FINANCIAL INFORMATION FORUM

June 5, 2023

By electronic mail to rule-comments@sec.gov

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

Re: File Number S7-06-23: Cybersecurity Risk Management for Broker-Dealers and Certain Other Entities Subject to Regulation Under the Securities Exchange Act of 1934
File Number S7-07-23: Regulation Systems Compliance and Integrity
File Number S7-05-23: Regulation S-P

Dear Ms. Countryman,

The Financial Information Forum ("FIF")[1] appreciates the opportunity to comment on the recent rule proposals by the Securities and Exchange Commission (the "Commission") on cybersecurity risk management for broker-dealers and other entities subject to regulation under the Securities Exchange Act of 1934,[2] Regulation Systems Compliance and Integrity ("Regulation SCI"),[3] and Regulation S-P.[4] This letter addresses specific issues raised by these three rule proposals and does not seek to address all issues of concern to FIF members relating to these proposals.

[1] FIF (www.fif.com) was formed in 1996 to provide a centralized source of information on the implementation issues that impact the securities industry across the order lifecycle. Our participants include broker-dealers, exchanges, back office service bureaus, and market data, regulatory reporting and other technology vendors in the securities industry. Through topic-oriented working groups, FIF participants focus on critical issues and productive solutions to technology developments, regulatory initiatives, and other industry changes.
[2] Securities Exchange Act Release No. 97142 (Mar. 15, 2023), 88 FR 20212 (Apr. 5, 2023) (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) ("Cybersecurity Proposing Release").
[3] Securities Exchange Act Release No. 97143 (Mar. 15, 2023), 88 FR 23146 (Apr. 14, 2023) (Regulation Systems Compliance and Integrity) ("Regulation SCI Proposing Release").
[4] Securities Exchange Act Release No. 97141 (Mar. 15, 2023), 88 FR 20616 (Apr. 6, 2023) (Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information) ("Regulation S-P Proposing Release").

A. Cybersecurity Risk Management rule proposal

Security concerns about the EDGAR system

Under the proposed cybersecurity Rule 10, Form SCIR would be filed through the Commission's Electronic Data Gathering, Analysis and Retrieval System ("EDGAR").[5] As proposed by the Commission, Covered Entities would be required to "… file Parts I and II of proposed Form SCIR in an eXtensible Markup Language ("XML")-based data language specific to the form ("custom XML," and in this release "SCIR-specific XML")."[6]

FIF members have concerns about the security of the EDGAR system in light of the 2016 intrusion of EDGAR during May to October 2016, which was publicly announced by the Commission on September 20, 2017.[7] According to a Commission press release, as a result of this intrusion, hackers "… traded before at least 157 earnings releases from May to October 2016 …."[8] The Commission's proposing release for proposed cybersecurity Rule 10 (the "cybersecurity proposing release") does not include any discussion of this intrusion and the steps that the Commission has undertaken, is currently undertaking, and plans to undertake in the future to prevent a recurrence of this type of intrusion.

Given the potential risk that malicious actors would seek to obtain unauthorized access to the Part I Form SCIR data stored in the EDGAR system, FIF members recommend that the Commission reissue the cybersecurity proposing release to discuss this potential risk and the steps that the Commission is currently undertaking, and plans to undertake in the future, to protect against this type of risk. The Commission should explain how the steps being undertaken by the Commission would prevent the type of intrusion to the EDGAR system that occurred during 2016. The Commission also should identify any third-party certifications that Covered Entities could rely upon as assurances relating to the security of the data that is submitted to EDGAR. The Commission also should provide detail on whether and how EDGAR incorporates secure software development practices.

