



Marcia E. Asquith

Executive Vice President,
Board and External Relations

Direct: (202) 728-8831
Fax: (202) 728-8300

June 5, 2023

Ms. Vanessa Countryman
Secretary
Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549-1090

Via Email to rule-comments@sec.gov

Re: Cybersecurity Risk Management Rule (Release No. 34-97142; File No. S7-06-23) and Amendments to Regulation Systems Compliance and Integrity (“Regulation SCI”) (Release No. 34-97143; File No. S7-07-23)

Dear Ms. Countryman:

The Financial Industry Regulatory Authority, Inc. (“FINRA”)¹ appreciates the opportunity to comment on the two Securities and Exchange Commission (“Commission” or “SEC”) proposals referenced above: the first, a proposed new rule to require FINRA and other key market participants to address their cybersecurity risks (“Proposed Rule 10”); the second, proposed amendments to expand the entities subject to Regulation Systems Compliance and Integrity (“SCI”) and require SCI entities to enhance their policies and procedures to address, among other things, cybersecurity events and threats (“SCI Proposal”) (together, “Proposals”).² Because the requirements of the Proposals are closely intertwined – and in some cases, compliance with Proposed Rule 10 may constitute compliance with the SCI Proposal – FINRA is submitting this comment letter to address both proposals.

¹ This letter does not represent the views of FINRA CAT, which is a distinct corporate subsidiary of FINRA that acts as the CAT Plan Processor pursuant to an agreement with the self-regulatory organization participants to the CAT NMS Plan.

² See Cybersecurity Risk Management Rule for Broker-Dealers, Clearing Agencies, Major Security-Based Swap Participants, the Municipal Securities Rulemaking Board, National Securities Associations, National Securities Exchanges, Security-Based Swap Data Repositories, Security-Based Swap Dealers, and Transfer Agents, Exchange Act Release No. 97142 (March 15, 2023), 88 FR 20212 (April 5, 2023) (“Rule 10 Proposing Release”); Regulation Systems Compliance and Integrity, Exchange Act Release No. 97143 (March 15, 2023), 88 FR 23146 (April 14, 2023) (“SCI Proposing Release”).

FINRA strongly supports efforts to strengthen the resiliency and integrity of critical market technology infrastructure and to mitigate the risks of cybersecurity incidents that threaten the continuous, fair and orderly functioning of the U.S. securities markets. These are important issues that impact FINRA—both as a regulated entity under Regulation SCI and Proposed Rule 10 and as a regulator overseeing member firms for compliance with these rules. FINRA has and will continue to prioritize its focus on system reliability and resiliency, data protection, and cybersecurity threats facing FINRA, its broker-dealer members and the broader financial markets.³ FINRA generally supports the Commission’s stated objectives as discussed in the Proposals; however, FINRA believes that some aspects of the Proposals may be unclear, unfeasible or unduly burdensome. As discussed in more detail below:

- There are several opportunities for harmonizing compliance requirements between the Proposals. For example, while the Commission characterizes the provisions in Proposed Rule 10 as being “broadly similar” to existing and proposed cybersecurity provisions in the SCI Proposal, the Proposals are not congruent, and therefore create uncertainty and, in some cases, duplicative or overlapping obligations.
- The Proposals’ requirements concerning the management and oversight of third-party service providers may involve efforts that extend beyond the negotiating power of regulated entities—including the need to evaluate extensive, sensitive information that service providers may be unwilling to provide or implement contractual provisions to which providers may not agree.

³ For example, FINRA has published extensive guidance emphasizing the importance of sound practices to manage cybersecurity risks, alerting members to emerging trends and threats, and providing compliance resources and other tools setting forth effective practices. *See, e.g.*, 2023 Report on FINRA’s Examination and Risk Monitoring Program (January 2023) (with a dedicated section focusing on Cybersecurity and Technology Governance); FINRA, Report on Selected Cybersecurity Practices (2018), available at https://www.finra.org/sites/default/files/Cybersecurity_Report_2018.pdf; Cybersecurity Checklist for Firms, available at <https://www.finra.org/compliance-tools/cybersecurity-checklist>; *Regulatory Notice 22-29* (December 2022) (FINRA Alerts Firms to Increased Ransomware Risks); *Regulatory Notice 22-18* (August 2022) (FINRA Reminds Firms of Their Obligation to Supervise for Digital Signature Forgery and Falsification); *Regulatory Notice 21-18* (May 2021) (FINRA Shares Practices Firms Use to Protect Customers From Online Account Takeover Attempts); *Regulatory Notice 20-32* (September 2020) (FINRA Reminds Firms to Be Aware of Fraudulent Options Trading in Connection With Potential Account Takeovers and New Account Fraud); FINRA Investor Insights: *Are You Staying Cyber Safe? 8 Tips for Securing Your Financial Accounts* (March 21, 2023), available at <https://www.finra.org/investors/insights/cyber-safe-financial-accounts>; FINRA, Industry Risks and Threats Resources for Member Firms, available at https://www.finra.org/compliance-tools/Industry_Risks_and_Threats.

- The breadth of several of the Proposals’ defined terms raises compliance concerns, including Proposed Rule 10’s “significant cybersecurity incident,” as well as the proposed expansions to “system intrusion” and “SCI review” under the SCI Proposal.
- The requirement under Proposed Rule 10 to publicly disclose cybersecurity risks and how FINRA assesses, prioritizes and addresses those risks is imprudent because it could reveal sensitive information that threat actors may exploit. In addition, the requirement to promptly publicly disclose significant cybersecurity incidents requires flexibility as to the timing of such disclosure in circumstances where there are ongoing security concerns. The risks of these disclosures may outweigh any potential regulatory or public benefit.
- The Proposals would impose and retain problematic, antiquated manual signature requirements.
- Finally, the Proposals would involve significant impacts on FINRA, some of which do not appear to be fully accounted for in the Commission’s proposing releases. In this regard, and given the breadth of the Proposals, FINRA urges the Commission to provide a suitable length of time before the compliance date, particularly given, among other considerations, the need to modify contracts and arrangements, add or train staff, update systems, modify compliance programs, and update policies and procedures.

