September 17, 2021

Board of Governors of the Federal Reserve System, Docket No. OP-1752
Federal Deposit Insurance Corporation, FDIC RIN 3064-ZA26
Office of the Comptroller of the Currency, Docket ID OCC-2021-0011

VIA ELECTRONIC SUBMISSION

RE: Proposed Interagency Guidance on Third-Party Relationships: Risk Management ("Proposal")

Please accept my comments on the above-noted proposal based on my experience as an independent auditor, over 35 years in banking as a finance, risk and operations officer and as a director of community and mid-sized banks. Experience includes auditing third party arrangements, negotiating numerous "critical" provider contracts and overseeing creation and development of a company-wide third-party provider risk management program that covered a wide range of providers and types of arrangements. Experience also includes leading 20+ due diligence teams for M&A transactions of banking companies where review and evaluation of critical third-party provider arrangements were required and preliminary assessments of so-called financial technology companies ("fintechs").

Comments are organized as (a) general comments and (b) specific comments on certain questions for which the Proposal requests feedback.

A. General Comments

1. Overall, it should be helpful to have the same rule or guidance for the same business activity (i.e., managing third party provider risks) rather than each regulator having its own similar but different rule. It is not uncommon for banking companies to have multiple regulators and multiple rules only complicate compliance and can distract the bank from actual management of the risk as time is required to develop and maintain overlapping requirements, policies and procedures.

   It is noted that the Consumer Financial Protection Bureau, which also has guidance on third party providers (i.e., service providers), is not a party to this Proposal. It is unfortunate that the CFPB is not participating in this effort.

2. There often arises questions as to the role of "guidance" and the extent to which guidance should specify process as opposed to principles and whether or not the guidance becomes de facto rules and regulations to which adherence is required. Guidance with extensive prescription as to process can become a check box rule book.

   The text of the Proposal (not counting those in the OCC FAQSs) calls out over 80 prescriptive process actions to be taken. The language used can easily be taken as the establishment of a requirement in each case and which examiners can interpret to be exceptions if not completed. An example of such a process requirement is "Understand the third party's metrics for its information systems…" While this may be helpful, it may not be a productive use of time in a given situation and may well not be practical, such as when a smaller bank is considering use of a large technology provider who has little incentive to provide the needed access to information.

The extensive specification of such process actions goes well beyond the stated objective "…to more clearly articulate risk-based principles". In spite of qualifying language about "…commensurate with …. its size, complexity, and risk profile…" the listing of so many specific process actions tends to over-ride the qualifying language.

It is simply not clear how this guidance is to be used….useful aid or required actions. Refer to A (3) following for comments regarding a related concern over the definition of "critical activities".

3. It is curious that the Proposal does not more firmly make a connection of managing third party risk to the bank's general program for managing risk. Third party risk is a subset of the risks faced by a bank and is a common risk faced by any business, bank or non-bank. That is, third party risk is not unique to banks.

   This lack of clear connection is illustrated by how the notion of "critical activity" is addressed and a seeming presumption that where a critical activity exists any third-party involvement leads to the risk that causes the activity to be considered critical. Except in the limited situations where an independent party must be utilized, any activity a bank engages or undertakes can be done in a range of ways including fully in-house to fully outsourced. Therefore, the activity should first be assessed using the bank's general program for managing risks and then the role of any third parties should be assessed in that context. Not only does an activity that is "non-critical" not involve "critical providers" that has higher risks, but a provider with a role in a "critical activity" is not necessarily a "critical provider" needing deeper vetting and monitoring.

   As currently written, an opportunity will be missed to reinforce the importance of a having in place an effective and practical program for managing risks which can help to more expediently consider the roles of third parties and whether risks are increased or decreased by their involvement. If the activity is not first assessed, the bank is left to somewhat randomly decide which providers necessitate close attention.

   For suggestions as to an alternative definition of "critical activities", see the response to Question 8 in the following section.

