October 4, 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: SIFMA Comment on Proposed Interagency Guidance on Third-Party Relationships: Risk Management (Docket No. OP-1752; FDIC RIN 3064-ZA26; Docket ID OCC-2021-0011)

Dear Sirs and Madams:

The Securities Industry and Financial Markets Association ("SIFMA")[1] appreciates the opportunity to submit this letter to the Board of Governors of the Federal Reserve System (the "Board"), the Federal Deposit Insurance Corporation ("FDIC") and the Office of the Comptroller of the Currency (the "OCC" and, collectively with the Board and FDIC, the "Agencies") on the proposed interagency guidance (the "Proposed Guidance") on third-party relationships and appropriate risk management practices for their respective supervised banking organizations.[2]

SIFMA welcomes the Agencies' efforts to increase transparency and consistency regarding expectations for third-party relationship risk management practices. Consistent with SIFMA's membership and organizational focus, our comments focus on issues most relevant for

[1] SIFMA is the leading trade association for broker-dealers, investment banks and asset managers operating in the U.S. and global capital markets. On behalf of our industry's nearly one million employees, we advocate on legislation, regulation and business policy affecting retail and institutional investors, equity and fixed income markets and related products and services. We serve as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance and efficient market operations and resiliency. We also provide a forum for industry policy and professional development. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association.

[2] 86 Fed. Reg. 38182 (July 19, 2021).

broker-dealers, the securities industry and the capital markets businesses and activities of our members, including our bank-affiliated members.

Executive Summary

Four principles motivate our comments. First, the scope of relationships covered by the Proposed Guidance is unnecessarily broad. Many third-party relationships merit the type of risk management envisioned by the Proposed Guidance, but not all relationships do. Therefore, there are instances in which the scope of the Proposed Guidance may be more circumscribed without undermining the core policy objectives at issue, which fundamentally are to encourage and facilitate sound risk management. Second, various relationships within the scope of the Proposed Guidance should be subject to a more tailored approach. In some cases, banking organizations simply are restricted in their ability to conduct diligence and negotiate contracts. In other cases, we believe the Agencies can and should play a role in addressing risks that third parties present. Third, although boards of directors have an important role to play in overseeing all risk management at banking organizations, including third-party risk management, the final guidance should not place unduly prescriptive expectations on boards. Fourth, we support the Agencies' endorsement of a risk-based approach as this allows firms to take into account the level of risk, complexity and the nature of the third-party relationship.

Accordingly, consistent with these principles and as explained below, SIFMA respectfully requests that the Agencies:

- narrow the definition of "business arrangement", align the definition of "critical activity" and clarify the role of the board of directors;
- acknowledge that banking organizations may tailor risk management procedures for third parties that are subject to supervision and regulation;
- clarify that the Proposed Guidance would not apply to relationships with data aggregators established pursuant to any final rule implementing section 1033 of the Dodd-Frank Act and clarify how the Proposed Guidance would apply to other data aggregation and screen-scraping circumstances;
- update how the Proposed Guidance treats relationships with information communication technology vendors, including cloud computing service providers, given the unique nature of such relationships; and
- more generally, revise the expectations regarding relationships with third parties where banking organizations have limited ability to acquire information, negotiate with and oversee the party.

In addition, we ask the Agencies to ensure that the final guidance and any FAQs that are incorporated into the final guidance are consistent with the Agencies' respective approach on supervisory guidance.[3]

Background

The Proposed Guidance notes that banking organizations routinely rely on third parties for various services and activities and that these third-party relationships offer banking organizations

[3] 12 CFR Part 4, Subpart F; *id.* at 262.7; *id.* at Part 302. Certain aspects of the Proposed Guidance appear inconsistent with recently adopted regulations clarifying that supervisory guidance does not form a basis for enforcement actions. For example, Section D (Supervisory Reviews of Third-Party Relationships) states, "actions [based on deficiencies in supervisory findings] may include issuing Matters Requiring Attention, Matters Requiring Board Attention, and recommending formal enforcement actions". This statement should be clarified and, more generally, the final guidance, including any FAQ incorporated into the final guidance, should be drafted to avoid suggesting it establishes requirements on banking organizations.

many advantages, such as access to new technologies, products, services and markets. The Agencies further note the importance of conducting and managing these relationships and related services in a safe and sound manner.