The Consolidated Audit Trail ("CAT") system, like the Commission's proposed Form SCIR, requires the reporting of sensitive data. The CAT system is governed by the CAT NMS Plan, which contains extensive security requirements for the protection of the data that is reported to CAT. These include requirements relating to the development of a comprehensive security plan, secure connectivity to the data repository, data encryption, data center controls, physical security controls, penetration testing, third-party application security code auditing, role-based access controls, logging of access to the data repository, monitoring to detect unauthorized access and associated escalation procedures, multi-factor authentication, and cyber incident management.[9] The Commission should implement equivalent

[5] Proposed Rule 10(c)(2) and 10(d)(2).
[6] Cybersecurity Proposing Release, at 176.
[7] See "SEC Chairman Clayton Issues Statement on Cybersecurity" (Sept. 20, 2017), available at https://www.sec.gov/news/press-release/2017-170. See "SEC Brings Charges in EDGAR Hacking Case" (Jan. 15, 2019), available at https://www.sec.gov/news/press-release/2019-1 ("SEC 2019 Press Release").
[8] SEC 2019 Press Release.
[9] Limited Liability Company Agreements of Consolidated Audit Trail, LLC (July 24, 1996), available at https://catnmsplan.com/sites/default/files/2020-07/LLC-Agreement-of-Consolidated-Audit-Trail-LLC-as-of-7.24.20.pdf, at D-10 to D-15.

controls for reporting of data on Part I of Form SCIR or explain why such controls would not be appropriate.

Other concerns about the proposed EDGAR filing process

FIF members also have more general concerns about the proposed EDGAR filing process and believe that extending this process to approximately 1,989 broker-dealers (as estimated by the Commission)[10] would be problematic. These concerns are discussed on Attachment I to this comment letter. While these concerns are very important for the Commission to consider, we have moved this discussion to an Attachment given the length of the comments about the EDGAR filing process and the number of sub-headings.

Transmission of copies of Part I of Form SCIR to a covered entity's examining authority

Proposed Rule 10 would require a covered entity that is a broker or dealer to "… promptly transmit a copy of each Part I of Form SCIR it files with the Commission to its examining authority …."[11] Presumably, each examining authority would need to update its rules and systems to accommodate this requirement, and the Commission would need to approve proposed rule amendments submitted by each examining authority. FIF members request that the Commission provide additional detail as to these required actions, including expected timing, and how these actions would impact the implementation of the proposed cybersecurity rule, including the implementation timeframe for Covered Entities. The Commission also should incorporate into the rule security requirements to be adopted by each examining authority with respect to the cybersecurity incident data that is reported by Covered Entities. The Commission should mandate that examining authorities implement security controls similar to the security controls implemented for CAT, as discussed above, or explain why such controls would not be appropriate.

Definition of cybersecurity incident

Under proposed cybersecurity Rule 10(a)(2), a "cybersecurity incident" is 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." The Commission proposes to impose certain obligations upon the occurrence of a cybersecurity incident, including a requirement for written documentation.[12] FIF members request for the Commission to clarify that an unsuccessful attempt to obtain unauthorized access to, or to interfere with the operations of, a covered entity's systems would not be considered a cybersecurity incident. If an attempt is unsuccessful, it means that the covered entity prevented the intended harm. The ratio of unsuccessful to successful cybersecurity attacks is high. Requiring written documentation of every unsuccessful attack would distract Covered Entities from focusing on the highest risk threats and incidents.

[10] Cybersecurity Proposing Release, at 132.
[11] Proposed Rule 10(c)(2)(iii)(A)
[12] Proposed Rule 10(b)(1)(v)(B).

It is likely that all Covered Entities, as well as the Commission itself, receive phishing attempts via email on a daily basis. To the extent that such phishing emails are either caught in an email security filtering system or do not launch a ransomware incident or the release of malware because the recipient did not click on a link or open an attachment in the email, that could be deemed to be an unsuccessful attempt to obtain unauthorized access to a covered entity's systems. The Commission should clarify that these types of attempts and others that are routinely blocked by Covered Entities' prevention and detection capabilities should not be reportable.

FIF members also recommend that the Commission modify the definition of cybersecurity incident to exclude the following:

- An incident impacting a single customer that would be reflective of the compromise of that customer's credentials (for example, an unauthorized party gains access to a customer's access codes and device as a result of the customer's negligence) as opposed to a compromise of the systems of the covered entity
- An incident that involves an employee at a covered entity mistakenly having access to data that is outside the scope of the employee's responsibility (as opposed to malicious activity by an employee, which could be considered a cybersecurity incident)
- Non-cyber threats to infrastructure, such as physical threats from extreme weather, accidental damage, and inadvertent disclosures by Covered Entities' personnel.

