American Bankers Association
Building Success. Together.

Krista Shonk
Vice President & Sr. Counsel
Regulatory Compliance and Policy
Phone: 202-663-5014
E-mail: kshonk@aba.com

October 18, 2021

VIA ELECTRONIC SUBMISSION

Ann E. Misback
Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Washington, DC 20551

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

Chief Counsel's Office
Attention: Comment Processing
Office of the Comptroller of the Currency
400 7th Street SW, Suite 3E-218
Washington, DC 20219

Re: Comment on Proposed Interagency Guidance on Third-Party Relationships: Risk Management (Docket No. OP-1752; FDIC RIN 3064-ZA26; Docket ID OCC-2021-0011)

Ladies and Gentlemen:

The American Bankers Association[1] is pleased to comment on the interagency third-party risk management guidance proposed by the Board of Governors of the Federal Reserve System (Federal Reserve), the Federal Deposit Insurance Corporation (FDIC) and the Office of the Comptroller of the Currency (OCC)(collectively, the agencies).[2] The proposed guidance describes the third-party risk management life cycle and identifies principles applicable to the six stages of a third-party relationship, including: (1) strategy and planning; (2) due diligence; (3) contract negotiation; (4) governance and oversight; (5) monitoring; and (6) termination.

Over the years, each of the agencies has issued third-party risk management guidance for its respective supervised institutions. To promote consistency across the agencies, regulators are

[1] The American Bankers Association is the voice of the nation's $22.8 trillion banking industry, which is composed of small, regional and large banks that together employ more than 2 million people, safeguard nearly $19 trillion in deposits and extend $11 trillion in loans.
[2] 86 Fed. Reg. 38182 (July 19, 2021).

jointly seeking comments on the proposed guidance, which is based largely on OCC Bulletin 2013-29. The proposed joint guidance would replace each agency's existing third-party risk management guidance.

ABA supports this joint effort. This undertaking is especially valuable as a bank's ability to compete in the marketplace depends increasingly on the institution's ability to leverage the expertise of third-party service providers and manage those relationships prudently.

I. Summary of Comments

Below are the highlights of our comments on the proposal.

- Scope and Application. The guidance is broad in scope, yet provides that a bank's third-party risk management efforts should be risk-based. As an initial step to addressing this tension, any final guidance should: (1) be limited to situations where there is a written contract between the bank and a third party pursuant to which a bank receives services on an ongoing basis and (2) exclude ad hoc arrangements with limited duration. We also recommend that the agencies explain how banks might apply the principles articulated in the guidance to relationships with particular characteristics.

- Contracting and Due Diligence. The guidance should clarify that the enumerated due diligence factors and suggested contractual considerations are not intended to apply to all third-party relationships and should not be viewed as a mandatory checklist. Our comments offer several examples to illustrate why applying the specified criteria to all third-party relationships is unnecessary and does not enhance a bank's ability to manage its third-party risk.

- Subcontractors. The guidance should expressly acknowledge that banks do not have legal standing with fourth parties and should specify that the recommended contractual considerations regarding bank approval of subcontractors are intended to apply only to a third party's subcontractors that are "material" or "significant" to the service that the third party is providing to the bank.

- FAQs. Any FAQs adopted as part of any updated guidance should be issued on an interagency basis.

- Implementation. Regulators should provide banks with sufficient time to adapt to any final guidance. The proposed guidance is broader and more detailed than the third-party risk management guidance that exists today for banks regulated by the FDIC and the Federal Reserve. Regulators should be mindful that banks regulated by these agencies will need time to identify any gaps between their current practices and the new guidance and align their programs accordingly.

- Opportunities for Agency Coordination and Communication. In addition to updating and aligning their respective third-party management guidance documents, the agencies should take additional actions to reduce some of the friction and duplication associated with third-party risk management. In particular, we urge each of the federal banking

agencies to participate in the FDIC's work to establish a public/private standard-setting partnership and corresponding certification program to help reduce the cost, inefficiencies, and uncertainty related to bank onboarding of third-party service providers. Additionally, the agencies should proactively share "lessons learned" from service provider examinations and should expedite the sharing of service provider examination reports to the extent permitted by law.

II. Comments on the Proposed Guidance

We appreciate and support the agencies' work to update and align their separate guidance documents. Below, we provide several suggestions for clarifying and improving the proposal. These comments were informed by conversations with and input from third-party risk managers, chief risk officers, model risk experts, cybersecurity practitioners, regulatory risk management professionals, and bank legal counsel.

We also note that the agencies request for comment seeks input on the extent to which the concepts discussed in the OCC's 2020 FAQs on third-party risk management should be incorporated into the final version of the guidance. We discuss the FAQs in the relevant topical sections, below. However, we note that the proposal is unclear as to how the FAQs might be incorporated into any final guidance. Specifically, would any FAQs be incorporated into the guidance document itself or would the FAQs remain separate from the guidance? Would the FAQs be issued jointly? To achieve the goal of developing updated, consistent guidance, we recommend that the agencies adopt any standalone FAQs on an interagency basis.

