August 22, 2023

VIA ELECTRONIC SUBMISSION (fsb@fsb.org)

Re: Third-Party Risk Management and Oversight

The Global Association of Central Counterparties ("CCP Global")[1] appreciates the opportunity to comment on the FSB's consultative document on Enhancing Third-Party Risk Management and Oversight. CCP Global represents 42 members from around the world, who operate over 60 individual central counterparties (CCPs), representing over 95% of the centrally cleared risk management in Initial Margin terms.

CCP Global welcomes and supports the FSB's approach to proposing an outcomes-based framework allowing financial institutions to tailor their third-party risk management programs according to their business models, risk profiles, product mix, etc.. It is important to highlight that while third- and nth-parties present risks, these relationships also benefit financial institutions. Financial institutions use third-party service providers to support their operations in a variety of ways to deliver higher quality services, which not only can provide risk management benefits, but also can lower costs, than if they kept (or could keep) these services in-house. In some cases, financial institutions do not have the resources, internal expertise or the scale to make keeping certain services in-house a viable option. However, financial institutions must effectively manage their risks in order to take advantage of the benefits that third-party service relationships provide in the delivery of critical and other services. As such, financial institutions have long employed robust practices for managing the risk presented by their third-party service relationships.

With respect to the proposed FSB toolkit for third-party risk management and oversight, CCP Global appreciates the FSB's flexible, proportionate, and risk-based approach. The FSB's proposed approach appropriately sets forth a toolkit that recognizes that differences exist across jurisdictions, and among financial institutions and authorities, their markets, business models, and legal/regulatory frameworks. CCP Global strongly supports such an approach, as prescriptive guidance would not allow for this recognition. We also agree that regulatory interoperability and complementing existing standards are important features of such a toolkit. CCP Global has put forward some specific comments on Chapters 1-4 below.

Chapter 1

CCP Global appreciates the FSB's focus on critical services to provide financial institutions the necessary flexibility and proportionality to manage third-party risks according to the level of risks posed to them and their services. Financial institutions should be left with appropriate flexibility to determine criticality based on their businesses, their structures, and their existing risk management practices.

[1] Previously known as "CCP12"

Furthermore, CCP Global supports the general harmonization of terminology across jurisdictions to provide for clarity, avoid fragmentation and promote efficiency. Accordingly, we appreciate FSB's attempt to provide common terms and definitions to promote clarity and consistency with respect to key third-party-risk-related terms. We also understand the challenges involved in trying to harmonize these terms across various jurisdictions and therefore appreciate that interoperability is a key part of the FSB's proposed approach. Along these lines, we appreciate the FSB's recognition that "complete harmonisation of terms is not always possible or desirable" and therefore, CCP Global believes that individual financial institutions and local financial authorities must continue to be able to adopt terminology that is appropriate for the institutions they oversee and services they offer, respectively.

CCP Global believes it is important for financial institutions and authorities to agree on a definition for "critical service", and generally agrees with the definition set forth in the toolkit: "a service whose failure or disruption could significantly impair a financial institution's viability, critical operations, or its ability to meet key legal and regulatory obligations." CCP Global believes that each financial institution is best placed to identify its critical services in the context of its local regulatory obligations based on their businesses, their structures, and their existing risk management practices.

Accordingly, financial institutions should be left the flexibility to categorize their third-party providers based on their usage and risk management practices. CCP Global requests the FSB consider amending the definition of critical service providers to ensure only service providers that are fundamental to the delivery of a critical service is considered a critical service providers. Therefore, we request that the FSB modify the definition of critical service provider to be: A service provider that is fundamental to the delivery of critical services with no readily available substitutes. This nuanced definition accounts for if there are a number of ancillary service providers that are supporting critical services but, not essential to the delivery of those critical services. Further, if a service provider is readily substitutable, meaning that an alternative can be found without significant impact, it may not be appropriate to classify it as a critical service provider.

Chapter 2

Focus on critical services

As noted above, CCP Global broadly supports the overall approach taken in the toolkit. In particular, we welcome the toolkit's emphasis on critical services given the potential impact of their disruption on financial institutions' critical operations. We further appreciate that the toolkit provides for an "aligned and comparable, outcomes-based frameworks to manage third-party risks, while avoiding a one-size-fits-all approach that does not permit differences in regulation or market structure".

In addition, we also support the FSB's recognition that "regulated financial institutions, to the extent they are engaging in financial services transactions, such as correspondent banking, lending, deposit-taking, provision of insurance, clearing and settlement, and custody services, are generally not considered as third-party service providers." As highlighted by the FSB, such institutions are already subject to comprehensive supervision and regulation by their respective local regulators.

