sifma

Invested in America

October 22, 2021

Jennifer Piorko Mitchell
Office of the Corporate Secretary
FINRA
1735 K Street, NW
Washington, DC 20006-1506

Re: Response to Request for Comments on FINRA Report, "Cloud Computing in the Securities Industry"

Dear Ms. Mitchell:

The Securities Industry and Financial Markets Association ("SIFMA")[1] welcomes the opportunity to present its views to the Financial Industry Regulatory Authority Inc. ("FINRA") in response to FINRA's request for public comment on its recent report discussing the adoption and deployment of cloud computing services and products within the securities industry (the "Cloud White Paper").[2]

SIFMA member firms have conscientiously addressed the importance of cloud services and the potential impact they may have in the securities industry, as well as the financial, reputational, and legal risks posed by the use of cloud services. Board-level oversight and thoughtfully developed regulatory, oversight and contracting policies, processes, and control functions associated with the adoption and deployment of cloud services are rapidly becoming industry standard and help to ensure that cloud services are adopted with an appropriate focus on existing regulations and risks to firms and their customers.

In the event FINRA determines further regulation or guidance is appropriate and necessary in the future, we encourage FINRA remain mindful of the challenges presented by the regulatory and contracting ecosystem, as further discussed below. In light of the rigorous existing regulatory landscape, and the significant impact vendors can have on firms' ability to develop compliant contracting practices within the cloud services ecosystem, a principles-based approach to further guidance on cloud may be appropriate. FINRA may continue to assess and clearly identify potential harms to be abated and empower firms to find appropriate, relevant, risk-based solutions. Focusing on risks and outcomes will allow firms to be flexible and pragmatic in response to the evolving challenges posed by the procurement of cloud services and permit FINRA to remain agile in its oversight of critical risks cared for by existing regulations.

---

[1] SIFMA is the leading trade association for broker-dealers, investment banks, and asset managers operating in the U.S. and global capital markets. On behalf of our members, we advocate for legislation, regulation, and business policy affecting retail and institutional investors, equity and fixed income markets, and related products and services. We serve as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency. We also provide a forum for industry policy and professional development. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (GFMA).

[2] Cloud Computing in the Securities Industry (August 16, 2021), https://www.finra.org/rules-guidance/key-topics/fintech/report/cloud-computing.

Our comments below address FINRA's request for comments on the Cloud White Paper, "including areas where guidance or modifications to FINRA rules may be desired to support cloud adoption while maintaining investor protection and market integrity" (p. 15). While we believe issuing additional guidance or modifying FINRA rules is not necessary at this time (as broker-dealers in the securities industry are already subject to complex and comprehensive regulations relevant to cloud services, noted in the Cloud White Paper (p. 12)), we wish to acknowledge a number of points on which FINRA's and SIFMA's views appear to align, as well as provide additional perspective on certain challenges SIFMA has noted in its examination of similar services and in its conversations with its members regarding the adoption of cloud services.

FINRA's recent Cloud White Paper provides a thorough and comprehensive overview of many of the challenges facing broker-dealers at various stages of their cloud adoption and migration journeys. The Paper captures and explains many of the experiences SIFMA members have reported, and it highlights many of the risks and benefits that cloud services offer our members and other firms within the industry. Broker-dealers continue to work with the cloud services providers to ensure cloud services delivery align with the business practices of and regulatory requirements within the industry. At times, however, cloud services providers engage in practices and adhere to customs that create new challenges to broker-dealers, particularly around disclosures of business continuity practices and flexibility relating to certain record-keeping and data access and retention requirements. SIFMA welcomes the guidance and clarity the Cloud White Paper provides around current challenges and risks, as well as existing regulatory requirements, firms must address when utilizing cloud services. The current range of regulations and regulatory guidance provide robust and extensive safeguards requiring complex relationships between firms and service providers maintaining a delicate balance between flexible, scalable, and resilient services provision within the range of required safety measures and regulatory demands. SIFMA encourages further exploration into the issues and a continued open dialogue with the industry.

