October 18, 2021

Via Electronic Mail

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

Ladies and Gentlemen:

The Bank Policy Institute[1] appreciates the opportunity to comment on the proposed interagency guidance and request for comment issued by the Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and Office of the Comptroller of the Currency (each an "Agency," and collectively, the "Agencies") on managing the risks associated with third-party relationships,[2] which would replace each Agency's existing guidance on this topic[3] with a framework based on specific risk management principles for banking organizations to consider in developing risk management practices for all stages in the life cycle of third-party relationships. BPI strongly supports the Agencies' efforts to harmonize supervisory expectations for banking organizations' management of third-party risk. BPI also strongly supports the extent to which the Proposed Guidance would emphasize

---

1 The Bank Policy Institute is a nonpartisan public policy, research and advocacy group, representing the nation's leading banks and their customers. Our members include universal banks, regional banks and the major foreign banks doing business in the United States. Collectively, they employ almost 2 million Americans, make nearly half of the nation's small business loans, and are an engine for financial innovation and economic growth.

2 *Proposed Interagency Guidance on Third-Party Relationships: Risk Management*, 86 Fed. Reg. 38182 (July 19, 2021) (hereinafter "Proposed Guidance").

3 *SR Letter 13–19/CA Letter 13–21, Guidance on Managing Outsourcing Risk* (December 5, 2013, updated Feb. 26, 2021) (Federal Reserve); *FIL–44–2008, Guidance for Managing Third-Party Risk* (June 6, 2008) (FDIC); *OCC Bulletin 2013–29, Third-Party Relationships: Risk Management Guidance* (Oct. 30, 2013) and *OCC Bulletin 2020–10, Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013–29* (March 5, 2020) (OCC).

the appropriateness of banking organizations' adopting risk management practices that are commensurate with the level of risk and complexity of their respective third-party relationships. To that end, BPI appreciates the Agencies' use of language in the Proposed Guidance that is, relative to existing Agency guidance on this topic, less prescriptive and that would, if adopted, better position banking organizations to apply the Proposed Guidance in a risk-based manner.

At the same time, this letter includes suggestions intended to build upon the Proposed Guidance's goal of establishing a third-party risk management framework based on sound risk management principles. There are a number of ways in which the Proposed Guidance may be improved and strengthened, in particular by clarifying the scope and application of the guidance. A major theme that runs throughout our comments is that, to ensure that banking organizations can apply the Proposed Guidance in a risk-based manner, key definitions and concepts should be revised to clarify that banking organizations have the flexibility to apply the Proposed Guidance as appropriate to the nature of the risk presented by a given third party. We also recommend that certain of the OCC's 2020 FAQs on Third-Party Relationships ("2020 FAQs")[4] be incorporated and revised, as appropriate, to reinforce this concept.

Part I of this letter provides an executive summary of our recommendations. Part II provides our overarching comments on the Proposed Guidance, and Part III provides a range of other comments on more discrete or technical matters. In addition, for convenience, Appendix A to this letter summarizes our recommendations with respect to each of the 2020 FAQs.

I. Executive Summary

Overarching comments on the Proposed Guidance:

- We support the Agencies' use of less prescriptive language throughout the Proposed Guidance;
- The Agencies should clarify the scope and application of the Proposed Guidance by revising key definitions and governing concepts:
  - The proposed definition of "business arrangement" is overly broad and inconsistent with the stated goals of the Proposed Guidance;
  - The proposed definition of "critical activities" should be revised to allow banking organizations the flexibility to determine which activities are, in fact, critical and align with existing definitions;
  - The Proposed Guidance's reference to risk management practices that are "typical" is an important improvement over prior, more prescriptive terminology, and should be construed and applied flexibly in practice;
- The Agencies should update and incorporate the 2020 FAQs, as appropriate; and

[4] *OCC Bulletin 2020-20, Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29* (March 5, 2020), https://www.occ.gov/news-issuances/bulletins/2020/bulletin-2020-10.html.

- Given the different and unique risks that they pose, the Proposed Guidance should take an alternative approach to managing the third-party risks of data aggregators, including by removing certain data aggregator relationships from the scope of the Proposed Guidance.

Other comments on the Proposed Guidance:

- The Proposed Guidance should permit senior management to establish policies governing third-party relationships;

- The Proposed Guidance should provide banking organizations with greater flexibility in the negotiations and approval of vendor contracts;

- The Agencies should use their existing regulatory tools and authorities, including the Bank Service Company Act, to directly obtain information from, and exercise oversight of, third-party vendors that serve a large number of banking organizations or over which banking organizations have little negotiating power;

- The Proposed Guidance should clarify that banking organizations are not expected to perform due diligence and oversight of subcontractors, and instead may assess the third party's third-party risk management program;

- Upon adopting final guidance on third-party risk management, the Agencies should review and revise the FFIEC's Information Technology Examination Handbook to ensure alignment; and

- Final guidance should outline the Agencies' views on services covered by the Bank Service Company Act and better define the Agencies' expectations for filings under the Act.

II. Overarching Comments on the Proposed Guidance

A. We support the Agencies' use of less prescriptive language throughout the Proposed Guidance.

Consistent with the Agencies' final rule clarifying the role of supervisory guidance,[5] the Proposed Guidance would not employ language stating that banking organizations "should" take certain actions or "ensure" certain results. Instead, the Proposed Guidance would list considerations "typically" considered by banking organizations relative to the scope, scale, and risk of their respective third-party

[5] We strongly support the Agencies' codification of their policies concerning the use of supervisory guidance, as doing so strengthened the important and helpful role that supervisory guidance plays in the U.S. system of bank regulation and supervision. 12 C.F.R. part 262, App. A (Federal Reserve); 12 C.F.R. part 302, App. A (FDIC); 12 C.F.R. part 4, App. A to Subpart F (OCC) (hereinafter "final rule on supervisory guidance"). Consistent with the final rule on supervisory guidance, we recommend that Section D (Supervisory Reviews of Third-Party Relationships) of the Proposed Guidance — which would state, "actions [based on deficiencies in supervisory findings] may include issuing Matters Requiring Attention, Matters Requiring Board Attention, and recommending formal enforcement actions" — be clarified to avoid suggesting that the Proposed Guidance would create requirements for banking organizations.

relationships.[6] As with the adoption of the final rule on supervisory guidance itself, this shift in language in the Proposed Guidance would represent a significant step forward in the Agencies' continuing work to examine and better communicate how they use supervisory guidance in practice, and to appropriately ground and align those practices with the fact that guidance cannot in and of itself create binding, enforceable legal obligations for the banking organization.

B. The Agencies should clarify the scope and application of the Proposed Guidance by revising key definitions and governing concepts.

1. The proposed definition of "business arrangement" is overly broad and inconsistent with the stated goals of the Proposed Guidance.

Consistent with OCC Bulletin 2013-29[7] and the 2020 FAQs, the Proposed Guidance would define a third-party relationship as "any business arrangement between a banking organization and another entity, by contract or otherwise." It would also note that the term ''business arrangement'' is meant to be interpreted broadly to enable banking organizations to identify all third-party relationships for which the Proposed Guidance is relevant.

