Financial Services Sector Coordinating Council
for Critical Infrastructure Protection and Homeland Security

January 8, 2021

Financial Stability Board
Submitted electronically to fsb@fsb.org

Re: *Public Comment on Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships* (January 2021)

To the Financial Stability Board:

On behalf of the United States financial services sector, the Financial Services Sector Coordinating Council (FSSCC) appreciates the opportunity to respond to the Financial Stability Board ("FSB") Discussion Paper ("Discussion Paper") on *Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships* and recognizes the FSB's continued efforts on this topic. The FSSCC appreciates the FSB's facilitation of this continued discussion in this area with supervisors and regulators, financial institutions, and third parties, and the effort taken to consolidate the current challenges related to outsourcing and third party risk management.

Introduction to the FSSCC
The Financial Services Sector Coordinating Council (FSSCC) "coordinates across sector participants to enhance the resiliency of the financial services sector, one of the United States' critical infrastructure sectors. The FSSCC proactively promotes an all-hazards approach to drive preparedness through its collaboration with the U.S. Government for the benefit of consumers, the financial services sector, and the national economy."[1]

We note that there are a number of coordinated industry-wide responses, including from the Global Financial Markets Association (GFMA),[2] the Institute of International Finance (IIF),[3] and the Bank Policy Institute (BPI),[4] which cover a broader range of topics and directly address the four questions posed by

[1] www.fsscc.org
[2] "The Global Financial Markets Association (GFMA) represents the common interests of the world's leading financial and capital market participants, to provide a collective voice on matters that support global capital markets. We advocate on policies to address risks that have no borders, regional market developments that impact global capital markets, and policies that promote efficient cross-border capital flows to end-users by efficiently connecting savers and borrowers, benefiting broader global economic growth. The Association for Financial Markets in Europe (AFME) in London, Brussels and Frankfurt, the Asia Securities Industry & Financial Markets Association (ASIFMA) in Hong Kong and the Securities Industry and Financial Markets Association (SIFMA) in New York and Washington are, respectively, the European, Asian and North American members of GFMA."
[3] "The Institute of International Finance (IIF) is the global association of the financial industry, with more than 450 members from more than 70 countries. Its mission is to support the financial industry in the prudent management of risks; to develop sound industry practices; and to advocate for regulatory, financial and economic policies that are in the broad interests of its members and foster global financial stability and sustainable economic growth. IIF members include commercial and investment banks, asset managers, insurance companies, sovereign wealth funds, hedge funds, central banks and development banks.
[4] The Bank Policy Institute (BPI) is a nonpartisan public policy, research, and advocacy group, representing the nation's leading banks. Its members include universal banks, regional banks and the major foreign banks doing business in the United States. Collectively, they employ nearly 2 million Americans, make 68% of all loans and nearly half of the nation's small business loans and serve as an engine for financial innovation and economic growth.

the FSB. In the following sections, we highlight key themes and observations in response to the DP. We look forward to continued engagement as authorities and industry evolve insights on this topic.

Regulatory Harmonization and Alignment to Existing Frameworks

As highlighted in the DP, most jurisdictions have longstanding regulatory requirements and/or supervisory expectations on outsourcing and third-party risk management. However, as technology evolves and the reliance of financial institutions on third-parties increase, jurisdictions are slowly beginning to diverge on supervisory approaches to outsourcing and third-party risk management. This divergence in approach is driven by market competition, national security, and varying perspectives on data and technology sovereignty. However, increasing fragmentation in regulatory approaches weakens financial stability, and industry would like to ensure that any new guidance is coordinated, complementary, and aligned with globally-accepted best practices. In an effort to address the challenges and mitigate related risks of this divergence, we encourage the FSB to look to the Cyber Risk Institute's (CRI's) Financial Sector Profile (FSP)[5]. The FSP is recognized as a global cyber tool and regulatory convergence instrument, bringing together a catalogue of globally-accepted security standards, regulations, and legal framework requirements including CPMI-IOSCO's *Guidance on cyber resilience for financial market infrastructures*[6], ISO/IEC 27001/2[7], and the NIST Cybersecurity Framework[8].