1. Background

SIFMA believes the Cloud White Paper provides a well-considered and detailed overview of the cloud computing landscape and represents valuable progress in developing a better understanding within the industry of broker-dealers' experiences navigating the many opportunities and challenges presented by an evolving cloud services ecosystem. The Paper is particularly effective in describing the opportunities for firms to leverage cloud computing to reduce long-term costs and augment the agility, efficiency, resiliency and security of such technology and business operations through the use of applications targeting productivity services, data management and analysis, and client-facing solutions while still emphasizing the considerable resources firms invest, the regulatory considerations firms must contemplate and other significant challenges firms may face in managing the risks associated with increased implementation of these services.

SIFMA finds the Cloud White Paper to be especially timely and informative in light of SIFMA's consideration of related issues (albeit, as applied to a narrower scope of services) in its own recent report discussing financial institutions' experiences navigating the regulatory challenges in cloud Infrastructure

as a Service ("IaaS") agreements (the "SIFMA Paper").[3] The SIFMA Paper was developed to examine the general regulatory and guidance requirements in the United States, the European Union, the United Kingdom, and Canada, applicable to financial institutions' use of IaaS services, to review the experience of financial institutions in attempting to address those expectations and requirements in their agreements for IaaS services, and to consider some of the issues that the IaaS vendors have raised in response to financial institutions' preferred contracting approaches, including how those requirements may conflict with IaaS vendors' "shared responsibility" models and the capabilities of IaaS services. Additionally, the SIFMA Paper aimed to identify contractual approaches that have been employed by IaaS vendors and financial institutions to accommodate the IaaS vendors' objections while satisfying the financial institutions' regulatory obligations. In reviewing the Cloud White Paper, SIFMA has found that, in many instances, the experiences of firms adopting and deploying cloud services generally, as described by FINRA, were strongly aligned with, and further validated, the experiences of financial institutions procuring IaaS services, based on the conclusions reached in the SIFMA Paper.

2. Benefits and Challenges of Cloud Adoption

The Cloud White Paper effectively identifies several key benefits, such as agility, resiliency, cost savings, and increased data security, as well as challenges firms face in their adoption and deployment of cloud services. The Paper appropriately recognizes the importance and potential difficulty of modifying workflows, especially for large firms, to take advantage of the increased agility in the deployment of new products firms may utilize as a result of adopting a more robust cloud services profile (p. 9). Additionally, the Paper notes that firms have faced challenges in ensuring their systems are properly configured to enable the secure use of cloud services and the importance of identifying the responsibilities of the firm and vendor in securing the services and any relevant data (p. 10). The Paper also highlights the wariness of firms in facing potential lock-in risk, and how this risk presents challenges to the significant benefits in resiliency found by firms adopting cloud (p. 9). Further, the Paper acknowledges that an organizational shift towards cloud services and away from similar on-premises tools may entail significant upfront costs associated with hiring and training new staff with appropriate expertise, transitioning workflows, and rearchitecting data to take advantage of potential long-term cost savings (p. 9).

The Cloud White Paper also appropriately recognizes a number of important regulatory considerations firms may contend with as they increase the scope of their use of cloud services and engage with third-party vendors in this space (p. 12). While not an exhaustive list, the Paper highlights central regulatory themes, such as cybersecurity, data privacy, outsourcing/vendor management, business continuity, and recordkeeping that firms contend with in their procurement of cloud services.

SIFMA has similarly found that firms adopt innovative technology, such as cloud services, to provide better client service, improve operational efficiency, enhance regulatory compliance, and save money. Many firms wish to expand their use of cloud technology for faster and cheaper scalability of computing power and data storage than what is currently offered by more traditional, locally installed solutions. However, to date, many firms have not expansively adopted cloud technology, partially due to the key challenges the Cloud White Paper so astutely recognizes, partially due to the industry's general judiciousness in

[3] Navigating Regulatory Challenges in Cloud Infrastructure Services Agreements (October 28, 2020), https://www.sifma.org/wp-content/uploads/2020/10/SIFMA-Cloud-White-Paper-BLG-October-23-2020.pdf.

adopting new technologies, and partially due to additional obstacles that may be imposed by regulatory guidance and the process of developing compliant, commercially pragmatic contracts.