I. Duplicative Requirements

A. Separate and Duplicative Reporting Structures

To avoid the burden of regulatory duplication, FINRA requests that the Commission exempt SCI entities from Proposed Rule 10’s SEC reporting requirements with respect to reportable SCI events, so that such events would not be reportable under two regulatory frameworks. Proposed Rule 10 and the SCI Proposal would require separate reporting structures that partially overlap with one another. Essentially, both rules generally would require immediate notification to the Commission of their respective triggering events and the filing of a form; however, the timing and means of notification differ—resulting in a duplicative and unnecessarily complex reporting regime.

For example, Regulation SCI requires that an entity, after having a reasonable basis to conclude that the triggering event has occurred or is occurring, (1) notify the Commission of the event immediately (which is not specifically required to be in writing); (2) follow-up with a written notification on Form SCI, filed through the Electronic Form Filing System (“EFFS”), *within 24 hours* that includes a description of the SCI event and the system(s) affected; (3) provide regular updates regarding the SCI event until the event is resolved; and (4) submit a final detailed written report on Form SCI regarding the SCI event.⁴ Further, “Responsible SCI personnel” must be involved in the determination of event occurrence.⁵ At the same time, Proposed Rule 10 would

⁴ See Rule 1002(b) and SCI Proposing Release, *supra* note 2, 88 FR 23146, 23151.

⁵ See Rule 1002(a). “Responsible SCI personnel means, for a particular SCI system or

require a covered entity to provide the Commission with immediate written electronic notice of a significant cybersecurity incident after having a reasonable basis to conclude that the incident has occurred or is occurring, and to report information about the significant cybersecurity incident promptly, but no later than *48 hours* by filing Part I of proposed Form SCIR through the Electronic Data Gathering, Analysis, and Retrieval System (“EDGAR”).⁶

These misalignments create unwarranted practical difficulties and inefficiencies for SCI entities with respect to events that are reportable under both Regulation SCI and Proposed Rule 10 because regulated entities would be subject to duplicative reporting on separate forms at different timeframes. The Commission stated that most broker-dealers that would be covered entities subject to Proposed Rule 10’s reporting requirements would not also be SCI entities and, consequently, would be unaffected;⁷ however, importantly, FINRA and other entities would be covered under both rules and subject to overlapping notification and reporting requirements. For those entities, the Proposal’s reporting requirements should be aligned. SCI entities have developed a well-established reporting framework to comply with Regulation SCI. FINRA believes that a reasonable and effective manner of achieving alignment in this regard is by exempting SCI entities from the reporting requirements under Proposed Rule 10 with respect to SCI systems and indirect SCI systems. This approach also would allow regulated entities to leverage existing effective practices. Alternatively, FINRA urges the Commission to create a unified reporting framework for SCI entities to mitigate the regulatory uncertainty inherent in two separate reporting requirements that use different terminology and require reporting through different systems (*i.e.*, EDFS for Form SCI versus EDGAR for Form SCIR).⁸ Doing so would not reduce the quality or timeliness of information received by the Commission in any meaningful way, as the SCI Proposal’s triggering events are broader than Proposed Rule 10’s⁹ as it relates to SCI systems and indirect SCI systems and its reporting timeframes are the same (immediate initial

indirect SCI system impacted by an SCI event, such senior manager(s) of the SCI entity having responsibility for such system, and their designee(s).” Rule 1000.

⁶ See Proposed Rule 10(c)(2). The Rule 10 Proposing Release is silent as to any expectations regarding the personnel that should be involved in event analysis and determinations.

⁷ See Rule 10 Proposing Release, *supra* note 2, 88 FR 20212, 20275.

⁸ Because Regulation SCI is narrower than Proposed Rule 10, FINRA recommends that the Commission establish a mechanism to permit an SCI entity to indicate in a Regulation SCI report that the event would also be considered a reportable “significant cybersecurity incident” under Proposed Rule 10.

⁹ See SCI Proposing Release, *supra* note 2, 88 FR 23146, 23197 (“The current and proposed definitions of ‘SCI event’ include not only cybersecurity events, but also events that are not related to significant cybersecurity incidents under the Exchange Act Cybersecurity Proposal.”).

notice) or faster (24 versus 48 hours for written information concerning the event) than Proposed Rule 10's.¹⁰

If the Commission determines that SCI entities must be subject to both reporting frameworks, FINRA requests confirmation that the reporting efficiencies currently permitted under Regulation SCI would also apply under Proposed Rule 10. For example, under Regulation SCI, the Commission staff have provided guidance to permit streamlined reporting for systems shared by multiple covered entities.¹¹ Specifically, the Commission's guidance recognizes that, where an SCI entity has contracted with a third party to perform certain functions on its behalf, the third party "may have more immediate access to information regarding SCI events affecting an SCI system," and the third party "may determine to take the initial and supporting role in complying with the rule's requirements relating to notifications of SCI events under Rule 1002."¹² In the context of SCI entities that are parties to the CAT NMS Plan, the Commission's guidance further permits the SCI entity operating the system to file the required notifications and/or reports with the Commission on Form SCI through the Commission's EDFS system on behalf of one or more CAT participants that are contracting SCI entities.¹³ FINRA requests confirmation that the same guidance would apply to Proposed Rule 10's requirements. Absent this, and contrary to the existing Commission staff guidance for Regulation SCI, Proposed Rule 10 would require duplicative reporting of events for multiple shared systems – including events that are subject to Regulation SCI – on top of unnecessarily duplicative reviews across multiple market entities.

B. Separate and Duplicative Policies and Procedures Requirements

FINRA recommends that the Commission clarify that compliance with the SCI Proposal's policies and procedures requirements is sufficient to satisfy Proposed Rule 10 with respect to SCI systems and indirect SCI systems. The Proposals would impose overlapping but different policies and procedures obligations, creating uncertainty, compliance challenges, and unnecessary duplication.

Specifically, under the SCI Proposal, SCI entities would be required to establish policies and procedures that require, among other things: (1) a third-party provider risk management program that would include an initial and periodic reviews of contracts with third-party providers, and a risk-based assessment of each third-party provider; (2) regular reviews and testing of SCI systems; (3) a systems inventory and classification and lifecycle management program; (4)

¹⁰ Compare Regulation SCI Rule 1002(b)(1) and (2) with Proposed Rule 10(c)(1) and (2).