A. Broad Scope and Risk-Based Approach

The breadth of the proposed guidance, coupled with expectations for risk-based third-party risk management, create tension. Further, the proposal articulates a detailed list of factors that banks should consider when conducting due diligence on third parties, but also states that rigorous due diligence efforts should be focused on third parties that support "critical activities," rather than conducting the same level of due diligence and oversight of all third parties regardless of the level of risk. Many of the concepts included in the due diligence and contracting sections of the guidance simply are not relevant to certain types of third-party relationships. In these situations, the proposed guidance would merely add to the "papering" of a bank's third-party risk management program; it would not meaningfully enhance a bank's risk management efforts with respect to those third parties.

1. Third-Party Relationship Characteristics That Should be Excluded From the Guidance

The scope of the proposal is very broad. It would apply to "any business arrangement between a banking organization and another entity, by contract or otherwise." A "business arrangement" includes "activities that involve outsourced products and services, use of independent consultants, networking arrangements, merchant payment processing services, services provided by affiliates and subsidiaries, joint ventures, and other business arrangements where a banking organization has an ongoing relationship or may have responsibility for the associated

records."[3] Based on this definition, the proposed guidance would apply to virtually all third-party relationships.

A fundamental principal of third-party risk management is that banks should focus their efforts on the third parties that present the most risk to the institution. To that end, we recommend that the agencies exclude from the guidance low-risk third party relationships with particular characteristics, such as those that do not involve a written contract or are ad hoc arrangements of limited duration. For these types of relationships, banks should not need to obtain due diligence information, negotiate certain contractual terms, or conduct ongoing oversight of the third party, but rather should apply appropriate controls tailored to the nature of the engagement.

Written Contractual Relationships. As a practical matter, it is highly unlikely that a bank would engage in any form of material or significant relationship with a third party without a written contract. For relationships not governed by a formal agreement, it is unproductive and impractical for a bank to institute due diligence, monitoring, and ongoing oversight, and other formal controls. As such, limiting the scope of the guidance to those third-party relationships that involve the existence of a contract would still capture relationships that may pose material risk to banks or consumers.

Ad Hoc Relationships. We further request that any final guidance be revised to clarify that it does not apply to low-risk, one-time, limited-purpose events that extend over a short period of time, even if a written contract is in place. For example, offsite events, such as customer appreciation outings or investor conferences typically involve legal contract review; however, banks do not conduct initial or ongoing due diligence on the providers of these services and may not include them in the bank's third-party risk management inventory. Further, due diligence for a short-term engagement would have limited value relative the effort expended since the activity would likely be removed from the third-party risk management program within a few months (if it is included at all).

2. Illustrative Examples

We agree that the proposed guidance should be principles-based. However, we also encourage the agencies to explain how banks might apply those principles based on the nature of a particular relationship and hypothetical set of risks. For example, the guidance could discuss situations where it would be appropriate for a bank to deem a third party "out of scope" for purposes of the bank's third-party risk management program or where a bank might apply some, but not all, due diligence factors and contracting considerations described in the proposal. This would help banks to focus their third-party risk management resources on entities that pose the most risk to the bank and reduce the "paper chase" often associated with third-party risk management of entities presenting very limited risk to the institution.

Data Aggregators. For example, we recommend that the agencies clarify that not all types of bank interactions with data aggregators constitute a third-party relationship subject to the proposed guidance.

[3] 86 FR 38186, footnote 10.

The OCC's FAQ #4 provides that even if a bank does not receive a direct service from a data aggregator, the bank should still perform due diligence and gain assurances that the data aggregator maintains controls to safeguard sensitive customer-permissioned data. This FAQ warrants significant revisions.

Today, banks interact with data aggregators in different ways. If a data aggregator provides services to a bank or performs functions on the bank's behalf, that relationship should be subject to the third-party risk management guidance. However, data aggregators often are authorized by and act on behalf of bank customers. These types of relationships are a customer-aggregator relationship; not a bank-aggregator relationship. As such, no business relationship exists and the agencies should not impose third-party management expectations in these situations.

Customer-directed data sharing may involve a contract between the bank and the data aggregator, but that does not make the data aggregator a service provider to the bank. Specifically, the bank and the data aggregator may enter into a contract that establishes the criteria that the data aggregator must meet in order to access customer data[4] and provides for fees (or reimbursement) for the costs of any required connectivity or certification. Banks enter into these agreements to reduce risk and to apply additional protections to their customers' data in the course of its access by the data aggregator in the banking environment. Such a contract does not result in the data aggregator becoming a third-party service provider to the bank and therefore should not be subject the due diligence, contracting, and oversight provisions of the proposed guidance.[5]

By the nature of their business, data aggregators hold a tremendous amount of consumer financial data. It is estimated that data aggregators hold the consumer log-in credentials for tens of millions of customers. ABA believes that data aggregators are subject to the Gramm-Leach-Bliley Act, but their compliance with its privacy and security obligations is not clear and, more importantly, is not subject to supervision or regular examination. Proactive supervision is critical to identifying risks before any harm is done to consumers.

A cornerstone of Title X of the Dodd-Frank Act was the authority given to the CFPB to establish a supervisory program for nonbanks to ensure that federal consumer financial law is "enforced consistently, without regard to the status of a person as a depository institution, in order to promote fair competition." Experience demonstrates that consumer protection laws and

[4] For example, "time, place, and manner" access requirements, representation that the aggregator has been granted formal authorization from the customer to receive log-in credentials allowing for account access, etc.