Scope and Definitions

Definitions form the foundation for the application of supervisory frameworks for third-party risk management. Therefore, it is important that a globally consistent set of definitions is established to align authorities and institutional expectations. Current supervisory frameworks differ in their definition of *outsourcing* and *third-party relationships* while others, like the *EBA Guidelines on Outsourcing Arrangements*[9], broadly define these terms and then provide exclusions for certain services.[10] In addition to these supervisory differences, the differences in the definition of *material*, *critical*, and *important* further complicate those external parties that should be considered in-scope under these frameworks. For financial institutions with international reach, these inconsistencies may lead to the development of complicated and complex financial institution risk management programs to address these differences. For small and mid-sized firms, there may be additional challenges and burdens in being able to comply with multiple guidance and regulations due to staff limitations and supporting resource availability.

---

[5] The CRI Financial Sector Profile (Profile), formerly known as the FSSCC Cybersecurity Profile, was developed as a collaborative effort between 150 financial firms, 300+ bank representatives and input from multiple regulatory agencies and experts. The result is a unified harmonized approach to cyber security assessments that can be used by the smallest and largest financial services firms: banks, securities, and insurance. Ownership and management of the Profile transitioned from FSSCC to the non-profit Cyber Risk Institute (CRI) in January 2020. The CRI Financial Services Profile can be found at https://cyberriskinstitute.org/the-profile/

[6] June 2016. bis.org/cpmi/publ/d146.pdf

[7] ISO/IEC 27001 Information Security Management, iso.org/isoiec-27001-information-security.html . ISO/IEC 27002:2013. Information technology — Security techniques — Code of practice for information security controls iso.org/standard/54533.html

[8] nist.gov/cyberframework

[9] 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

[10] EBA Guidelines @ 19

We encourage supervisors to adopt risk-based, outcomes-based, and proportionate approaches to third-party arrangements. Consistent use of terminology, together with principles and expected outcomes, should guide how firms identify what is material/critical/important to protecting consumers from irreparable harm, preserving ongoing firm viability, and maintaining financial stability.

Cloud Computing

Regulators diverge on approaches to oversight of cloud computing, including views on level of risk and controls needed for various application of cloud computing, e.g., intragroup, public cloud, private cloud. The differences in views are often driven by national security, perspectives on sovereignty, market competition, paths to innovation, and systemic risk.

The December 2019 *FSB Third-party dependencies in cloud services* report outlined the benefits and risks of cloud computing to the financial services sector. We acknowledge that cloud technology is new and rapidly developing. While the risks are different, we encourage global regulators to approach the oversight of Cloud Service Providers (CSPs) under existing supervisory outsourcing frameworks as opposed to developing a separate framework for these services. This framework should remain flexible and allow for the risks presented by other new and emerging technologies, (e.g., Distributed Ledger Technology, Artificial Intelligence), to be covered under the single framework.

We also encourage the FSB to take a lead role in helping supervisors more completely understand the risks and benefits of different types of outsourced technology and how a comprehensive framework may benefit both financial institutions and authorities.

Concentration Risk

The Discussion paper covers three (3) primary forms of concentration risk:

- A single financial institution's use of a single third party for multiple services
- The financial services sector's use of a single third party
- The use of a subset of *n*th parties by numerous third parties

The FSSCC understands supervisory concerns regarding the possibility of systemic risk arising from concentration in the provision of some outsourced and third-party services to financial institutions. While a financial institution may balance the risks that are inherent to its risk exposure to a single third party through its operational risk processes, a single financial institution would not have the visibility into the concentration risk across the financial services sector. Additionally, if a financial institution 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. Financial institutions would need to rely on authorities to conduct a sector-wide assessment and provide further guidance on any necessary mitigation measures.

Lastly, a single financial institution would not have visibility into concentration risks of *n*th party providers utilized by these third parties and are limited in their ability to affect the activities of said vendors. Contract privity means that only the parties to a contract can be bound by its terms. Therefore, it is legally difficult to bind *n*th parties of a third-party service provider to the terms of an agreement to which they are not a party. While a financial institution could require a third-party to amend its own contracts with the *n*th party, the financial institution may not have the ability or means to review and approve contracts between the third-party and *n*th party and existing arrangements may be difficult to amend.

We also caution any requirements for a multi-cloud strategy. While multi-sourcing may be a business strategy, it should not be mandated by regulation as this approach may not be feasible in all instances. This is especially true with information technology service providers where the proprietary nature of

the service may, at best, require a different architecture to implement within a separate vendor solution and, at worst, the change may be feasible within a vendor solution but not in the other vendor solution, thereby creating operational and functional mismatches. This challenge also extends to the integration of a hybrid cloud solution where these same risks apply. It should be noted that while different critical applications can be distributed amongst different clouds, a single application's workloads should not be distributed amongst different clouds.

