Stephen Scharf
Managing Director &
Global Chief Security Officer

DTCC Boston
55 Thomson Place
Boston, MA 02210

October 18, 2021

Via Electronic Mail (regs.comments@federalreserve.gov)

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

RE: Proposed Interagency Guidance on Third-Party Relationships: Risk Management (Docket No. OP–1752)

Ladies and Gentlemen:

The Depository Trust & Clearing Corporation ("DTCC"), on behalf of its central securities depository subsidiary, The Depository Trust Company ("DTC"), appreciates the work of the Board of Governors of the Federal Reserve System ("Federal Reserve"), the Office of the Comptroller of the Currency ("OCC"), and the Federal Deposit Insurance Corporation ("FDIC") (collectively, the "Agencies") in connection with the proposed interagency guidance on managing risks associated with third-party relationships (the "Proposal" or the "Proposed Guidance").[1] We welcome the opportunity to comment on the Proposal, and hope that our comments will be taken into consideration in finalizing the Proposed Guidance.

Introduction

DTCC is the parent company and operator of DTC, which is the U.S. central securities depository, and the National Securities Clearing Corporation ("NSCC") and Fixed Income Clearing Corporation ("FICC"), which are the U.S. cash market securities central counterparties. DTC, NSCC and FICC are registered under the Securities Exchange Act of 1934, as amended, as clearing agencies. In addition, DTC, NSCC and FICC have been designated as systemically important financial market utilities ("SIFMUs") by the U.S. Financial Stability Oversight Council ("FSOC") pursuant to Title VIII of the Dodd-Frank Wall Street Reform and Consumer

[1] 86 Fed. Reg. 38182 (July 19, 2021).

Protection Act of 2010 (the "Dodd-Frank Act"). In accordance with Title VIII, the U.S. Securities and Exchange Commission ("SEC") is the Supervisory Agency for DTC, NSCC and FICC. DTC also is licensed as a New York Limited Purpose Trust Company and state member bank of the Federal Reserve System and, as such, is subject to supervision and examination by the New York State Department of Financial Services and the Federal Reserve Bank of New York under delegated authority from the Federal Reserve.

Executive Summary

DTCC recognizes the effort of the Agencies in preparing the Proposal, which builds off the foundational work of the past several years and seeks to modernize and promote consistency in third-party risk management guidance among the Agencies. DTCC agrees that a banking organization's use of third parties does not diminish its accountability to perform activities in compliance with applicable laws and regulations. DTCC appreciates the Agencies' work to provide a consolidated framework that banking organizations may use in developing practices for risk managing third-party relationships. This clarity and consistency will help banking organizations enhance their risk management practices in a manner commensurate with the risk posed by their third-party relationships.

DTCC believes, however, that there are a few instances where further refinement might strengthen this framework. First, DTCC notes that the parts of the proposed framework are prescriptive in their design. DTCC believes that a more principles-based approach to third-party risk management would enable banking organizations that differ in their size, market interconnectedness, and organizational structures to take different approaches to achieve a common desired result. A principles-based approach would also provide banking organizations with the flexibility necessary to tailor and/or redesign their third-party risk management frameworks, as appropriate, to better address the evolving technological landscape, changing markets, and each organization's unique structure. In addition, DTCC believes that certain sections of the framework would benefit from clarification, and some revision to avoid duplicative - and potentially conflicting - application.

Further, and as discussed in more detail below, DTCC wishes to make the following points:

- The proposed definition of business arrangements is overly broad and would be difficult to implement in practice. DTCC recommends reverting to language in the Federal Reserve's 2013 guidance, which focuses on third parties with written contractual relationship with a financial institution to provide business functions or activities.

- A banking organization's board of directors oversees management's activities and should not be responsible for day-to-day management of the banking organization (such as by being required to approve specific contracts). DTCC recommends that the Agencies provide clarity in this regard to preserve the board of directors' independence and role.

