October 18, 2021

James P. Sheesley, Assistant Executive Secretary
Attention: Comments-RIN 3064–ZA26
Federal Deposit Insurance Corporation
550 17th Street NW
Washington, DC 20429

Delivered via email: Comments@fdic.gov

Re: Feedback Letter for RIN 3064–ZA26

BancorpSouth Bank ("Bank") appreciates the opportunity to provide the following feedback concerning the request for information on the proposed interagency guidance for third-party relationships. Attached in a separate document we address the questions raised in the proposed rule.

We thank the FDIC for allowing the Bank to comment on the proposed interagency guidance. This guidance will provide clarity on the requirements of financial institutions when engaging third-party vendors. This will allow the industry to continue to provide safe and convenient banking to all consumers.

Sincerely,

[redacted]

Tricia Bellamy, CRCM
BancorpSouth Bank
EVP, Chief Compliance Officer

Enclosure

A. General

1. *To what extent does the guidance provide sufficient utility, relevance, comprehensiveness, and clarity for banking organizations with different risk profiles and organizational structures? In what areas should the level of detail be increased or reduced? In particular, to what extent is the level of detail in the guidance's examples helpful for banking organizations as they design and evaluate their third-party risk-management practices?*

   The guidance does not provide clarity for banking organizations that operate multiple divisions, such as an insurance services division of the company. For example, are there different expectations given that a Business Associate Agreement (BAA) may be in place due to HIPAA requirements? Additionally, do insurance carriers need to be included in the TPRM program? The guidance seems to be lacking in comprehensiveness for varying divisions that could be owned by a banking organization which may or may not be applicable to the same guidance.

   The examples are helpful, but they need to be further defined to align with more complex institutions which have non-typical business arrangements.

2. *What other aspects of third-party relationships, if any, should the guidance consider?*

   With the prior answer being addressed, the guidance would address all aspects of third-party relationships adequately.

B. Scope

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

   A more encompassing definition of third-party provider. There seems to be varying opinions among peers about what constitutes a third-party provider, and the the proposed guidance states "any business arrangement" which is vague. The definition could be enhanced by including all vendors in accounts payable.

2. *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?*

   The description of a "business arrangement" in the proposed guidance provides sufficient clarity to identify those types of arrangements. However, more information examples should be provided regarding banking organizations that have roles in leasing

and renting office space. Are tenants that lease office space from the banking organization considered a "business arrangement" that should be managed by Third-Party Risk? Are property management companies considered "business arrangements" if the banking organization leases office space from them? If so, the guidance needs to cover expectations for those types of arrangements and the amount/level of due diligence.

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

   Further definition and clarification of what constitutes a foreign service provider is needed. For example, vendors are considered foreign to our institution if certain factors are met, including if any Personally Identifiable Information (PII) is housed internationally. Just because the vendor has a foreign mailing address doesn't necessarily imply that they have access to or store any sensitive information internationally which would lead to a higher and more increased level of due diligence and place an undue burden on the banking organization.

C. Tailored Approach to Third-Party Risk Management

1. *How could the proposed guidance better help a banking organization appropriately scale its third-party risk management practices?*

   The proposed guidance states that banking organizations typically consider many factors, among others, in planning for a third party relationship. If any "business arrangement" should be considered as part of Third-Party Risk Management, then there needs to be further clarification or thresholds regarding the applicability to all "business arrangements" otherwise this will place an undue burden on the banking organization. For example, "evaluating whether the potential financial benefits outweigh the estimated costs (including estimated direct contractual costs as well as indirect costs to augment or alter banking organization processes, system, or staffing to properly manage the third-party relationship or to adjust or terminate other existing contracts)." This type of evaluation would not be practical for a $200 per year software license, a plumber, caterer, etc. If this type of evaluation is needed for every "business arrangement" as the guidance seems to suggest, then the burden of establishing and evidencing this would be significant. To scale practices, a monetary threshold, criticality, or the risk posture should be considered.

   The proposed guidance does not address if certain types of relationships, such as: appraisers, legal firms for loan-related activities, insurance carriers, and mortgage investors, can be managed through individual business lines outside of the broader third-party risk program.

2. *In what ways, if any, could the proposed guidance be revised to better address challenges a banking organization may face in negotiating some third-party contracts?*

   The materiality and criticality of contracts is not addressed in the proposed guidance as it relates to negotiating.

   More clarification is needed regarding how often a banking organization should review existing contracts as "periodically" is vague. Additionally, language should be added to specify who should review existing contracts, whether it be a third-party risk management group, the legal team, relationship owner, or another source.

   Banking organization's in some negotiations do not have enough leverage to negotiate and would not be able to obtain all items requested in negotiations. There should be some direction on situations where the banking organization cannot negotiate all requirements.

   Further clarification is needed in regards to documentation. What is the expectation around documenting and collecting the provisions a third party agrees to (or doesn't agree to)? Is the banking organization expected to collect contract data points in a reportable format for key terms and conditions in order to evaluate and assess the potential impacts of important program and legal changes? If required, this will create a significant burden on the program to identify, extract, and populate these data points, which will lead to an increase in staffing requirements.

   The guidance should also address expectations for how examiners will evaluate the challenges a banking organization faces in contract negotiations.