FIF members also recommend that the definition of cybersecurity incident be limited to U.S. incidents. More specifically, FIF members recommend that the definition of cybersecurity incident be limited to incidents that directly impact U.S. customers or disrupt the operation of infrastructure owned and operated by a U.S. company. Otherwise, multinational entities and the Commission could be burdened with regulatory requirements, including reporting of cybersecurity incidents, that do not directly impact U.S. economic and national security interests.

Definition of significant cybersecurity incident

Proposed cybersecurity Rule 10(a)(10) defines a "significant cybersecurity incident" to include a cybersecurity incident that leads to unauthorized access to or use of information or information systems,

> "… 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."

FIF members request that the Commission provide clarification as to what would represent substantial harm to a customer or other party.

FIF members also recommend that the Commission establish thresholds for a cybersecurity incident to qualify as a significant cybersecurity incident. This is important to avoid Covered Entities and the

Commission being overburdened with reporting events and to allow Covered Entities and the Commission to focus on the most material incidents. Thresholds could be based on financial impact, number of consumers impacted, or volume of data impacted. The following are examples of the types of thresholds that the Commission could consider as delineating the materiality or significance of an incident:

- Impacts the non-public personal information (NPI) of greater than 250,000 U.S. consumers
- 25% to 50% of an organization is unavailable due to destructive malware or Denial of Service (DDoS) based attacks greater than 24 hours
- The ability of an organization to operate in its primary function is impacted for greater than 12 hours
- The incident would cause significant U.S. economic harm or is a national security threat.

Penetration testing

A covered entity could commission a penetration test that results in the testing party obtaining unauthorized access to the covered entity's systems. FIF members request confirmation that this would not be considered to be either a cybersecurity incident or a significant cybersecurity incident under proposed cybersecurity Rule 10.

Continued operations

The proposed cybersecurity Rule 10 would require a covered entity to establish, maintain, and enforce written policies and procedures "… that are reasonably designed to ensure … [T]he continued operations of the covered entity."[13] The decision of whether to maintain operations should be a commercial decision by each entity, subject to providing appropriate disclosure to customers and counter-parties. In certain scenarios where a covered entity has been subject to a cybersecurity attack, the covered entity continuing certain activities could present risk to the covered entity and its customers and to other market participants. There are certain systems that are necessary for the proper functioning of the equity, option and other markets. It is reasonable to impose continuing operational requirements for these core market systems. However, this type of requirement is more appropriately addressed through a more targeted rule such as the Commission's current Regulation SCI.

Notification and update requirements

The proposed cybersecurity Rule 10 would require a covered entity to provide immediate "… electronic notice to the Commission of a significant cybersecurity incident upon having a reasonable basis to conclude that the significant cybersecurity incident has occurred or is occurring."[14] FIF members are concerned about the requirement for "immediate" notification. In particular, FIF members are concerned that the requirement for "immediate" notification would interfere with the need for a covered entity to maintain as its primary focus mitigating and resolving the cybersecurity incident.

[13] Proposed Rule 10(b)(1)(v)(A)(1).
[14] Proposed Rule 10(c)(1).

The proposed Rule 10 also would require the filing of Part I of the proposed Form SCIR within 48 hours.[15] The proposed Rule 10 would further require a covered entity to file an amendment under certain circumstances, including upon any "… information previously reported to the Commission in Part I of Form SCIR pertaining to a significant cybersecurity incident becoming materially inaccurate…."[16]

FIF members recommend that the Commission provide a longer time period for initial reporting of the detailed information required to be reported on Form SCIR as this would enhance the quality of the information reported for a cybersecurity incident. FIF members also are concerned about the burden of having to update Form SCIR filings on an ongoing basis as new material information becomes available and recommend limiting the requirement for the filing of an amendment to a scenario where new information becomes available to a covered entity that reflects a material change in the level of risk associated with the reported cybersecurity incident. The Commission also could potentially require periodic (for example, monthly) updates to reflect other material changes to a previously reported incident.