- The proposed definition of critical activities is overly broad and does not align with other regulatory requirements. DTCC encourages the Agencies to grant banking organizations with broad discretion in structuring their third-party risk management programs to allow for better alignment with other regulatory requirements and support of a banking organization's comprehensive risk strategy.

Discussion of Specific Comments

1. *Scope* - Business arrangements

The scope of the Proposed Guidance is broader in many respects and represents an expansion from existing Federal Reserve guidance, which is generally less prescriptive and detailed than the Proposal. As drafted, the Proposed Guidance would cover any "business arrangement" between a banking organization and another entity.[2] The discussion in the proposed guidance regarding the meaning of the term "business arrangements" makes clear that banking organizations should broadly interpret what constitutes a "business arrangement" to allow banking organizations to identify those third-party relationships subject to the Proposed Guidance.[3] These arrangements, therefore, do not require a written contract or a monetary exchange to be established. The breadth of this scope, however, is overly burdensome and not practicable and, as discussed below, may de facto require contractual provisions to meet the supervisory expectations set forth in the Proposal.

a. Written Contracts

DTCC agrees that there may be business arrangements for which a contract or remuneration is not required. These business arrangements, however, are not typically arrangements that present significant risk to a banking organization. For example, the use of a food delivery service for a business meeting is unlikely to be covered by a written agreement or present significant risk to a banking organization. Where risk is presented to a banking organization, written agreements are used to make sure that the banking organization has a way to enforce its legal rights and to communicate its, and its regulators', expectations. This practice aligns to existing Federal Reserve guidance, which sought to "highlight the potential risks arising from the use of service providers and to describe the elements of an appropriate service provider risk management program."[4] The 2013 Federal Reserve Guidance states that "'service providers' is broadly defined to include all entities[5] that have entered into a contractual relationship with a financial institution to provide business functions or activities."[6] By contrast and as discussed above, the Proposed Guidance states that a "third-party relationship may exist despite a lack of a contract or remuneration."[7] The proposed guidance then provides comprehensive guidance and expectations for each stage of the third-party risk management lifecycle, including with respect to contract negotiations. The lack of contractual privity, however, would make it difficult for a banking

[2] Proposal at 38185.

[3] Id.

[4] SR Letter 13–19/CA Letter 13–21, "Guidance on Managing Outsourcing Risk", 1 (December 5, 2013, updated February 26, 2021) ("2013 Federal Reserve Guidance").

[5] "Entities may be a bank or nonbank, affiliated or non-affiliated, regulated or non-regulated, or domestic or foreign." Federal Reserve 2013 Guidance at 1

[6] Federal Reserve 2013 Guidance at 1.

[7] Proposal at 38186.

organization to exercise and enforce its legal rights against a third party, which would, in turn, frustrate a banking organization's ability to meet the expectations set forth in the Proposed Guidance. This would, in turn, de facto require every business arrangement, including those that present little to no risk to the banking organization, to be supported by a written agreement, which would be costly and overly burdensome. DTCC therefore recommends that the Agencies revert to the language in the 2013 Federal Reserve guidance, which focuses on third parties with written contractual relationship with a financial institution to provide business functions or activities.

b. Discrete Services

The Proposed Guidance would capture discrete, as well as on-going, services. However, many discrete, single-service, or one-off arrangements are frequently subject to tailored risk management approaches that may fall outside a banking organization's third-party risk management framework as such programs are designed to focus on on-going arrangements. Indeed, the expectations set forth in the proposed guidance for each stage of the third-party risk management life cycle appear designed for third parties that provided on-going services. As such, DTCC recommends that the Proposed Guidance be limited to those business functions or activities that are provided on a continuous and on-going basis.