¹¹ See SEC Division of Trading and Markets, Responses to Frequently Asked Questions Concerning Regulation SCI, Question 2.03, available at <https://www.sec.gov/divisions/marketreg/regulation-sci-faq.shtml>.

¹² *Id.*

¹³ *Id.* at n.19.

business continuity and disaster recovery plans; and (5) a program to prevent unauthorized access to SCI systems. Relatedly, a “covered entity” under Proposed Rule 10 must have policies and procedures that require, among other things: (1) third-party provider management and oversight; (2) periodic assessments of cybersecurity risks associated with the entity’s information systems and information on those systems;¹⁴ (3) categorization and prioritization of cybersecurity risks based on an inventory of the components of the entity’s information systems and information residing on those systems and the potential effect of a cybersecurity incident on the entity;¹⁵ (4) measures designed to detect, mitigate, and remediate any cybersecurity threats and vulnerabilities with respect to the entity’s information systems and information residing on those systems; and (5) user security and access.¹⁶

The Commission recognized that, in some cases, the same entities would be required to comply with both Proposals’ policies and procedures requirements. In this regard, the Commission stated that an SCI entity’s compliance with Proposed Rule 10’s policies and procedures requirements with respect to SCI systems and indirect SCI systems regarding cybersecurity, requirements to oversee service providers, unauthorized access requirements, review and testing requirements, and response programs “should generally satisfy” Regulation SCI’s comparable requirements.¹⁷ However, the Proposals do not specify whether the converse is true — that is, whether compliance with the SCI Proposal’s policies and procedures requirements would satisfy Proposed Rule 10’s policies and procedures requirements with respect to SCI systems and indirect SCI systems.

FINRA also notes that, even where compliance with Proposed Rule 10 “should generally satisfy” compliance with the SCI Proposal with respect to SCI systems and indirect SCI systems, this does not appear to be true in every case, adding to potential uncertainty (*e.g.*, Regulation SCI would require annual penetration testing, which is not required under Proposed Rule 10).¹⁸ Given that Regulation SCI is the current baseline – familiar to both the Commission and SCI entities – the Commission should streamline the Proposals by clarifying that compliance with Regulation SCI’s requirements would satisfy any corresponding policies and procedures requirements under Proposed Rule 10 with regard to SCI systems and indirect SCI systems. At a minimum, FINRA requests that the Commission provide clear and meaningful guidance regarding, and fully analyze the economic impacts of, the delta between the current and mature Regulation SCI policies and procedures requirements and those of Proposed Rule 10.

¹⁴ See Proposed Rule 10(b)(1)(i)(A).

¹⁵ See Proposed Rule 10(b)(1)(i)(A)(1).

¹⁶ See Proposed Rule 10(b)(1)(iv).

¹⁷ See Rule 10 Proposing Release, *supra* note 2, 88 FR 20212, 20272-73.

¹⁸ See SCI Proposing Release, *supra* note 2, 88 FR 23146, 23196 (“Further, while proposed Rule 10 does not require penetration testing, the proposed rule requires measures designed to protect the covered entity’s information systems and protect the information residing on those systems from unauthorized access or use, based on a periodic assessment of the

II. Requirements Concerning Third-Party Providers

FINRA agrees with the Commission regarding the importance of third-party provider oversight, as these entities can play a significant role with respect to an SCI entity's systems. FINRA is concerned, however, regarding the scope of the proposed requirements. First, the application of the risk assessment requirements of the Proposals to all third-party systems—irrespective of criticality—is overbroad and would not yield benefits commensurate with the imposed burdens. Second, the Proposals' requirements for third-party providers could require contractual changes that may be unfeasible or unduly costly. In addition, the SCI Proposal's requirements related to third-party risk and business continuity may be overly restrictive and impracticable.

FINRA recognizes the importance of third-party service providers given their prominence and potential impact on the stability of the U.S. securities markets. To that end, FINRA has long had in place policies and procedures related to third-party provider management and oversight that employ a risk-based approach considering criteria such as data sensitivity, the importance of the provider to the organization (including the number of providers' services relied upon and their expected recoverability), and the third-party system's status under Regulation SCI. Moreover, as a regulator, FINRA has repeatedly emphasized that regulated entities are ultimately responsible for compliance, including for services operated by third-party providers.¹⁹ However, FINRA is concerned that the Proposals' requirements regarding third-party providers are not well-calibrated to achieve the Proposals' objectives.

With respect to third-party provider management, Proposed Rule 10 would require a covered entity to: identify its service providers that receive, maintain, or process information, or are otherwise permitted to access the covered entity's information systems and the covered entity's information residing on those systems; assess the cybersecurity risks associated with the covered entity's use of the service providers;²⁰ and oversee these service providers pursuant to a written contract that provides that the service provider will implement and maintain appropriate measures, including the prescriptions of the extensive policies and procedures requirements of Proposed Rule 10.²¹

covered entity's information systems and the information that resides on the systems.”).

¹⁹ See, e.g., *Regulatory Notice 21-29* (August 2021) (FINRA Reminds Firms of their Supervisory Obligations Related to Outsourcing to Third-Party Vendors).

²⁰ See Proposed Rule 10(b)(1)(i)(A)(2).

²¹ See Proposed Rule 10(b)(1)(iii)(B). As noted below, compliance with Proposed Rule 10's service provider provisions as they relate to SCI systems and indirect SCI systems “should generally satisfy” the third-party provider requirements of Regulation SCI. See Rule 10 Proposing Release, *supra* note 2, 88 FR 20212, 20271.

Similarly, the SCI Proposal would require an SCI entity to manage and oversee third-party providers that provide functionality, support or service, directly or indirectly, for SCI systems and indirect SCI systems.²² These requirements would include an initial and periodic review of contracts with such third-party providers for consistency with the SCI entity's obligations under Regulation SCI; and a risk-based assessment of each third-party provider's criticality to the SCI entity, including analyses of third-party provider concentration, of key dependencies if the third-party provider's functionality, support, or service were to become unavailable or materially impaired, and of any potential security, including cybersecurity, risks posed.