This definition is unnecessarily broad and goes beyond the scope of what is necessary to achieve the objectives of the Proposed Guidance. To address these concerns, the Agencies should narrow the definition of "business arrangement" to mean "any mutual understanding or agreement between a banking organization and a third-party entity *by which the entity is required or commits to provide ongoing goods or services to or for the banking organization pursuant to a written contract*." This revised definition would be more appropriate for several reasons. First, and helpfully, it would more clearly exclude banking organization to customer relationships, which involve the provision of goods and services *to* customers, *by* the banking organization.[8]

---

[6] We note that, in certain instances, the Proposed Guidance nonetheless would use the terms "ensure" and "should" when describing risk management life cycle activities. The final guidance should omit these terms, both because these terms are inconsistent with the risk-based approach articulated in the Proposed Guidance and because it is not clear whether their use is intended to imply a higher standard than for those other considerations "typically" taken into account by banking organizations. To the extent that the Agencies wish to establish any particular practice or result as required in all cases, they should do so by notice-and-comment rulemaking as required by law, and not through the use of prescriptive language in supervisory guidance.

[7] *OCC Bulletin 2013-29, Third-Party Relationships: Risk Management Guidance* (Oct. 30, 2013), https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html.

[8] In today's financial services marketplace, we acknowledge that whether a banking organization is providing or receiving goods or services may depend on the perspective of the relevant parties. For example, the Federal Reserve describes "front-end fintech partnerships" in its recent report on community bank partnerships with fintech companies (such as where a banking organization has entered into a contractual arrangement with a third party, pursuant to which depositors may open and access deposit accounts at the banking organization through a technology platform owned and operated by the third party). In this third-party relationship, the banking organization may be viewed as both a recipient and a provider of services. BPI recognizes, and believes it would be appropriate for the Agencies to clarify, that in "front-end" business arrangements between a banking organization and a third party, the third party should be viewed as a service provider to the banking organization, notwithstanding the fact that the third party may view itself as a customer of the banking organization. Federal Reserve Board, *Community Bank Access to Innovation through Partnerships* (Sept. 2021),

Second, the addition of language specifying that the arrangement must be "pursuant to a written contract" would address circumstances in which a third party may pose a risk to the banking organization, but there is no mutuality by which the banking organization may exercise any control over the third party and its actions. While the Proposed Guidance and OCC Bulletin 2013-29 state that a written contract is not necessary to establish a business arrangement, it is the written contract that provides a banking organization with the legal authority to direct the third party to comply with the majority of the third-party risk management life cycle practices described in the Proposed Guidance.[9] The approach we suggest here is consistent with the Federal Reserve Board's 2013 guidance, which focuses on relationships with "entities that have entered into a contractual relationship with a financial institution to provide business functions or activities."[10] For a third-party risk management framework to be effective, a banking organization must have a mechanism that allows the organization to enforce legal rights relative to a third party and an avenue through which the organization can ensure that each and every third party captured by the risk management framework is required to comply with supervisory expectations for the relationship. Indeed, the importance of contractual relationships in implementing an effective third-party risk management framework is highlighted by the Proposed Guidance itself, which devotes a significant portion of its content to the contract negotiation stage of the third-party risk management life cycle.

Moreover, the addition of "pursuant to a written contract" would make clear that local police, fire, social services, and other municipal services are explicitly out of scope of the Proposed Guidance. That result is appropriate because these services are not "business arrangements" of which a banking organization can conduct due diligence or to which it can otherwise apply the third-party risk management life cycle.

Third, the proposed definition of business arrangement should include a "continuous basis" element. Without this element, a one-off or single service would be included within the scope of the Proposed Guidance and trigger application of the full risk management life cycle described in the Proposed Guidance. However, these non-ongoing services generally have a different and significantly lower risk profile and do not require ongoing management over a life cycle in the way a recurring arrangement does.[11] Certainly, these discrete services may pose risks that can and should be addressed through risk management, but will frequently call for risk management approaches and principles that

---

https://www.federalreserve.gov/publications/files/community-bank-access-to-innovation-through-partnerships-202109.pdf.

9 We note that the Proposed Guidance would also describe the "Oversight and Accountability" practices within its life cycle model of risk management, which implies that these activities are being identified as an additional stage to the life cycle. Proposed Guidance at 38193. Since it is not a life cycle phase, we request that Oversight and Accountability be moved elsewhere in the guidance to clarify that it is not one of the steps to the life cycle.

10 Federal Reserve Board, *SR 13-19: Guidance on Managing Outsourcing Risk* (Dec. 5, 2013), https://www.federalreserve.gov/supervisionreg/srletters/sr1319a1.pdf.

11 We also note that including a "continuous basis" element in the definition of "business arrangement" would promote consistency with international regulatory approaches, which is particularly important for banking organizations subject to multiple regulatory regimes. *See, e.g.,* Bank of England Prudential Regulatory Authority, *Outsourcing and third party risk management* (effective March 31, 2022) and Swiss Financial Market Supervisory Authority, *Circular 2018/3 Outsourcing - banks and insurers* (effective April 1, 2018) (each including an ongoing basis component within the equivalent definition of business arrangements subject to the guidance).

are different than the continuous, multi-phase life cycle framework described in the Proposed Guidance.[12]

If the Agencies choose not to incorporate a "continuous basis" element into the definition of "business arrangement," at a minimum and in the alternative, the Agencies should make clear in the final guidance that one-off or non-ongoing business arrangements may often pose substantially less and different risks than those posed by continuous services and therefore, consistent with the risk-based nature of the Proposed Guidance, a number of the activities described as "typical" in the third-party risk management life cycle may not be warranted for such a business arrangement. The final guidance should acknowledge that it is entirely appropriate for a banking organization to take into account the length of service (i.e., whether it is ongoing or temporary) when assessing the risk of a particular business arrangement and to apply the third-party risk management life cycle accordingly. As one example, a short-term proof of concept engagement would not necessarily warrant the same risk-management approach as a longer-term, ongoing partnership, as it may be appropriate for the banking organization to implement fewer controls or contractual protections, and to conduct less rigorous due diligence, for the former.

We also recommend that the Agencies explicitly recognize that arrangements with affiliates of the banking organization may present lower and different types of risks than those with unaffiliated third parties, and thus, consistent with the risk-based nature of the Proposed Guidance, a number of the activities described as "typical" in the third-party risk management life cycle may not be warranted for such a business arrangement. For example, the Agencies should recognize that not all of the due diligence and ongoing monitoring factors "typically" considered in the Proposed Guidance would be warranted for arrangements with affiliates; in many such cases, it would be more appropriate to employ compensating controls, such as monitoring internal audit reports, than to employ many of the "typical" practices outlined in the Proposed Guidance. Incorporating this concept would reinforce the risk-based nature of the Proposed Guidance and clarify its application to business arrangements with affiliates.

Additionally, we note that there are a range of third-party relationships that present significantly lower risk than others and/or unique risk management considerations.[13] For that reason, we urge the Agencies to (i) make clear in any final guidance that such relationships are outside the scope of the definition of "business arrangement" and thus not subject to the final guidance, and/or (ii) to the extent any of such relationships may be included within the scope of the final guidance, acknowledge in the final guidance that certain relationships may pose different or lesser risks than other third-party relationships and thus some or all of the risk management practices described in the Proposed Guidance may not be typical or necessary with respect to these relationships, consistent with the risk-based nature of the Proposed Guidance.

---

[12] Moreover, it is not necessarily appropriate in all instances for banking organizations to apply every aspect or stage of the risk management life cycle to a given third-party relationship, even if this relationship constitutes a "business arrangement" under the guidance. Even the applicability of a life cycle stage should be commensurate with the risk that the third party imposes on the banking organization.

[13] By way of example, such third-party relationships may include certain advisory services, clearing and settlement arrangements, correspondent banking services, financial market utilities, global financial messaging infrastructures, market information services, trust and custody services, screen scrapers (see Section II.D), and utilities and public services (e.g., electricity, gas, water, telephone line, and internet services).