Regulatory Interoperability

We appreciate that the toolkit highlights that there are a range of practices for effectively managing third-party risks. This allows the toolkit to complement the practices that are already employed by financial institutions and the local regulatory requirements that are already in place, as opposed to adding potentially conflicting and duplicative obligations that are not only inefficient, but can create undue costs. Regulatory interoperability is a first step towards promoting and achieving "comparable, outcomes-based frameworks" across jurisdictions going forward. This will appropriately allow financial institutions to tailor their practices to meet their needs, while streamlining compliance obligations, reducing costs, enhancing efficiency for the financial institutions, and facilitating coordination among financial authorities.

CCP Global encourages the FSB to promote interoperable third-party registers of information and identify minimum data fields generally applicable to global financial authorities. CCP Global discusses additional comments on third-party risk registers below.

Proportionality

Similarly, the proportionality feature of the FSB toolkit allows financial institutions and authorities to "focus primarily on how financial institutions' management of third-party risks may vary based on their business model, complexity, cross-border presence, function, risk profile, scale, structure and size" and to focus on the third-party service providers whose failure would have the greatest impact on its critical services. CCP Global is pleased that the FSB did not adopt a one-size-fits-all approach, given what is appropriate for a large, complex service provider may not be appropriate for a small one that does not support a critical service, which does not need the level of oversight that one that does support a critical service does. Along these lines, it is important that proportionality be applied related to financial institution's management of nth party risk, as further discussed below.

Chapter 3

Toolkit

As noted above, we support the toolkit's approach as it allows the financial institutions flexibility to choose the tools that best assist them to manage the risks related to third-party service relationships and corresponding supply chains. In particular, we support the inclusion of tools such as "internationally recognized certifications or standards, and audit or testing reports by independent parties, and pooled audits."

Incident reporting

As highlighted by the FSB, most financial institutions are required to provide an incident response report to their local regulators after an incident such as a cyberattack, within a given timeframe. CCP Global appreciates the emphasis in the toolkit on the need to balance timely reporting with remediating the incident. As is noted in the consultation, accurate and complete information is hard to produce while the source and the scope of the disruption is still being investigated. With respect to

third-party service providers, CCP Global agrees that it is important to highlight the importance of incident reporting from third-parties to financial institutions and depending on the criticality of the service provider, for financial institutions to assess third-party service providers' incident response approaches and/or to include incident response requirements in their contracts.

Third-party registers

CCP Global embraces the flexible approach the FSB has taken with respect to registers of third-party service providers. It is important that populating such a register does not end up being a check-the-box exercise that does not serve a clear purpose. CCP Global cautions, for example, against requesting information that can already be found elsewhere. In general, CCP Global believes that sharing registers' information with financial authorities should only be on an *ad hoc* and on a need-to-know basis. Each financial institution should determine the information to include on critical service and other service providers on its register. Ultimately, for a register to be useful, a financial institution must be able to tailor it to their needs.

Nth-party risk

Third-party service providers often contract other providers in their supply chain to deliver the services and therefore nth-party risk is a consideration. We appreciate the FSB's recognition that there are challenges to supply chain risk management, as there may often be limited visibility and transparency with respect to nth-parties. For example, third-parties may not be able to disclose information on their third-parties due to the contractual provisions governing these relationships. We believe the best way to approach potential risks in the supply chain is to assess in a proportionate and risk-based manner how a financial institution's third-party service provider manages its own supply chain risks and depending on the criticality of the third-party, to include provisions in the contract regarding notifications and sub-outsourcing of a particular service. CCP Global would also like to emphasize that a financial institution only has a legal relationship with its third-parties and must be able to negotiate terms of the contracts with those third-parties with respect to nth-parties that fit within its risk appetite.

Other tools for mitigating supply chain risks

As mentioned above, CCP Global appreciates the recognition of the challenges of managing risks associated with critical service providers' supply chains and fully supports the need for financial institutions to have a good understanding of critical third-party service provider key dependencies as part of their on-going due diligence. However, section 3.5.4 indicates that financial institutions may create a risk rating of the critical service provider's supply chain; this seems duplicative to the risk rating of the critical service provider. It is not clear how this risk rating would be used and how this should (or should not) influence the overall risk rating that a financial institution already manages at the third-party level. While CCP Global agrees that supply chain risks can be considered when determining the overall risk of the third party, developing another separate risk rating of the chain that exists outside of the third-party risks rating does not seem to enhance a financial institution's risk management practices given that the third-party risk rating (which includes supply chain risks) is what drives the

controls required by the financial institution. CCP Global encourages the FSB to revisit the separate supply chain risk rating and provide more clarity on how this rating is expected to enhance third-party risk management practices.