A. Third-Party Risk Assessments

As stated above, FINRA agrees with the Commission regarding the importance of third-party provider oversight. FINRA requests that the Commission modify or clarify the Proposals in a manner that, in our view, would better target the rule and allow regulated entities to focus resources and efforts in a manner that would facilitate the benefits sought to be achieved by the Commission. The Proposals would require a risk assessment of *each* implicated third-party provider; however, third-party providers' systems can vary greatly in their significance to a regulated entity's operations. FINRA believes that the goals set forth in the Proposals can be achieved by requiring comprehensive risk assessments only for third-party providers that, based on the regulated entity's reasonable assessment, *pose systemic risk* to the functionality, service, or support of the regulated entity's systems.

Proposed Rule 10's third-party oversight requirements would broadly require an assessment of the cybersecurity risks associated with the use of service providers related to any "information" or "information system," which, based on the potentially expansive meaning of these terms, could include systems and information that have no bearing on FINRA's regulatory oversight or the fair and orderly functioning of the U.S. securities markets²³—for example, the internal system that allows FINRA employees to informally commend or reward other employees, which is administered and supported by a service provider. Similarly, Proposed Rule 1001(a)(2)(ix) would require an SCI entity to conduct a risk-based assessment of each third-party's criticality to the SCI entity.²⁴ As part of the assessment, an SCI entity would be required to, among other things, review third-party provider concentration and key dependencies should the

²² See SCI Proposing Release, *supra* note 2, 88 FR 23146, 23176.

²³ See Proposed Rule 10(a)(6) ("*Information* means any records or data related to the market entity's business residing on the market entity's information systems, including, for example, personal information received, maintained, created, or processed by the market entity."); Proposed Rule 10(a)(7) ("*Information systems* means the information resources owned or used by the market entity, including, for example, physical or virtual infrastructure controlled by the information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of the covered entity's information to maintain or support the covered entity's operations.>").

²⁴ See SCI Proposing Release, *supra* note 2, 88 FR 23146, 23181.

third-party provider become unavailable or materially impaired. This analysis would be required for each third-party provider, despite the fact that, as the Commission recognized in the SCI Proposal, there are many third-party providers that “provide [only] relatively minor functions, support, or services for an SCI entity.”²⁵

FINRA recommends that the Proposals be amended to apply these requirements only to third-party providers that, based on the regulated entity’s reasonable assessment, pose systemic risk to the functionality, service, or support of its systems. Alternatively, FINRA requests clarification that a regulated entity’s reasonable assessment that a third-party provider’s system does not pose systemic risk to the functionality, service, or support of its systems would satisfy the Proposals’ risk assessment requirements, without a deep review of that third party provider’s systems and controls.

B. Requirements Related to Third-Party Contracts

FINRA is concerned that the third-party management contractual requirements under the Proposals may be unfeasible. A covered entity and an SCI entity will likely not be able to accomplish these measures for a variety of practical reasons. In the case of a third-party service provider that is a relatively small component of a regulated entity’s system that is sold to a large number of clients across different industries, the provider could potentially refuse to customize its standard contractual terms in the manner contemplated in the Proposals. The same may be true for third-party providers that are large industry leaders, such as providers of enterprise cloud services, that will likely not be willing to customize their contractual terms along the lines described in the Proposals. In addition, a third-party provider may decline, due to its own security concerns, to provide increased access to or share in-depth security information. Even where potentially achievable, it would be a significant undertaking to review and negotiate every contract with third-party service providers as would be required under the Proposals and would necessitate a significant increase in legal, operational, and business resources dedicated to third-party management. Further, it is unclear that commensurate benefits would accompany a review of every third-party provider contract, regardless of its criticality to an SCI system.

For example, Rule 1001(a)(2)(ix) would require that an SCI entity conduct initial and periodic reviews of contracts with third-party providers for consistency with the SCI entity’s obligations under Regulation SCI. As a general matter, FINRA currently undertakes such reviews. When entering into contractual relationships with third-party providers that may operate or support direct or indirect SCI systems, FINRA conducts due diligence to confirm that the providers can be used consistent with Regulation SCI and, throughout the duration of the contractual relationships, FINRA performs oversight of the provider’s performance. However, FINRA is concerned that the SCI Proposal introduces obligations that would be unfeasible. The SCI Proposal cautions SCI entities to “consider whether or not it is appropriate to rely on a third-party provider’s standard contract or standard service level agreement (“SLA”), particularly if such contract or SLA has not

²⁵

Id.

been drafted with Regulation SCI’s requirements in mind.”²⁶ The SCI Proposal states that an SCI entity may want to consider negotiating provisions with third-party providers “that provide priority to the SCI entity’s systems, such as for failover and/or business continuity and disaster recovery . . . if needed to meet the SCI entity’s obligations under Regulation SCI.”²⁷ FINRA believes it is unlikely that providers would consent to providing additional benefits to FINRA, at the expense of other clients.²⁸ In addition, the SCI Proposal states that an SCI entity should consider negotiating, among other things, an addendum to separate and highlight the contractual understanding of the parties with respect to SCI-related obligations; or to include terms using the same definitions provided in Regulation SCI.²⁹

FINRA agrees that regulated entities should assess outsourcing arrangements, including considering whether arrangements can be appropriately managed consistent with the obligations of the Proposals. However, requiring a regulated entity to attempt to negotiate the types of contractual terms suggested by the Proposals may not be feasible and could unnecessarily constrain a regulated entity’s provider options to the detriment of its technological infrastructure. As a result, FINRA urges the Commission to reconsider these requirements and instead amend the Proposals to require that the third-party management requirements emphasize provider due diligence and oversight, rather than mandate specific contractual provisions. A regulated entity’s determination to choose one third-party service provider rather than another should be driven by the quality of the provider’s services, including an assessment of such party’s ability to comply with applicable regulatory obligations—rather than a provider’s willingness to modify its SLAs. Thus, FINRA believes emphasizing provider due diligence and oversight would achieve a more reasonable and, on balance, effective outcome.

In addition, the examples provided in the SCI Proposal, while presented as measures to “consider,” are concerning because many are unachievable and may run counter to the overall goals of the proposal. To the extent a contract review requirement is retained in the SCI Proposal, SCI entities’ review requirements should be limited to third-party provider systems that, based on an SCI entity’s reasonable assessment, pose systemic risk to the functionality, service, or support of a SCI system. Further, FINRA requests clarification as to how often a “periodic” review must take place. Requiring annual, biennial, or more frequent reviews of contracts would substantially increase the cost and burden of compliance for SCI entities with uncertain benefits. Following the initial contract negotiations, absent significant intervening regulatory changes, FINRA suggests

²⁶ See SCI Proposing Release, *supra* note 2, 88 FR 23146, 23179.

