BlackRock

January 8, 2021

Submitted via email to fsb@fsb.org

RE: Discussion Paper on Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships

BlackRock, Inc. (together with its affiliates, "BlackRock")[1] respectfully submits its comments to the Financial Stability Board ("FSB") in response to its Discussion Paper on Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships ("Discussion Paper"). Our views in this letter reflect our *ViewPoints* on Lessons from COVID-19: Operational Risk and Resilience and The Role of Third Party Vendors in Asset Management.

Asset managers have relied on outsourcing and third party relationships for many years. Asset managers decide which functions to perform in-house and which to outsource to a third party vendor. That decision reflects a combination of where their core expertise lies and considerations on control, risk profile, cost, and scale. Virtually all asset managers rely on third party vendors for at least some functions. Regardless of the approach taken, asset managers need to implement clear processes with the appropriate checks and balances to ensure operational soundness throughout the investment process.

Utilizing vendor solutions can provide a number of benefits to asset managers and their clients, including more specialized products and services offered, greater operational resilience, cost savings, and innovation. Vendors often have the scale to dedicate resources to specific functions, bringing specialized expertise and risk management to those areas that asset managers may not have the resources or proficiency to develop in-house. As outlined in our *ViewPoint* The Role of Third Party Vendors in Asset Management, there are a diverse range of services utilized by asset managers to perform numerous functions – from obtaining security data and risk analytics that inform investment decisions, to order management and trade execution systems that facilitate placing and executing trades, to accounting and performance systems used for reporting and recordkeeping purposes, to client relationship management and digital marketing systems. While there may be risk in relying on a third party, this risk is often lower than the risk of building and maintaining internal solutions.

In some cases, asset managers have a choice of vendors, while in others they are required to use specific financial market infrastructures ("FMIs"). There are a variety of

---

[1] BlackRock manages assets on behalf of individual and institutional clients across equity, fixed income, real assets, and other strategies. The funds that we manage represent our clients' futures and the investment outcomes they seek, and it is our responsibility to help them better prepare themselves and their families to achieve their financial goals. BlackRock also offers Aladdin, an information processing platform that combines risk analytics with comprehensive portfolio management, trading and operations tools on a single, unified platform.

FMIs upon which all market participants rely, including exchanges, central clearing counterparties ("CCPs"), electronic trading and affirmation platforms, and trade messaging systems. Asset managers are required to use these infrastructures, unlike third party vendors where an asset manager can choose one provider or another and the vendor must meet certain due diligence requirements or face the risk of termination. In considering the potential vulnerabilities in the system, special attention should be given to FMIs that are critical to managing assets and must be used by asset managers who do not have a choice on outsourcing. While these firms and services may not technically be defined as "third party vendors", asset managers and asset owners alike are dependent on the critical infrastructure that is provided by these firms.

As the FSB notes in the Discussion Paper, most jurisdictions have longstanding regulatory requirements and/or supervisory expectations on outsourcing and third party risk management, and many jurisdictions have updated their regulatory frameworks in recent years. Following the 2008 Global Financial Crisis, regulators and industry participants reviewed operational risk frameworks under business as usual ("BAU") and stressed scenarios. These scenarios covered operational and/or external events and plans for orderly wind-downs; this review led to several policy recommendations. In its January 2017 report on "Policy Recommendations to Address Structural Vulnerabilities from Asset Management Activities", the FSB included a recommendation addressing operational risks and challenges in transferring client accounts and investment mandates from one asset manager to another.[2] In line with this recommendation, most jurisdictions reviewed existing guidance and in some cases published new standards for risk management, including operational risk management and business continuity management ("BCM").

Over the last decade, the asset management industry has carefully implemented this guidance by regulators. In addition to BCM, standard vendor management risk mitigation techniques have been developed, including evolution of the types and depth of risks assessed, contractual provisions, formal relationship structures, service level measurements, continuous monitoring best practices, and other similar due diligence and governance mechanisms. Prudent risk management includes a holistic 360-degree view on vendor management, and many asset managers have programs in place that are far more comprehensive than what is legally required.

To ensure robust protections are in place at every firm, we believe that **all** asset managers should practice good vendor management, including ongoing due diligence and oversight of third party service providers. The assessment of a vendor's BCM program, disaster recovery planning, reliance on critical sub-contractors, financial stability, operational strength, and information security practices should be an integral part of the vendor selection and assessment process in order to mitigate the risk of operational errors and disruptions. This oversight should be risk-tiered, with additional review measures in place when a vendor has been retained for critical operational services.

[2] Policy Recommendations to Address Structural Vulnerabilities from Asset Management Activities: https://www.fsb.org/wp-content/uploads/FSB-Policy-Recommendations-on-Asset-Management-Structural-Vulnerabilities.pdf.

As the FSB points out, vendor oversight is especially critical in cases where asset managers rely on a small group of third party providers for certain critical services, or when one specific function is outsourced to a single or a few geographic regions. When enlisting a third party vendor, firms should consider exit strategies and substitutability assessments (e.g., transferring an outsourced service to an alternate provider or reincorporating this service in house) and should manage vendor lock-in risks. We recommend policymakers continue to work with asset managers to ensure robust BCM procedures are in place to address situations when a disruption may affect a specific vendor, group of vendors, or geographic region. While most vendors operated smoothly during COVID-19, the crisis has highlighted the importance of resilience of third party and fourth party service providers.