2. The proposed definition of "critical activities" should be revised to allow banking organizations the flexibility to determine which activities are, in fact, critical and align with existing definitions.

Consistent with OCC Bulletin 2013-29 and the 2020 FAQs, the Proposed Guidance would define "critical activities" as significant bank functions[14] or other activities that (i) could cause a banking organization to face significant risk if the third party fails to meet expectations; (ii) could have significant customer impacts; (iii) require significant investment in resources to implement the third-party relationship and manage the risk; or (iv) 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. This definition of "critical activities" is crucial to the overall scope and effect of the Proposed Guidance because the guidance elsewhere indicates that the involvement of critical activities may trigger the need for, among other things, (i) review and approval of plans by an organization's board of directors ("board of directors") or a committee thereof, (ii) more extensive due diligence, (iii) periodic independent reviews, and (iv) more comprehensive monitoring. Importantly, this designation would also trigger an expectation under the Proposed Guidance that the board of directors (or a designated committee thereof)[15] approve the banking organization's contract with the third party. Because of the significance of this definition and the consequences under the Proposed Guidance of an activity being deemed critical for this purpose, it is important that the Agencies revisit and better tailor this definition to cover only those third-party arrangements that are truly higher-risk and critical in nature, in three specific ways.

First, we suggest that the third prong of the definition, which would capture activities that "require significant investment in resources to implement the third-party relationship and manage the risk," be eliminated. Absent true indicia of criticality, the mere fact that certain activities may involve significant implementation costs does not mean they pose greater risk, nor is it clear how or why they would benefit from enhanced risk management, such as more extensive due diligence, periodic independent reviews, or more comprehensive monitoring. We recommend that this third prong be struck because it is inconsistent with, and would undermine, the risk-based nature of the Proposed Guidance.

Second, the Proposed Guidance should also clarify that banking organizations may employ different risk-tiering processes when identifying "critical activities" (e.g., the use of questionnaires, decision-trees, business continuity factors, and senior management review, among other processes), and that the level of "criticality" of a particular third-party arrangement or activity may vary by institution.

We also note that the identification of "critical activities" through a banking organization's risk management process is often also used as the means to identify which third-party activities merit special consideration for purposes of resiliency and resolution and recovery planning. It is therefore important that the Proposed Guidance's definition of "critical activities" aligns with similar terms and

---

[14] Significant bank functions include any business line of a banking organization, including associated operations, services, functions, and support, that upon failure would result in a material loss of revenue, profit, or franchise value. Proposed Guidance at 38187.

[15] See Section III.A for our recommendations with respect to this proposed language.

definitions used in the interagency *Sound Practices to Strengthen Operational Resilience*[16] (i.e., "critical operations" and "core business lines") and the Federal Reserve's and FDIC's resolution planning rules[17] (i.e., "critical operations" and "critical services").

Finally, the Agencies should explicitly incorporate FAQ 8 of the 2020 FAQs into the Proposed Guidance, which FAQ recognizes that (i) not every relationship involving critical activities is necessarily a critical third-party relationship and (ii) mere involvement in a critical activity does not necessarily make a third party a "critical third party." FAQ 8 acknowledges that it is common for a banking organization to have several third-party relationships that support the same critical activity (e.g., a major bank project or initiative), but not all of these relationships are critical to the success of that particular activity, and thus only relationships that are critical to the success of a critical activity are themselves critical. The Proposed Guidance should incorporate this important clarification.

3. The Proposed Guidance's reference to risk management practices that are "typical" is an important improvement over prior, more prescriptive terminology, and should be construed and applied flexibly in practice.

As described above, the Proposed Guidance would generally employ less prescriptive language than prior Agency guidance on this topic by describing "typical" risk management practices, rather than practices that a banking organization "should" employ or results it must "ensure." Similarly, the Proposed Guidance would articulate risk-based "principles" by which banking organizations can manage the risks presented by third-party relationships.

To be clear, we strongly support both the principles-based nature of the Proposed Guidance and its use of illustrative examples rather than prescriptive mandates. This change is an important improvement that should allow banking organizations to more effectively employ an appropriate, risk-based approach to the varied business arrangements they enter into with third parties. To further reinforce this approach, it would be helpful for the Agencies to reinforce in the final guidance that banking organizations may apply these principles flexibly in practice, based on a wide range of factors that may be applicable under the circumstances. Specifically, the final guidance should clarify that, for any particular risk management practice described in the Proposed Guidance, that practice may be "typical" only to the extent (i) *relevant* in light of the nature of the third-party relationship and services provided, and (ii) *warranted* by the risks posed to the banking organization and how those risks may be mitigated.

This recognition is important because there are a wide range of reasons that any specific risk management practice described in the Proposed Guidance as "typical" may be not relevant, warranted, realistic, feasible, or even legally defensible in any particular case. For example, as we describe in Section II.B.1 above, certain phases of the third-party risk management lifecycle may not be applicable to isolated or episodic business arrangements. Similarly, in the due diligence phase, it is not necessarily "typical" to evaluate in all cases:

---

[16] *Federal Reserve SR 20-24* (Nov. 2, 2020), *FDIC FIL-103-2020* (Nov. 2, 2020), and *OCC Bulletin 2020-94* (Oct. 30, 2020), https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20201030a1.pdf.

[17] 12 C.F.R. part 243 (Federal Reserve) and 12 C.F.R. § 360.10 (FDIC).

- The third party's ownership structure, including any beneficial ownership, whether public or private, foreign or domestic ownership (e.g., because the arrangement may be non-ongoing and pose low risk);

- The third party's employee training program or policies and procedures for identifying and removing employees who do not meet minimum background check requirements or are otherwise barred from working in the financial services sector (e.g., because the third party's employees may not always play a role in providing the service);[18]

- Risks presented by different programming languages used by the third party (e.g., because programming languages may not be relevant to the arrangement); or

- The third party's legally binding arrangements with subcontractors or other parties to determine whether the third party has indemnified itself (e.g., because obtaining this information may create its own risks related to confidentiality or material non-public information).

Finally, as we describe in detail in Sections III.B-D, numerous aspects of the contract negotiation stage identified in the Proposed Guidance should not be considered "typical" in many or all cases.[19]

In circumstances like these and others, it may be the case that other practices or controls are more appropriate means by which a banking organization may mitigate certain third-party risks. And in some cases where a particular practice is not appropriate or feasible, banking organizations may pursue compensating controls or alternative practices to mitigating the risk and, where such controls or practices are not available or practicable, the banking organization may consider whether to proceed nonetheless because the benefits of the relationship nonetheless outweigh the risks, and the risks are within its overall risk appetite. The Agencies should affirm that such alternative approaches are entirely consistent with the Proposed Guidance, given its risk-based nature.

For these same reasons, it will also be important that the Agencies reinforce to examiners, through education, outreach, and similar efforts, that examiners should not view any particular "typical" consideration as necessarily required or expected, as doing so would undermine the risk-based nature of the Proposed Guidance by treating each practice as a *de facto* requirement in practice. Business and risk management groups within a banking organization can decide how best to manage the underlying risk, and examiners can approach and evaluate the suitability of a banking organization's risk management practices using their experience and expertise, informed by the final guidance.

---

[18] Indeed, federal and state laws relating to joint employment can create significant liability for banking organizations with regard to their third-party vendor relationships. For this reason, banking organizations generally are careful to exercise any duty (contractual or in day-to-day practice) for background checks, employee discipline, training programs, and other policies and procedures for non-employees that may not be strictly necessary.