4. It is not clear the purpose of including the OCC FAQs in the Proposal as an appendix or any type of separate component and it is not clear what authority such FAQs carry as to the enforcement of the Proposal. If there are elements of the FAQ that are necessary for inclusion in the Proposal, then the better approach is to integrate into the relevant section of the Proposal and take the FAQs out entirely. If a Q&A is considered helpful and useful, then such should only be clarifications of the text of the Proposal sans OCC FAQs. The inclusion of the OCC FAQs as a separate component will unnecessarily be confusing for banks and possibly for examiners assessing the bank's adherence. Note that state-chartered banks are not subject to OCC rules and an appendix in the final guidance so clearly from the OCC opens the door for state-chartered banks to ignore, a door which can be easily closed.

B. Specific Comments

Question 1. To what extent does the guidance provide sufficient utility, relevance, comprehensiveness, and clarity for banking organizations with different risk profiles and organizational structures?

If the Proposal is meant and implemented as informational only, then there is much data that can be helpful to a wide range of banks, especially smaller banks.

However, if the Proposal is implemented as requirements, then the usefulness quickly diminishes for a great majority of banks and instead becomes an exercise in doing the minimum to "comply". Few smaller banks likely have the resources to actually comply with all the prescriptive process actions specified.

It is one thing to make clear that the bank's general program of managing risks is to include consideration of third-party risks coupled with an identification of what the agencies view as the foundational principles of assessing third party risk. This would lead to clarification of what is expected by examiners. It is quite another to issue a highly prescriptive set of process actions that have to be undertaken. Providing foundational principles address the "what" is expected while prescriptive process actions designate the "how" to show compliance. Boards of directors are held to account for exercising their best business judgment and extensive prescription undermines that accountability. The more a board is told how to do something, the more the board can with good reason hold that what the regulator instructed was done. This is true not only of managing risks of third-party relationships but applies to any risk faced by a bank.

The section on contracts is a good example of this. There is much in the contract section that provides helpful background information for bankers to be aware of as contracts are negotiated. However, the usefulness to the bank plummets if this becomes a check box requirement. It is more important for the bank to utilize legal counsel, whether in-house or outside counsel, well-experienced in contract law and negotiating contracts than to have a checklist. Contracts vary widely in what aspects are most important to managing the associated risks and spending time and energy on getting boxes checked is a distraction. The very act of negotiating a contract requires a mutually acceptable balancing of contractual terms and conditions that affect the risks assumed. Further, the relative position of each party (e.g., small bank versus large technology provider) is a major factor in negotiating a contract.

The Proposal says the objective is to focus on risk-based principles but where are those principles enumerated? There are statements in different places that sound like "principles" but are not well organized into a helpful working tool. It would be helpful to start with a clear and concise identification of what is being set out as "principles" in assessing third party risks.

The phrase "risk-based" is fuzzy and without sufficient clarity. Exactly what is meant by "risk-based" in this Proposal? It is also not enough to simply list "principles" without a clear connection as to how those principles are based on risk. Managing risks is first and foremost about what risks to accept or reject in accordance with the risk appetite and tolerance of the bank. Actions needed to mitigate higher risks to within tolerances are a direct result. Bank regulators certainly have a say in a bank's acceptance of risk that materially affect safety and soundness. However, while regulatory requirements are preferably obvious as to mitigating material risks, at least any requirement should be closely and clearly tied to concepts of risk.

With respect to the many process actions stated, perhaps these are better placed in an appendix of additional information that is intended to aid the bank in being aware of steps that *may* be appropriate as

the bank conducts its due diligence and monitoring in applying the *principles*. This would help in avoiding a check box implementation from occurring. Every action required by the Proposal takes time to perform in order to "check the box" whether or not there is an actual business value in managing risks and that time is lost to perform more needed actions.

Question 3. In what ways, if any, could the proposed description of third-party relationships be clearer?

The term "third party relationship" is not intuitively clear. In addition, many relationships that tend to get lumped into "third parties' only involve two parties.

In practice there are various types of third parties with which banks have dealings. One type is a "third party provider" which "provides" goods, services or both. Sometimes the word "vendor" is used regarding providers of goods and "service providers" used for those providers of services. These are somewhat arbitrary differentiations. Normally, banks have many third-party providers in this sense most of whom do not create appreciable risks and often reduce risks.