While institutions should identify strategic alternatives for scenarios where the vendor relationship is no longer desirable, exit strategies are not a solution to respond to short-term technical shortcomings. Exiting a vendor during a material operational event may serve to further complicate recovery or create other cascading impacts to business processes.

With respect to portability, there are technologies that ease the transition of certain workloads across CSPs. These technologies only work for service solutions that are similar across CSP offerings. Given that CSPs' proprietary service offerings provide the most value to financial institutions, many financial institutions' products are delivered through these proprietary services limiting the practical use of portability technologies to financial institutions.

Undoubtedly, the use of cloud is increasing, and with it, the possibility of concentration risk both within the global financial services sector and also within firms. Much still needs to be done to gain better visibility into concentration risk within the sector. It is critical that public and private sector work together to develop better ways to measure, monitor, and manage this risk

We believe that the right path forward is not to seek the elimination, drastic reduction, or even equitable distribution of these risks; instead, the path forward should be focused on gaining visibility into concentration risk, building the right security and resiliency framework to manage these risks, and for public and private sector to work together deliberately and incrementally to create an environment whereby the benefits of cloud computing – and any other new technology that may come along – can be realized.

Regulatory Reporting of Outsourcing Inventories

Regulators globally have varying approaches to outsourcing governance processes. This adds complexity to reporting, governance, and location-specific processes. We hope that global regulators can help make reporting of third-party arrangements more standardized, using common data standards, and potentially finding a way to digitize and streamline reporting. If a jurisdiction seeks information beyond what is required in a standardized report, we would urge that this decision accounts for the additional burden both on firms and on the regulator in generating and ingesting this additional data, and that this additional requirement is necessary and proportionate to the risk it seeks to mitigate.

Industry would also like to highlight that the public sector, including regulatory agencies, face cyber risk as well. Given the collection of highly-sensitive financial data collected through supervision, regulatory agencies are a high-value target for cyber-criminals and nation states. We urge regulators to consider the principle of data minimization whereby regulators can reduce cyber-risk by reducing the volume and type of data they collect and store within their own networks.

Approvals & Notifications

Regulators globally also have different risk tolerances on firms' approaches to outsourcing, especially with regards to cloud. Different approval and notification periods are often required for material/critical/important arrangements, and can impact a firm's ability to adequately manage its

resiliency posture. Authorities may seek to approve all applications a financial institution moves to the cloud. However, lengthy approval periods for the deployment of cloud solutions impede the ability for firms to leverage cloud solutions in a timely and cost-effective manner in response to business strategy, client needs, and market conditions. Authorities may require notifications to help increase visibility into potential concentration risk and create an outsourcing registry by which to better map concentration risk amongst the sector; however, authorities should not seek to enforce approval processes for financial institutions to move applications into the cloud. By limiting financial institutions' ability to quickly adopt cloud solutions, they will need to continue to rely on legacy systems and deprecated assets, which prevents firms from decreasing their attack service and improving their resilience posture. Instead, notification should provide supervisors the ability to object in the rare circumstance where they believe that a firm has not adequately controlled for the risk involved with moving a critical function or service to the cloud.

Data Handling – Data localization and technology requirements have emerged as the digital economy has grown and reliance upon cloud computing has increased, which has in some instances meant an offshoring of data about local customers. Jurisdictions seek to maintain control of information in order to satisfy public policy goals that include data protection, government access, and economic stability. To maintain control, some jurisdictions seek to place limitations on the cross-border transfer of data, requiring that data be stored and accessible within a country's borders. However, limiting the cross-border data flow or storage limits the effectiveness of security and compliance programs. In other instances, outsourcing regulations require firms to obtain confirmation from a foreign regulator that ensures the ability of the local regulator to have continued access to information related to an outsourcing arrangement, where that service is provided outside the relevant entity. This presents a challenge that is outside the control of firms, and may jeopardize the ability to rely on essential outsourcing services.

We encourage regulators to support an open global economy that enables trade, investment, and growth through the secure and efficient transfer of data across borders.

Thank you for the opportunity to respond to the consultative document. I invite you to contact me directly with questions.

Sincerely,

Ron Green, Chair
Financial Services Sector Coordinating Council (FSSCC)
Ronald.Green@mastercard.com | tel 1-636-722-6640 | mobile 1-636-439-8304