c. Relationships Types – Affiliates and Regulated Entities

The scope of relationships covered by the Proposal expressly covers "services provided by affiliates and subsidiaries."[8] Third-party business arrangements among and between affiliates are typically arms-length transactions that are documented with written agreements. Because the scope of this guidance includes undocumented and informal business arrangements, the Proposed Guidance as drafted could include intragroup activities that fall under a shared services model. Shared services models are used to, among other things, enhance operational efficiencies and resiliency. The prescriptive nature of this framework could limit potential enhancements to a banking organization's ability to promote such efficiencies and resilience. It's unclear, for example, how the Proposed Guidance impacts the use of a third-party for intragroup purposes, such as for intragroup data storage facilities. DTCC believes it is not necessary or appropriate to have to conduct the level of diligence set forth in the Proposal on organization-wide risk management that apply to affiliates. Rather, this activity can be covered through appropriate internal documentation and service level agreements. Similarly, federally regulated third parties providing services in their regulated capacity present different risks to a banking organization and that banking organization should be given the discretion to tailor its third-party risk management process accordingly. We note that both regulated and unregulated third parties are treated the same under this Proposed Guidance.[9] Risks posed by third parties, even with respect to critical activities, are not generally comparable, and banking organizations and supervisory oversight should be proportionate to the risks posed by the type of third-party or by service provided. Specifically, a banking organization's relationships with regulated third parties and

[8] Proposal at 38185.

[9] In addition, DTCC notes that this deviates from the approach taken in other jurisdictions.

FMIs that are well-known and already regulated should be subject to different treatment proportionate to the risks of the services they provide. Sufficient flexibility should also be incorporated in the guidance to allow banking organizations to incorporate different factors into their due diligence process. For example, DTCC notes that FAQ 14 of the OCC's 2020 Frequently Asked Questions on Third-Party Relationships ("OCC FAQs") discusses whether, in lieu of on-site audits, a bank can rely on reports, certificates of compliance, and independent audits provided by financial market utilities with which it has a third-party relationship. FAQ 14 states that one key objective of the PFMI "is to encourage clear and comprehensive disclosure by financial market utilities, which are often in third-party relationships with banks."[10] It further recognizes that "financial market utilities typically provide disclosures to explain how their businesses and operations reflect each of the applicable Principles for Financial Market Infrastructures."[11] FAQ 14 makes clear that "[b]anks that have third-party relationships with financial market utilities can rely on these disclosures."[12] This recognition that banking organizations may treat regulated third parties and unregulated third parties differently under their risk management frameworks is important and should be reflected in every part of the guidance with appropriate differentiation where necessary. In particular, DTCC agrees with the language in FAQ 14 and believes that given the sensitivities associated with on-site visits, the guidance should make pellucidly clear that onsite visits are not necessary for financial market utilities. Regulatory guidance should therefore recognize and differentiate distinct third-party services (e.g., regulated financial service providers, financial market utilities, regulated entities that provide non-financial services, entities within the same corporate family, unregulated third parties providing critical services, and government-owned service providers). A failure to distinguish regulated entities from other third-party providers may result in a duplication of regulatory regimes, which risks creating a more complex regulatory landscape.

In addition, this Proposed Guidance would apply to privately owned third parties as well as government operated service providers without distinction. However, government operated service providers, such as the Fedwire Funds Service, which is provided by Federal Reserve Banks, generally deliver unique services to a broad range of market participants and, due to their government operated status, have different security concerns and needs. Accordingly, DTCC believes that government operated service providers should be explicitly carved out from this Proposed Guidance so that the Agencies may, to the extent necessary and appropriate, provide separate guidance covering these entities.

2. Role of the Board of Directors

DTCC agrees that the board of directors is responsible for overseeing the overall risk management framework of a banking organization, which includes third-party risk management processes. In addition, DTCC appreciates that the Proposed Guidance seeks to provide greater guidance around the responsibilities of the board of directors and the responsibilities of

[10] Proposal at 38200.

[11] *Id.*

[12] *Id.*

management. DTCC is concerned, however, that some of the language in the guidance as drafted could be read to shift the board of director responsibilities away from oversight and into day-to-day managerial responsibilities.