There are other relationships where more than two parties are involved that are more accurately described as third party such as a loan closer who closes loans for Bank A and Borrower B and disburses loan proceeds to Borrower B obtained from Bank A. Note that Closer C provides a service to Bank A, that is, a closing of a loan which the bank could do itself.

There are other relationships that at least border on some type of joint venture. An example is when Bank A contracts with Company B to offer auto warranty policies to borrowers of Bank A and Bank A earns part of the premium paid by Customer C to Company B.

The gist of all of these type arrangements is a contract to which the bank is a party and goods or services are provided to the bank or its customers. For arrangements where the bank is the provider of goods or services, the other party is typically referred to as a customer. Note that every deposit account, mobile banking agreement, loan, safe deposit agreement, brokerage account and trust or fiduciary account results in a contract between the bank and its customer and a relationship or arrangement between the parties. It is not customary that depositors are seen as providers to the bank although funds are "provided" to the bank.

Of interest is that some arrangements with fintechs may be a combination of relationships. One type might be simply for the Bank to contract with a fintech to provide the bank a system to conduct some activity. In that sense the fintech looks like a more traditional service provider. Then again, the bank might enter into an agreement with a fintech whereby the fintech is allowed to use bank customer data to develop marketing campaigns for the bank and the bank and the fintech share some defined revenues generated. In this case, the fintech provides the bank a service (developing customized marketing campaigns) yet the relationship has a joint venture component through the revenue sharing element. Where the arrangement includes an actual entity created to create the revenues to be shared, then that begs consideration as a joint venture and be subject to the bank's general program for managing risk and not subject to this Proposal.

Note that in mortgage lending, the bank may be required to provide customer, including privacy-protected, data to title insurance companies which the borrower selects and pays for. It is not clear what relationship exist between the bank and the title insurance company. It is also often impractical to obtain data needed to assess risk from the title insurance company and its agent given no privity of contract. Where the bank recommends (sometimes indicated by an "approved list") a particular title agent or

underwriter, the ability to assess the risk is likely achievable as the agent or underwriter would desire the referral or recommendation.

A simplified definition might be that the Proposal would apply to any contractual relationship (whether or not in writing) where the bank is provided goods or services by the other party (including where the bank arranges with the third party to provide bank customers or the public with goods or services). The risks associated with the presence of other elements, such as revenue sharing, would fall under the bank's general program for managing risk. It should be abundantly clear how the Proposal applies to cases where privacy-protected data is provided to a third party (other than when required by law or court order) whether or not revenue sharing is involved.

See also the comment for Question 4 that follows.

Question 4. To what extent does the discussion of "business arrangement" in the proposed guidance provide sufficient clarity to permit banking organizations to identify those arrangements for which the guidance is appropriate? What change or additional clarification, if any, would be helpful?

Two sentences on page 18 in the description of business arrangement, as stated below, raise questions:

> "A third-party relationship is any business arrangement between a banking organization and another entity, by contract or otherwise."
>
> "Third-party relationships can include relationships with entities such as vendors, financial technology (fintech) companies, affiliates, and the banking organization's holding company."

First, the initial sentence defines "third party" as an arrangement between *two* parties, the bank and another *entity*. This seems to exclude arrangements between the bank and an individual acting as a contractor, such as a specialist computer programmer. Is that the intent?

Second, the initial sentence says "…any business arrangement…" which is a very broad term. A checking account with a local business where the bank is the service provider to the local business would be included were it not for the subsequent wording that such arrangements "…generally exclude a bank's customer relationships..." However, it is not clear what the "…generally..." refers to. It would be helpful to indicate, perhaps by giving an example, what types of arrangements with customers *would not be excluded*.

Third, when a bank holding company ("BHC") that owns Bank A and acquires Bank B, and prior to merger of the two banks Bank A provides services to Bank B meant to be transitional in nature. While Bank B is an affiliate of Bank A during the pre-merger period, the Proposal would require application of the guidance by Bank B to Bank A as a third-party provider and the burden that would entail. Where regulatory approval has been received for merger of the two banks, the provisions of the Proposal should not apply.