[5] Relatedly, we note that section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act provides that subject to rules prescribed by the CFPB, a consumer financial services provider must make available to a consumer information in the control or possession of the provider concerning the consumer financial product or service that the consumer obtained from the provider. The CFPB has issued an Advance Notice of Proposed Rulemaking to solicit comments to assist in developing regulations to implement section 1033. Given that banks would be providing such access as a result of a legal mandate and at the direction of the bank's customer, we do not believe that such arrangements constitute a business relationship for purposes of the third-party risk management guidance or the Bank Service Company Act.

regulations must be enforced in a fair and comparable way if there is to be any hope that legal and regulatory obligations are observed. Accordingly, the CFPB should expeditiously initiate the rulemaking process under Section 1024 of the Dodd-Frank Act to define those "larger participants" in the market for consumer financial data that will be subject to regular reporting to and examination by the CFPB. Once the CFPB has imposed supervisory authority over the larger data aggregators, it will be better able to monitor—and react to—risks to consumers in this rapidly evolving marketplace.

Holding Companies and Affiliates. Another area warranting further clarification is the treatment of holding companies and affiliates. The proposal provides that third-party relationships can include affiliates and the bank's holding company, but notes that the determination of whether a banking organization's relationship constitutes a business arrangement may vary depending on the facts and circumstances. However, the proposal does not provide further discussion of the circumstances in which an affiliate or a holding company would be considered within scope for purposes of the guidance. We request that any final guidance elaborate on this point.

As a general matter, a bank should not be expected to conduct the same level of third-party due diligence on affiliates as it conducts on non-affiliated service providers. Rather, a bank should be able to leverage the existing organization-wide internal control framework and document this arrangement accordingly. While it should be unnecessary for the bank to apply the full scope of due diligence factors articulated in the proposal, banks would benefit from an additional explanation of how the detailed list of factors, criteria, and considerations enumerated in the guidance might apply to affiliates, including situations where an affiliate is removed and independent from the bank itself (but perhaps may have some nexus with the bank's holding company).

Appraisers. It would also be appropriate for the agencies to expand on the discussion in the OCC's FAQ #2 to further distinguish between relationships with individual appraisers versus those with appraisal management companies. In discussing the meaning of the term "business relationship," the FAQ states that when a bank requests an appraisal, it enters into an agreement with an individual appraiser. This establishes a business arrangement for purposes of the guidance. The FAQ goes on to discuss appraisal management companies (AMCs) and states that when banks outsource the process of engaging real estate appraisers through AMCs, the bank has a business arrangement with the AMC.

FAQ #2 should be updated to further specify that when banks conduct due diligence on the AMC as an entity, the bank is not required to duplicate the AMC's evaluation and oversight of individual appraisers. In addition, the FAQ should clarify that banks are not required to conduct due diligence on appraisers required by government loan programs. Certain federal loan guarantee programs (e.g., VA and FHA) require that banks use certain appraisers that have been vetted by that particular program. In these situations, appraiser selection is outside of the bank's control and the bank does not have the right to refuse the service or select a different provider.

Further, commercial appraisals pose their own challenges, particularly for out-of-market transactions where there are not AMCs that specialize in commercial properties. In these situations, a bank must locate an appraiser for a single transaction. Banks abide by the

prudential regulators' guidelines for appraisal practices and conduct a baseline of due diligence to ensure that the appraiser is licensed and/or certified as per applicable state requirements. We believe it would be inefficient and unproductive for the bank to collect multiple years of financial statements, conduct a data security review, etc. prior to engaging an individual appraiser to evaluate the property and provide one appraisal report.

3. Optionality

We also request that any final guidance continue to permit banks to oversee vendors and suppliers pursuant to a traditional third-party risk management program while having separate oversight mechanisms and controls for other types of counterparty relationships. Management of these relationships requires specialized expertise that often is not housed in a bank's third-party risk management organization. The guidance should make clear that the appropriate structure for managing these relationships should be based on the nature of the engagement and the risk that it poses to the bank.

For example, correspondent relationships, loan participations, purchases of loan pools, and relationships with retail or merchant establishments where the bank provides consumer financing products and services to these entities do not involve the provision of a service by the third party and are typically overseen by the applicable business unit. In these examples, the third parties are not providing services to a bank nor are they providing services to customers on the bank's behalf.

Similarly, banks that engage in indirect lending for financing automobiles or outdoor power equipment commonly manage dealer relationships within a particular business unit rather than within the bank's third-party risk management program. These dealer management practices are shared with the bank's primary regulator, and the agencies should permit banks to continue this approach so long as dealer oversight is consistent with the third-party risk management principles articulated in the guidance.

Another example involves banks that service mortgages on behalf of their clients that hold the loans. The bank servicers are expected to monitor those clients, but do so as part of the banks' client management function, not as part of third-party risk management.

Merchant payment processing services may likewise have separate oversight mechanisms in place at the business unit level and within the risk team.