The Proposed Guidance would offer a framework for banking organizations to consider in each of six stages of the life cycle of third-party relationships. Specifically, the Proposed Guidance provides that effective third-party risk management generally follows a continuous life cycle and incorporates the following principles: (1) making assessments and plans regarding the inherent risks, strategic purposes and other relevant factors of the activity, (2) conducting proper due diligence in third-party selection, (3) adequately negotiating contracts, (4) requiring the board of directors and management to review the banking organization's risk management process, (5) performing ongoing monitoring of the third-party activity and overall performance and (6) planning a contingency strategy for terminating a third-party relationship. The framework is intended to be based on sound risk management principles, such as risk management programs and adequate due diligence, and is meant to be tailored based on the level of risk, complexity and size of the banking organization as well as the nature of any particular third-party relationship. This risk-based approach allows each banking organization to develop its own third-party risk management practices that reflect the nature of its business, operations and resources.

Under the Proposed Guidance, third-party relationships are "business arrangements" between a banking organization and another entity, which can be established through contract or otherwise. The Proposed Guidance notes that the use of the term "business arrangement" is intended to be interpreted broadly so that a banking organization can identify all third-party relationships with respect to which the Proposed Guidance would apply. The Proposed Guidance also notes that third-party business arrangements generally exclude a banking organization's customers.

The Agencies should narrow the definition of "business arrangement".

The Proposed Guidance's current definition of "business arrangement" is unnecessarily broad, beyond what we believe is necessary to achieve the policy objectives of the Proposed Guidance. Specifically, the scope of the definition in the Proposed Guidance appears to cover relationships that should not be subject to the third-party risk management principles because they do not involve any business relationship.

We suggest that the definition should cover relationships:

1. that in the ordinary course would be covered by a written contract; and
2. pursuant to which a banking organization, on a continuous basis, receives services or through which a banking organization works with a third party to provide the banking organization's services to customers.

This latter category would include, for example, an arrangement pursuant to which banking services are provided through a financial technology company. This scope, and the requirement for a written contract, would be consistent with the Board's 2013 guidance, which defines the scope of arrangements subject to that guidance as those involving "a contractual relationship with a financial institution to provide business functions or activities".[4] The approach the Board took in 2013 is sensible because, for example, a written contract provides the binding commitment for the third party to comply with the majority of the third-party risk management life cycle guidance.

[4] Federal Reserve, *SR Letter 13-19 / CA 13-21: Guidance on Managing Outsourcing Risk* (Dec. 5, 2013, rev. Feb. 26, 2021).

We also believe that certain relationships should be excluded from the definition for purposes of providing clarity. Specifically, the Agencies should clarify that three groups of relationships are excluded:

1. relationships with a customer, client or counterparty that do not involve services;[5]
2. relationships where a banking organization offers its employees services, but the relationship is directly between a service provider and employee; and
3. relationships that are not customer or business relationships, such as reliance on governmental organizations for the provision of services (*e.g.*, local emergency services).

These exclusions would clarify that a banking organization does not need to undertake risk assessments of certain inapplicable relationships with third parties, such as local police, fire and social services (or need to evaluate municipalities' own emergency management and contingency plans).

If non-contractual relationships (*i.e.*, relationships that were not covered by a written contract in the ordinary course) were to be subject to third-party risk management principles, then the banking organization should determine the extent to which the final guidance is applicable, if at all, based on the amount of negotiating power it has, as discussed below.

The Agencies should align the definition of "critical activity" with existing definitions.