Fourth, footnote 10 on page 18 states that "…services provided by …. subsidiaries…" and "…other banking arrangements…" are included as third-party relationships. Subsidiaries are a different issue than "affiliates" that lay beyond the bank's board of directors' purview (say a subsidiary of the bank's holding company subject to the BHC board). Further, bank subsidiaries can be grouped into at least three categories…wholly-owned, majority-owned and consolidated and less than 50% owned and not consolidated (such as an investee entity in which the bank owns less than 50% and does not exercise control). It is not clear why a bank subsidiary that is controlled by the bank would be considered a "third

party", especially where the bank owns 100% or a voting majority. Such situations should be addressed by the bank's general risk management program and not by the Proposal.

Question 5. What changes or additional clarification, if any, would be helpful regarding the risks associated with engaging with foreign-based third parties?

There does not appear to be a definition in the Proposal of the term "foreign-based". There might be several different ways to engage a third-party provider that calls into question a foreign element. For example, the provider may actually be domiciled in a foreign nation and services are provided from that location or others outside the US. Alternatively, the provider might be a US corporation that is owned or controlled by a foreign entity and the actual services may or may not be provided from within the US. However, the US subsidiary of a foreign company may be a substantial company on its own that presents the same or similar risk of doing business with a fully US company.

Rather than attempt to spell out specific process actions to be undertaken, it should be sufficient for the bank to apply the Proposal as if the provider is a fully US provider and to identify, and assess, any unique risks related to the provider being "foreign-based".

It would be helpful for the Proposal to provide more insight into what regulators consider "foreign".

Question 8. In what ways could the proposed description of critical activities be clarified or improved?

The Proposal includes the following statement on page 10:

> "The proposed guidance is intended for all third-party relationships and is especially important for relationships that a banking organization relies on to a significant extent, relationships that entail greater risk and complexity, and relationships that involve critical activities as described in the proposed guidance."

This statement clearly establishes that the provisions of the proposal would apply to "…all third-party arrangements…" then introduces the notion of "critical activities". The implication is that there exist activities that are "critical" and others that are "non-critical" although it can be read that, to paraphrase Orwell, all activities are critical but some are more critical than others. If the latter is the intent that would be an overstatement that would lead to a serious distraction (i.e., applying the provisions to all providers) in managing risk. There are clearly third-party providers that banks retain for activities that are not critical.

The term "critical activities" is then defined in the text of the Proposal on page 20 as follows:

> "Critical activities" are significant bank functions or other activities that:
>
> • could cause a banking organization to face significant risk if the third party fails to meet expectations;
>
> • could have significant customer impacts;
>
> • require significant investment in resources to implement the third-party relationship and manage the risk; or

> • could have a major impact on bank operations if the banking organization has to find an alternate third party or if the outsourced activity has to be brought in-house."

Footnote 13 on the same page provides a description of "significant bank functions" in terms of activities with potential material adverse impacts on revenue, profit or franchise value.

It is not clear what is meant by the phrase "... or other activities..." if not "significant bank functions". It would be helpful to at least provide an example or two of such other activities.

The phrasing of the bullet points as "could" result in undesirable outcomes literally can be construed to include everything a bank might undertake. Meteors could destroy both the bank's data center and remote back-up location simultaneously but is highly unlikely to occur. The reality in designating an activity as "critical" is that classification is founded on reasonable expectations and not on extremely unlikely occurrences. An alternative definition would be as follows;

> "Critical activities" are any activities in which the bank engages or undertakes, whether or not third-party providers are utilized, that reasonably is expected to present the bank with material risk exposures to (a) financial loss, (b) adverse impacts on customers, (c) diminution of the bank's reputation or franchise value or (d) impairment of the bank's ability to operate in a safe and sound manner.

The alternative definition deals with activities the bank may do by itself (i.e., "in-house") or outsource to third party providers, in whole or in part. The provisions of the Proposal would then apply to arrangements where third-party providers are utilized and where those providers serve a significant role in conducting the activity. Note that a critical activity may involve the use of a third-party provider in a non-critical role which would not be considered a "critical provider". Notably, in those cases where the bank performs the critical activity "in-house", the bank would be expected to manage the risk as part of its general risk management program. The suggested alternative definition also has the benefit of avoiding use of another ill-defined term ("significant bank functions") in defining an already difficult term to define.