For example, the Proposal states that "[t]he board (or a designated committee reporting to the board) should be aware of and approve contracts involving critical activities before their execution."[13] However, contract approval is a managerial responsibility that should reside with management and not the board or a board committee. DTCC notes that FAQ 26 of the OCC FAQs provides further clarity regarding how a board of directors approves contracts with third parties that involve critical activities. Helpfully, FAQ 26 states that it did not mean "to imply that the board must read or be involved with the negotiation of each of these contracts."[14] Rather, "[t]he board should receive sufficient information to understand the bank's strategy for use of third parties to support products, services, and operations and understand key dependencies, costs, and limitations that the bank has with these third parties."[15] DTCC believes that this clarity with respect to expectations around board involvement should be moved to the body of the guidance and should apply to all stages of the third-party life cycle. That is, for the entire relationship and not just with respect to contract negotiations, the board should be in a position to oversee management's actions and compliance with the banking organization's strategy for use of third parties. Such clarity would preserve the board's independence while providing clarity around the board's role. Clearly distinguishing the roles and responsibilities of boards from those of senior management also aligns with SR Letter 21-4/CA 21-2,[16] which provides supervisory guidance on board of director effectiveness for large financial institutions.[17]

3. Critical activities

The Proposed Guidance defines critical activities as significant bank functions (i.e., "any business line of a banking organization, including associated operations, services, functions, and

---

[13] Proposal at 38191.

[14] Proposal at 38203.

[15] *Id.*

[16] Federal Reserve, SR Letter 21-4/CA 21-2: Inactive or Revised SR Letters Related to the Federal Reserve's Supervisory Expectations for a Firm's Boards of Directors (February 26, 2021) , available at https://www.federalreserve.gov/supervisionreg/srletters/SR2103.htm.

[17] As discussed in SR Letter 21-4/CA 21-2, most daily and operational decisions are within management's responsibilities while the board is responsible for, among other things, the following:

- setting clear, aligned, and consistent direction regarding a banking organization's strategy and risk appetite;
- directing senior management to provide directors with information that is sufficient in scope, detail, and analysis to enable the board to make sound, well-informed decisions and consider potential risks; and
- overseeing and holding senior management accountable.

support, that upon failure would result in a material loss of revenue, profit, or franchise value"[18]) "or other activities that:

- could cause a banking organization to face significant risk if the third party fails to meet expectations;
- could have significant customer impacts;
- require significant investment in resources to implement the third-party relationship and manage the risk; or
- could have a major impact on bank operations if the banking organization has to find an alternate third party or if the outsourced activity has to be brought in-house."[19]

The Agencies' requested comment on the ways that this proposed description of critical activities could be clarified or improved.[20] To this end, DTCC believes that the definition is both overly broad and does not align with other regulatory requirements. For example, banking organizations typically identify critical services for resiliency purposes, as well as in their living wills or, for banking organizations that are also financial market utilities, in their recovery and wind-down plans.[21] As discussed above, DTC is a financial market utility and, as such, prepares and files its recovery and wind-down plan with the SEC in accordance with the SEC's covered clearing agency standards.[22] DTC's recovery and wind-down plan is intended to be a roadmap of those actions that DTC may employ to either recover, in the event it experiences losses that exceed its prefunded resources or wind-down its business in a manner designed to permit the continuation

[18] Proposal at FN13, 38187.

[19] Proposal at 38187.

[20] Proposal at 38185.