²⁷ See *id.*

²⁸ FINRA is concerned that Proposed Rule 10 may contemplate requiring covered entities to disclose significant cybersecurity incidents on behalf of or occurring at third-party service providers that are not independently subject to the Proposals. Service providers are often reticent to provide information into issues impacting their confidential proprietary applications and infrastructure.

²⁹ *Id.*

instead that subsequent reviews of contracts be required only upon contract renewal or changes in service that require contract modifications.

C. SCI Proposal's Requirements Regarding Third-Party Provider Risk and Business Continuity Plans ("BC/DR")

FINRA is concerned that the SCI Proposal's requirements related to third-party risk and business continuity may be overly restrictive, particularly insofar as the SCI Proposal suggests that Commission staff may question the use of single-provider arrangements. Proposed Rule 1001(a)(2)(ix) would require an SCI entity to conduct a risk-based assessment of the criticality of each third-party provider, which would include, among other things, a consideration of third-party provider concentration. Under the SCI Proposal, SCI entities would also be required to properly account for and prepare contingencies or alternatives to avoid the overreliance on cloud service providers ("CSPs") or other third-party providers. In conducting this assessment, the Commission recommends that SCI entities consider the costs and benefits of potential alternatives that could reduce the SCI entity's dependence on a single third-party provider.³⁰ The SCI Proposal states that an SCI entity should consider both temporary and long-term outages by third-party service providers in developing its BC/DR plans, and notes that any CSP utilized by an SCI entity would be required to participate in BC/DR testing under the proposed amendments to Rule 1004 (discussed below).³¹ In addition, the SCI Proposal suggests that any SCI entity engaging a CSP for its critical SCI systems, should consider maintaining an "on-premises" backup data center or develop alternative contingency plans.³²

FINRA notes that, with respect to select systems and applications, there can be significant benefits single-providers or CSPs can provide for certain functions related to SCI systems, which also can make it ineffective, impracticable and potentially riskier to utilize multi-providers to perform services. For example, establishing multi-cloud architecture can add substantial risks and operational complexity throughout the development and complete lifecycle of an SCI system without a corresponding benefit (where the SCI entity believes there is a low likelihood of a full-blown service outage by a single CSP). In many cases, alternatives, such as multi-region backups that rely on the same CSP provider but replicate data to different regional hosting sites, can provide the same benefits as provider diversity but without the complexity and associated risk of operating multiple cloud systems. In addition, maintaining an "on-premises" backup data center is impracticable or prohibitively expensive. As the Commission acknowledges in the SCI Proposal, CSPs are able to develop certain applications or systems that an SCI entity would not be able to produce in-house or provide services that an SCI entity may not have the ability to operate.³³ FINRA agrees with these statements. In addition, the SCI Proposal acknowledges that there are

³⁰ See SCI Proposing Release, *supra* note 2, 88 FR 23146, 23178.

³¹ *Id.* at 23180.

³² *Id.*

³³ *Id.* at 23235-36.

significant benefits associated with utilizing CSPs, including cost efficiencies and increased automation, with CSPs providing invaluable expertise in areas such as security and data latency.³⁴ FINRA also agrees with these statements and notes that FINRA’s use of CSPs (and other third-party providers) overall has resulted in cost savings, automation, increased security and resiliency, along with other efficiencies that may not otherwise be achievable, and certainly not at a remotely comparable cost.

While the proposed rule text does not explicitly require SCI entities to engage or retain multi-provider alternatives (such as multi-cloud arrangements), the discussion in the SCI Proposal raises questions regarding the expectations of the Commission, especially given that an SCI entity may not be able to eliminate reliance on a single provider, including a CSP.³⁵ Despite these discussions, it is FINRA’s understanding that proposed Rule 1001(a)(2)(v) and (ix) does not preclude single provider arrangements and understands that SCI entities would have significant flexibility to tailor their BC/DR plans to their specific systems and unique circumstances and to consider the costs and benefits of different provider options when conducting risk-based assessments of CSPs and other third-party vendors as envisioned by the Commission under the Proposal. These assessments would then be subject to appropriate SEC oversight to ensure the reliable, resilient, and secure operations of the SCI entities’ SCI systems and indirect SCI systems. To the extent these amendments are adopted, FINRA requests that the Commission further clarify that the Rule does not preclude single-provider arrangements, and SCI entities will have an appropriate degree of flexibility—subject to SEC oversight—in conducting their risk-based assessments to determine that a single-provider or provider concentration yields benefits that outweigh the costs and risks of utilizing multi-cloud architecture or strategies or maintaining “on-premises” backups.

While FINRA generally supports the SCI Proposal’s amendments to Rule 1004 to require that SCI entities designate key third-party providers for participation in annual BC/DR testing, with respect to third-party providers who provide software as a service (“SaaS”), FINRA is concerned that it may not always be feasible for an SCI entity to compel these providers to participate in its DR testing. Also, it is unclear what type of “participation” would be required during a BC/DR test. For many SaaS providers, the software is run on an SCI entity’s own systems, so the availability of the software would generally not be dependent on the provider. Further, to the extent a direct or indirect SCI system is operated by a third-party provider that is itself an SCI entity, FINRA requests the Commission clarify that, in such instances, an SCI entity

³⁴ *Id.*

³⁵ Moving to multi-cloud architecture would result in FINRA expending extensive resources—potentially multiple millions of dollars to copy and move the data—on rewriting its complex technological platforms to a cross-cloud operation, and incurring substantial management and monitoring costs. These costs may well exceed the estimates discussed in the SCI Proposal. At the same time, the proposal would eliminate the benefits associated with the use of single-provider arrangements, including standardized tools and services across FINRA’s technological enterprise.

may reasonably rely on representations from the third-party SCI-entity provider to satisfy the requirements of Rule 1001(a)(2)(v) and Rule 1004.

