DTCC
ADVANCING FINANCIAL MARKETS. TOGETHER.™

Stephen Scharf
Managing Director &
Global Chief Security Officer

DTCC Boston
55 Thomson Place
Boston, MA 02210

Tel: +1 212 855 4844
sscharf@dtcc.com

8 January 2021

VIA Electronic Mail

Secretariat to the Financial Stability Board
Bank for International Settlements
Centralbahnplatz 2
CH-4002 Basel
Switzerland
fsb@fsb.org

RE: Outsourcing and third-party relationships

Ladies and Gentlemen:

The Depository Trust & Clearing Corporation ("DTCC") welcomes the opportunity to comment on the discussion paper issued by the Financial Stability Board ("FSB") entitled "Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships" (the "Discussion Paper").[1] DTCC recognizes the importance of the FSB's efforts on this topic and appreciates the FSB's continued engagement to facilitate and inform discussions among authorities (including supervisory and resolution authorities), financial institutions and third-parties. While the Discussion Paper focuses on financial institutions, DTCC believes that, as the owner and operator of several financial market infrastructures,[2] our unique perspective is important as this dialogue progresses.

DTCC agrees that the COVID-19 pandemic has highlighted the benefits and challenges of managing risks related to third-party interactions.[3] DTCC cautions, however, against prescriptive requirements, particularly with respect to supply chain management, given the complexity of the financial services industry and the jurisdictional challenges associated with outsourcing and third-party risk management. Accordingly, DTCC emphasizes the importance of global coordination, alignment to industry standards and best practices, and a principles-based approach to provide financial institutions with flexibility in the development and implementation

[1] See FSB, Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships (November 9, 2020), available at https://www.fsb.org/wp-content/uploads/P091120.pdf.

[2] As discussed in greater detail below, DTCC owns and operates two central counterparties, a central securities depository, and several trade repositories.

[3] For purposes of this discussion, DTCC views third-parties as external service providers.

of comprehensive outsourcing and third-party risk management programs. When financial entities follow flexible principles-based regulatory requirements and proven industry standards and best practices, the combination/application of these practices result in a solid foundation for a robust risk management and resilience program.

The Discussion Paper poses a series of questions grouped around specific themes and issues, so DTCC's comments below are focused around these questions and issues thematically.

I. Overview of DTCC

DTCC, through its subsidiaries, is the largest post-trade market infrastructure for the global financial services industry and supports its mission to protect clients and the financial markets. DTCC is the parent company and operator of The Depository Trust Company ("DTC"), the U.S. central securities depository, as well as the U.S. cash market securities central counterparties, National Securities Clearing Corporation ("NSCC") and Fixed Income Clearing Corporation ("FICC"). DTC, NSCC and FICC have each been designated as systemically important financial market utilities ("SIFMUs") by the U.S. Financial Stability Oversight Council pursuant to Title VIII of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010.[4] NSCC and FICC provide critical clearing and settlement services for multiple asset classes, including U.S. equities, corporate and municipal bonds, and government and mortgage-backed securities. DTC, a limited purpose trust company and state member bank of the Federal Reserve System, is the largest central securities depository in the U.S. for the book entry settlement of securities transactions for eligible securities and other financial assets. DTC, NSCC and FICC are registered under the Securities Exchange Act of 1934, as amended, as clearing agencies and are supervised by the U.S. Securities and Exchange Commission. In addition, DTC 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 Board of Governors of the Federal Reserve System.

As the parent company and operator of these SIFMUs, DTCC's primary focus is continuity of services to its members and preserving financial market stability.[5] Given its critical

---

[4] DTCC also provides services for a significant portion of the global over-the-counter derivatives market and has extensive experience operating repositories to support derivatives trade reporting and market transparency. DTCC's Global Trade Repository service supports reporting across all five major derivatives asset classes and exchange-traded derivatives in the U.S., Europe and Asia.