3. Contractual Challenges

In the context of IaaS services in particular, SIFMA has noted that firms weigh the overall risks associated with having only a small number of vendors that provide these services. The same vendors provide IaaS services directly to firms as well as indirectly as subcontractors to many Software as a Service ("SaaS") vendors, Platform as a Service ("PaaS") vendors, and other types of vendors (e.g., managed and professional service providers, consultants, law firms) that provide services to firms. Widespread reliance on cloud services vendors in general, and IaaS vendors in particular, constitutes a concentration risk to firms. To help mitigate concentration risks and other risks associated with the failure or poor performance of cloud vendors, firms work to develop contractual obligations that support, and are consistent with, the applicable regulatory expectations and requirements. However, gaps often exist between what firms require and what vendors are willing, or operationally able, to agree to contractually. Firms have found that cloud services vendors may resist accepting some of the contractual obligations that firms must have in place to meet their own regulatory obligations.

As the Cloud White Paper correctly notes, particularly in the context of outsourced services, firms have "…a continuing responsibility to oversee, supervise, and monitor the service provider's performance of covered activities. This requires the member to have in place specific policies and procedures that will monitor the service providers' compliance with the terms of any agreements and assess the service provider's continued fitness and ability to perform the covered activities being outsourced" (p. 13). Developing and implementing appropriate policies and procedures to meet these necessary obligations further contributes to the challenges firms face in the adoption and deployment of cloud services, as noted above. While firms have embraced the need for such policies, successfully implementing these vital programs not only requires a significant investment of time and resources, as well as major operational shifts within member firm organizations, but also the willing cooperation and participation of service providers within the space.

For example, regulators generally expect cloud service agreements to impose comprehensive information security program requirements on vendors, particularly where outsourcing of services is involved. This can include requiring vendors to have policies and procedures to ensure the confidentiality, security, integrity, and availability of firm or customer data and the vendors' systems. To impose these requirements on vendors, service agreements often must include specific provisions relating to the vendors' administrative, technical, organizational and physical controls to safeguard data and the vendors' own systems against unauthorized access, use, disclosure, modification, deletion and unavailability. As a result, firms look for cloud service providers willing to commit to these requirements.

4. Shared Responsibility

The Cloud White Paper insightfully highlights the shared responsibility model often employed by cloud service providers and the challenges that model can present, in particular with respect to configuration of services, data access and security (p. 10). The Paper notes the "importance of correctly identifying responsibilities for maintaining cloud security…to limit control gaps or misconfiguration of cloud resources

based on the mistaken assumption that the cloud service provider would take on cloud security tasks that the firm should be assuming," (p. 10) and further instructs that the "division of tasks should also be reflected in the contractual agreement between the firm and cloud services provider" (p. 12). While firms recognize that they are ultimately responsible for understanding their use cases and making determinations regarding the appropriateness of the service offering, firms have found that vendors may rely on the shared responsibility model to inappropriately shift certain responsibilities better managed by the vendor to the firm. Vendors often resist express obligations in an agreement to provide and maintain the features, functionality and tools necessary to comply with requirements for all use cases and ensuring that they work properly.

5. Business Continuity

The Cloud White Paper also discusses firms' obligations to "create, maintain, annually review and update written business continuity plans relating to an emergency or significant business disruption" (p. 14). Similar to a firm's oversight and cybersecurity obligations, when a firm engages a vendor for cloud services, especially in an outsourcing context, the firm will assess how that vendor maintains continuity of its services so that the firm can comply with applicable regulations and maintain continuity and resilience of its overall operations. To ensure vendors will maintain appropriate continuity controls, service agreements must impose comprehensive business continuity requirements on vendors (including appropriate relationship exit strategies). This may include requiring vendors to implement and maintain business continuity plans, to share these plans with the firm, and to establish and follow procedures for testing and updating these plans. In addition, due to potential latency and availability issues, as the Cloud White Paper suggests, "…firms may wish to consider testing the redundant configuration to ensure business services can continue in the face of a disruption, and update test plans and procedures accordingly" (p. 14). The right to conduct such testing must be included in the service agreement to be effective. Firms also expect vendors to remediate any issues discovered during these tests.