[19] The Proposed Guidance also would state that contract negotiation typically addresses a third party's procedures for "immediately notifying" the banking organization whenever service disruptions, security breaches, compliance lapses, or other types of events pose a significant risk to the banking organization. However, "immediate notification" is not commercially practicable and there are competing regulatory requirements for notification of such incidents. Accordingly, the Proposed Guidance should be amended to add "consistent with applicable regulatory requirements" to this consideration.

C. The Agencies should update and incorporate the 2020 FAQs, as appropriate.

The Proposed Guidance would include the 2020 FAQs as an exhibit, separate from the Proposed Guidance, and requests comment on the extent to which the concepts included in the 2020 FAQs should be incorporated into the final version of the proposal. Many of the 2020 FAQs provided helpful clarifications to OCC Bulletin 2013-29, and these clarifications should be incorporated directly into the final guidance and modified as necessary. To that end, throughout this letter, we reference instances in which incorporating one of these FAQs into a particular section of the Proposed Guidance would be appropriate. Similarly, where any of the 2020 FAQs are *not* incorporated into the Proposed Guidance, we suggest that the FAQ be rescinded, rather than continuing to be appended to the Proposed Guidance as an exhibit. Retaining the 2020 FAQs as a separate document would create the potential for confusion in the application of the Proposed Guidance by both banking organizations and the Agencies, particularly where the same topic is addressed in both the Proposed Guidance and 2020 FAQs. For convenience, Appendix A to this letter provides our recommendation for the disposition of each FAQ.

We also note that, when the Agencies incorporate the 2020 FAQs, as appropriate, into the final version of the Proposed Guidance, it will be essential that the language of each FAQ is conformed to the less prescriptive language that is appropriately employed throughout the Proposed Guidance. For example, the FAQs should no longer state that banking organizations "should ensure" a particular outcome, but rather should list a range of considerations that banking organizations may take into account under the circumstances. This change would ensure that the Proposed Guidance continues to align with the final rule on supervisory guidance and that it establishes consistent expectations for banking organizations.

D. Given the different and unique risks that they pose, the Proposed Guidance should take an alternative approach to managing the third-party risks of data aggregators, including by removing certain data aggregator relationships from the scope of the Proposed Guidance.

The Agencies have requested comment on the extent to which the 2020 FAQs should be incorporated into the final version of the guidance, including FAQ 4, which states that a banking organization may have "business arrangements" and third-party relationships with data aggregators, and therefore should manage these relationships consistent with the third-party risk management guidance. We believe the approach to data aggregators taken in FAQ 4 is the wrong one, and recommend that the final guidance instead adopt an alternative approach to managing the third-party risks of data aggregators.

Specifically, it is clear that data aggregators — including both those that engage in unilateral "screen-scraping" and those with which a banking organization may have a contract or other data sharing relationship established with an aggregator solely to facilitate and create a structure around the sharing of data required under section 1033 of the Dodd-Frank Act — can pose meaningful risks to banking organizations and their customers. We disagree, however, that the third-party risk management practices and expectations described in the Proposed Guidance would be appropriate for either type of activity for several reasons.

First, and most importantly, in all such cases it is the data aggregator, and *not* the banking organization, that is providing a good or service to the banking organization's customers in this

arrangement, and the data aggregator provides such goods or services pursuant to its own independent relationship with a customer. There is no sound reason to believe that the risk management practices that are appropriate for a banking organization to use vis-à-vis its own vendors can or should be extended to its customers' own vendor relationships.

Second, because the banking organization is not obtaining any good or service, it has very little leverage to use vendor-style third-party risk management techniques, such as due diligence and ongoing oversight, over data aggregators — and indeed, in the case of screen scrapers, an organization has no leverage at all. It is difficult for banking organizations to learn that screen scraping is occurring until after it occurs, and banking organizations are generally unable to ensure that aggregators are accessing data only relevant to the fields for which the customer is authorizing access.[20]

Third, a banking organization's desire to limit the risk that data aggregators may pose must be balanced with (i) customers' needs and rights under section 1033 of the Dodd-Frank Act to access their financial information and (ii) the fact that customers can access their financial information today using online and mobile banking tools and services that banking organizations offer to their customers. Customers often engage with third parties to provide a particular service, and these third parties in turn may assert data access rights on behalf of their customers. However, these services often assert data access rights on behalf of their customers without evidence of the customers' valid consent and without their customers fully understanding of the scope, nature, and use of their data. Most consumers are not aware of (i) what personal and financial information can be accessed by financial applications, (ii) the length of time that such applications have access to their information, and (iii) what actions the application can take with their information.[21] Any supervisory expectation that banking organizations will remain responsible for ongoing monitoring and due diligence over customer-requested data sharing with data aggregators therefore must be balanced with (i) customer requests to make their data available on other platforms; (ii) the fact that data access should be limited to situations in which a third party provides services to the customer, reasonably requires the data for those services, and does so in a way that is transparent and consistent with the customer's expectations; and (iii) the Consumer Financial Protection Bureau's ("CFPB") guidance that banking organizations should ensure that customers have access to their account data through these platforms.[22]

For these reasons, we strongly recommend that the Agencies take a substantially different approach to managing the risks presented by data aggregators, taking three concrete first steps.

1. We strongly encourage the Agencies to coordinate with the CFPB in any efforts by the latter to implement section 1033 of the Dodd-Frank Act to ensure those efforts do not

---

[20] The banking sector continues to move away from screen scraping and credential-based data access toward data sharing through an Application Programming Interface ("API"). An API facilitates the transfer of consumer financial data through tokenized access, thus removing credential sharing and allowing users to be securely authenticated at their own financial institution. Data sharing through APIs is more accurate and secure than screen scraping and credential-based data access, and continued adoption of APIs will benefit consumers and all market participants.

[21] *See* The Clearing House, *Consumer Survey: Financial Apps and Data Privacy*, p. 3 (Nov. 2019), https://www.theclearinghouse.org/-/media/new/tch/documents/data-privacy/2019-tch-consumersurveyreport.pdf.

[22] CFPB, *Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation* (Oct. 18, 2017), https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf.

undermine bank safety and soundness and prudent risk management. For similar reasons, the Agencies should support and promote current cross-industry and trade initiatives to facilitate safe and secure access through common interoperable standards.

2. For the reasons discussed above, we urge the Agencies to remove "relationships" with data aggregators — whether (i) screen scrapers or (ii) those aggregators with which a banking organization may have a contract or other relationship solely to facilitate the sharing of data as required under section 1033[23] — from the scope of "business arrangements" to which the Proposed Guidance would apply.[24]

3. We urge the Agencies, in an appendix to any final guidance or in supplementary material thereto, to affirm that banking organizations may take a range of steps to manage and mitigate the risks of data aggregators. These steps should include imposing reasonable time, place, and manner conditions on data access by third parties, such as blocking or cutting off access if needed for safety and soundness reasons.[25]

In addition to the above, we recommend that the Agencies work with the CFPB as the section 1033 rulemaking process unfolds to ensure that parties that access data from banking organizations are subject to appropriate data protection and other risk management standards. This coordination should be guided by two propositions regarding the section 1033 rulemaking. First, section 1033 does not prevent a banking organization from imposing reasonable time, place, and manner conditions on data access by third parties. This is paramount to ensure the safety and security of mandated data access. And second, the Agencies and CFPB should provide additional clarity concerning the application of the security and privacy provisions of the Gramm-Leach-Bliley Act ("GLBA") to data aggregators, in particular by (i) requiring that data aggregators comply with security standards that are no less protective than those applicable to institutions governed by the GLBA and (ii) amending each Agency's respective GLBA implementing regulations to clarify that the section 1033 implementing regulations, when adopted, are the only regulations that govern a financial institution's obligations with respect to data shared pursuant to section 1033 once the financial institution has allowed access to that data in compliance with the section 1033 implementing regulations.