The Proposed Guidance provides a four-prong definition of "critical activities", with each prong being sufficient to make a "significant bank function" or other activity a critical activity. Separately, the Agencies have established varying definitions for concepts similar to what the "critical activities" definition is intended to capture. For example, the Agencies have established consistent definitions for "critical operations" and "core business lines" for purposes of the Agencies' "Sound Practices to Strengthen Operational Resilience" guidance and the Board's and FDIC's resolution planning rule.[6] To help a achieve a consistent framework, the Agencies should conform the definition of "critical activity" to existing definitions. This approach would allow the Agencies to achieve the policy objectives of the Proposed Guidance and, also, allow banking organizations to comply efficiently with various regulatory standards.

[5] We recognize the Proposed Guidance states that third-party business arrangements generally exclude relationships with customers, but we ask that the final guidance explicitly make clear that such relationships, including client and counterparty relationships, are out of the scope of the guidance. For clarity, while it is important to distinguish between business arrangements where a banking organization provides goods or services to a customer from those where a third party provides goods and services to the banking organization, in today's financial service 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, where a bank has entered into a contractual arrangement with a third party, pursuant to which depositors may open and access deposit accounts at the bank through a technology platform owned and operated by the third party, the bank may be viewed as both a recipient and a provider of services. SIFMA recognizes, and believes it would be appropriate for the Agencies to clarify, that in business arrangements between a banking organization and a third party, where the products or services of a third party are used to provide services to depositors or other customers of the banking organization, the third party should be viewed as a service provider to the banking organization, notwithstanding the fact that the third party (*e.g.*, a fintech firm) may view itself as a customer of the banking organization (*e.g.*, because the fintech firm contracts with the banking organization to provide banking services to the fintech firm's customers).

[6] 12 CFR 243.2; *id.* at 381.2.

The Agencies should clarify that the board of directors of a banking organization has flexibility in how it oversees third-party risk management.

The Proposed Guidance delineates various ways the board of directors could be involved in approving third-party relationships. We believe the final guidance should adopt FAQ No. 26 and clarify that a board would be expected to satisfy its obligations if the board received sufficient reporting and other information regarding a banking organization's third-party risk management program. To that end, we ask that the Agencies state that the board of directors is not responsible for approving specific contracts, including contracts involving critical activities, and that the board is only responsible for overseeing the third-party risk management generally. Consistent with FAQ No. 26, this would allow the board of directors to delegate approval of contracts. Of course, if a board wished, it could retain for itself (or delegate to a committee of the board) approval authority with respect to any particular category of arrangements or policies more generally. Overall, the board of directors should be responsible for overseeing adoption and administration of appropriate third-party risk management principles, but not accountable for the decision to enter into specific third-party relationships, unless that relationship otherwise would require board approval under the banking organization's governance model.

In addition, as the Proposed Guidance applies to "banking organizations" generally, the Agencies should clarify that (1) this board oversight may be conducted at a consolidated level, if that would be consistent with the banking organization's generally applicable governance model and (2) the board should act in a manner consistent with other guidance on governance practices.[7]

The Agencies should acknowledge that certain relationships with affiliates and regulated entities are examples of relationships where a tailored approach to applying the Proposed Guidance would be appropriate.

We support the Agencies' endorsement of a risk-based approach, as this allows firms to take into account the level of risk, complexity and the nature of a third-party relationship. The usefulness of this approach is particularly evident for relationships with affiliates and relationships with regulated entities.

Affiliates

Banking organizations should be able to rely on organization-wide risk management that applies to affiliates through documenting its own arrangement with the affiliate without conducting the full scope of diligence suggested by the Proposed Guidance. Given that interaffiliate services are likely well established, the banking organization would have enhanced oversight of the affiliate and input into the services the affiliate provides. One or more regulators also likely would have oversight over the affiliate.

Given this context, under the Proposed Guidance, it would be appropriate for banking organizations to leverage their own internal risk and control framework to satisfy third party controls. This approach would allow a proportionate approach to these arrangements, which should not require the same type of due diligence as conducted on external service providers, if the group entity is already operating under an internal control framework.[8]

---

[7] *See*, *e.g.*, Federal Reserve, *SR Letter 21-3 / CA 21-1: Supervisory Guidance on Board of Directors' Effectiveness* (Feb. 26, 2021).

