shape modernization of the financial regulatory system for the Digital Age. We produce thought leadership, convene gatherings for learning and problem-solving, and conduct tech sprints and proof of concept projects to develop and demonstrate digital solutions to regulatory challenges. In 2020 we released a seminal paper in the form of a Request for Comments, titled A Regtech Manifesto: Redesigning Financial Regulation for the Digital Age.

AIR commends the Board, FDIC, and OCC for coming together to invite comment on proposed guidance on managing risks associated with third-party relationships. We hope that the proposed guidance will offer the framework to develop risk management practices for all stages in the life cycle of third-party relationships.

Attached is the full comment letter.

Thank you,

Katherine



Katherine Hartley
Operations Manager
Alliance for Innovative Regulation
Katherine@regulationinnovation.org
regulationinnovation.org

October 18, 2021

Via email submission

Federal Deposit Insurance Corporation
550 17th Street NW
Washington, DC 20429

Re: FDIC RIN 3064- ZA26 Proposed Interagency Guidance on Third-Party Relationships: Risk Management

To Whom It May Concern,

The Alliance for Innovative Regulation, AIR, appreciates the opportunity to submit comments in response to the Interagency Proposed Guidance on Third Party Risk.

AIR is a nonprofit organization co-founded in 2019 by Jo Ann Barefoot, former Deputy Comptroller of the Currency, to help catalyze and shape modernization of the financial regulatory system for the Digital Age. We produce thought leadership, convene gatherings for learning and problem-solving, and conduct tech sprints and proof of concept projects to develop and demonstrate digital solutions to regulatory challenges. In 2020 we released a seminal paper in the form of a Request for Comments, titled A Regtech Manifesto: Redesigning Financial Regulation for the Digital Age.

AIR commends the Board, FDIC, and OCC for coming together to invite comment on proposed guidance on managing risks associated with third-party relationships. We hope that the proposed guidance will offer the framework to develop risk management practices for all stages in the life cycle of third-party relationships.

General Recommendation: Reframe guidance to encourage modernization of banks' relationship models

The proposal asks in multiple places whether additional guidance would be helpful. We urge the agencies to consider widening the lens for assessing third party risk. While retaining the critical focus on risks that may arise from banks working with any given third party, interagency guidance should also address the related realm of risk that is developing in the traditional model that banks currently use to engage in and manage these relationships. Specifically, we recommend advising banks that they should set up their third party strategies to maximize flexibility and the ability to add and upgrade vendors. This capacity will be crucial as a new

generation of digital services emerge that can help banks, and especially community banks, rapidly upgrade their technology over the next five years.

Third party relationships are becoming increasingly crucial for banks and may, in fact, determine whether some individual banks and banking sub-sectors will remain viable in the future. Small community banks, in particular, face existential risks related to their use of technology. They carry major disadvantages in relation to large banks, fintechs and Big Tech competitors in producing the products and user experience expected by today's customers (especially now that digitally-native millennials have become the largest generation in history, and the oldest among them are turning 40). These small banks are also disadvantaged by "back-office" technology that generates disproportionately high operating costs and regulatory compliance burden. Modernizing and digitizing their technology is critical to the future of these institutions.

For nearly all of these banks, this modernization can come only through third party relationships. Unlike both large banks and fintechs, most individual small banks will not be able to attract and sufficiently compensate the kinds of software engineers and designers who create such technology. They will have to access the needed solutions through vendors and partners. Small banks will not have Silicon Valley engineers on their staff, but their vendors (and, importantly, their regulators) will.

This means that prudential regulators face an urgent need to foster an industry-wide shift to new models for selecting and managing third party relationships. This framing widens the risk management lens from assessing the potential hazards presented by any given relationship, to addressing the risks presented by *failing to modernize the bank's third party risk management model* to make the bank successful in accessing and using the needed technology from vendors and partners.

It is worth asking what the ideal system would look like if it could be designed and built today from scratch, using digital technology design. In the industry's current legacy systems, the dominant model is that technology and data are organized in vertical technology stacks that tend to be siloed off from other technology and that tend to be rigid. We believe that this model must be replaced by a new one built around horizontal "platforms" that easily accommodate modular solutions. In the new system, the bank's architecture will incorporate standardized data and technology protocols that facilitate interoperability. Banks will use APIs to connect data and analytical functions easily.

