MAYSTREET

135 W. 26th Street, 2nd Floor
New York, NY 10001
+1 212 600 1639
www.maystreet.com

October 15, 2021

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

Re: Cloud Computing in the Securities Industry

Dear Ms. Mitchell:

MayStreet appreciates the opportunity to comment on the Cloud Computing in the Securities Industry paper (the "paper") published on August 16, 2021. By combining ultra-low latency software with an advanced approach to the cloud, MayStreet offers the highest-quality, most complete global market data available. We provide lossless consolidated top-of-book and full-depth-of-book data across asset classes and geographies in raw and normalized formats. Given our work delivering data in the cloud to our FINRA-registered broker-dealer customers, we believe we can meaningfully contribute to this discussion.

Key Takeaways

- Our clients' use of the cloud is focused on promoting innovation and collaboration.
- Although the cloud provides significant cost savings, it is not free, and there are key differences in cost management in the cloud versus on-premises environments.
- Each cloud is unique, and those differences must be taken into account in multi-cloud implementations.
- The shared security model extends beyond cloud providers and broker-dealers. It includes application providers offering services in a cloud environment.
- FINRA should take a principles based approach to regulating security in the cloud, recognizing established standards and how they apply to cloud environments.
- Applying best practices in cloud security should include incorporating controls into design, development, and operations, as well as at the organization level.

MAYSTREET

135 W. 26th Street, 2nd Floor
New York, NY 10001
+1 212 600 1639
www.maystreet.com

Cloud Adoption Observations

We concur with the observations made in the paper regarding the growth of cloud adoption and the applications best suited for the cloud (e.g., data analysis). One of the key value propositions our clients identify with cloud adoption is the ability to quickly spin up an environment and focus on analysis rather than infrastructure or data processing. The ability to innovate and collaborate across the organization are among the key reasons that our clients are moving to the cloud. Effective cost management in the cloud often requires a change of mindset as firms adjust to variable pricing and new ways to manage costs.

We also note that multi-cloud strategies require careful planning because minor differences between cloud providers can have a big impact on operations. Our experience is that maximizing performance in one cloud includes taking advantage of cloud-specific tools and offerings. Multi-cloud implementations often require a combination of cloud-specific and open source technologies that are usable across clouds.

Managing Cloud Security

The paper discusses the shared security model between cloud hosting providers (CHPs) and end user firms. Cloud deployments often include 3rd party application providers, particularly cloud service providers ("CSPs"). The cloud model by design relies on the CHP to perform services on behalf of the CSP. To address this complexity, we recommend firms use established security frameworks adapted to the unique attributes of the cloud. Several frameworks are available for this purpose including:

- NIST 800-53
- FedRamp
- OWASP
- ISO 27002
- Center for Internet Security (CIS)
- System and Organizational Controls (SOC)

The choice of framework depends on a number of factors including the security and compliance requirements of the organization, the product, the company's culture and its risk tolerance. These considerations should be factors in FINRA's examination of firms' security regimes.

MAYSTREET

135 W. 26th Street, 2nd Floor
New York, NY 10001
+1 212 600 1639
www.maystreet.com

Taking a closer look at NIST 800-53[1], it is a well-vetted security framework implemented by many firms both in the private and public sector. NIST 800-53 includes the following control families:

1. Access Control 2. Audit and Accountability 3. Awareness and Training 4. Assessment, Authorization, and Monitoring 5. Configuration Management 6. Contingency Planning 7. Identification and Authentication 8. Incident Response 9. Maintenance 10. Media Protection	11. Physical & Environmental Protection 12. Planning 13. Program Management 14. Personnel Security 15. Personally Identifiable Information Processing & Transparency 16. Risk Assessment 17. System and Services Acquisition 18. System and Communication Protection 19. System and Information Integrity 20. Supply Chain Risk Management

While well-established, NIST 800-53 pre-dates the formation of the cloud. As such, we would recommend an initial focus on the following areas when establishing a cloud security program to guide controls across all families:

- Vulnerability Management - The process of identifying, reporting, and remediating vulnerabilities. For example, controls should be implemented to promote early identification of vulnerabilities across the entire surface area of your solution.

- Risk Model Considerations - Risk models should be tailored across a number dimensions including:
    - Cloud configurations: public cloud, private cloud, hybrids, etc.
    - Access: Understand the baseline of who, by default, has access to your application. You may have a different set of security priorities if only a few people have access to your application versus millions on the internet.

[1] During his time as a Global Network Vulnerability Analyst at the National Computer Security Center, Daniel Hestad, who is currently MayStreet's Director of Information Security, was a contributor and evaluator of controls for the initial release of the NIST 800-53.

135 W. 26th Street, 2nd Floor
New York, NY 10001
+1 212 600 1639
www.maystreet.com

- Access Controls and Authentication
    - Application access - required versus actual user base
    - Multiple roles required to secure application
    - Availability of multi-factor and other authentication methods

- Encryption - for the storage, processing and transmission of data

- Due diligence - The CHP performs various services and firms should verify these are being performed to the required standards.
    - Data destruction upon hardware refresh
    - CHP human resources controls
    - CHP audits/controls
    - Ability to audit CHP

Conclusion

MayStreet applauds FINRA for recognizing the importance of the cloud as a transformative technology that has the potential to improve the quality of securities firms' trading decisions and overall operations. Firms need to adapt to the uniqueness of each cloud and overall cloud dynamics like variable pricing.

MayStreet recommends that FINRA permit firms to use security frameworks as the basis for their cloud security programs. Using a framework such as NIST 800-53 as a backdrop while architecting and implementing cloud solutions promotes security not only as part of a secure SDLC process but also as part of maintaining secure operations on an ongoing basis.

MayStreet would welcome further discussions with FINRA on cloud computing. Please do not hesitate to contact us at +1 312-953-9228 or manisha@maystreet.com.

Regards,

Manisha Kimmel
Chief Policy Officer, Maystreet

Daniel Hestad
Director, Information Security