FIF members also are concerned that the notification requirements above would take effect upon a covered entity "having a reasonable basis to conclude" that a significant cybersecurity incident has occurred or is occurring.[17] FIF members are not clear as to the circumstances that would constitute "reasonable basis" as this concept is not defined in the proposed Rule 10. FIF members recommend, as an alternative, that the notification requirement take effect upon a covered entity concluding that a significant cybersecurity incident has occurred or is occurring.

Certification requirement

Given the expedited time periods for reporting on Form SCIR and the significant time that it can take to research and ascertain the details of a cybersecurity incident, FIF members disagree with the proposed certification requirement that the information and statements contained in the form are "current, true and complete."[18] This type of certification might be appropriate for other forms where a firm has sufficient time to carefully review the form prior to submission, and where the firm is reporting on matters that are known to the firm (for example, a firm describing the functionality of its ATS system on Form ATS-N). FIF members do not consider this type of certification to be appropriate for Form SCIR, where the filing timeframes would not provide a covered entity sufficient time to carefully review the form prior to submission and where the covered entity would be reporting on matters that, in many cases, would not be clearly known to the covered entity. As evidenced by the breach of the EDGAR system discussed above, it often can take time to investigate and ascertain the details of a cybersecurity incident, and a covered entity's understanding of a cybersecurity incident often evolves over time as additional information is uncovered. In many cases, a covered entity discovers that aspects of its prior understanding of a cybersecurity incident are proven to be mistaken as additional information becomes available.

[15] Proposed Rule 10(c)(2)(i).
[16] Proposed Rule 10(c)(2)(ii).
[17] Proposed Rule 10(c)(1) and 10(c)(2)(i).
[18] Cybersecurity Proposing Release, at 141.

Question 2 of Part I of Form SCIR

Question 2 of Part I of Form SCIR requires a covered entity to report "[T]he approximate date the significant cybersecurity incident was discovered."[19] The reference to the term "discovered" adds a new undefined term to Form SCIR. FIF members recommend that Question 2 of Part I be revised to mirror the definition of significant cybersecurity incident that is ultimately adopted by the Commission. This would provide consistency between Form SCIR and the associated Rule 10.

Public disclosure of significant cybersecurity incidents

The proposed cybersecurity Rule 10 would require a covered entity to provide, through a mandated public disclosure on Part II of the proposed Form SCIR, "… a summary description of each significant cybersecurity incident that has occurred during the current or previous calendar year."[20] This summary description must include, to the extent known, "… the person or persons affected."[21] FIF members strongly disagree with any requirement to publicly identify specific persons that have been impacted by a significant cybersecurity incident. Apart from the fact that this type of disclosure would be a violation of customer trust, this disclosure could violate federal and state privacy laws, the privacy laws of other countries and confidentiality agreements and obligations to which a covered entity is subject. Any affected persons should be notified directly by the covered entity and should not be identified in a public disclosure.

* * * * *

More generally, the proposed cybersecurity Rule 10 would require public disclosure of the following information, to the extent known, for any significant cybersecurity incident:

> (A) The person or persons affected; (B) The date the incident was discovered and whether it is ongoing; (C) Whether any data was stolen, altered, or accessed or used for any other unauthorized purpose; (D) The effect of the incident on the covered entity's operations; and (E) Whether the covered entity, or service provider, has remediated or is currently remediating the incident.[22]

FIF members are opposed to this public disclosure requirement for at least seven reasons. First, this disclosure, in many cases, could provide valuable information to malicious third-party actors that seek to obtain unauthorized access to, or interfere with the operations of, a covered entity's systems. Second, the requirement for public disclosure presents the risk that the failure of a covered entity to provide a public disclosure would signify to attackers that the covered entity is not aware of an attack. Third, the

[19] Cybersecurity Proposing Release, at 494.
[20] Proposed Rule 10(d)(1)(ii).
[21] Proposed Rule 10(d)(1)(ii)(A).
[22] Proposed Rule 10(d)(1)(ii).