This design will achieve several crucial goals. It will facilitate banks' use of best-available technology. It will facilitate banks being able to easily integrate new technology solutions. It will also enable banks to "future proof" their technology operations by enabling continuous improvement. If one vendor falls behind best practice, the bank will be able simply to "unplug" it and plug in a better solution, which will be pre-designed to work interoperably with its systems and data.

It is worth noting that most large fintech firms already use this kind of technology architecture and many are able to produce very high levels of compliance at low cost. These firms generally avoid reliance on “one size fits all” vendors. Instead, they select each third party tool individually, choosing the one that is the best for a specific need. Few full-service solutions are actually the best at every aspect of the functions they provide. When modular solutions can easily be added into the tech stack, companies can also use more than one vendor. For example, some Know-Your-Customer solutions are very strong for mainstream banking while others are best for complex situations such as identifying interests related to sanctioned entities. Banks can benefit from being able to easily use several KYC vendors, and easily switch to new ones that emerge and prove to be superior -- a process that is occurring at an accelerated pace in today’s financial world.

Such a system will also enable banks to take full advantage of the emergence of new regtech and suptech strategies from their own regulators, a shift that will reduce their comparative compliance burdens and help level the playing field in regulatory burden carried by different kinds of providers. This shift will also enhance regulatory outcomes, by equipping regulators with better information and analytical tools than they have today.

While migration to such a system will take time, it is underway. Regulators in several countries are moving to foster these kinds of strategies. There are also industry initiatives, such as the Orchestrate project of ING Bank in Europe, which is linking companies that offer regtech solutions so that if a bank integrates one of them, the solutions of the others will automatically integrate as well.

Underlying this analysis is the fact that the marketplace is inventing a new generation of digital solutions that are inherently superior to those from the analog era. These new solutions, in general, are leveraging the explosion of digitized data impacting every realm of life and are combining it with new analytical techniques that use artificial intelligence -- methods like machine learning and natural language processing. They are superior to older technology in the same way that a smartphone is superior to a landline phone, or that a digital camera is superior to one using film. They open an opportunity for both banks and regulators to make enormous leaps in addressing long-standing challenges like financial systemic risk, financial inclusion, and countering financial crime.

If the thesis is correct that banks must move toward a new third party relationship model of this kind, it makes sense to incorporate that assumption into agencies’ guidelines for third party risk management. It seems likely that regulators will increasingly be targeting outdated technology and third-party models as sources of unacceptable risk in their own right. These aging tools will increasingly threaten bank competitiveness, and therefore safety and soundness. They will also, in the coming years, produce unacceptably poor results in compliance activities like fair lending, anti-money laundering, and cyber security. Increasingly, the core problem with banks’ third party relationships will be that banks are trying to plug superior new technology into legacy technology, and that it will be the legacy technology that must change.

We recommend that new joint guidance explicitly reflect the regulators' interest in shifting the system toward new models in which banks, and especially community banks, can develop and manage relationships with vendors and partners that will facilitate and accelerate this future state for the industry.

Specific Comments

Given this perspective, we offer several recommendations relating to specific parts of the proposed guidance.

C. Risk Management / Third-Party Life Cycle
C-3: Planning (page 22)
Cost/benefit analysis

The draft guidance suggests that the bank should weigh whether the cost of integrating a third party solution would outweigh the costs of integrating it. We suggest adding language to say that this analysis should incorporate the bank's larger strategy of modernizing its overall technology, which may make an integration worth doing as part of a larger transition. The reality today is that many new regtech offerings are point solutions that, while potentially superior to a bank's legacy technology, are difficult to integrate into it. If banks consider only the cost of integrating a single vendor, they may conclude that the expense is too high. If, in contrast, they commit to a larger redesign of their technology, these projects may be deemed to be worth their cost.

C-3. Due Diligence and Third Party Selection (page 24)
Addressing track record

In this section, and later in the OCC guidance from 2020, the issuance talks about ways to perform due diligence on firms that are too young to meet traditional requirements -- for instance, in not having a lengthy history of audited financial statements.

While there are many exceptions, digital age technology is largely being produced by young firms that are "digitally-native" -- that were, in effect, born digital and have therefore not had to layer this technology on top of old tech foundations. This means banks will increasingly need to work with younger firms, and to break away from the tendency to default to old, established providers that are well known and therefore already familiar to the bank's risk managers and examiners.

Firms with limited track records need to be vetted in two ways. First, banks must determine whether the firm has staying power; as the guidance suggests, banks must have a contingency plan in case the firm ceases to provide services. The OCC guidance on pages 78 and 78 is helpful in this regard.