4. Criticality

The proposed guidance indicates that banks should "engage in more comprehensive and rigorous oversight and management of third-party relationships that support "critical activities," which 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.

We have two observations regarding a determination of criticality. First, while the proposed list is instructive for purposes of determining criticality, any final guidance should state expressly that the list articulates factors that a bank may apply in determining the criticality of a third party. The significance of an activity or the criticality of a third party will vary from bank to bank depending on the bank's business strategy and the nature of a particular engagement. For this reason, meeting one item on the enumerated list should not automatically deem a third-party relationship "critical" and therefore subject to more in-depth due diligence and oversight. In sum, regulators should defer to a bank's determination of criticality.

Second, the potential for customer impact should not automatically result in a third party being classified as "critical." Rather, criticality should focus on whether a disruption or other service provider event would render the bank unable to perform its core function. For example, third-party services that support transactions that can be accomplished through alternative means, such as online banking, bill pay, or mobile banking, should not automatically be deemed "critical." To address these concerns, the agencies could align the criticality concept with the Federal Reserve and FDIC rules on Resolution Plans for large financial firms and the Interagency Paper on Sound Practices for Strengthening Operational Resilience.[6]

5. Marketplace Lending

ABA supports responsible bank-fintech partnerships. Structured appropriately, these partnerships can increase access to affordable credit, expand financial inclusion, and promote economic growth.

Importantly, marketplace lending arrangements should be structured in a manner that is consistent with bank safety and soundness and prioritizes consumer protection. For these reasons, we believe there is value in incorporating OCC FAQ #19 into the guidance, subject to certain modifications. FAQ #19 describes the third-party risk management considerations a bank should take into account when entering a marketplace lending arrangement with a nonbank entity.

However, we recommend that the FAQ be updated to align with the Federal Reserve's SR Letter 13-19, Guidance on Managing Outsourcing Risk, which clarifies the responsibilities of a bank's board of directors. In particular, we request that FAQ #19 be revised to distinguish between the role of the board and management by clarifying that management (and not the Board) is expected to develop the understanding of the relationship and the risks that it poses. Similarly, the FAQ should be revised to state that senior management should develop policies

[6] 12 CFR pt. 243 (Federal Reserve); 12 CFR pt. 381 (FDIC). A resolution plan, known as a "living will," describes a firm's strategy for orderly resolution under bankruptcy un the event of material financial distress or failure of the firm. The Resolution Planning rule defines "core business lines" as those business lines of the firm, including associated operations, services, functions, and support, that, in the view of the firm, upon failure would result in a material loss of revenue, profit, or franchise value.

governing the relationship, which should be approved and overseen by the board or a board committee.

We understand that the OCC is gathering and analyzing data on bank-fintech partnerships to determine which partnerships present risk to consumers and which promote financial inclusion. This work represents an opportunity to underscore expectations for regulatory compliance and consumer protection that will distinguish responsible bank-fintech partnerships from predatory and abusive lending. We request that the OCC publish the data that it analyzes and provide an opportunity for the public to comment on that data before it takes any additional action related to marketplace lending partnerships.

B. Due Diligence Factors

The due diligence section of the guidance states that "the degree of due diligence should be commensurate with the level of risk and complexity of each third-party relationship" and then provides a detailed list of factors that banks "typically consider" when conducting due diligence on a third party. While these factors are instructive, not all of these due diligence items will be applicable to every third party relationship. Therefore, we recommend that the proposal be revised to (1) state that a bank may take the factors into consideration and (2) expressly state that not all of the factors may be applicable to all third-party relationships. These revisions would better align the due diligence section with the guidance's overarching principle that third-party risk management should be risk-based and tailored to the nature of the relationship involved. These changes would also help to avoid the impression that regulators expect banks to conduct all of the enumerated due diligence factors on all third parties.

Below, we offer several examples of why the enumerated factors may not be applicable to or practicable for all third-party relationships.

1. Business Strategy and Goals

The proposed guidance recommends that a bank assess a third party's overall business strategy and goals, including how the third party's current and proposed strategic business arrangements (such as mergers, acquisitions, divestitures, partnerships, joint ventures, or joint marketing initiatives) may affect the activity; the third party's service philosophies, quality initiatives, efficiency improvements, and employment policies and practices; and whether the selection of a third party is consistent with a bank's broader corporate policies and practices, including its diversity policies and practices.

The guidance should acknowledge that due to confidentiality and competitive concerns, third parties are unlikely to disclose meaningful information related to business strategy and goals that is not already in the public domain. For example, it is not uncommon for banks to conduct reasonable due diligence, enter into a contract with the third party, and subsequently learn that the third party is contemplating a merger.

Also, we agree with the agencies that information pertaining to quality considerations, efficiency improvements, and customer success may be relevant factors for a bank to include in a due diligence review. However, as a practical matter, this information does not help a bank

understand whether the third-party is raising capital, divesting, having liquidity challenges, or looking for a strategic partner.

2. Financial Condition

The proposed guidance suggests that a bank include in its due diligence a review of the third party's financial condition, including an evaluation of audited financial statements, annual reports, filings with the Securities and Exchange Commission, and other available financial information. The guidance also suggests alternative information that a bank may want to consider in its assessment, such as expected growth, earnings, pending litigation, unfunded liabilities, or other factors that may affect the third party's overall financial stability.