[5] DTCC is user-owned and governed pursuant to a shareholders' agreement. The DTCC common shareholders include hundreds of banks, broker-dealers, and other companies in the financial services industry that are participants of one or more of DTCC's clearing agency subsidiaries. The DTCC board is currently composed of 20 directors and includes representation from clearing agency participants, including international broker-dealers, custodian and clearing banks, and investment institutions, as well as non-participant directors. The non-participant directors are individuals with specialized knowledge of financial services, but who bring an independent perspective since they are not affiliated with firms that use DTCC services.

role in the industry, DTCC has comprehensive risk management and resilience programs, and maintains and invests in sophisticated information security programs to protect against attacks and safeguard the integrity of its systems.

II. Discussion Paper Questions

A. What do you consider the key challenges in identifying, managing and mitigating the risks relating to outsourcing and third-party relationships, including risks in sub-contractors and the broader supply chain?

There are several challenges in identifying, managing and mitigating the risks relating to outsourcing and third-party relationships. First, a globally consistent lexicon of relevant key concepts, particularly with respect to the definitions of outsourcing and third-party relationships, would help align supervisory and institutional expectations and understandings. It would also facilitate the creation of effective and efficient outsourcing and third-party risk management programs because identifying the scope of the relationships that should be included in risk management programs can be challenging in practice. For example, it is unclear how to categorize the growing number of partnerships between financial institutions and BigTech/FinTech organizations, which may fall outside the definitions of outsourcing and third-parties. In addition, since risk management approaches and requirements may deviate based on the type of regulatory requirements and oversight underpinning a particular service, appropriate care should be taken to distinguish between regulated and unregulated services in an outsourcing and third-party framework. As such, additional guidance as it relates to distinguishing between regulated and unregulated services would be beneficial.

Second, the increased focus on operational resilience enhances traditional processes used by financial institutions to understand risks posed by external parties, which largely focus and rely on tools like third party interviews, meetings, and questionnaires. Operational resilience, on the other hand, requires financial institutions to both understand and validate the ability for third parties to respond to and recover from a disruptive event measured within a specific time interval. The complexity associated with these processes and the linkage between risk management and resilience are leading financial institutions to measure and manage the resilience capabilities of, and the risks posed by, external parties through the creation of a single comprehensive program. Ongoing discussions between authorities and the financial services industry may help provide additional clarity around supervisory expectations related to how to measure the resilience of a third-party service provider. This clarity could then be used to enhance individual firm capabilities for both risk management and resilience purposes.

Third, risk management of subcontractors ("nth parties") presumes a financial institution's ability to oversee the nth party's activities and have visibility into potential concentration risks from multiple third-parties using the same nth party. Many financial institutions use contractual clauses that balance the risk of nth party subcontractors selected by the third-party. However, as recognized by the Discussion Paper, these clauses may not be

negotiable based on the size of the financial institution, the value of the contract, and the concentration of providers for the outsourced service.

B. What are possible ways to address these challenges and mitigate related risks? Are there any concerns with potential approaches that might increase risks, complexity or costs?

The development of a globally consistent lexicon would help create a foundation against which additional policies and best practices could be developed. A public/private working group could also be formed to define an outsourcing / third-party oversight framework for financial institutions and authorities. This framework could leverage different tools (*e.g.*, testing, exit strategies, questionnaires, contractual clauses, certifications) and establish consistent expectations around the minimum assurance required for comfort in an external party's risk and resilience controls. In addition, working groups and tools, such as the Cyber Risk Institute's Cyber Profile,[6] should be considered for use globally to identify minimum controls across the sector.

C. What are possible ways in which financial institutions, third-party service providers and supervisory authorities could collaborate to address these challenges on a cross-border basis?

The creation of a public/private working group organized by an international standards body (*e.g.*, FSB) that includes market participants, market infrastructures, cloud service providers/IT infrastructure providers, and authorities would facilitate information sharing and help identify possible solutions to the challenges that have been identified.