---

[23] Rather than using third-party risk management guidance to place the burden on banking organizations to meet these obligations of the data aggregator, data aggregators should be subject to the same data security standards as banking organizations given the volume and type of data that data aggregators access and store. For this reason, we believe that the CFPB should extend its supervisory authority to data aggregators.

[24] Conversely, we agree that it would be appropriate for the third-party risk management guidance to apply where the banking organization contracts with a data aggregator to provide a service to the banking organization, such as importing data or validating external account numbers before the banking organization initiates a transfer.

[25] For example, recent FFIEC guidance lists a range of information security program practices and controls that relate to access management and authentication. FFIEC, *Authentication and Access to Financial Institution Services and Systems* (Aug. 11, 2021), https://www.occ.treas.gov/news-issuances/bulletins/2021/bulletin-2021-36a.pdf.

III. Other Comments on the Proposed Guidance

A. The Proposed Guidance should permit senior management to establish policies governing third-party relationships.

The Proposed Guidance would note that banking organizations typically consider "approving the banking organization's policies that govern third-party risk management" to be a responsibility of the board of directors. However, this is not consistent with the core oversight functions of the board of directors as recognized by the Federal Reserve's February 26, 2021, revision to SR 13-19, in which the Federal Reserve revised its expectation with respect to "policies governing the use of service providers," stating that "senior management should establish policies governing the use of service providers that are appropriate for the range and risks of the institution's outsourced activity and organizational structure."[26] Prior to the February 2021 revisions, SR 13-19 provided that the board of directors should establish and approve such policies.

This change to SR 13-19 aligned with the proper role of the board of directors and senior management, in which the board of directors is responsible for overseeing the business and affairs of the banking organization and senior management is responsible for day-to-day operations. Agency third-party risk management guidance should track with SR 13-19 and the expectations set forth therein and should recognize that the board of directors must focus on core oversight functions and top-tier strategy, which are fundamental to the safe and sound operation of the banking organization. Consistent with this critical distinction, the board of directors should be expected to review, discuss, and approve overall risk management strategy for the banking organization and oversee the establishment of policies, but the policies that are to be *approved* by the board of directors should be limited to the most important ones (e.g., the banking organization's capital policy).[27] Approval of the vast majority of policies that address day-to-day operations — including, for many banking organizations, the third-party risk management policy — should be within the sole purview of senior management, which has the subject matter expertise, experience, and time to perform this role effectively.[28]

B. The Proposed Guidance should provide banking organizations with greater flexibility in the negotiations and approval of vendor contracts.

The Proposed Guidance would establish "contract negotiation" as the third stage in the third-party risk management life cycle and would list a series of considerations that banking organizations typically take into account when negotiating contracts with third parties. The Proposed Guidance would also state that the board of directors (or a designated committee reporting to the board of directors) should be aware of and approve contracts involving critical activities before their execution. The

---

26 Federal Reserve Board, *SR 13-19: Guidance on Managing Outsourcing Risk*, 2.

27 The Proposed Guidance also should note that a banking organization's third-party risk management policy need not be a standalone policy; banking organizations should have the flexibility to develop appropriate risk management frameworks, including frameworks in which policies for third-party risk management are included within a broader policy or set of policies.

28 For additional discussion of the core functions of the board of directors and senior management, see BPI, *Guiding Principles on Enhancing Banking Organization Corporate Governance* (Jan. 12, 2021), https://bpi.com/wp-content/uploads/2021/01/BPI-Guiding-Principles-on-Enhancing-Banking-Organization-Corporate-Governance.pdf.

Proposed Guidance should be amended in several ways to better reflect marketplace realities and the appropriate role of the board of directors and senior management.

First, the Proposed Guidance should explicitly incorporate FAQ 26, which states that the board of directors may delegate actual approval of contracts with third parties involving critical activities to a committee of the board of directors or senior management. The Proposed Guidance would permit the board of directors or "a designated committee reporting to the board" to approve such contracts, and it is ambiguous whether this designated committee may be solely comprised of senior management. Boards of directors themselves, however, should have flexibility in assessing whether (and, if so, how) they approve individual contracts consistent with their oversight role; the Proposed Guidance should focus on allowing the board of directors to determine how best to provide effective oversight of high-risk third-party relationships, which may involve delegation of contract reviews and approvals to management, thereby allowing the board of directors to focus on material matters such as program maturity, structure, and overall risks. FAQ 26 appropriately permits the board of directors *or senior management* to fulfill these respective responsibilities, and the Proposed Guidance should be amended accordingly.[29]

Second, the Proposed Guidance should more explicitly recognize that, for reasons of relative negotiating power or otherwise, contracts with third parties may not always address the items listed as "typical" considerations in contract negotiation.[30] We note that this leverage can differ depending on the banking organization in question. For example, as discussed below, information communication technology vendors ("ICTs"), including cloud service and other hardware and software vendors, often have substantially more negotiating leverage against banking organizations, leaving banking organizations with reduced opportunity to negotiate for the rights and provisions that would be expected by examiners in applying the Proposed Guidance — and, for the same reason, banking organizations often cannot turn to an alternative service provider.

In other cases, a straightforward contract is entirely appropriate, and the costs of negotiating bespoke contract terms would outweigh the benefit of obtaining them. To account for the varied nature of contracts that banking organizations may enter into with third parties, and to emphasize the risk-based nature of this guidance, the Proposed Guidance should affirm that appropriate contract terms are commensurate with the level of risk and complexity of the third-party relationship.

---

[29] Further, the Proposed Guidance should more clearly state that approval by the board of directors (or a delegated committee of the board of directors or senior management) may only be typical at the contract negotiation stage and not, for example, in the planning stage or when the contract becomes due for renewal. Approvals at additional stages in the life cycle or the renewal of contracts by a committee of the board of directors or senior management could materially impede the speed at which a banking organization would be able to execute new relationships or renegotiate existing contracts, which could be particularly problematic for critical activities and/or third-party relationships that are necessary to replace a vendor that previously provided or supported a critical activity but is no longer available to do so.

[30] We appreciate the Agencies' inclusion of the following statement in the Proposed Guidance: "In situations where it is difficult for a banking organization to negotiate contract terms, it is important for the banking organization to understand any resulting limitations, determine whether the contract can still meet the banking organization's needs, and determine whether the contract would result in increased risk to the banking organization." Proposed Guidance at 38191. We suggest several ways in which the Agencies should further clarify this recognition.

Third, the Proposed Guidance would include a substantial number of "typical" practices in the context of contract negotiation. However, certain of these specific risk management practices are unrealistic in practice and should be removed from the Proposed Guidance, as they are not "typical" or appropriate considerations under most circumstances. For example:

- The Proposed Guidance would note 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."[31] These provisions are not typical; for example, there may be M&A exceptions allowing the third party to assign unilaterally. The Proposed Guidance should more narrowly refer to this practice as "typical" only where a fourth party processes or has access to a banking organization's client, employee, or business sensitive data or where the subcontractor performs a critical service related to a "critical activity."

- The Proposed Guidance would note that, in the event the third party is unable to provide services as agreed, the contract would provide access to data in order to transfer services to another provider for continuity of operations.[32] However, in some cases it may be unrealistic to expect the third party to provide access to its data under these circumstances, particularly after the contract has been terminated.