[8] A similar approach is reflected in the UK Prudential Regulation Authority's (PRA) policy (PS7/21) and supervisory statements (SS2/21) on outsourcing and third-party risk management from March 2021—based on the level of "control and influence" over the group entity—as well as the Financial Stability Board's (FSB) discussion paper entitled *Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships* from November 2020.

Consistent with the Proposed Guidance's risk-based approach, the final guidance should therefore support the ability of banking organizations to adopt a risk-based approach to intragroup outsourcing, which provides affiliates the ability to rely on robust, well-controlled and globally consistent group policies and processes.

Regulated Entities

Similarly, the final guidance should provide that when a third party is a federally regulated entity providing a service in its capacity as a regulated entity, a banking organization may tailor its third-party risk management process accordingly. For this purpose, federally regulated entities would include banks, broker-dealers, asset managers, exchanges, trading platforms and market infrastructures subject to supervision by a primary federal regulator (*e.g.*, the Agencies, the U.S. Securities and Exchange Commission or the Commodity Futures Trading Commission).[9] More specifically, subject to the discussion below regarding the appropriate diligence review for such relationships, banking organizations should be able to assume, in the absence of knowledge to the contrary, that the entity is complying with laws, regulations and other public regulatory expectations of its regulator(s). In addition, banking organizations should be permitted to assume that the entity has performed adequately with respect to any applicable regulatory reviews or examinations. Thus, banking organizations should be permitted to place more reliance on existing controls and systems in place with a regulated entity.

Banking organizations should still be required to conduct a diligence review on federally regulated entities, focused at least on whether there is any information in the public domain about the regulated entity that raises warnings or indicators suggesting that there is a potential problem or elevated risk relevant to the proposed business arrangement. For example, this type of diligence could include reviewing public records of enforcement actions for some reasonable prior period. In addition, a banking organization's particular needs for a relationship with such regulated entity should also be considered when tailoring the third-party risk management principles. A full scope diligence review, however, should not be necessary.

Further, the Agencies should acknowledge that in due diligence review of foreign entities, banking organizations may also take into account whether such foreign entity is regulated in its jurisdiction. For example, a banking organization may make the judgment that a foreign entity being subject to a strong and well-regarded regulatory framework makes the need for primary due diligence less acute.[10]

The Agencies should update the treatment of relationships with data aggregators and information communication technology vendors.

i. Data Aggregators

We believe data aggregators should fall within one of three categories. First, if a banking organization has established a contractual relationship with a data aggregator that directly relates to the provision of products and services offered by the banking organization (*e.g.*, a banking organization's important data or a strategic partnership between a banking organization and a data aggregator), that relationship should be subject to the final guidance. Second, consistent with SIFMA's comments on the Consumer Financial Protection Bureau's ("CFPB") Advance

[9] In addition, organizations that serve as a primary federal regulator and also provide services to banking organizations should be subject to this limited due diligence approach for similar reasons.

[10] Regulatory frameworks in a number of countries share many similarities with those in the United States. In fact, the European Banking Authority's *Guidelines on Outsourcing Arrangements* (EBA/GL/2019/02), which came into effect in September 2019, could be seen as an analogue to the Proposed Guidance.

Notice of Proposed Rulemaking regarding section 1033 of the Dodd-Frank Act,[11] banking organizations' arrangements with data aggregators or data users that are established solely to facilitate and create a structure around the sharing of data under any rule implementing section 1033, should not constitute third-party vendor relationships subject to the final guidance.[12] Third, the final guidance should not apply to screen-scraping activities. We believe the first category is appropriately captured by the proposed definition of "business arrangement" provided above, and explain the latter two categories below. The changes below, if addressed in the final guidance, would address the issues discussed in the OCC's 2020 FAQ No. 4.