Business Continuity Plans

CCP Global agrees with the proposed consultation stating that financial institutions may have in place business continuity plans ("BCP") that "implement, maintain, and regularly test BCPs to anticipate, withstand, respond to, and recover from the disruption or failure of critical services" to safeguard the operational resilience of financial institutions. On a proportionate and risk-based manner, financial institutions should ensure that their critical services providers do the same. It is important to note, that BCP/disaster recovery plans typically focus on short-term solutions that can be executed through the course of an event until the business returns to normal operations and that some of the contingency plans proposed to mitigate disruptions are costly and may not be feasible (e.g., retaining the ability to bring data or applications back on-premises, using multiple service providers).

Exit Strategies

CCP Global appreciates concerns expressed in the preceding paragraph over the ability to maintain operations when using critical services when financial institutions face stress events. Financial Institutions, however, may also put in place longer-term exit strategies for when the financial institution (or the third-party service providers involved in the delivery of critical services) choose to end their relationship (e.g., due to recurring regulatory breaches, poor quality of service, etc.). A third-party provider may also choose to, for example, exit financial services for business reasons. As the proposed toolkit notes this may include contractually agreed-upon provisions on terms for termination, which include transitional periods to minimize disruption, the return of data and applications, and record retention.

CCP Global appreciates that FSB has not prescribed or proposed a preferred form of exit strategy. A financial institution should have the ability to build the necessary flexibility into its contracts and other documentation with respect to a potential exit strategy and should not be expected to granularly define a strategy for an unlimited amount of potential fact patterns.

Consistent with the FSB's recognition that "[t]here is no one-size-fits-all approach to exit planning," CCP Global believes that exit plans (as well as business continuity plans) are best left to the financial institution to design. This will allow a given financial institution to assign clear roles and responsibilities that are appropriate for its individual structure.

CCP Global would like to stress that an approach that advocates a full back up (i.e., a primary and back up providers) for all critical service providers would be costly and involve numerous implementation challenges, which may pose risks to the financial institution. Moreover, it is challenging to find substitutes for or to bring some critical services in-house. Each third-party service provider may have proprietary requirements for implementation making it highly complicated to switch third-party

service providers with reasonable assurance that the application or system would operate in the new technology environment without incident. For example, given the complexities involved in enabling a transfer of operations from one cloud service provider ("CSP") environment to another due to inconsistent features, using multiple CSPs to enhance CCP resilience is not the preferred solution. U.S. Treasury noted in their whitepaper, The Financial Services Sector's Adoption of Cloud Services, that "swapping complex workloads to another CSP or bringing services in-house was often estimated to take months, if not years to successfully execute in almost all cases.[2]"

Concentration Risk

Financial institutions have long taken into account concentration risk related to their third-party service providers as part of their third-party risk management programs and have measures in place to both assess and mitigate these risks. It is important to note that concentration risk is only one example of a risk, which is monitored and managed through financial institutions' existing frameworks and practices. Broadly, concentration risk is not new to financial institutions (e.g., SWIFT) and something the industry has long been able to effectively manage; financial institutions are best placed to continue to manage this risk based on their experience. In addition, as the proposed toolkit points out, risks to third-parties must be managed holistically; avoiding concentration risk, for example, could potentially come at the cost of heightened security and compliance risks.

Chapter 4

With respect to identifying systemic risk dependencies, financial institutions generally lack visibility into potential industry-wide concentrations. CCP Global therefore concurs with the consultation statement that "[f]inancial authorities are primarily responsible for identifying potential risks to financial stability in their jurisdictions. Moreover, they are best positioned to identify and assess systemic third-party dependencies and potential systemic risks arising from such dependencies […]." It would be helpful if financial authorities could provide information on systemic third-party dependencies to financial institutions so that they could also take the broader concentration risks into account as part of their own third-party risk management programs. Notwithstanding this, it is important to note that financial institutions do not have control over the availability of third-party service providers in the market or how these providers are used by other financial institutions. Finally, as the toolkit acknowledges, financial institutions should not be required to avoid using a certain third-party provider solely due to risk of concentration. These institutions must have the ability to weigh the risk of third-party provider concentration against other risk management benefits and expected gains in resiliency, efficiency, and effectiveness.

[2] U.S. Department of the Treasury "The Financial Services Sector's Adoption of Cloud Services" - https://home.treasury.gov/system/files/136/Treasury-Cloud-Report.pdf

About CCP Global

CCP Global (previously "CCP12") is the global association for CCPs, representing 42 members who operate over 60 individual central counterparties (CCPs) across the Americas, EMEA, and the Asia-Pacific region.

CCP Global promotes effective, practical, and appropriate risk management and operational standards for CCPs to ensure the safety and efficiency of the financial markets it represents. CCP Global leads and assesses global regulatory and industry initiatives that concern CCPs to form consensus views, while also actively engaging with regulatory agencies and industry constituents through consultation responses, forum discussions, and position papers.

For more information, please contact the office by e-mail at office@ccp12.org or through our website by visiting www.ccp12.org.

CCP Global Members