As with many of the other due diligence factors enumerated in the proposed guidance, the level of financial due diligence a bank should conduct on a prospective third party and the bank's risk rating of that third party should depend on the nature of that relationship, the services provided, and risk to the bank. It is not uncommon for a privately held firm to decline to share its financial information, or, the requested information may simply be unavailable. In these situations, a bank's inability to evaluate a firm's financial information will become one of the factors in the bank's assessment of that prospective third party, and in some cases, may elevate the bank's risk conclusion. However, the inability to review certain information should not—and does not—automatically preclude the bank from engaging with the third party in all cases.

Relatedly, the guidance provides that "depending on the significance of the third-party relationship or whether the banking organization has a financial exposure to the third party, the banking organization's analysis may be as comprehensive as if it were extending credit to the third party" [emphasis added]. This language is overbroad and implies that any financial exposure merits robust financial due diligence. We suggest that the agencies limit this statement to "significant" or "material" financial exposure.

3. Fee Structure and Incentives

The proposed guidance suggests that banks evaluate a third party's fee structure and incentives to determine if either would create burdensome upfront or termination fees or result in inappropriate risk taking by the third party or the banking organization. The guidance also recommends that banks consider whether any fees or incentives are subject to, and comply with, applicable law.

This section of the proposed guidance should clarify that it is intended to address incentives the bank pays the third party under the contract and that it is not intended to suggest that banks evaluate how the third party compensates it employees or other business partners. Banks expect third parties to refrain from compensating employees working on a bank's behalf in a manner that incentivizes inappropriate risk taking or other inappropriate behavior. While it may be desirable to know what a vendor's policies and practices are in this regard, as a practical matter, third parties are not always willing to disclose compensation practices, and even when third parties share this information, they could adjust the policies without the bank's knowledge after contracting.

4. Risk Management

The proposed guidance recommends that banks evaluate the effectiveness of a third party's risk management protocols, including policies, processes, and internal controls. Among other things, the guidance suggests that banks consider whether the third party's risk management processes align with the bank's practices and assess the third party's change management process to ensure that clear roles, responsibilities, and segregation of duties are in place.

We request that the agencies revise this section of the guidance to recommend that banks evaluate whether the third party has risk management processes that are commensurate with the risk and complexity of the service that the third party is providing. Many third parties will not have the same level of robust risk management practices that banks have. This is particularly the case if the bank is operating under the OCC's Heightened Standards for Large Financial Institutions.

5. Programming Languages

The proposal suggests that banks consider the risks and benefits of different programming languages. Presumably, this requirement is designed to limit bank exposure to outdated languages that may become obsolete. While a bank should evaluate whether a third-party's programming language will be supported, the expectation that banks have the expertise or opportunity to prescribe a third party's programming language is unrealistic. Therefore, we recommend that the agencies significantly revise or omit this due diligence factor.

6. Information Security

The proposed guidance also states that a bank's due diligence should include an evaluation of the third party's information security program and identify key elements of that assessment.

Consistency With the Bank's Program. Among other things, the proposal states that banks should evaluate whether the third party's information security program is "consistent with" the bank's information security program and determine whether there are gaps that present risk to the bank.

Importantly, the proposal does not indicate that a third party's information security program must be identical to the bank's program. This is an important distinction. To avoid confusion and differing interpretations of this element of the guidance, we request that the agencies explain what it means for a third party's information security program to be "consistent with" the bank's program.

While it is unrealistic to expect that all third parties have information security programs that are as robust as banks, if a third party has connectivity to a bank's systems or access to non-public personal information, the third party should have processes, controls, authentication, and recovery procedures the bank deems acceptable. However, as with all other aspects of third

party management, banks should have the flexibility to evaluate the relationship, assess the risk and criticality, and make a determination as to whether the third-party's information security program is adequate as it relates to the bank's relationship with that particular third party.

Expertise. The proposed guidance also states that banks typically determine whether the third party has sufficient experience in identifying, assessing, and mitigating known and emerging threats and vulnerabilities. Evaluating a third party's experience and expertise pertaining to information security helps banks to understand a third party's overall information security posture.

Ideally, banks would be able to obtain information, such as the number of people in the third party's development organization, the number of employees that support their accounts, and the number of personnel with a certain level of experience or who maintain particular credentials. However, our members report that it is often challenging to obtain information about the credentials of the third party's employees, the employees' experience, and information regarding ongoing employee training. This information is not described in any depth in the SOC 1 or SOC 2 and banks report that it is difficult to obtain any information about employees beyond what is included in a firm's sales presentation. Therefore, we recommend that the agencies provide illustrative examples of the types of qualifications and documentation that would be sufficient. We also suggest that the agencies inform fintechs about these expectations during workshops and other outreach events that the agencies host for firms seeking to do business with the banking industry.

Operational Resilience. The proposed guidance includes a detailed list of factors to help a bank assess the third party's preparation for and ability to withstand and recover from operational disruptions.