Second, banks must evaluate whether younger solutions are effective. Some of this can be ascertained by directly evaluating the technology and checking the firm's reputation, references and track record. In addition, the bank will want to test the solution by trying it out in a "sandbox" environment and/or by running it in parallel with existing systems for some period. Agency guidance should encourage these strategies and could offer guidelines for crafting them, including on protecting customer data in experimentation settings. Guidance should be explicit that banks are permitted, and even encouraged, to pilot test potential solutions. (The agencies have previously issued this kind of guidance regarding AML and fair lending practices.)

Various (pages 39-53)
Contracts

The proposed guidance contains good material on contracts, including in Section 3f on page 39 and the statement on page 43 that contracts should permit banks to "change providers without undue restrictions, limits or cost." We recommend expanding on this with language that warns strongly against banks entering into rigid and long term contracts and into contracts that work against building interoperability of information and technology.

In every industry, a common vendor business model is to build so-called "walled garden" environments in which a client company can only use solution solutions provided by the same vendor, or in which the clients will at least face great difficulty in using other options. This model is sometimes referred to as "vendor capture." In banking, it should be increasingly viewed as inherently unsafe. No matter how strong a track record any vendor may have built, every firm today is at risk of falling behind the exponentially changing rates at which technology is improving.

We think that, given this rapidly changing environment, banks should generally be discouraged from entering into long term technology contracts. They should be discouraged from signing contracts for add-on services that will, in effect, force them later to renew non-contemporaneous contracts for other technology services. They should be discouraged from signing contracts that require them to pay extra to access and use their own data that is being held by their vendor. They should be discouraged from entering into contracts with vendors where the technology is designed to make interoperability difficult or impossible and where integrating a solution from a different vendor is likely to be so time consuming and costly that it will probably be deemed to be not worth the effort.

Legacy vendors in the banking space are rapidly building a new generation of digital solutions. Regulators should foster a vendor landscape in which these will compete with the solutions of other providers with a level playing field and with little opportunity for any vendor to lock out newer, better approaches.

One can argue that the current technology non-competitiveness of community banks -- and the attendant risks relating to it -- derives heavily from reliance on vendors whose technology

impedes adoption of innovation that keeps pace with rising customer expectations regarding services and user experience, and that impedes gains in operating efficiency when compared with large banks, digitally-native fintechs, and the financial offerings of Big Tech firms. The best way to give community banks a viable future is to be sure that they are able to select and easily work with the best technology partners.

It should be clear that the contract termination guidance on page 53 encourages banks to terminate contracts if vendors produce outcomes that put the bank or its customers at risk by falling significantly below industry standards or regulators' compliance expectations, with the understanding that standards are likely to be rising rapidly as better technology becomes widespread.

C. Risk Management
8. Ongoing monitoring (page 51)

We recommend that the third party guidance encourage banks to work with vendors that enable ongoing and real time monitoring of effectiveness. Work is underway by regulators and firms throughout the world to move to digital regulatory reporting (DRR). This model will work through a direct API interface, enabling regulators and risk managers to see into system activity and to analyze data using tools like machine learning. Vendors that enable this kind of monitoring by banks can help assure desired results while lowering costs of review.

V. OCC's 2020 Frequently Asked Questions
Question 4, Data aggregators (page 63)

We recommend that this discussion in the OCC 2020 guidance be expanded to warn banks against using risk management requirements as a pretext for unnecessarily preventing their customers from accessing services by third party providers. As written, the OCC guidance could open the door for banks hoping to avoid competition from firms that their customers want to use, either because the customer wants a service the bank does not provide, or because she wants a better version of something the bank does offer. Government risk management rules should be used to address genuine risk and should not be misused in ways that impede consumer choice or otherwise harm customers. Arguably, banks that add barriers and friction into these choices should be expected to show why these are necessary.

It seems likely that the industry is moving toward more "open banking" in which consumers can readily switch and add services into their financial tools. This model has evolved in other countries and provides consumers with valuable options and flexibility. Clearly banks participating in such arrangements must address a range of valid risks and should appropriately take steps to protect their customers and their own proprietary information. Again, however, regulation should not be used as a shield against safe, desirable services that consumers want.

Question 25 and Question 27 (page 80 and page 88)
Underserved Consumers

We recommend that the examples given on how vendors can help banks meet the needs of underserved consumers be expanded to mention new models for credit underwriting. This topic is also touched on in the alternative data discussion in item 27 of the OCC 2020 guidance.