D. What lessons have been learned from the COVID-19 pandemic regarding managing and mitigating risks relating to outsourcing and third-party relationships, including risks arising in sub-contractors and the broader supply chain?

The COVID-19 pandemic reinforced the importance of being prepared for extreme events. The actions taken by DTCC in recent years to plan for disruptive scenarios involving third parties allowed us to act quickly to maintain stability at the height of the crisis and through the subsequent months. In addition, the pandemic further highlighted the intrinsic role technology plays in the provision of business services and support of virtual work. With companies continuing to adopt new technologies and outsource operational services, the effective management and mitigation of third-party and potential supply chain risks remain key areas of focus. The pandemic highlighted the need for strong coordination and information sharing with peers, regulators, and other key stakeholders with respect to threat information and incident reporting data, and potential risks arising out of a third-party. This information sharing is particularly key as the use of a specific third-party's service becomes more prevalent, and

[6] The Cyber Risk Institute was created by Bank Policy Institute to carry forward the work completed by the Financial Services Sector Coordinating Council on the Financial Services Cybersecurity Profile ('Profile'). The Profile can be found at https://cyberriskinstitute.org/the-profile/.

therefore concentrated, across the financial services sector.[7] Finally, the pandemic highlighted the opportunities that can be gained by the implementation of new/emerging technology and financial digitalization of certain financial products and services. Both of these phenomena may lead to the increased use of third-parties by financial institutions.

III. Key Themes

A. Definitions of outsourcing and third-party relationships

Definitions provide the foundation for the effective application of standards and regulation. For entities with an international reach, a globally consistent set of definitions is critical for market participants and regulators alike. They help shape consistent expectations between and among the public and private sectors and mitigate the potential for market fragmentation and regulatory arbitrage. A common taxonomy also is needed for regulators across the globe to collect consistent information in support of systemic risk monitoring, while also reducing operational burdens for market participants. As noted in the Discussion Paper, jurisdictions have not consistently defined outsourcing or third-party relationships.

With respect to the definition of outsourcing, it is important that the activities of regulated entities be excluded from the scope of the definition to avoid unintentionally capturing tasks, functions, processes, services or activities ("outsourced tasks") of entities that are actively regulated and supervised under comprehensive regulatory infrastructures. A broad definition of outsourcing with appropriate carve-outs should allow for global consistency in a manner that allows authorities to take into account any jurisdiction-specific requirements. For example, the 2019 European Banking Authority Guidelines on Outsourcing Arrangements ("EBA Guidelines")[8] broadly defines outsourcing as "an arrangement of any form between an institution, a payment institution, or an electronic money institution and a service provider by which that service provider performs a process, a service, or an activity that would otherwise be undertaken by the institution or electronic money institution itself."[9] The EBA Guidelines definition then provides the following exclusions:

> [I]nstitutions and payment institutions should not consider the following as outsourcing:
>
> a. a function that is legally required to be performed by a service provider (e.g., statutory audit)

---

[7] In particular, additional work to facilitate the sharing of threat information by public sector authorities with key entities in the private sector (*e.g.*, SIFMUs) would help enhance the resilience of the financial sector by further facilitating collaboration between the public and private sectors. Such information sharing is particularly important during broad-based, cross-sectoral attacks.

[8] EBA Guidelines on Outsourcing Arrangements (EBA/GL/2019/02), available at https://eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf

[9] EBA Guidelines at 19.

b. market information services (e.g., provision of data by Bloomberg, Moody's, Standards & Poor, Fitch)

c. global network infrastructures (e.g., Visa, MasterCard)

d. clearing and settlement arrangements between clearinghouses, central counterparties and settlement institutions and their members

e. global financial messaging infrastructures that are subject to oversight by relevant authorities

f. correspondent banking services, and

g. the acquisition of services that would otherwise not be undertaken by the institution or payment institution (e.g., advice from an architect, providing legal opinion and representation in front of the court and administrative bodies, cleaning, gardening and maintenance of the institution's or payment institution's premises, medical services, servicing of company cars, catering, vending machine services, clerical services, travel services, post-room services, receptionists, secretaries and switchboard operators), goods (e.g. plastic cards, card readers, office supplies, personal computers, furniture) or utilities (e.g. electricity, gas, water, telephone line)).[10]