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

   The proposed guidance includes relationships that are considered critical if they require "significant investment in resources to implement the third-party relationship and manage the risk". However, the guidance doesn't specifically mention a monetary threshold. For example it could be further clarified to state that all relationships that constitute a one-time technical capital investment within a certain threshold of are considered a critical vendor. Additionally, all vendors considered "Consumer-Related" that have direct contact with a customer should be considered critical due to the high reputational risk that could be involved. The description could also be improved by considering the third-party service providers deployment model (i.e. whether it's a hosted application) and whether they are storing, accessing, transmitting, or performing transactions on sensitive customer information.

D. Third-Party Relationships

1. *What additional information, if any, could the proposed guidance provide for banking organizations to consider when managing risks related to different types of business arrangements with third parties?*

   The proposed guidance should provide additional clarification regarding concentration risk and include regulator expectations. This would allow the banking organization to build reports and datasets for reporting to assist in managing the risk. Additionally, it would be useful to include what specific relationship concentration risk applies to, i.e. third-parties, 4th parties, 5th parties, etc.

   The oversight of the program by the Board of Directors includes approval of contracts with third-parties that involve critical activities so they will understand the banking organizations strategy for use of third-parties to support products, services and operations and understand key dependencies, costs, and limitations. t This will significantly affect the operational process of third-party risk management if a vendor cannot be fully approved and onboarded until after the Board meets, reviews, and approves contracts that involve critical activities. Additionally, the guidance states the Board should review the results on ongoing monitoring of third-party relationships for critical activities. There needs to be clarification about examiner expectations and what specific criteria should be reported to the Board. For example, should this include third-parties that don't provide the requested due diligence documents, the individual risk reviews that are determined to be suspect, etc.

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

   Addressing relationships where the banking organization has a relationship with a third-party who utilizes their own third-party for hosting services, i.e. Amazon Web Services and Azure. The banking organization is required to conduct due diligence on the 4th party due to the subcontractor relationship. In a vast majority of the time there will not be a contract between the banking organization and the 4th party. Without this contractual relationship, due diligence information is hard or impossible to obtain as confidentiality is cited due to lack of a direct relationship. The same would be true for any critical sub-processor for the banking organization's third-party.

   Further clarification on examiner expectations regarding on-site visits is needed, specifically regarding the circumstances and frequency to which they are to occur. Additionally, what documentation and evidence is expected to be gained during on-site

visits? This could cause staffing and resource burdens for all banking organizations depending on the requirements.

Clarification is also needed for examiner expectations surrounding a formal risk acceptance process including what documentation will be acceptable.

3. *What additional information, if any, could the proposed guidance provide to banking organizations in managing the risk associated with third-party platforms that directly engage with end customers?*

   Additional information should be provided about the criticality of third-party platforms that engage directly with customers due to the increased reputation and operational risk.

4. *What risk management practices do banking organizations find most effective in managing business arrangements in which a third party engages in activities for which there are regulatory compliance requirements? How could the guidance further assist banking organizations in appropriately managing the compliance risks of these business arrangements?*

   When there are third-party activities for which regulatory compliance requirements exist, we request information on cybersecurity, privacy, PCI-DSS, ISO, and various internal questionnaires to address compliance. This is completed at the onboarding stage as well as annually for critical third-party relationships. The guidance could further assist banking organizations by expounding on examiner expectations during an exam.

E. Due Diligence and Collaborate Arrangements

1. *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?*

   The proposed guidance provides sufficient information.

2. *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?*

   The proposed guidance provides sufficient information.

F. Subcontractors (a third party's subcontractors)

1. *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?*

   The proposed guidance could be enhanced to clarify expectations on conducting due diligence for subcontractor relationships. It is difficult, at best, to obtain due diligence documents for a third-party's critical vendors (4th party) when there is no contractual agreement between the banking organization and the 4th party. Examiner expectations need to be clarified as to what is actually required as part of due diligence and how far that due diligence should be extended. Should the banking organization consider 5th and 6th parties? If so, that creates an undue burden on the banking organization. Changing the terms used in explaining matters involving subcontractors would be welcome. It's often difficult to explain 4th parties to third-party providers.

2. *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?*

   A banking organization should consider the presence of a contractual obligation with the subcontractor where they could be held accountable for service-level agreements. Additionally, the banking organization should consider the criticality of the services provided and what access the subcontractor will have to sensitive customer and corporate information, whether that information is transmitted, stored, or housed by the subcontractor, and whether proper security controls are in place, such as multi-factor authentication.

G. Information Security

1. *What additional information should the proposed guidance provide regarding a banking organization's assessment of a third party's information security and regarding information security risks involved with engaging a third party?*

   The proposed guidance should clarify examiner expectations and provide more information on how the risk gaps should be managed and documented.

H. OCC's 2020 Frequently Asked Questions (FAQs) on Third-Party Relationships

1. *To what extent should the concepts discussed in the OCC's 2020 FAQs be incorporated into the guidance? What would be the best way to incorporate the concepts?*

   The OCC's 2020 Frequently Asked Questions (FAQs) on Third-Party Relationships should be incorporated into the guidance by way of an exhibit, abstract, or FAQ at the end of the guidance. They provide useful information that is beneficial to understanding and interpreting the guidance.