III. Key Definitions in Proposed Rule 10 and the SCI Proposal

FINRA strongly supports efforts to improve the Commission’s ability to monitor and evaluate the effects of cybersecurity events on entities and their customers, counterparties, members, registrants, or users, as well as assess the potential risks affecting the financial markets more broadly. However, FINRA urges the Commission to consider how best to tailor event reporting under the respective proposals. For example, overbroad triggers could undermine the utility of the requirements by creating a deluge of noise that will interfere with regulators’ ability to meaningfully assess market implications and also be overly burdensome on regulated entities.

A. Proposed Rule 10

As noted above, under Proposed Rule 10, a covered entity, including FINRA, would be required to provide immediate written electronic notice to the Commission upon having a reasonable basis to conclude that a significant cybersecurity incident has occurred or is occurring, and to report detailed information about the significant cybersecurity incident by filing, on a confidential basis, Part I of Form SCIR through EDGAR.³⁶ Paragraph (a)(10) of Proposed Rule 10 defines a “significant cybersecurity incident” as “a cybersecurity incident, or a group of related cybersecurity incidents, that: (i) Significantly disrupts or degrades the ability of the market entity to maintain critical operations; or (ii) Leads to the unauthorized access or use of the information or information systems of the market entity, where the unauthorized access or use of such information or information systems results in or is reasonably likely to result in: (A) Substantial harm to the market entity; or (B) Substantial harm to a customer, counterparty, member, registrant, or user of the market entity, or to any other person that interacts with the market entity.”³⁷ FINRA notes that this definition is potentially broad, and without additional guidance and clarity from the Commission could result in overinclusive and uninformative reporting.

In addition, FINRA notes that “cybersecurity incident” – defined as “an unauthorized occurrence on or conducted through a market entity’s information systems that jeopardizes the confidentiality, integrity, or availability of the information systems or any information residing on those systems” – needs further consideration, in part due to the inclusion of the broad definitions of “information” and “information systems,” which, as noted above, may include information and systems that have no bearing on FINRA’s regulatory oversight or the fair and orderly functioning of the U.S. securities markets. If these terms are not clarified and narrowed, the cascading impact could result in an inundation of trivial “significant cybersecurity incidents.” The breadth of “cybersecurity incident” also materially impacts other requirements, aside from reporting, under Proposed Rule 10. For example, the incident response policies and procedures required under Proposed Rule 10 must include written documentation of all cybersecurity incidents (rather than

³⁶ Proposed Rule 10(c)(1) and (2).

³⁷ See Proposed Rule 10(a)(10).

significant cybersecurity incidents), and the entity’s response to and recovery from each incident, which is a potentially unfeasible burden if not appropriately narrowed.³⁸

FINRA also requests narrowing of other terms that are integral to Proposed Rule 10. For example, the term “cybersecurity risk” in the proposal does not rely on a standard definition focused on security vulnerabilities leading to actual or potential loss of confidentiality, availability, and integrity. Rather, it focuses on financial, operational, legal, reputational, or adverse *consequences* that may result from a cybersecurity incident, a cybersecurity threat, or a cybersecurity vulnerability. Entities typically assess the financial, operational, legal, reputational, or other adverse consequences as risks they consider when developing cybersecurity responses and protections. Accordingly, FINRA suggests that the Commission narrow the definitions to ensure that the cybersecurity controls are focused on the *confidentiality, availability, and integrity of the information and information systems* and not on the risks associated with potential gaps. For example, the Commission could define “cybersecurity risk” to mean “security vulnerabilities or threats or cybersecurity incidents that the entity determines are likely to result in the loss of confidentiality, integrity, or availability of a market entity’s information systems or any information residing on those systems.”

Finally, as noted above, the definitions of “information” or “information systems” are also potentially broad and would capture systems and information that are not critical to FINRA’s operations and, if breached, would not impact the continuous, fair and orderly functioning of the U.S. securities markets (*e.g.*, the internal system that allows FINRA employees to informally commend or reward other employees). FINRA encourages the Commission to allow covered entities to take a risk-based approach in assessing the information and information systems covered by Proposed Rule 10’s requirements.

B. Regulation SCI

FINRA believes that the current definition of “systems intrusion” properly focuses on unauthorized entry into an SCI system or indirect SCI system, rather than including within its scope unsuccessful attempts. Under the SCI Proposal, the definition of “systems intrusion” (which itself is included within the scope of the definition of the term “SCI event”) would be amended to include a “[s]ignificant attempted unauthorized entry into the SCI systems or indirect SCI systems of an SCI entity, as determined by the SCI entity pursuant to established reasonable written criteria.”³⁹ As a result, an SCI entity would be required to: (1) “take appropriate corrective action” with respect to such significant attempted unauthorized entries (under Rule 1002(a)), and (2) report such events to the Commission (under Rule 1002(b)).

FINRA is concerned that this proposed expansion of the definition of “systems intrusion” is not calibrated to reasonably balance benefits and burdens. The attempts sought to be captured by the SCI Proposal, by definition, were successfully defended against by the SCI entity, and would

³⁸ See Proposed Rule 10(b)(1)(v)(B).

³⁹ See SCI Proposing Release, *supra* note 2, 88 FR 23146, 23185.

therefore provide the Commission with little information that could alter its general assessment of the security status of the SCI entity's systems.⁴⁰ The SCI Proposal discusses criteria that could encompass a very large number of incidents—operational events that occur hundreds or even thousands of times a day. FINRA does not agree that the criteria identified in the SCI Proposal as indicia of “significant” attempts are inherently “significant” in all cases. And in some cases, whether or not a particular attempt meets these criteria would not be readily apparent from the activity detected and would require further investigation into the activity to discern—a time and resource expenditure that is not justified by any commensurate benefit. Specifically, the SCI Proposing Release discusses criteria including, an SCI entity becoming “aware of reconnaissance that may be leveraged by a threat actor”; “a targeted campaign that is customized to the SCI entity's system”; “an attempted attack from a known sophisticated advanced threat actor”; and “a cybersecurity event that, if successful, had meaningful potential to result in widespread damage and/or loss of confidential data or information.”⁴¹ Many entities with a significant online presence constantly experience scanning efforts by attackers designed to identify and exploit potential system vulnerabilities. FINRA has a sophisticated cybersecurity infrastructure to defend against attackers, and this infrastructure combats these scanning efforts as part of its ordinary operations. Such activity does not indicate an event that in FINRA's view should be deemed “significant.” The potential ramifications of such a broad scope are concerning because reporting these types of events to the Commission would be impractical and impose a substantial and distracting burden on an SCI entity's cybersecurity program. And, even if reporting were practical, the information would be of very little or no value.