The EBA Guidelines approach described above allows for a more tailored approach by addressing third-party relationships using a risk-based approach, and in a manner consistent with existing regulatory frameworks. Though regulated outsourced tasks should be managed and assessed by financial institutions, they do not pose the same risks to financial institutions as unregulated outsourced tasks, such as those posed by outsourcing to information technology providers. Additionally, including financial services regulated entities could result in the mitigation of risks that are already being addressed by other supervisors, resulting in a more complex regulatory landscape.

B. Intra-group outsourcing

DTCC believes that intra-group outsourcing does not pose the same level of risk as outsourcing to an unaffiliated provider. Intra-group arrangements often allow regulated entities to efficiently deploy resources on an enterprise-wide basis in a manner that safeguards the safety and soundness of the entity. For example, DTCC's intra-group relationships are subject to service level agreements. In addition, these subsidiaries are part of the risk and resilience governance structures which review and determine the group's risk tolerance. These arrangements are subject to existing regulatory requirements that typically make sure that inter-affiliate arrangements are subject to robust risk management requirements. In addition, rigid requirements applicable to intra-group arrangements that are not proportionate to the relevant risks posed by these arrangements may serve to place regulated entities at a competitive disadvantage vis-à-vis unregulated competitors.

[10] EBA Guidelines at 26.

C. Supply chain management

DTCC agrees that companies are limited in their ability to identify and mitigate risks relating to managing nth party sub-contractors along the supply chain across jurisdictions. Contract privity typically means that only the parties to a contract can be bound by its terms. In other words, a contract only confers rights and imposes obligations on the parties to the contract. Thus, it may be difficult for a financial institution to legally bind the subcontractor of a third-party service provider to the terms of an agreement to which the subcontractor is not a party. This complexity is intensified when the parties are based in different jurisdictions, thereby implicating multiple legal regimes that may not complement each other. Absent a contractual right, it is also difficult for a financial institution to assess the operational resilience of an nth party. While a financial institution could attempt to require a third-party service provider to amend its contracts with an nth party, the financial institution may not have the ability or means to review and approve contracts between the third-parties and nth parties, and existing arrangements may be difficult to amend. This challenge is amplified with each move further down the supply chain. Finally, scope and volume present practicable challenges with any attempts to manage supply chain risks in this manner given the number of potential third parties and their respective nth parties, which further increases for entities operating across jurisdictions.

D. Access, audit and information rights

DTCC agrees that including rights to access, audit, and information from third-parties in contractual arrangements can be contentious. While these provisions are important, DTCC believes that it is important to differentiate between regulated and unregulated third-parties. For example, access, audit, and information rights present unique issues with respect to financial market infrastructures ("FMIs") that provide services to the financial services sector (*e.g.*, clearing and settlement) to promote efficient markets and provide risk management services. Given their importance to market stability, FMIs are highly regulated entities that are subject to comprehensive supervisory oversight. Extending right to audit clauses to FMIs would create significant operational, financial, and legal complexities that could result in the loss of market efficiencies, increase FMIs' risks, and reduce the ability of FMIs to provide certain risk management services. Additionally, because of the lack of standardized controls, processes, and reporting across the industry, these requirements could lead to conflicting control requirements arising from different firms, thereby making it difficult, if not impossible, for an FMI to satisfy each firm's controls.

DTCC notes that there may also be cross-border implications resulting from rules or restrictions imposed under the laws of a third-party's home country. For example, it may not be possible or advisable for on-site audits to be conducted at the third-party. There may also be instances where certain reports include confidential information that cannot be shared externally without regulatory approval.