[21] See, e.g., Bank of England, Supervisory Statement, Operational Resilience: Central counterparties (March 2021) ("UK CCP Paper"), available at https://www.bankofengland.co.uk/-/media/boe/files/paper/2021/operational-resilience-central-counterparties-ss.pdf; Bank of England, Supervisory Statement, Operational Resilience: Central Securities Depositories (March 2021) ("UK CSD Paper"), available https://www.bankofengland.co.uk/-/media/boe/files/paper/2021/operational-resilience-central-securities-depositories-ss.pdf; and Bank of England, Supervisory Statement, Operational Resilience: Central Securities Depositories (March 2021) ("UK RPSO Paper"), available https://www.bankofengland.co.uk/-/media/boe/files/paper/2021/operational-resilience-central-securities-depositories-ss.pdf. The UK CCP Paper, UK CSD Paper and UK RPSO Paper each take a service based focus and requires certain regulated entities to adequately identify important business services, set an impact tolerance for each important business service; and identify and address any risks to its ability to remain within its impact tolerance for each important business service. *See also* 17 CFR § 240.17Ad-22(e)(15) (requiring an SEC registered clearing agency to "[i]dentify, monitor, and manage the covered clearing agency's general business risk and hold sufficient liquid net assets funded by equity to cover potential general business losses so that the covered clearing agency can continue operations and services as a going concern if those losses materialize, including by…(ii) Holding liquid net assets funded by equity equal to the greater of either (x) six months of the covered clearing agency's current operating expenses, or (y) the amount determined by the board of directors to be sufficient to ensure a recovery or orderly wind-down of critical operations and services of the covered clearing agency…"(emphasis added)).

[22] 17 CFR § 240.17Ad-22(e)(3)(ii).

of its critical services in the event that such recovery efforts are not successful.[23] DTC builds off of this foundational analysis to identify critical services for resiliency purposes and the alignment of what is identified as a critical service is crucial for DTC's various risk management and resilience related initiatives to be effective. The Proposed Guidance risks breaking this alignment by requiring the application of a new approach to identifying and managing third-party relationships.

In addition, we note that existing Federal Reserve guidance states that a banking organization's third-party risk management program should "focus on outsourced activities that have a substantial impact on a financial institution's financial condition; are critical to the institution's ongoing operations; involve sensitive customer information or new bank products or services; or pose material compliance risk."[24] As currently drafted, Federal Reserve guidance aligns with the service or operations based approach undertaken for resiliency and recovery and winddown purposes. The use and definition of critical activities for third-party risk management purposes does not necessarily align with a service-based strategy, which, as described above, can be important for a banking organization's overall risk program. Lastly, the risk measurement statement set forth in the Proposal, which requires "significant investment in resources to implement the third-party relationship and manage the risk" may not be a good measure of the risks posed by the third party relationship as there is often not a direct correlation between resources used to, for example, on-board a third-party and risks posed to the viability of the financial institution or the ability of the financial institution to provide market services. Thus, we encourage the Agencies to grant banking organizations with broad discretion in structuring their third-party risk management programs so that they may focus on critical services rather than critical activities to the extent that such a shift aligns with and supports the banking organization's comprehensive risk strategy.

4. Contractual requirements

The Proposed Guidance requests comment on the ways in which it could be revised to better address the challenges a banking organization may face in negotiating third-party contracts. To this end, DTCC notes that the Proposed Guidance is prescriptive and appears to require contractual provisions that may not be necessary or appropriate for certain third-party arrangements. For example, contractual notification requirements covering key personnel changes are not typically captured in contractual arrangements outside of agreements for professional services. The Proposal, however, appears to require notification of such changes for all third parties. Other than with respect to professional services, where the value of the provided

---

[23] *See* Self-Regulatory Organizations; The Depository Trust Company; Order Approving a Proposed Rule Change, as Modified by Amendment No. 1, to Adopt a Recovery & Wind-down Plan and Related Rules, Securities Exchange Act Release No. 83972 (Aug. 28, 2018) (SR-DTC-2017-021) ("DTC R&W PLAN").