fact that a large number of broker-dealers would be subject to this public disclosure requirement[23] would further increase the risk that at least some broker-dealers would inadvertently disclose information that would be of value to malicious third-party actors. Fourth, the fact that so many broker-dealers would be subject to the public reporting requirement would likely result in patterns of public disclosure reporting that would be of value to malicious third-party actors. Fifth, the structured nature of the proposed reporting could provide additional value to malicious third-party actors (see the discussion in the next following paragraphs). Sixth, all of the following cybersecurity regulations applicable to financial services industry registrants ***do not*** require public reporting of cybersecurity incidents: Federal Trade Commission, "Standards for Safeguarding Customer Information";[24] Office of the Comptroller of the Currency, Federal Reserve System, Federal Deposit Insurance Corporation, "Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers";[25] and New York State Department of Financial Services, "Cybersecurity Requirements for Financial Services Companies."[26] Seventh, the requirement for public disclosure is inconsistent with the confidentiality requirements for suspicious activity reports filed with the Financial Crimes Enforcement Network.[27]

* * * * *

In the cybersecurity proposing release, the Commission discusses the benefits of centralized and structured disclosure of cybersecurity incidents to the public:

> Centralized filing of structured public disclosures of cybersecurity risks and significant cybersecurity incidents during the current or previous calendar year in EDGAR by Covered Entities would enable customers, counterparties, members, registrants, and users, as well as financial analysts—and even the Covered Entities themselves— to more efficiently discern broad trends in cybersecurity risks and incidents, which would enable Covered Entities and other market participants to more efficiently determine if they need to modify, change, or upgrade their cybersecurity defense measures in light of those trends.[28]

While, as noted by the Commission, the structured nature of the publicly disclosed information could be of benefit to Covered Entities and other market participants, the structured nature of this information also could assist malicious third-party actors in discerning broad trends in cybersecurity risks and incidents that could enable these malicious actors to more efficiently determine if they need to modify, change or upgrade their cybersecurity attack measures in light of these trends. FIF members are concerned that the risks of public disclosure greatly outweigh the potential benefits.

[23] The Commission estimates in the Cybersecurity Proposing Release that approximately 1,989 firms would qualify as Covered Entities. Cybersecurity Proposing Release, at 132.
[24] 16 CFR Part 314.
[25] 12 CFR Parts 53, 25 and 304.
[26] 23 NYCRR Part 500.
[27] 31 CFR §1023.320(e).
[28] Cybersecurity Proposing Release, at 408.

* * * * *

For all of the reasons above, FIF members strongly oppose any requirement for public reporting, and the Commission also should be opposed to this. The Commission should consider potential alternatives that would not involve the risks of public disclosure. One potential alternative would be to expand data breach notification requirements to include legal entity customers.

* * * * *

The proposed rule would appear to require that significant cybersecurity incidents be publicly disclosed and updated on an ongoing basis in real-time.[29] This would impose an unreasonable burden on Covered Entities and their representatives.

* * * * *

If the Commission were to impose a public disclosure requirement, a covered entity that does not have any customers (for example, a proprietary trading firm) should not be subject to the public disclosure requirement.

Service providers

Under proposed cybersecurity Rule 10, a covered entity's policies and procedures must

> Require oversight of service providers that receive, maintain, or process the covered entity's information, or are otherwise permitted to access the covered entity's information systems and the information residing on those systems, pursuant to a written contract between the covered entity and the service provider, through which the service providers are required to implement and maintain appropriate measures, including the practices described in paragraphs (b)(1)(i) through (v) of this section, that are designed to protect the covered entity's information systems and information residing on those systems.[30]

Paragraphs (b)(1)(i) through (v) referenced in the passage above contain detailed prescriptive requirements.[31] FIF members are concerned that broker-dealers would have limited ability to negotiate contract changes with certain vendors, such as cloud providers. This is an increased concern given that the large number of broker-dealers that would qualify as Covered Entities would include many small and mid-size broker-dealers. FIF members believe that oversight of specific requirements in relation to service providers can be demonstrated through various means other than contract provisions (such as review of completed cybersecurity questionnaires, review of vendor documentation, and review of third-party certifications obtained by a service provider). FIF members also recommend that exceptions be provided with respect to service providers that are authorized under The Federal Risk and

[29] Proposed Rule 10(d)(1)(ii).
[30] Proposed Rule 10(b)(1)(iii)(B).
[31] Proposed Rule 10(b)(1).