E. Concentration risks

DTCC understands regulatory concerns regarding the possibility of systemic risks arising from concentration in the provision of some outsourced and third-party services to financial institutions. While DTCC recognizes the importance of balancing third-party concentration risk

given the potential impact on overall market stability, it would be incumbent on the respective authorities to determine this overall risk, as individual firms do not have an accurate overview of which providers are being used by other firms across the industry.[11] DTCC and many other market participants have robust third-party risk management programs. These programs take into account concentration risks, as appropriate, and balance efforts to minimize risks in a manner that aligns with efforts to modernize existing infrastructures, improve efficiency, and identify opportunities to reduce operational complexity and lower costs.[12]

Moreover, DTCC believes it is important to differentiate between the concentration risks that may exist where multiple regulated entities use a common service provider and instances where a group is dependent on a single service provider for the provision of outsourced tasks. Industry-wide concentration risks are not within the control of individual financial institutions. First, individual institutions lack the information necessary to identify and assess sector-wide concentration risks. Second, even if individual institutions had this information, it is unclear what they should do with it and if, and whether, they have the power to address any identified issues. Rather, it is up to the regulators to conduct such sector-wide assessment efforts and provide further guidance on any necessary mitigation measures.

DTCC also cautions against movements to require a multi-vendor strategy or require certain contracts to be exited for concentration reasons because such requirements could be potentially detrimental to a financial institution's business from an operational perspective. With respect to multi-vendor strategy requirements, DTCC notes that there may be a limited number of vendors for certain services, such as cloud service providers, that are able to accommodate and achieve the safety and soundness requirements of the financial services sector. Where there are small numbers of vendors that are able to provide a service, an institution's ability to execute a multi-vendor strategy could be frustrated. Second, different vendors, especially information technology infrastructure service providers, provide differentiated, proprietary offerings to their customers. For example, a business application running within one cloud solution would need to be architected differently for another cloud solution. This complexity makes a multi-vendor approach difficult to implement in practice where, at best, a change would need to be implemented differently for each vendor or at worse, a business application change may be feasible in one cloud offering but not the other creating operational and functional mismatches.

With respect to exit requirements, DTCC notes that such requirements, particularly in times of market stress, may lead to unintended consequences. For example, a vendor under duress from an operational outage may further complicate recovery or cause cascading impacts to other business processes. In addition, while some financial institutions may be able to bring services back 'in-house' in the event of an external failure or a requirement to exit, there may be instances where the software (*e.g.*, code libraries) and technology-based services are proprietary

---

[11] For example, one cloud service provider could be used by multiple financial institutions, but for different services or in different geographic locations. These factors could complicate or even impede a financial institution's ability to understand sector-wide concentration risks.

[12] In the case of internal dependency (*i.e.*, a group is dependent on a single service provider for the provision of outsourced tasks), financial institutions typically have risk management programs that mitigate these concentration risks, such as by conducting internal assessments and putting in place measures based on their risk appetite.

to the service provider, which would prevent the service from being brought back in-house without significant, and potentially costly, product alterations.

Finally, DTCC notes that access to the specialized services that a third-party provides could facilitate a financial institution's innovation efforts, while the lack of access could place an institution at a competitive disadvantage vis-à-vis its peers.

****

DTCC appreciates the opportunity to respond to the issues raised in the Discussion Paper and your consideration of the views expressed in this letter. As this discussion progresses, DTCC encourages policy-makers to consider a risk-based approach to these issues that allows for flexibility in the development and implementation of a comprehensive outsourcing and third-party risk management program. Such an approach should also align with existing regulatory frameworks and standards, and industry best practices. We would welcome the opportunity to provide further detail regarding any of the matters discussed herein. If you have any questions or need further information, please contact me at sscharf@dtcc.com.

Sincerely,

Stephen Scharf
Managing Director & Chief Security Officer
DTCC