In relevant part, section 1033 establishes, subject to rules to be prescribed by the CFPB, a consumer's right to access information in the control or possession of a "covered person",[13] "including information relating to any transaction, series of transactions, or to the account including costs, charges and usage data" and further provides that this information "shall be made available in an electronic form usable by consumers".[14]

The CFPB's rulemaking process is at an early stage and it is not yet clear that banking organizations necessarily would have a direct contractual relationship with a third party that accesses data pursuant to a section 1033 rule. Moreover, given that banking organizations would be providing such access as a result of a legal mandate, we believe the onus should not be on the banking organization, but on the party accessing the data, to ensure the party appropriately manages the attendant risks to that activity. Other aspects of the Proposed Guidance, such as those regarding planning and termination, would be largely irrelevant for the same reason. Thus, as noted, data aggregators and data users are better positioned to ensure that their use of consumer data complies with relevant legal and risk management obligations than banking organizations. To this end, we urge the Agencies to coordinate 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.

As part of that coordination, we urge the Agencies to 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 (1) requiring that data aggregators comply with security standards that are no less protective than those applicable to institutions governed by the GLBA and (2) 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.

In addition, the Agencies should clarify that the final guidance does not include requirements for screen-scraping activities that are not business relationships. The final guidance should be limited to business relationships and not seek to impose expectations on other types of

[11] 85 Fed. Reg. 71003 (Nov. 6, 2020).

[12] *See* SIFMA Response to CFPB Advance Notice of Proposed Rulemaking on Consumer Access to Financial Records (Feb. 4, 2021), available here.

[13] A "covered person" is defined in section 1002(6) of the Dodd-Frank Act, in part, as entities engaged in offering or providing consumer financial products or services. 12 USC § 5481(6).

[14] Pub. L. 111-203, Title X, § 1033(a) (codified at 12 USC § 5533(a)).

relationships. Thus, screen-scraping activities should be entirely outside of the scope of the final guidance.[15]

ii. Unique Services with a Limited Number of Service Providers

From time to time, banking organizations may enter into arrangements with companies that provide important or unique services in industries with a limited number of service providers. Good examples of this circumstance include cloud computing service providers and utility service providers, such as telecommunications, electric and gas, where banking organizations have limited ability to identify alternative providers.[16] The OCC's 2020 FAQ No. 5 acknowledges banking organizations' limited ability to implement the guidance with some companies and suggests how the organization may nonetheless consider establishing such relationships while appropriately managing risk. SIFMA encourages the Agencies to incorporate FAQ No. 5 into the final guidance, subject to including some explanation on what documentation a banking organization should retain to demonstrate that its decision to move forward with a third-party relationship was sound. We suggest the standard should be to maintain documentation for a banking organization's reasoning of why it entered into such third-party relationship and how it anticipates managing the relevant risks.

Along similar lines, banking organizations may not be able to conduct due diligence or ongoing monitoring in certain cases. As the OCC's 2020 FAQ No. 14 acknowledges, cloud computing service providers may distribute data across several physical locations and on-site audits could be inefficient and costly.[17] This point should be reflected in the final guidance.

The Agencies also should clarify that, when considering concentration risk for third-party relationships, banking organizations may take into account that certain industries may be, at times, relatively concentrated (*e.g.*, cloud computing service providers and other information communication technology vendors), and that engaging in such relationships would be appropriate as long as other potential risks of the Proposed Guidance are appropriately addressed. Banking organizations are able to consider and weigh appropriately concentration risk within their own organization in light of the relevant risk mitigants, benefits and costs associated with such third-party relationships, including in concentrated industries. We recommend that the Agencies allow concentration risk to be tiered based on the role the information and communications technology provider serves.

We also respectfully request that cloud computing service providers that are examined under the Bank Service Company Act (the "BSCA") be subject to less stringent diligence expectations by banking organizations. As noted above, banking organizations may not have as much flexibility in negotiating with certain of these service providers. The Agencies have much greater ability to perform diligence of the service providers, particularly in situations where a service provider may be important for the industry generally or present system-wide (as compared to institution-specific) concerns. As such, expectations on banking organizations should be limited

[15] On a related note, we request the Agencies consider, in light of the administration's heightened concerns about cyber security, consulting with the public regarding establishing a date certain to end the practice of screen-scraping. As screen-scraping is widely used as a means for customers to obtain access to their data, such consideration of ending screen-scraping practices should be coupled with movement towards a full application programming interface system. Moreover, we urge the Agencies to strongly discourage the practice of soliciting customer credentials to access accounts at third-party financial institutions.