C. The Agencies should use their existing regulatory tools and authorities, including the Bank Service Company Act, to directly obtain information from, and exercise oversight of, third-party vendors that serve a large number of banking organizations or over which banking organizations have little negotiating power.

A number of third-party vendors perform critical activities for banking organizations but are each themselves substantially larger than banking organizations and not substitutable given that they operate in a highly concentrated sector. In many such cases, banking organizations may lack the negotiating leverage as individual institutions to negotiate for the type of protections, rights, and other provisions listed in the Proposed Guidance, as well as to perform risk management activities such as due diligence and ongoing monitoring. This is often the case with respect to ICTs, such as cloud service providers offering software-as-a-service and infrastructure-as-a-service processing capabilities to banking organizations.[33]

Given the unique third-party risk management challenges that these vendors pose, we strongly suggest the Agencies consider exercising their existing regulatory tools and authorities to improve banking organizations' ability to manage these risks in three ways. First, the Proposed Guidance should be revised to better address challenges a banking organization faces when negotiating with third parties, including dominant cloud service providers, that have greater negotiating leverage and can dictate contract terms. The Proposed Guidance should more explicitly recognize that banking organizations

---

31 Proposed Guidance at 38191.

32 Proposed Guidance at 38192.

33 Other examples of third parties with greater negotiating leverage may include credit card and loan servicing platforms; mortgage origination and servicing companies; utility service providers, such as telecommunications, electric, and gas providers; and insurance companies or other firms providing health care or other benefits, such as retirement planning, to employees of the banking organization.

may have difficulty obtaining "typical" terms under these circumstances. Second, to account for instances in which banking organizations have difficulty gaining access to perform due diligence and audits, the Proposed Guidance should further address due diligence options in these circumstances by providing regulatory certifications of third parties or, at a minimum, ensuring access to reports of examination of third parties subject to oversight under the Bank Service Company Act, as discussed further below. These certifications and reports would be particularly beneficial in risk management practices associated with providers that restrict access to information.[34] Third, the Agencies should consider exercising direct agency interaction with key cloud and other regulated service providers in order to improve the ability of banking organizations to negotiate the inclusion of "typical" terms. As global regulators have increasingly recognized, the increasing reliance by banking organizations on a small number of cloud service providers and other technology platforms could increase financial stability risks without greater direct regulatory oversight of the services they provide.[35] The Bank Service Company Act subjects certain third parties to regulation and examination to the same extent as if such services were being performed by the depository institution itself on its own premises, and accordingly provides the basis for the Agencies to more closely review certain risks and activities of these providers with respect to banking organizations and, in some cases, share the results of those reviews with serviced financial institutions.[36]

D. The Proposed Guidance should clarify that banking organizations are not expected to perform due diligence and oversight of subcontractors, and instead may assess the third party's third-party risk management program.

The Proposed Guidance would state that banking organizations, as appropriate, typically conduct due diligence on a third party's "critical subcontractors." The Proposed Guidance would provide three examples of "critical subcontractors": those subcontractors that may introduce additional risk due to concentration risk, material risk, or the conduct of significant activities.[37] The Proposed Guidance should be clear, however, that banking organizations are not expected to perform due diligence and oversight over a fourth party, particularly given the limited authority and legal rights a banking organization has over a subcontractor with which it does not have contractual privity. Consistent with FAQ 11, the final guidance should reflect a more realistic, limited expectation that banking organizations assess a third party's third-party risk management program, rather than supplant

---

34 Along these lines, we note that the Agencies are uniquely situated to assess concentration risk on an industry-wide level. Any information relating to concentration risk that the Agencies can provide to banking organizations, such as market data, general reports, and industry risk assessments, may be helpful to the banking sector in identifying, assessing, and mitigating this risk.

35 *See, e.g.,* Bank of England, *Financial Stability Report* (July 2021), https://www.bankofengland.co.uk/-/media/boe/files/financial-stability-report/2021/july-2021.pdf.

36 In addition, the FFIEC's Multi-Regional Data Processing Servicers and Retail Payment Systems supervisory programs provide for limited review and disclosure of these results before the third party enters into a contract with the banking organization. *See* FFIEC, *Supervision of Technology Service Providers Handbook*, https://ithandbook.ffiec.gov/it-booklets/supervision-of-technology-service-providers/risk-based-supervision/roe-distribution.aspx. Under the current FFIEC framework, FFIEC examination reports generally are not provided to banking organizations that are considering engaging a service provider, but have not yet done so. To facilitate and support diligence efforts by banking organizations in such cases, we suggest that the Agencies agree as matter of policy to permit technology service providers to share reports of examination with banking organizations with which they have entered into good faith negotiations to provide a service.

37 Proposed Guidance at 38191.

the third party's practices with its own with regard to fourth parties over which the banking organization has limited or no legal authority to conduct any such review. The approach in this FAQ is appropriate and aligns with marketplace realities and existing practices, in which the ability of a banking organization to conduct diligence directly on fourth parties generally is very limited. Consistent with current expectations, a banking organization should focus on the controls and ongoing monitoring the third-party service provider has in place with respect to the fourth party.

In the alternative, if the Agencies do not adopt the above recommendation, the Agencies should clarify the definition of "critical subcontractor." The definition of "critical subcontractor" should align with FAQ 8, which recognizes that not all third parties involved in a critical activity are themselves critical to the success of that activity, and also should reflect our recommended revisions to the definition of "critical activity" in Section II.B.2 above. The same principles should apply at the subcontractor level, and banking organizations should have the flexibility to evaluate which subcontractors meet this definition by conducting an appropriate, risk-based evaluation under the circumstances.

E. Upon adopting final guidance on third-party risk management, the Agencies should review and revise the FFIEC's Information Technology Examination Handbook to ensure alignment.

The Proposed Guidance and the FFIEC's Information Technology Examination Handbook both address third-party risk management practices by banking organizations. For example, the *Information Security* booklet of the FFIEC Handbook includes a section on the oversight of third-party service providers. These guidance documents deviate in a number of ways and, after the Proposed Guidance is finalized, we urge the Agencies to update the FFIEC Handbook to align with this finalized guidance. Importantly, among other changes, the FFIEC Handbook should be revised to reflect that (i) the Agencies view APIs as more secure and effective than screen scrapers, and (ii) despite their obligations under section 1033 of the Dodd-Frank Act, banking organizations also must act appropriately to combat fraud and abuse of their systems. Agency guidance should outline consistent practices, thereby assisting banking organizations in meeting supervisory expectations.

Moreover, to that end, we respectfully request that the Agencies conduct examiner education on the updated third-party risk management guidance and corresponding changes to the FFIEC Information Technology Examination Handbook.

F. Final guidance should outline the Agencies' views on services covered by the Bank Service Company Act and better define the Agencies' expectations for filings under the Act.

If adopted, the Proposed Guidance would replace existing guidance issued by the Agencies on third-party risk management, including a portion of the FDIC's commentary associated with the filing requirement and covered services of the Bank Service Company Act. As noted above in Section III.C, we recommend that the Agencies leverage their authority under the Bank Service Company Act to examine certain third-party service providers, both for the benefit of the Agencies in their understanding of systemic risk and for the benefit of banking organizations receiving services from such service providers.