The question still remains as to how to define which providers should be subject to a high level of due diligence and monitoring. As noted above, non-critical activities do not give rise to critical providers and not all providers involved in critical activities are critical providers.

As noted, the statement that the proposal applies to *all* (my emphasis) third party relationships muddies the water. The Proposal should be crystal clear that the provisions are intended to be applied where the assessed risk is highest and not to lesser risks.

The Proposal should also make clear that the bank is to make its own determination as to which third parties are considered in a risk category deserving of a high level of due diligence and monitoring based on its assessment of the risk level of the bank's activities. The method the bank uses to make this determination is fundamental but can be developed as in assessing any risk and would be part of the bank's policy for managing risks associated with use of third parties. An obvious approach would be to evaluate the expected impact the failure of the third party to perform its role has on the four elements in the alternative definition (e.g., financial loss, adverse impact on customers).

The provisions of the Proposal, including the 80+ specific process actions, should only be applied to those providers determined by the bank to be of higher risk (and then only where practically applicable) or at least be considered as informational only to lower risk providers.

10. What revisions to the proposed guidance, if any, would better assist banking organizations in assessing third-party risk as technologies evolve?

By the very nature of evolving technologies, the activity is fluid, not well-developed and not time tested by real life use and at the fringe of reliability and understanding. As a result, the task of assessing risks is made more difficult and complex. In general, the risk assessment (both at the initial stage and during the development and implementation stages) needs to be ongoing and involve extensive review of information. Where an established and well understood activity might suffice with an annual review, in the case of evolving technology, interactions may be monthly or more frequently and ongoing.

The process includes digging deeper into the capabilities and resources of the provider (people, financial, etc.) and obtaining a deep understanding of the provider's understanding of what is expected of banks by regulators, the marketplace and the legal system. For example, it seems that a common thread, although certainly not universal, among fintechs is a lack of appreciation for bank regulatory requirements such as for AML and consumer compliance. A superficial level of understanding and appreciation by the provider can be a serious problem later.

As many providers involved with evolving technologies are themselves newer organizations, there may not be well developed processes for design, development and process management so far more than cursory attention given to process documentation, project management and testing may be necessary.

13. In what ways, if any, could the discussion of shared due diligence in the proposed guidance provide better clarity to banking organizations regarding third-party due diligence activities?

Due diligence addresses both general matters as well as matters very specific to the party conducting the due diligence. For example, in considering a bank to purchase, a buyer may review closely the general financial position of the seller to gain a better understanding of the buyer in a general sense but also to identify specific ways to enhance deal value such as a need for core deposits that fit well with the buyers funding profile. The former is general in nature while the latter is specific to the buyer.

A shared due diligence review works best for general information (especially where the third party offers complex services), such as obtaining and reviewing a SOC report concerning the provider's system or process. To reasonably address the unique interests of each of the parties involved requires the due diligence to address specifics of what is most relevant to each party. While that can be done, it also complicates the work to protect confidentiality of work process, business strategies and the like.

In addition, sharing due diligence may not be as effective for any given party as each party has a different risk appetite. It is important that the shared review appreciate the range of risk appetites of the users of the report so that the due diligence obtains the data needed to help each use to make their analysis in the context of their risk appetite.

The key point is that due diligence of a third party is primarily driven by the risk concerns of the bank and seeking to obtain information that will help understand how the third party will affect the risks involved in the activities being undertaken. This presumes that the bank has first identified the risks inherent in the activity that the third party may affect.

While the person or firm performing an assessment to be shared should preferably be independent of any party involved, whether the third party or a user of the assessment to be shared, that may not always be

practical. In those cases, the lack of independence, and nature thereof, should be disclosed so parties can take that into account.

In any case, banks should clearly understand the implications of anti-trust and possibly privacy laws when involved in sharing arrangements in addition to the issues related to giving or obtaining proprietary information. Of course, banks should be aware of whether sharing of information is within the provisions of any confidentiality and/or non-disclosure agreements that may apply and that sharing what could be detrimental to the third party's reputation may create legal liability.