[16] With respect to utility service providers, banking organizations do not have access to incident-related data to evaluate any risk, for example.

[17] More generally, we believe the Agencies should not focus the guidance on on-site visits, given that the utility of this diligence method has declined over time. Instead, the guidance should focus on control validations more generally, allowing banking organizations to determine the best route to undertake such validation.

to aspects of the Proposed Guidance specific to the banking organization and the contemplated business relationship (*e.g.*, supplier's compliance to contractual requirements, engagement risk and supplier technical and operations control environment). Similarly, the Agencies may ensure more directly that banking organizations' relationships with cloud computing service providers comply with appropriate risk management expectations by including them within the scope of the Agencies' examinations of cloud computing service providers. If there are confidentiality concerns about publicly identifying the cloud service providers that have been subject to examination by one of the Agencies, the Agencies could communicate that information through the supervisory process. Adopting a less stringent diligence review of cloud computing service providers examined under the BSCA would not preclude a banking organization from using a cloud computing service provider that is not examined under the BSCA. In such a case, however, the banking organization would be required to conduct a necessary level of diligence to satisfy that the relationship met the appropriate risk management standards.

The Agencies should revise the Proposed Guidance's expectations regarding third parties that banking organizations have limited ability to acquire information from, negotiate with and oversee.

As noted, banking organizations sometimes have limited negotiating power with certain third parties, in addition to data aggregators, cloud computing service providers and other information technology (which are discussed above).[18] As indicated by the examples below, we respectfully ask that the Proposed Guidance should be revised to be tailored for relationships in which the banking organization has limited negotiating power but where the relationship is necessary. Updating the expectations regarding relationships with limited negotiating power on the banking organization's part should have the benefit of aiding smaller and mid-sized banking organizations that do not have the leverage and/or expertise to negotiate. Overall, and as stated above, we note that a banking organization should tailor its due diligence review of third parties based on the size, risk and complexity of the relationship.

i. Required Relationships

The final guidance should not apply, or should not fully apply, to relationships that are established due to legal requirements imposed on the banking organization or that are provided via non-negotiable service contracts. Such relationships will limit the banking organizations' negotiating power, either explicitly, in the case of non-negotiable service contracts, or effectively, in the case of legally-required relationships, due to the third party's knowledge that the banking organization must enter into the relationship to satisfy a legal requirement. If the final guidance were to apply to these circumstances, the banking organizations should be allowed to tailor the third-party risk management in light of the banking organization's negotiating power and the inapplicability of certain aspects of the Proposed Guidance (*e.g.*, planning, termination).

Similarly, we ask that the Agencies exclude from the final guidance situations where a client directs the banking organization to use a particular provider and the client controls access to such provider, such that the provider is unaware that the banking organization is using its services. For example, clients can request certain services be used to transmit trade information between a banking organization and its clients, and also can request a banking organization to use a particular third-party data aggregator.

[18] Another example of a relationship with limited negotiating power is a banking organization's relationship with a self-regulated organization, such as a stock exchange. As self-regulated organizations, stock exchanges are required to treat all member consuming firms equally, resulting in banking organizations being placed in a position to accept non-tailored terms and conditions in certain agreements. Furthermore, these exchanges often reserve the right to update and change their policies and terms and conditions by solely notifying the firm, leading to even less leverage on the firm's part.

ii. Subcontractors

The Agencies also should provide alternative approaches for satisfying third-party risk management expectations with respect to subcontractors. We ask that the Agencies acknowledge the lack of leverage and lack of contractual relationship between the banking organizations and subcontractors and, thus, allow for flexibility in performing due diligence.