Obtaining a third party's business continuity plan is the most significant challenge banks face in evaluating a third party's operational resilience. While some of the larger vendors provide this information, small and medium-sized firms commonly view this information as proprietary. In addition, most third parties do not conduct tabletop exercises and are unable to provide the level of detail about their operational resilience that is discussed in the proposal. Therefore, any final guidance should expressly state that consideration of a third party's operational resilience should depend on the criticality of the service that the third party provides and the relative level of risk provided by the particular relationship.

7. Model Due Diligence

As technology continues to evolve, relationships with third parties commonly involve models. However, conducting due diligence on models used by third parties presents multiple challenges.

First, the guidance should recognize the various ways that models are used. For example, a model used by a third party to form a professional opinion and provide consulting advice presents a different risk to the bank than a third-party model used to underwrite loans. In the first scenario, the consultant owns the professional opinion and associated model risk. In the second scenario, the bank bears the risk of the model's outputs.

Second, it can be difficult for a bank to detect all third- and fourth-party models. Third parties are not directly subject to regulations on model risk management and may fail to identify all "models" as defined by the federal banking agencies.

Third, banks are often limited in their ability to obtain detailed model information because third parties often decline to disclose proprietary information about algorithms and model design, thus creating a "black box" issue. Banks manage these risks is by periodically evaluating performance against credit metrics and other performance measures to verify that the models are performing consistently and align with the institution's expectations.

OCC FAQ #22 provides a useful discussion of these issues and its concepts should be incorporated into any final guidance. In particular, FAQ #22 provides an important connection between third-party risk management and model risk management. As described above, it can be difficult for a bank to identify all significant or material third-party and fourth-party models. By addressing model risk issues that exist in the third-party risk management context, the guidance would reinforce the importance of identifying and appropriately managing these models.

Fourth, regulators should be aware that third parties update and revise their models frequently, often without providing advance notice to the bank. Some banks (primarily large institutions) have incorporated contractual language that requires a third party to provide notice prior to deploying model updates so that the bank can perform testing. However, most third parties notify banks of model changes after they have been implemented.

Fifth, third parties commonly rely on models developed by fourth parties. However, because fourth parties are not contractually obligated to the bank, it can be difficult for the bank to obtain detailed information about the model's design. In these situations, banks may try to contractually obligate the third party to provide information about the model's performance. As a practical matter, third parties possess a wide range of expertise and ability regarding model risk management. Third parties that are unwilling or unable to evaluate and share information about fourth-party models are considered a red flag identifying inherent risk to the bank.

C. Contracting

As with the due diligence section of the proposed guidance, the portion of the proposal that addresses contracts with third parties contains a detailed list of factors that a bank "typically considers" during contract negotiations with a third party. However, not all third-party relationships warrant each of these contractual terms. Therefore, we suggest that the guidance be revised to state that banks may consider these factors but that not all factors would be relevant to all third-party relationships. We also offer the following additional observations and suggestions for improving the provisions of the guidance that address bank contracts with third parties.

1. Significant Contracts

The proposed guidance states that legal counsel review may be necessary for "significant contracts." We believe that the term "significant contracts" is appropriate and provides banks

with discretion in how they manage their in-house legal departments and outside counsel. Further, the "significant" standard is compatible with existing bank practices that establish a template of standard terms and conditions required for bank contracts. Under these arrangements, banks do not require legal review if the relationship falls within a particular tier on the bank's risk rating and includes the approved terms and conditions.

We also want to make the agencies aware of the challenges of reviewing, managing, and cataloguing "click through agreements." In these agreements, one party sets up a proposed electronic form agreement to which another party may consent by clicking an icon or a button or by typing in a set of specified words. These agreements are commonly used for technology products, including hardware, software, apps, and other tools. These agreements come up in the third-party management context when the bank enters into a relationship with a third party and is subsequently instructed to download a particular type of software or app so that the third party may complete the task or deliver the service that the bank hired it to perform. It is difficult—if not impossible—for third-party risk managers and attorneys to be aware of—much less negotiate the terms of these agreements. It is a "take it or leave it" scenario and there is no indemnity and no opportunity for recourse should an issue arise. In most instances, click through agreements do not constitute a "significant" contract. However, the technologies associated with these agreements can be necessary in order for a third party to provide a critical service.

2. Contract Approval

The proposed guidance provides that a bank's board of directors (or a designated committee reporting to the board) should be aware of and approve contracts involving critical activities prior to execution. We request that the guidance more closely align with OCC FAQ #26 by distinguishing between board review and approval of a relationship versus board review and approval of contract language. In particular, the guidance should specify that management may present to the board a summary of key contractual terms and the rationale for those terms, which is common practice today. The guidance should not suggest that the board or a board committee must review, challenge, or approve specific contract language.

3. Limits on Liability

The guidance also notes that a contract may limit the third party's liability, in which case the bank may consider whether the proposed limit is in proportion to the amount of loss the bank might experience because of the third party's failure to perform or comply with applicable laws. The bank may also want to consider whether the contract would subject the bank to undue risk of litigation. We do not have suggested revisions to this portion of the guidance; however, we note that third parties commonly seek to limit their liability to the amount that the bank would have paid under the contract over the preceding 12 months. Many times, this is inadequate and banks sometimes struggle with negotiating what is acceptable. This is particularly common with intellectual property indemnities.