FINRA requests clarification that the existence of one or more of the criteria identified in the SCI Proposal is not determinative of an unauthorized entry attempt's significance. Rather, the criteria used by an SCI entity to define “significant” can focus on identifying attempted unauthorized entry events that are discernably out of the ordinary for the SCI entity—that is, they represent deviations from the malicious activity that the SCI entity's cybersecurity program successfully defends against in the ordinary course.⁴² For example, more relevant factors might look to the depth of the breach in terms of proximity to SCI systems and critical SCI systems⁴³ and real-time escalation to senior management in the cybersecurity program (beyond triage by front-line cybersecurity personnel), potentially in conjunction with one or more of the factors discussed above (*e.g.*, a targeted campaign that is customized to the SCI entity's systems).

⁴⁰ *See id.*

⁴¹ *Id.* at 23185.

⁴² As the Commission explained in the SCI Proposing Release, “SCI entities differ in nature, size, technology, business model, and other aspects of their business” and what may be “significant” for one SCI entity may not be “significant” for another. *Id.*

⁴³ An SCI entity may employ multilayer firewalls, and it is not uncommon for an attack to traverse outer firewall layers.

FINRA also requests clarification regarding what “corrective action” the Commission expects SCI entities to take with respect to “significant attempted unauthorized entry” events, given, by definition, the SCI entity’s cybersecurity program successfully defended against the attempted unauthorized entry. Under Rule 1002(a), “corrective action” includes, “at a minimum, mitigating potential harm to investors and market integrity resulting from the SCI event and devoting adequate resources to remedy the SCI event as soon as reasonably practicable.” The Commission has explained that “Rule 1002(a) will likely result in SCI entities developing and revising their processes for corrective action as well as review them annually.”⁴⁴ However, where an SCI entity’s cybersecurity program operated successfully, beyond having blocked the attempt in real time, it is not clear what additional steps the Commission believes would be required to satisfy Rule 1002(a).

IV. Public Disclosure Under Proposed Rule 10

Under Proposed Rule 10, FINRA and other covered entities would be required to publicly disclose, by filing Part II of Proposed Form SCIR, a summary description of: (1) the cybersecurity risks that could materially affect the entity’s business and operations and how the entity assesses, prioritizes, and addresses those cybersecurity risks; and (2) each significant cybersecurity incident that has occurred during the current or previous calendar year.⁴⁵ As noted above, FINRA, in developing its cybersecurity program, views the protection of industry and customer information as a key responsibility, and prioritizes the securing of its information. However, FINRA believes the requirement to publicly disclose material cybersecurity risks and how a regulated entity assesses, prioritizes, and addresses those cybersecurity risks could encourage and enable the very malicious conduct that the Proposed Rule 10 seeks to mitigate. Additionally, FINRA is concerned that the requirement to promptly disclose significant cybersecurity incidents to the public does not allow sufficient flexibility to, for example, delay disclosing a significant cybersecurity incident if particular security concerns warrant delaying such disclosure.

The Commission has long recognized that risks involved with public disclosure are heightened for market regulation and surveillance systems. Accordingly, under Regulation SCI, the requirement to publicly disseminate information about SCI events (including intrusions) is specifically tailored to exclude market regulation and surveillance systems, because “dissemination of such information to an SCI entity’s members or participants or the public at large could encourage prohibited market activity.”⁴⁶ The same reasoning should apply with respect to

⁴⁴ See SCI Proposing Release, *supra* note 2, 88 FR 23146, 23209.

⁴⁵ See Proposed Rule 10(d).

⁴⁶ See Regulation Systems Compliance and Integrity, Exchange Act Release No. 73639 (November 19, 2014), 79 FR 72252, 72336 (December 5, 2014) (“Regulation SCI Adopting Release”). In addition, dissemination of information to members or participants is permitted to be delayed for systems intrusions if such dissemination would likely compromise the security of the SCI entity’s systems or an investigation of the intrusion. See Rule 1002(c).

Proposed Rule 10's requirement to publicly disclose cybersecurity risks. The disclosure of FINRA's cybersecurity risks, how FINRA prioritizes and addresses those risks, even in summary fashion, could encourage bad actors and – in contravention of the very purpose of the proposed rule—would create the same risks the Commission sought to avoid under Regulation SCI. Furthermore, FINRA notes that requiring public disclosure of FINRA's cybersecurity risks would not inform investor choice as it does with respect to covered entities with customers. For these reasons, FINRA believes Proposed Rule 10's requirement to publicly disclose sensitive cybersecurity information pose risks that outweigh any potential regulatory or public benefit.

The same may be true of the requirement to quickly publicize significant cybersecurity incidents because bad actors may capitalize on this information, particularly with respect to ongoing incidents. FINRA recognizes that disclosure of significant cybersecurity incidents has utility, especially when disclosure of confidential customer information is at stake. Nonetheless, FINRA believes the nature and risk of a particular cybersecurity incident must be considered in determining the timing of publicizing a cybersecurity incident or notifying affected customers. Accordingly, as is permitted under Regulation SCI,⁴⁷ FINRA recommends the Commission provide flexibility under the cybersecurity incident public disclosure requirement to delay disclosing significant cybersecurity incidents where such disclosure would risk continuing or exacerbating a security concern.

FINRA notes that it would separately be obligated under Proposed Rule 10 to give the Commission immediate written electronic notice of a significant cybersecurity incident upon having a reasonable basis to conclude that the significant cybersecurity incident has occurred or is occurring. FINRA believes this requirement sufficiently augments the information to which the Commission already has access to allow the Commission to effectively oversee FINRA's robust cybersecurity program.

Finally, to the extent that the proposal contemplates a requirement to publicly disclose a summary description of the cybersecurity risks of service providers or information regarding significant cybersecurity incidents on behalf of or occurring at service providers, FINRA would oppose such requirements as unfeasible, as noted above in the comments regarding third-party providers. Third-party providers would likely raise compelling concerns with the public disclosure of their proprietary and sensitive risk information.