The requirements in respect of subcontractors should be limited to fourth parties that either process or have access to a banking organization's client, employee, or business sensitive data, or that perform a service related to a "critical activity", as defined above. SIFMA suggests the Agencies clarify that a banking organization would not be expected to undertake a vendor risk assessment unless the banking organization has a direct relationship with the subcontractor. Instead, risks arising from subcontractors should be handled solely with respect to the banking organization's relationship to the third party using the subcontractor. Specifically, banking organizations may manage the risk of subcontractors through contractual relationships with third-party service providers that obligate the third party to ensure subcontractor compliance, require the third party to report to the banking organization any incident of material noncompliance and permit the banking organization to terminate the relationship if there is material noncompliance (with the third party or subcontractor).[19] In addition, management of risk of subcontractors can also be realized by the banking organization assessing the third party's own third-party risk management program, to evaluate how well the third party manages its third-party risk.

The above changes, if adopted, would replace FAQ No. 11.

iii. Conflict With Laws

The Agencies should clarify that there is no expectation for third parties to provide notification of financial difficulties, significant incidents, security breaches, legal or compliance lapses and M&A activity when such a disclosure would conflict with other legal obligations, such as obligations under securities laws.

Furthermore, we ask that the Agencies acknowledge that relationships with foreign-based third parties have become more complicated due to the EU General Data Protection Regulation ("GDPR") and that banking organizations lack leverage with such foreign-based third parties. Given that GDPR protects the privacy right of the European Union's citizens at a higher privacy standard compared to the United States, banking organizations would have limited negotiating power with foreign-based third parties that are subject to the GDPR, as they would have to comply with the GDPR standards. Similarly, conflicting regulation is seen within the United States through state privacy regulations, including California's Consumer Privacy and Privacy Rights Acts, Virginia's Consumer Data Protection Act, Colorado's Privacy Act and New York's SHIELD Act. Thus, the Agencies should acknowledge that due diligence may be tailored to take into account the legal obligations of a third party subject to conflicting laws or regulation.

iv. Reliance Upon Industry-Accepted Certifications and Reports; Alternative Sources of Information

We also request the Agencies confirm that a banking organization may rely upon industry-accepted certifications and reports. This approach is already in practice as an industry standard. Thus, we ask that the Agencies adopt FAQ Nos. 14 and 24. Examples of industry-accepted

[19] Our request appears to be consistent with the approach taken in the illustrative example on page 14 of the Agencies' August 2021 guide entitled *Conducting Due Diligence on Financial Technology Companies: A Guide for Community Banks* (the "Community Bank Guide"), and the discussion of subcontractors on page 17 of the document.

certifications and reports include, but are not limited to, SOC 1 and SOC 2 Type 2 reports and financial market utilities disclosures.

We also ask that the Agencies incorporate FAQ No. 17, which states that banking organizations can consider alternative information sources when third parties, such as fintechs and small businesses, have limited due diligence information, and that a banking organization's management has the flexibility to apply appropriate methods of due diligence.[20]

v. Data Retention after the Termination of a Relationship

We believe that in circumstances where a third party requires the retention of data after the termination of a relationship to satisfy standards required by local law to retain certain data that are apply to that third party, the engagement with such third party would not be inconsistent with the Proposed Guidance. Such a circumstance could be remediated through the inclusion of a contract clause that the third party would destroy the data upon the expiry of the retention period, if it is not feasible to return the data. We respectfully ask the Agencies to acknowledge our understanding.

Conclusion

We support the Agencies adopting on an interagency basis a framework for managing risks associated with third-party relationships. We hope the above comments are helpful to the Agencies.

* * *

SIFMA greatly appreciates the Agencies' consideration of these comments and would be pleased to discuss any of these views in greater detail if that would assist the Agencies' deliberations. Please feel free to contact me at mmacgregor@sifma.org if you would like to discuss further.

Sincerely,

[redacted]

Melissa MacGregor
Managing Director, Associate General Counsel

cc: David L. Portilla and Will C. Giles, Cravath, Swaine & Moore LLP

[20] We note that the Community Bank Guide provides alternate approaches in conducting due diligence of fintech companies that (1) may have limited experience working within the legal and regulatory framework in which a community bank operates and (2) may not have supporting information that responds in full to a bank's typical due diligence questionnaires.