Asset managers should review vendor management and BCM programs with service providers, and the extent of back-up arrangements should be proportional to the materiality of a service provider to an asset manager's business. Any regulation of BCM for vendors of data, systems, or outsourcing services should be risk-based. To reduce regulatory arbitrage, rules and regulations should be applied equally to all vendors with similar offerings, regardless of their organizational structure or affiliation with another organization. In addition, we support coordination across regulators in different jurisdictions to ensure a more globally consistent approach.

Below, we outline some additional feedback in response to the questions posed by the FSB in the Discussion Paper.

Question 1: 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?

In today's increasingly complex global operating environment, asset managers may face challenges in vendor management and oversight in several regards. While many firms may rely on the same critical vendors, concentration risk is mitigated by the robust oversight programs in place at the contracting firms and the ability for firms to select an alternative vendor if they choose. In some cases, a lack of transparency and ability to influence the vendors' reliance upon key sub-contractors who are directly not contractually bound to the asset manager can pose oversight challenges. As oversight challenges are continuously evolving, asset managers continue to seek greater intelligence to monitor risks. As we discuss in response to questions 2 and 3 below, there are several ways asset managers and regulators can work together to ensure globally robust oversight practices are in place.

Question 2: 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?

To ensure robust risk management, we recommend that regulators continue to focus on standards for regulated financial institutions. Regulated institutions, such as asset managers, should continue to manage contracts with critical vendors. The way each asset manager assesses and implements vendors is unique to the individual firm, as vendors are part of an asset manager's overall infrastructure and each manager must consider the risk of their infrastructure on the whole. As the FSB notes, as part of this responsibility, financial institutions must ensure that they can access, audit, and obtain information from third parties they contract with.

As discussed in response to question 3 below, globally consistent standards for vendor management could help facilitate asset managers' oversight of third parties. Too much direct regulation of vendors could stifle innovation and competition and discourage new vendors from joining the market. To avoid increasing the cost of entry into the space, we recommend that regulators work with asset managers to create globally consistent standards, while continuing to clarify that asset managers are responsible for managing vendors relative to those standards to ensure compliance.

Where asset managers rely on specific FMIs and do not have vendor choice, we encourage regulators to take a more direct approach to oversight. When using an FMI, an asset manager is generally unable to use a different provider in the event that the FMI does not meet its due diligence requirements, which underscores the importance of oversight of FMIs.

Question 3: 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?

We recommend that policy makers clarify and harmonize, where appropriate, third party risk management guidance across borders to ensure all regulated financial institutions are implementing robust risk management oversight of third party vendors. As discussed on page 2, robust risk assessments should be risk-tiered based on the criticality of services provided. Regulated financial institutions should consider the substitutability of vendors and transition plans as appropriate. Third party vendors should be able to demonstrate reliability they have on additional vendors and provide the regulated financial institution with access to relevant data, information, premises, personnel, and systems.

We support the FSB's efforts to create a more consistent and organized oversight framework for third party vendors, and we encourage regulators to agree upon a common set of global principles that form a universal standard across jurisdictions. These principles should include an assessment of a vendor's BCM program; disaster recovery planning; financial, compliance, operational, and information security practices; and right to terminate for poor performance. Such standards could help asset managers with due diligence and ongoing governance of relationships with vendors. Consistent standards would also make it easier for vendors to provide information in a timely and efficient manner.

One emerging practice the FSB mentions in the Discussion Paper is the provision of certificates and reports by third parties evidencing compliance with industry-recognized standards. We believe that such certifications provide a helpful piece of information to asset managers during their due diligence of vendors, and broad adoption of such certifications could be considered but not mandated. Standard attestations that can provide helpful information may include the International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), Center for

Internet Security (CIS), Statement on Standards for Attestation Engagements 18 (SSAE 18), System and Organization Controls (SOC 2), Shared Assessments Standard (SIG), and equally valuable attestations or other similar standards. The appropriate certification requirement or attestation will depend on the operating jurisdiction and regulatory framework in which the firm operates. If a certification is not in place for a given vendor, a risk-tiered assessment model should be used to oversee that service provider. We agree with the FSB that individuals with appropriate expertise should review the information in any such reports, and undue reliance on such certifications or attestations is not appropriate. While certifications or attestations can streamline the review process, they do not replace the need for a risk assessment.

Question 4: 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?

Although most vendors operated smoothly during COVID-19, the crisis highlighted the importance of sustained resilience of third parties and the full supply chain, including those further removed from the asset manager. While an asset manager may not have granularity on fourth party service providers, robust and formal governance around third party providers can help identify and mitigate issues. Third party vendors should outline the capabilities and oversight of vendors they rely on. In our *ViewPoint* Lessons from COVID-19: Operational Risk and Resilience, we outline specific areas that faced challenges during COVID-19, including pricing services and the delivery of shareholder documents in the US.

****

We thank the FSB for providing the opportunity to comment on the Discussion Paper, and we welcome the opportunity to further discuss any of the information or recommendations we have provided.

Sincerely,

Justin Chan
Managing Director, Legal & Compliance

Shirlee Tevet
Managing Director, BlackRock Solutions

Rachel Barry
Director, Global Public Policy Group

Michelle Clement
Director, Risk and Quantitative Analysis