D. Subcontractors

Multiple sections of the guidance discuss a third party's reliance on subcontractors and provide suggestions for managing those relationships from a due diligence and contracting perspective. We address both of these sections here and offer the following observations regarding fourth party relationships.

First, any final guidance should expressly acknowledge that banks do not have a contractual relationship with fourth parties. As such, fourth parties are not obligated to respond to due diligence requests from the bank. As a result, banks focus on ensuring that the third party adequately oversees its fourth parties and that contractual language between the bank and the third party obligates the third party to obtain the bank's consent to use a subcontractor that is material to the service that the third party is providing.

Second, both the due diligence and the contracting sections of the guidance should clarify that they apply only to subcontractors that are "material" or "significant." For example, the proposal provides that "[a] material or significant contract with a third party typically prohibits assignment, transfer, or subcontracting by the third party of its obligations to another entity without the banking organization's consent." This provision could be interpreted to imply that a bank must approve the use of all subcontractors, which is unrealistic and would not be helpful in managing risk. Further, requiring a bank to approve any assignment would be inconsistent with common M&A contractual exceptions that permit the third party to assign unilaterally (e.g., in the event the third-party is acquired). Generally, the bank's only recourse in these circumstances is replacing the third party. Practically speaking, the violation would need to be material to the relationship before the bank would declare a breach of contract.

III. Opportunities for Enhanced Agency Coordination and Communication

While banks can benefit significantly from the technological capabilities and efficiencies that third parties provide, they face several challenges in engaging with third-party service providers:

- The increasing sophistication of the products and services provided by third parties makes it difficult for many banks to conduct the requisite due diligence for onboarding innovative, technology-focused service providers;
- Vendor due diligence and oversight is duplicative and inefficient for both banks and third parties; and
- Banks do not have access to important regulatory information prior to entering into contracts with service providers that are examined by the banking agencies.

The proposed joint guidance is one step toward addressing these issues. We also suggest the following additional actions that the agencies could take to reduce some of the friction and duplication associated with third-party onboarding and oversight.

B. Public/Private Standard Setting Program

Banks that are unable to adopt new technologies or partner with new third parties will not be able to provide the products and services that customers increasingly want and expect. Unfortunately, the due diligence necessary to onboard a prospective vendor is costly, inefficient,

and time consuming. In addition, it is often difficult for banks to obtain certain types of due diligence information from prospective third parties—either the third parties cannot provide the requested information or they are unwilling to disclose it. These burdens exist for all institutions, but are particularly acute for community banks.

To help address these challenges, we urge the OCC and the Federal Reserve to join the FDIC's work to create a public/private standard-setting partnership and corresponding certification program to help reduce the cost, inefficiencies, and uncertainty related to bank onboarding of third-party service providers.[7] As envisioned, the standard setting organization would support banks' third-party risk management efforts by assessing and certifying certain aspects of a third party's products or models or by evaluating a third-party provider's operations or condition. By establishing certification standards, the public/private partnership could help to address some of the hurdles that banks face in collecting the requisite due diligence information, enhance the level of scrutiny and in-depth analysis given to certified providers (particularly in the technology space), and alleviate some of the inefficiencies and redundancies in the onboarding and oversight of third-party service providers.

While this initiative has the potential to benefit banks, third-parties, and regulators, two elements are critical in order for a certification program to be successful:

First, all of the federal banking agencies must be active standard setting contributors. Standing up and maintaining a standard-setting and certification mechanism would be a large and complex undertaking that would benefit from being conducted on an interagency basis. Buy-in from all of the agencies would enhance the credibility and reliability of the standard and corresponding certification. Moreover, for a standard-setting and certification mechanism to be successful, regulators will need to be full contributors to the standard setting process, not just observers. Their involvement would distinguish the public/private partnership from other standard setting organizations that exist today and would incentivize banks and service providers to participate in the public/private partnership and certification process.

Second, regulators must give clear and unequivocal assurances in amended third-party guidance statements and exam procedures that banks may rely on information and findings provided by a certifying organization. Regulators should expressly state that banks may rely on such certification in lieu of collecting and analyzing due diligence information independently. Failure to provide (and reinforce with examiners) these unambiguous assurances would miss an opportunity to leverage collective industry expertise in order to improve the quality of third-party risk management and meaningfully reduce cost and duplication of effort.[8]

---

[7] *See* ABA's comment letter responding to the FDIC's Request for Information on Standard Setting and Voluntary Certification for Models and Third-Party Providers of Technology and Other Services dated September 22, 2020.

[8] We acknowledge, however, that there are circumstances in which banks may need to conduct additional due diligence and analysis of a firm or technology, for example, if the bank's use of that product exceeds the scope or tier of a particular certification. Additionally, we recognize that any certification or due diligence information would represent a third-party's condition, features, internal controls, and compliance status as of a specific point in time. As a result, we understand that banks have an independent obligation to monitor the product, technology, and performance of the service provider. However, banks should be able to rely on updated information gathered via certification updates in order to help perform this task.