This is one of the most promising areas where fintech and regtech innovation is opening the potential for major improvements for consumers and small businesses. New underwriting models that use new kinds of data, beyond the applicant's credit history, show great promise for enabling more inclusive lending without loss of loan loan quality, and sometimes even with gains in quality. This point is made in the introductory section of the draft guidance but would be worth emphasizing in this section.

These third party tools can be used by banks in several ways. The bank can work with fintechs offering "banking as a service" (BaaS) to provide or augment its underwriting models. It can also work with regtech firms that provide compliance tools that identify potential bias in lending decisions, especially regarding unintentional disparate impact. These solutions can be the main tool in use, or can be positioned as "adversarial AI" models that optimize for different outcomes and act as a check on other models.

(We also urge regulators, themselves, to adopt the latter kinds of tools in their own examination procedures. Again, these methodologies have potential to identify problems with much greater accuracy than older tools. Adoption by regulators would have the salutary effect of encouraging the industry to enhance fair lending tools.)

Model Risk Management (page 83)

We want to call out the section on model risk management (MRM) to highlight our view that this will be a fast-growing area of both opportunity and risk. It will be important for regulators to keep pace with the changes underway in the industry.

One of these, which may be beyond the scope of third party risk but should be kept in mind, is the advent of smart tools that enable models to be built as do-it-yourself projects by business people in the bank who are not technology experts. This process might be compared to using software to prepare one's income tax returns, with the tax rules built into the technology so that a person can complete forms without actually understanding the tax requirements. As these kinds of models proliferate in banking, significant risk will arise around them. What is the governance model for overseeing them? Who is assuring that the data they are using is clean and current? Who is assuring that the model's rules and standards are being kept up to date? How is the bank monitoring the activities of these models over time? Such issues will increasingly need attention from bank risk managers and regulators alike.

Simplifying Reviews and Certifications (page 77 and page 86-7, items 24 and 25)

The logic of the draft guidance is sound in emphasizing that every situation is different and must be analyzed individually for risk. At the same time, agencies may want to consider creating greater structure, standardization, and possibly "safe harbor" scenarios to make it easier for both banks and third parties to know what to do.

An example is that it could be worth creating a rebuttable presumption that certain high risk situations call for vendors to have SOC 2 certification and that vendors that do so are presumed to meet the required standard of due diligence on data security for specified situations.

There could also be opportunities to create more clarity through standard-setting and certification. Last year the FDIC invited comments on the concept of creating an independent standard-setting organization, or SSO, and standards that could be audited for by third parties that want to deal with banks. We think this idea has great merit. UK regulators are exploring something similar, with the idea of creating a "kite mark" indicating that certain regtech solutions meet certain standards. There could also be value in setting standards for the "third party assessment service companies" discussed on page 87 in item 25.

In addition, it could help for the agencies to encourage wider use of the shared questionnaire concept discussed in the guidance. This idea has been widely discussed in the fintech community and has been likened to the adoption, in the realm of higher education, of the FAFSA form -- the Free Application for Federal Student Aid for applying for college financial aid. Families applying for federal education financial assistance complete this single standard form, which is accepted by nearly all colleges, nonprofit organizations, and state and local governments. Its universality enables families to fill out the needed information one time, rather than having to complete individual forms for every entity from which they hope to receive funding. The pre-FAFSA world in education was akin to today's third party risk process in banking, in which banks' vendors and prospective partners must fill out due diligence information for every bank. These questionnaires often encompass hundreds of questions, and each third party must fill them out individually, even though the banks are seeking virtually the same information. The current process is a major anchor weighing down and slowing development of vibrant bank relationships with technology firms.

Standard-setting

A number of our comments have urged adoption or encouragement of standardization in data and technology. Standard-setting must always be approached with care because, in itself, it creates risks. One problem is that any standards that are set will become outdated. A common phenomenon is that standards are introduced to solve a problem and do so effectively for a period of time, but that these same standards eventually become outmoded, undermining market efficiency and quality outcomes, rather than enhancing them. A second risk is that standard-setting efforts can be dominated and even captured by incumbent entities and can be made to function as gatekeeping exercises aimed at blocking new market entrants.

These hazards should be proactively guarded against as the system moves toward great standardization, interoperability, efficiency, and effectiveness.

We appreciate the opportunity to comment on the interagency issues on proposed guidance on third party risk and hope that our observations are useful to the agencies engaged in this important exercise.