However, the Proposed Guidance does not address the Agencies' expectations with respect to banking organization obligations under the Bank Service Company Act, and the absence of language on this topic is to the detriment of banking organizations, third parties, and the Agencies alike. Section 7(c)(2) of the Bank Service Company Act states that any banking organization that has certain services performed by a third party "shall notify [its primary federal regulator] of the existence of the service relationship within 30 days after the making of such service contract or the performance of the service, whichever occurs first."[38] Guidance associated with this filing requirement and the services covered by the Act is currently reflected in the FDIC's FIL-49-99 and FIL-19-2019, which would remain in effect if the Proposed Guidance is finalized, and in the FDIC's FIL-44-2008, which would be superseded by the final guidance. Given the utility of examination reports compiled by the Agencies under their Bank Service Company Act oversight authority and in light of the public consensus among the Agencies on the types of services covered by the Act and the implementation of the Act's notice requirement, we recommend that the Agencies address the Bank Service Company Act in final guidance or, in the alternative, issue a separate interagency policy statement covering the Act and the related authority and responsibilities of the Agencies and banking organizations, respectively, under the Act. In particular, the Agencies should permit banking organizations to meet the notice requirement of the Bank Service Company Act by maintaining an inventory of all third-party relationships and making it available to examiners upon request, which is the OCC's current approach for national banks and federal savings associations.[39]

---

[38] 12 U.S.C. § 1867(c)(2); 12 C.F.R. § 304.3(d). As defined in Section 3 of the Bank Service Company Act, these services include "check and deposit sorting and posting, computation and posting of interest and other credits and charges, preparation and mailing of checks, statements, notices, and similar items, or any other clerical, bookkeeping, accounting, statistical, or similar functions performed for a depository institution." 12 U.S.C. § 1863. The FDIC has interpreted "similar functions" to also include "data processing, Internet banking, or mobile banking services." *FDIC FIL-19-2019* (April 2, 2019), https://www.fdic.gov/news/financial-institution-letters/2019/fil19019.pdf.

[39] *OCC Bulletin 2013-29, Third-Party Relationships: Risk Management Guidance* (Oct. 30, 2013), fn. 10.

*****

If you have any questions, please contact the undersigned by phone at 917-863-5945 or by email at gregg.rozansky@bpi.com.

Respectfully submitted,

Gregg L. Rozansky
Senior Vice President, Senior Associate General Counsel

Bank Policy Institute

cc: Mark E. Van Der Weide, General Counsel
Michael S. Gibson, Director, Division of Supervision and Regulation
(Board of Governors of the Federal Reserve System)

Nick Podsiadly, General Counsel
Doreen R. Eberley, Director, Division of Risk Management Supervision
(Federal Deposit Insurance Corporation)

Michael J. Hsu, Acting Comptroller of the Currency
Benjamin W. McDonough, Senior Deputy Comptroller and Chief Counsel
(Office of the Comptroller of the Currency)

Appendix A: Recommendations for 2020 FAQs

#	Question	Recommendation
1.	What is a third-party relationship?	***Do not further incorporate this FAQ.*** The Proposed Guidance would retain the definition of "third-party relationship" from OCC Bulletin 2013-29 and the 2020 FAQs. The definition is appropriate, provided the definition of "business arrangement" is modified as proposed in Section II.B.1. The Proposed Guidance would largely retain the set of actions that a banking organization may take when it does not receive all the information it is seeking about a third party that supports the banking organization's critical activities, and appropriately clarifies that these actions may be taken by "bank management." Accordingly, this component of the FAQs should not be further incorporated into the Proposed Guidance.
2.	What is a "business arrangement?"	***Do not further incorporate this FAQ.*** As discussed in Section II.B.1, the definition of "business arrangement" should be revised to, "any mutual understanding or agreement between a banking organization and a third-party entity by which the entity is required or commits to provide ongoing goods or services to or for the banking organization pursuant to a written contract." The Proposed Guidance should not incorporate the examples of "business arrangement" contained in this FAQ, as doing so would limit the flexibility of banking organizations to make determinations based on the particular facts and circumstances. The Proposed Guidance would retain the explanation in this FAQ that "business arrangements" generally exclude bank customers. However, the Proposed Guidance should clarify the application of this principle in the context of data aggregators, as discussed further in response to FAQ 4.
3.	Does a company that provides a bank with cloud computing have a third-party relationship with the bank? If	***Do not further incorporate this FAQ.*** The Proposed Guidance need not incorporate this FAQ, as the Proposed Guidance already would expect banking

#	Question	Recommendation
	so, what are the third-party risk management expectations?	organizations to employ a risk-based approach to cloud computing third-party relationships. To the extent this FAQ is incorporated, however, the language should be revised to be less prescriptive and instead to describe factors that a banking organization may take into account under these circumstances. As described in Sections III.B-C, the Proposed Guidance should acknowledge that banking organizations may face challenges when negotiating with cloud service providers and other ICTs, which have a dominant market position, and therefore that banking organizations may be unable to obtain the types of contractual rights that can be obtained with other third parties.
4.	If a data aggregator collects customer-permissioned data from a bank, does the data aggregator have a third-party relationship with the bank? If so, what are the third-party risk management expectations?	***Do not incorporate this FAQ*.** In Section II.D above, we propose an alternative approach to the risk management of certain types of data aggregators. For several reasons, the third-party risk management guidance is not the appropriate risk management regime for addressing the risks posed by these data aggregators.
5.	What type of due diligence and ongoing monitoring should be conducted when a bank enters into a contractual arrangement in which the bank has limited negotiating power?	***Incorporate aspects of this FAQ into the Proposed Guidance, but modify the language in certain respects.*** This FAQ may be incorporated into the Proposed Guidance to the extent it lists actions that a banking organization *may* take. However, the FAQ should be modified to reflect marketplace realities and acknowledge that, in some cases (particularly non-traditional vendor relationships), certain of the third-party risk management life cycle elements may not be relevant or applicable.
6.	How should banks structure their third-party risk management process?	***Incorporate aspects of this FAQ into the Proposed Guidance, but modify the language in certain respects.*** The acknowledgment that there is no one way for banking organizations to structure their third-party risk management processes is helpful in reinforcing that banking organizations may have flexibility to implement an appropriate, risk-based approach based on their particular circumstances.

#	Question	Recommendation
		To the extent this FAQ is incorporated, the language should be revised to be less prescriptive (e.g., the Proposed Guidance should not note that certain personnel "should" be involved in a particular process).
7.	OCC Bulletin 2013-29 defines third-party relationships very broadly and reads like it can apply to lower-risk relationships. How can a bank reduce its oversight costs for lower-risk relationships?	***Do not further incorporate this FAQ.*** The Proposed Guidance already would note that the banking organization's risk management practices for each relationship should be commensurate with the level of risk and complexity of the third-party relationship.
8.	OCC Bulletin 2013-29 states that the OCC expects more comprehensive and rigorous oversight and management of third-party relationships that involve critical activities. What third-party relationships involve critical activities?	***Incorporate aspects of this FAQ into the Proposed Guidance, but modify the language in certain respects.*** This FAQ helpfully acknowledges that not every relationship involving critical activities is necessarily a critical third-party relationship, and that mere involvement in a critical activity does not necessarily make a third party a "critical third party." As described in Section II.B.2 above, this clarification is helpful and appropriate.
9.	How should bank management determine the risks associated with third-party relationships?	***Do not further incorporate this FAQ.*** The Proposed Guidance already would note that the banking organization's risk management practices for each relationship should be commensurate with the level of risk and complexity of the third-party relationship.
10.	Is a fintech company arrangement considered a critical activity?	***Do not further incorporate this FAQ.*** The Proposed Guidance already would describe the meaning of "critical activity," and we have suggested changes to this definition to better align with the goal of the Proposed Guidance and avoid confusion in its application. If this FAQ is incorporated, the expectation that, "The board (or committees thereof) should approve the policies and procedures that address how critical activities are identified" should be removed or modified to align with SR 13-19 and with our comments in Section