Firms have noted that vendors may sometimes resist participation in firm-driven business continuity plan testing. Vendors may agree to provide only summaries of their business continuity plans and test results, citing security and confidentiality reasons for refusing to permit their customers to conduct or participate in plan testing or to review the full details of their plans and test results, which may present challenges to firms in meeting their own compliance obligations. In these instances, firms must be empowered to use a risk-based approach to determine if a vendor's business continuity contractual commitments are sufficient in light of the nature of the Vendor's service and the scope of the data provided to the vendor.

6. Recordkeeping Obligations

The Cloud White Paper appropriately notes that firms "are increasingly looking to utilize cloud storage for data and information maintained by the firm" (p. 14) and that such uses require firms to comply with FINRA and Securities and Exchange Commission rules requiring firms "to preserve specified records for certain periods." (p. 14). The Paper correctly suggests that "[f]irms should be aware of their recordkeeping obligations and assess any such recordkeeping products or services offered by their cloud providers" (p. 14). However, as noted above, vendors may not always be willing or operationally able to facilitate firm compliance with existing regulatory requirements. As a result, firms must seek vendors that are prepared to provide the tools necessary to manage and ensure proper retention of firms' books and records,

including mechanisms to identify the type of books and records and apply the relevant retention period (including records subject to a legal hold).

As discussed in the Cloud White Paper, recordkeeping rules "…require that such records be preserved during the retention period in a format and media that complies with Exchange Act Rule 17a-4 ("Rule 17a-4"), including, among other requirements, a requirement that records preserved on electronic storage media be stored exclusively in a non-rewriteable and non-erasable format." (p. 14). Additionally, firms are expected to have facilities available for regulators to readily access in a readable format those records that may be requested. To comply with these requirements, firms seek to include contractual obligations around storing books and records in a readily accessible format and define specific protocols by which the firm can access the books and records.

Rule 17a-4 also requires firms to retain a duplicate copy of relevant books and records. Accordingly, firms seek solutions that have functionality that maintains synchronized books and records (often in different locations), including the attending indexes. Firms also favor vendors that provide and maintain mechanisms for financial institutions to monitor the duplication process or provide sufficient documentation, including periodic testing, that the process is effective. Contractual assurances that an appropriate process is in place may include notification provisions for system outages, incomplete data duplication, or other information that a firm may seek. As noted above, seeking vendors willing and able to cooperate with firms' various compliance requirements may significantly limit available service providers and present further challenges to the increased adoption of cloud services.

We are hopeful that the insights recognized in the Cloud White Paper encourage FINRA to continue to pursue efforts to learn, develop, and disseminate information about practices employed and challenges faced in the procurement of cloud services, including the role that vendors of these services play in successful contracting and regulatory compliance, rather than move to issue additional rules or offer prescriptive guidance regarding particular recommended practices. The Cloud White Paper refers to multiple regulatory schemes and detailed guidance documents, which are already in place to sufficiently address the risks posed by cloud services. The complex landscape of legal requirements already applies to the ways firms must ensure data privacy, store information, ensure appropriate cybersecurity and business continuity programs and controls are in place, keep records, inform customers and secure their consent where needed, and protect particularly sensitive types of information. If FINRA were to contemplate imposing additional requirements or obligations, it may consider carefully assessing whether there is any relevant regulatory gap to be remedied, how any such requirements may interact with existing guidance and the various processes firms have invested in and developed to ensure compliance with them, and whether any of the key risks discussed in the Cloud White Paper may be unnecessarily increased by further regulation.

* * *

SIFMA strongly encourages the continuation of open, ongoing, and transparent communication between FINRA and member firms and would welcome the opportunity to continue to contribute to and participate in this valuable process. In addition to our comments above, SIFMA has attached a copy of the SIFMA Paper to this letter, for convenience, should FINRA wish to review.

SIFMA greatly appreciates FINRA's consideration of these comments and would be pleased to discuss any of these views in greater detail if that would assist FINRA's deliberations. Please feel free to contact me at (202) 962-7385 if you would like to discuss further.

Sincerely,

Melissa MacGregor

Melissa MacGregor
Managing Director and Associate General Counsel

cc: Haimera Workie, Head of Financial Innovation, FINRA
Larry Bortstein, Samantha Baer, and Louis Trotta, Bortstein Legal Group

Attachment