14. In what ways, if any, could the proposed guidance further address due diligence options, including those that may be more cost effective? In what ways, if any, could the proposed guidance provide better clarity to banking organizations conducting due diligence, including working with utilities, consortiums, or standard-setting organizations?

With respect to SOC reports on page 29, the following is provided:

> "For example, consider whether or not SOC reports from the third party include within their coverage the internal controls and operations of subcontractors of the third party that support the delivery of services to the banking organization."

While subcontractors may be an issue, the sentence would be more helpful for those not accustomed to working with SOC reports as follows:

> "For example, when a relevant SOC report is available, note (a) that the report covers the particular service/s used by the bank without any scope limitations related to features of the services used, (b) whether or not the opinion is unqualified and, if qualified, how that affects the risk assessment, (c) how subcontractors might be used in areas of significance and (d) any control deficiencies that may be relevant to the portion of the service used."

One tool that is often very useful is asking the third party to provide a self-assessment that addresses its experience, capabilities, resources, process effectiveness, quality control and assurance functions and the like. While self-assessments are likely to not address all issues or in fully sufficient depth, the self-assessment is an efficient tool to obtain at least partial information, provides a basis for a more in-depth discussion and helps the bank set the scope of the due diligence (e.g., whether an on-site visit is needed). The Proposal should not discourage a bank from use of third-party self-assessments as a tool. The nature and format of a useful self-assessment can vary widely.

When evaluating a third party using a shared assessment of some type, the bank essentially uses the work product of a third party in its assessment of another third party. Therefore, the assessment third party ("assessor") should also be assessed by the bank if the bank actually relies on the assessor's report in a material way or degree. Alternatively, if the assessor's report is used to set the scope of its own due diligence or to corroborate any results its own efforts, the extent to which the bank needs comfort with the assessor is much lessened. Where the assessor's report is the primary source relied on, the bank would need greater comfort with the assessor and likely some level of corroborating data from another trusted source. The existence of a well-established and independent industry standards-setting body would add value but not be sufficient unless the particular concerns of the bank are addressed.

See also comments for Question 13 as to limitations of shared assessments.

15. How could the proposed guidance be enhanced to provide more clarity on conducting due diligence for subcontractor relationships? To what extent would changing the terms used in explaining matters involving subcontractors (for example, fourth parties) enhance the understandability and effectiveness of this proposed guidance? What other practices or principles regarding subcontractors should be addressed in the proposed guidance?

First, the choice of descriptors (subcontractor or fourth party) used should have little impact on understanding. However, the term sub-contractor is probably more often used by smaller banks.

As with "third parties", the activity involved must first be assessed as "critical" and the role of sub-contractors of the third party would have to be significant to the third party's performance. In most cases it would be expected that the key is how the third party uses sub-contractors and how those are managed. Rarely would it be expected to be necessary to perform due diligence procedures specifically for the subcontractor. Even where subcontractors have a role worthy of additional attention, descriptive information provided by the third party would normally suffice. Where subcontractors are used in roles warranting specific attention, the bank has no privity of contract and relies on the third party's performance thus increasing the importance of a well written contract with the third party including clear and relevant protections.

16. What factors should a banking organization consider in determining the types of subcontracting it is comfortable accepting in a third-party relationship? What additional factors are relevant when the relationship involves a critical activity?

In reality, "third parties" almost always have their own third parties (i.e., subcontractors) even if solely in non-critical roles. It would be rare that a bank could only use third parties who do not have its own third-party providers.

The issue should not be factors to consider but being aware of any significant work being contracted out by the bank's third party so that the bank can assess that risk when assessing the third party. Depending on the bank's risk tolerance, there may be reason for pause where a subcontractor of third party does such a large and significant portion of the service that the bank's third party is little more than a shell.

******

Thank you for this opportunity to comment and provide feedback. Should you wish to discuss any of these comments further, please do not hesitate to contact me.

J. Robert Kelly

/s/

Rogers, Arkansas