#	Question	Recommendation
		III.A above regarding the proper role of the board of directors.
11.	What are a bank management's responsibilities regarding a third party's subcontractors?	***Incorporate aspects of this FAQ into the Proposed Guidance, but modify the language in certain respects.*** FAQ 11 differs from the Proposed Guidance in that, where the Proposed Guidance would suggest that banking organizations should conduct due diligence on the subcontractors directly in certain cases, FAQ 11 would contemplate that the banking organization conduct an appropriate review of the third party's third-party risk management practices. As we describe in Section III.D, the approach in FAQ 11 is appropriate and aligns with marketplace realities, in which it is generally not possible for the banking organization to conduct diligence directly on fourth parties. In addition, FAQ 11 helpfully notes that, to demonstrate its oversight of its subcontractors, a third party may provide a banking organization with independent reports or certifications. To the extent that FAQ 11 is incorporated into the Proposed Guidance, it should be modified (i) to differentiate between key areas of consideration for the banking organization with respect to "material" or "critical" subcontractors, which distinction does not exist in FAQ 11; and (ii) to be less prescriptive (e.g., the Proposed Guidance should not note that certain personnel "should" be involved in a particular process).
12.	When multiple banks use the same third-party service providers, can they collaborate to meet expectations for managing third-party relationships specified in OCC Bulletin 2013-29?	***Do not further incorporate this FAQ.*** The Proposed Guidance would already incorporate the substance of this FAQ.
13.	When collaborating to meet responsibilities for managing a relationship with a common third-party service provider, what are some of the responsibilities that each bank still needs to undertake	***Do not further incorporate this FAQ.*** The Proposed Guidance would already incorporate the substance of this FAQ.

#	Question	Recommendation
	individually to meet the expectations in OCC Bulletin 2013-29?	
14.	Can a bank rely on reports, certificates of compliance, and independent audits provided by entities with which it has a third-party relationship?	***Incorporate aspects of this FAQ into the Proposed Guidance.*** The Proposed Guidance would already incorporate the substance of this FAQ. However, the Proposed Guidance should reflect, as this FAQ acknowledges, that on-site audits for some third-party relationships can be inefficient and costly.
15.	What collaboration opportunities exist to address cyber threats to banks as well as to their third-party relationships?	***Do not incorporate this FAQ.*** It would be more appropriate to incorporate this FAQ into the Agencies' guidance addressing cybersecurity risk.
16.	Can a bank engage with a start-up fintech company with limited financial information?	***Incorporate aspects of this FAQ into the Proposed Guidance.*** The Proposed Guidance would already incorporate the substance of this FAQ. However, the Proposed Guidance would not include one helpful clarification. The Proposed Guidance would state that, depending on the significance of the third-party relationship, a banking organization's analysis of a third party's financial condition may be as comprehensive as if the banking organization were extending credit to the third party. The FAQ clarifies that this statement does not mean that a banking organization may not enter into relationships with third parties that do not meet the bank's lending criteria. This clarification should be incorporated into the Proposed Guidance.
17.	Some third parties, such as fintechs, start-ups, and small businesses, are often limited in their ability to provide the same level of due diligence-related information as larger or more established third parties. What type of due diligence and ongoing monitoring should be applied to these companies?	***Do not further incorporate this FAQ.*** The Proposed Guidance already would incorporate the substance of this FAQ.

#	Question	Recommendation
18.	How can a bank offer products or services to underbanked or underserved segments of the population through a third-party relationship with a fintech company?	***Do not incorporate this FAQ.*** It would be more appropriate to incorporate this FAQ into Agency guidance addressing financial inclusion.
19.	What should a bank consider when entering a marketplace lending arrangement with nonbank entities?	***Do not incorporate this FAQ.*** The Proposed Guidance would provide general principles that can be applied to any particular type of third party, including marketplace lending arrangements, and incorporating this FAQ would only diminish banking organizations' flexibility to apply these principles as appropriate when engaging with third-party marketplace lenders.
20.	Does OCC Bulletin 2013-29 apply when a bank engages a third party to provide bank customers the ability to make mobile payments using their bank accounts, including debit and credit cards?	***Do not incorporate this FAQ.*** The term "business arrangement," as modified by our suggestion above, sufficiently captures these circumstances, and additional discussion in the context of mobile payment partnerships would not be additive or clarifying.
21.	May a community bank outsource the development, maintenance, monitoring, and compliance responsibilities of its compliance management system?	***Do not incorporate this FAQ.*** It would be more appropriate to incorporate this FAQ into the Agencies' guidance addressing compliance management systems. The Proposed Guidance already would acknowledge that banking organizations may outsource significant activities.
22.	How should bank management address third-party risk management when using a third-party model or a third party to assist with model risk management?	***Incorporate aspects of this FAQ into the Proposed Guidance.*** We recommend incorporating the general concept that a banking organization may engage a third party to assist with modeling or model risk management, but do not agree that the level of prescriptive discussion or detail in this FAQ should be incorporated into the guidance. Instead, the Proposed Guidance should state that, if the banking organization lacks sufficient expertise in-house, it may decide to engage external resources (i.e., a third party) to help execute certain activities related to model risk management and the banking organization's

#	Question	Recommendation
		ongoing third-party monitoring responsibilities. These activities may include model validation and review, compliance functions, or other activities in support of internal audit. Bank management may use this type of modeling to understand and evaluate the results of validation and risk control activities that are conducted by third parties.
23.	Can banks obtain access to interagency technology service providers' (TSP) reports of examination?	***Incorporate aspects of this FAQ into the Proposed Guidance, but modify the language in certain respects.*** This FAQ helpfully clarifies the circumstances under which banking organizations may obtain technology service provider ("TSP") reports of examination. This FAQ thus assists banking organizations in negotiating with and managing TSPs, because it notifies TSPs that banking organizations may obtain this information, and in turn reinforces safety and soundness by allowing the banking organization additional control over its TSPs. This FAQ therefore should be incorporated into the Proposed Guidance, but modified to align with our recommendations in Section III.C above, including that the Agencies should agree as matter of policy to permit TSPs to share reports of examination with banking organizations with which they have entered into good faith negotiations to provide a service.
24.	Can a bank rely on a third party's Service Organization Control (SOC) report, prepared in accordance with the American Institute of Certified Public Accountants Statement on Standards for Attestation Engagements No. 18 (SSAE 18)?	***Do not further incorporate this FAQ.*** The Proposed Guidance would already incorporate the substance of this FAQ.
25.	How may a bank use third-party assessment services (sometimes referred to as third-party utilities)?	***Do not further incorporate this FAQ.*** The Proposed Guidance would already incorporate the substance of this FAQ.
26.	How does a bank's board of directors approve contracts with third parties that involve critical activities?	***Incorporate this FAQ into the Proposed Guidance.*** This FAQ should be incorporated into the Proposed Guidance, particularly its statement that the board of directors may delegate contract approval for contracts involving critical activities to senior management. As

#	Question	Recommendation
		discussed in Section III.A above, the Proposed Guidance would state that the board of directors or "a designated committee reporting to the board" approves such contracts, and this is both ambiguous with respect to the role of senior management and inconsistent with Agency guidance on the proper role of the board of directors.
27.	How should a bank handle third-party risk management when obtaining alternative data from a third party?	***Do not incorporate this FAQ.*** It would be more appropriate to incorporate this FAQ into the Agencies' guidance addressing the use of alternative data.