V. Manual Signature Requirement

The Proposals appear to impose (or, with respect to Regulation SCI, retain) outdated manual signature requirements. As the Commission considers ways to adapt Regulation SCI to evolving technology and business practices, FINRA urges the Commission to reconsider the manual signature requirement. While Rule 1006(a) requires an electronic signature on Form SCI and electronic filing of Form SCI, Rule 1006(b) also requires the signatory to an electronically filed Form SCI to manually sign a signature page or document, in the manner prescribed by Form

⁴⁷ See Rule 1002(c).

SCI, authenticating, acknowledging, or otherwise adopting the signature that appears in typed form within the electronic filing.

Similarly, the instructions to Proposed Form SCIR indicate that a covered entity must retain a “paper copy, with original signatures, of Part I and Part II of Form SCIR and make the copy available for inspection upon a regulatory request.”⁴⁸ In recent years, the Commission has modernized signature requirements, amending rules to allow for the use of electronic signatures in lieu of manual or “wet” signatures,⁴⁹ and the Commission recently proposed eliminating an identical manual signature requirement for Form 19b-4 where the form is also required to be signed and filed electronically.⁵⁰ As the Commission recognized in the similar context of Form 19b-4, “the manual signature requirement under Rule 19b-4 is redundant and therefore unnecessary given that Form 19b-4, which is filed electronically, already requires an electronic signature.”⁵¹ Considering the Commission’s general movement toward electronic signature and filing requirements and the redundancy of Form SCI and Form SCIR’s manual signature requirements, FINRA requests that the Commission reconsider the necessity of these manual signature requirements.

VI. Impact of the Proposals on FINRA

FINRA has a comprehensive cyber and information security program, and we have made significant investments to secure the data and information residing on our systems, including in the areas specifically discussed by the Commission in its Proposals (*e.g.*, user security and access). When estimating the costs for FINRA to comply with Proposed Rule 10’s policies and procedures requirements, the Commission stated that it “does not expect” FINRA to incur significant costs because FINRA is already subject to Regulation SCI and FINRA has strong incentives to invest in comprehensive cybersecurity programs.⁵² However, FINRA is concerned that the Proposals’ requirements – in particular those related to third-party provider oversight and event reporting – would require FINRA to expend significantly more resources than are accounted for in the Commission’s cost estimates.

In addition, FINRA believes the SCI Proposal also may have underestimated the cost impacts in some regards. For example, to the extent the SCI Proposal’s business continuity plan

⁴⁸ See Proposed Form SCIR Instructions A.4.c.

⁴⁹ See, *e.g.*, Electronic Signatures in Regulation S-T Rule 302, Exchange Act Release No. 90441 (November 17, 2020), 85 FR 78224 (December 4, 2020).

⁵⁰ See Electronic Submission of Certain Materials Under the Securities Exchange Act of 1934; Amendments Regarding the FOCUS Report, Exchange Act Release No. 97182, (March 22, 2023), 88 FR 23920 (April 18, 2023).

⁵¹ *Id.* at 23944.

⁵² See Rule 10 Proposing Release, *supra* note 2, 88 FR 20212, 20303.

provisions would require the onboarding of an additional provider(s) to avoid reliance on a single provider for critical systems, compliance costs could easily reach the tens of millions of dollars range *for a single SCI entity*. Similarly, other requirements discussed by the Commission—such as the SCI Proposal’s discussion that an SCI entity should consider if use of a CSP for its critical SCI systems warrants maintaining an “on-premises” backup data center—would be cost prohibitive.⁵³

FINRA also is concerned that the Proposals underestimate the costs associated with reporting requirements. The SCI Proposal’s cost estimates appear to assume that the expanded definition of “systems intrusion” will result in existing SCI entities reporting only another three non-*de minimis* SCI events per year.⁵⁴ However, the requirement to report “significant attempted unauthorized entry” events may involve a very large number of reports to the Commission per day (and there would be no *de minimis* exception for reporting systems intrusions under the SCI Proposal as there is today).

Separately, in addition to the impacts on FINRA as a regulated entity, the Proposals will also require FINRA to expand its existing regulatory programs to include oversight for compliance with these new requirements. While FINRA does not currently have enough information to fully assess the costs involved with the new requirements of Proposed Rule 10 and Regulation SCI, we expect these costs will be significant, involving changes to our regulatory systems and infrastructure, as well as additional staff resources, and may require future funding solutions. In addition, given the significant changes that the Proposals contemplate for FINRA and other market participants, a sufficient implementation timeframe should be provided prior to the Proposals’ compliance dates.

VII. Conclusion

FINRA thanks the Commission for its attention to FINRA’s comments on the Proposals and looks forward to continued engagement with the Commission to work toward strengthening the resiliency and integrity of critical market technology infrastructure and mitigating the risks of cybersecurity incidents that threaten the continuous, fair and orderly functioning of the U.S. securities markets. FINRA believes the requested clarification and proposed alternatives would preserve the objectives of the Proposals while reducing regulatory duplication under the two rules, simplifying compliance for covered entities and reducing costs, without materially reducing the benefits sought to be achieved by the Commission as described in the Proposals. If you have any questions or would like to further discuss FINRA’s views and comments, please contact Racquel

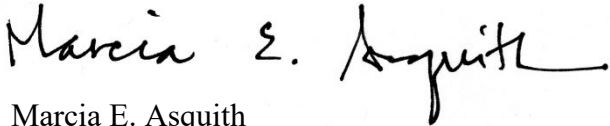
⁵³ See SCI Proposing Release, *supra* note 2, 88 FR 23146, 23180. In addition, FINRA requests that the Commission clarify that any system that falls within the scope of the term “indirect SCI systems” solely by virtue to its relationship to an SCI system directly supporting market regulation or market surveillance would be subject to the SCI review cadence described in proposed paragraph (3) of the definition of “SCI review.”

⁵⁴ See *id.* at 23210-11.

Ms. Vanessa Countryman
June 5, 2023
Page 20 of 20

Russell, Senior Vice President and Director of Capital Markets Policy, FINRA, at (202) 728-8363
(racquel.russell@finra.org).

Sincerely,

A handwritten signature in black ink that reads "Marcia E. Asquith". The signature is written in a cursive style with a long horizontal flourish at the end.

Marcia E. Asquith
Corporate Secretary, EVP
Board and External Relations