[24] SR Letter 13–19/CA Letter 13–21, ''Guidance on Managing Outsourcing Risk'' (December 5, 2013, updated February 26, 2021).

service is typically tied to a specific individual providing a continuous service, DTCC believes that the benefits of including personnel-based notification requirements for general third-party risk management purposes is unclear and could greatly increase costs and compliance burdens for both the banking organization and the third-party. As such, DTCC requests that the guidance be revised to make clear that contractual notification requirements are not necessary.[25]

Similarly, the proposal suggests that contracts include provisions stipulating "whether and how often the banking organization and the third party will jointly practice incident management exercises involving unauthorized intrusions or other breaches of confidentiality and integrity."[26] While incident management exercises may be necessary for some third-party business arrangements, they are not necessary for all. Including this level of specificity in every contract with every third-party increases the costs associated with contract negotiation and execution while providing little benefit. Further, and as stated earlier in our response, banking organizations should have flexibility to risk manage this type of third party service. The implementation of this provision by banking organizations on market utilities (e.g., clearing, settlement, payments) could lead to an obtuse testing regime where these utility services could potentially be responsible for conducting hundreds of tests, which could be costly, overly burdensome, and unnecessary.

In addition, the proposal states that "banking organizations may also gain advantage by negotiating contracts as a group with other users."[27] While DTCC appreciates the Agencies' work to identify ways to reduce the burdens associated with contractual negotiations, DTCC does not believe that negotiating contracts as a group with other banking organizations is a viable or advisable option. First, banking organizations typically have bespoke needs that are confidential, which would limit the practicability of group negotiations. Second, there are legal impediments (e.g., antitrust concerns) associated with this type of activity that could be difficult, costly, and risky to try to overcome.[28]

Banking organizations retain responsibility for meeting their regulatory responsibilities and must make sure that their contractual agreements with third parties do not impair or impede their ability to meet their regulatory obligations. Given the bespoke needs of different types of banking organizations and the services they may desire, banking organizations need maximum flexibility when negotiating contracts to meet their regulatory obligations in a manner that aligns

[25] For these purposes, continuous basis would mean services provided continually to a banking organization for at least 12 months on a rolling basis.

[26] Proposal at 38192.

[27] Proposal at 38191.

[28] To the extent the Agencies believe that specific contractual terms are necessary to comply with specific regulatory requirements, guidance in this regard would be beneficial and would mitigate the need for contract negotiations to ensure their inclusion.

with their organizational requirements. The level of prescription included in the guidance could inadvertently hinder this goal. As such, DTCC believes that a more principles-based approach is necessary to provide banking organizations with sufficient flexibility to identify and tailor contractual provisions to the legal and business needs of the banking organization based on the service being provided.

5. Due diligence and on-going monitoring

The Proposed Guidance is also prescriptive with respect to conducting due diligence on a third-party and suggests actions that may not be necessary, appropriate, or viable. For example, the Proposal states that a banking organization should review a prospective "third party's overall business strategy and goals to consider how the third party's current and proposed strategic business arrangements (such as mergers, acquisitions, divestitures, partnerships, joint ventures, or joint marketing initiatives) may affect the activity."[29] However, obtaining a third-party's business strategy and proposed strategic business arrangements is unlikely as this information is typically considered confidential business information that needs to remain protected.

6. Complexity

The Proposal notes that increased risk often arises from greater complexity.[30] Complexity, however, is a subjective factor that is not independently considered in evaluating third-party risks. Rather, the complexity examples included in the Proposed Guidance such as volume of activity, potential for subcontractors, technology needed, and use of third parties, are typically subsumed in a banking organization's third-party risk management program. Though complexity may be considered based on the type of third-party service, given the minimal benefits associated with incorporating such a factor for all third-party risk evaluations, DTCC suggests removing it from the guidance as a factor that would be applicable and considered in all third-party risk evaluations.

[29] Proposal at 38189.

[30] Proposal at 38187.

Conclusion

DTCC appreciates the opportunity to provide comments on the Proposal and your consideration of the views expressed in this letter. DTCC welcomes the opportunity for further discussions and engagement on the topics raised in this letter. If you have any questions or need further information, please contact me at (212) 855-4844 or sscharf@dtcc.com.

Sincerely,

Stephen Scharf
Managing Director and Global Chief Security Officer
DTCC