C. Sharing of Service Provider Examination Information

The federal banking agencies have statutory authority to supervise third-party service providers that enter into contractual arrangements with regulated financial institutions.[9] By virtue of this examination authority, bank regulators possess a great deal of information pertaining to the regulatory compliance and overall condition of service providers examined pursuant to the Bank Service Company Act. We recommend that regulators share this information with banks in the following ways.

Automated, Timely Distribution of Examination Reports. Today, regulators provide a third party's examination report to banks that have contracted with and receive services from the service provider. Whether these reports are distributed automatically or upon request varies according to the exam rating that the service provider receives. According to the Federal Regulatory Agency Administrative Guidelines published in 2012, the agencies distribute exam reports to banks that had a valid and current contract with the service provider as of the date of the examination as follows:

- Exam rating of 4 or 5: Automatically distribute service provider exam reports.
- Exam rating of 3: May distribute an exam report without a bank request.
- Exam rating of 1, 2, or 3: Distribute upon request from a bank.

This distribution system presents several drawbacks. First, banks do not know when a service provider has been examined and therefore do not know when to ask the agencies for copies of the exam report. Another challenge is the varying levels of documentation that regulators require banks to demonstrate that they are in a contractual relationship with the service provider and are therefore entitled to a copy of the examination report.[10]

In 2019, the agencies piloted a new distribution system under which the agencies would automatically provide exam reports to banks that are in a contractual relationship with the service provider, regardless of the provider's exam rating. The pilot has ended and interagency work is underway to refine the process and apply lessons learned. We understand that the agencies are still 12 months away from rolling out this new process. These are positive, common sense changes and we urge the agencies to accelerate the timeline of this initiative.

Relatedly, we note that the CFPB has begun to examine service providers pursuant to the agency's supervisory authority established in the Dodd-Frank Act. We are aware of some instances in which individual banks are coordinating with CFPB examiners to obtain copies of

[9] 12 USC 1464(d)(7), 1867(c)(1). In addition, the Consumer Financial Protection Bureau (CFPB) has authority as described in 12 USC 5514(e), 5515(d), and 5516(e). See CFPB Bulletin 2012-03 (Apr. 13, 2012).

[10] For example, banks must provide listing of service(s) contracted for and date(s) contracted for the service(s). Presumably, if the list does not match the exam scope, the request for the exam report may be denied

service provider exam reports. This is a positive development, and we encourage the CFPB to share this information with all banks who are in a contractual relationship with an examined service provider, not just banks that are supervised by the CFPB. Further, we suggest that the CFPB coordinate with the banking agencies to leverage the lessons learned from the 2019 pilot project to distribute service provider exam reports automatically.

Topical List of Findings Prior to Contracting. Second, regulators should institute a mechanism that helps—not hinders—banks evaluate a service provider's compliance with applicable laws and regulations prior to entering a contractual relationship with a third party that is examined by the agencies pursuant to the Bank Service Company Act. While we recognize that sharing copies of examination reports may be prohibited, regulators should consider sharing a topical list of Matters Requiring Attention (MRAs) that have been issued to a particular service provider as long as a bank has formally extended a Request for Proposal (RFP) to that service provider and is subject to a confidentiality agreement.

D. Regulatory Observations/Trends

We appreciate the agencies' newly-released guide on *"Conducting Due Diligence on Financial Technology Companies — A Guide for Community Banks"* (the Guide), which is intended to help community banks assess risks when considering relationships with fintech companies. The Guide is a helpful compilation of regulatory expectations and provides a useful roadmap of topics on which regulators are likely to focus during examinations. In particular, the Guide will be a useful resource that banks can use to educate prospective fintech partners about the categories of information that banks are likely to request as part of the due diligence process.

We urge the agencies to seek additional opportunities to share information and observations pertaining to third party risk management. For example, the agencies could identify and publish information about "hot topics" involving third-party management, examination trends, and lessons learned from bank-fintech relationships. This could be a joint, FFIEC project that is similar to the CFPB's Supervisory Highlights publication. Such a publication would be informative for banks and fintechs alike and could be especially useful for educating non-bank firms.

IV. Looking Forward

Thank you for the opportunity to comment on potential revisions to the proposed third-party risk management guidance. We support the agencies' work to align their existing guidance and believe that updated guidance will enhance banks' third-party risk management efforts. Importantly, regulators should provide banks with sufficient time to adapt to any final guidance. As proposed, the guidance is broader and significantly more detailed than the current third-party risk management guidance for banks that are regulated by the FDIC and the Federal Reserve. Accordingly, we request that the agencies provide flexibility to these institutions as they work to identify any gaps between their current practices and the new guidance and make any necessary adjustments.

Finally, we reiterate our recommendation that the agencies continue to explore additional actions that would address some of the challenges that banks face in onboarding and

overseeing third parties. In particular, we strongly support the FDIC's work to establish a public/private standard-setting partnership and corresponding certification program to help reduce the cost, inefficiencies, and uncertainty related to bank onboarding of third-party service providers and recommend that the Federal Reserve and the OCC join that effort.

We welcome the opportunity to provide additional information and input as the agencies' work on third-party risk management issues proceeds. Should you have any questions regarding our comments, please contact Krista Shonk.

Sincerely,

Krista Shonk
Vice President and Sr. Counsel
Fair & Responsible Banking
Regulatory Compliance and Policy