Authorization Management Program (FedRAMP) program,[32] registered with the Commission and subject to the proposed cybersecurity Rule 10 or equivalent Commission cybersecurity requirements, or subject to the Interagency Guidelines Establishing Information Security Standards.[33]

B. Proposed amendments to Regulation SCI

Proposed transaction activity thresholds

As proposed by the Commission, Regulation SCI would apply to broker-dealers that satisfy a total assets threshold or one or more transaction activity thresholds.[34] There are four distinct transaction activity thresholds, which are applicable for NMS stocks, exchange-listed options contracts, Treasury securities, and agency securities, respectively.[35]

The transaction activity threshold for NMS stocks is based on the "… average daily dollar volume reported by or pursuant to effective transaction reporting plans…."[36] The transaction activity threshold for exchange-listed option contracts is based on "… the average daily dollar volume reported by an applicable effective national market system plan…."[37] The transaction activity threshold for Treasury securities (and for agency securities) is based on the "… total average daily dollar volume made available by the self-regulatory organizations to which such transactions are reported…."[38]

In each case, all data necessary to determine whether a broker-dealer has exceeded one or more of the applicable transaction activity thresholds for a particular month is available to the Commission. In place of approximately 1,989 broker-dealers having to perform these calculations independently,[39] it would be more efficient for the Commission (or FINRA) to perform these calculations each month and to make the results of these calculations available to each firm through a password-protected website or search tool. Since FINRA currently maintains password-protected data for every FINRA-registrant, it could be appropriate for FINRA to make this data available to broker-dealers.

Whether or not the Commission adopts this approach recommended by FIF members, it is important that the Commission provide clear guidance to broker-dealers as to how the numerator and denominator should be calculated by a broker-dealer (or for the broker-dealer, if the Commission will

---

[32] See https://www.fedramp.gov/.
[33] 66 FR 8616 (Feb. 1, 2001) (Interagency Guidelines Establishing Standards for Safeguarding Customer Information). 69 FR 77610 (Dec. 28, 2004) (Proper Disposal of Consumer Information Under the Fair and Accurate Credit Transactions Act of 2003).
[34] Proposed Rule 1000.
[35] Ibid.
[36] Ibid.
[37] Ibid.
[38] Ibid.
[39] The Commission estimates in the Cybersecurity Proposing Release that approximately 1,989 firms would qualify as Covered Entities. Cybersecurity Proposing Release, at 132. This corresponds generally with the number of broker-dealers that would need to compute whether they have crossed the proposed Regulation SCI transaction activity thresholds. FIF members have advised FIF that FINRA, in prior audits, has indicated that ATS operators with relatively low volume in particular asset classes are still expected to have procedures in place to document that they do not exceed the applicable ATS thresholds.

perform this calculation) when determining whether the broker-dealer has reached the applicable transaction activity threshold for a particular month. For the denominator for each activity threshold, the Commission should identify the specific source that broker-dealers should reference, including the author and title of the report, how the report can be publicly accessed and the specific column and row of the report that should be referenced. In each case, the source should be publicly available at no charge.

The following are specific questions from FIF members relating to these calculations. For each scenario below, FIF members request clarification on how the numerator and the denominator would be calculated. In providing guidance on the scenarios below, the Commission should explain how such guidance is consistent with the stated objective of Regulation SCI, which is to "… help ensure that the technology infrastructure of the U.S. securities markets remains robust, resilient, and secure."[40]

Which broker-dealers should include the executed volume in the numerator

- ***Exchange crosses NMS stock transaction between two broker-dealers.*** The proposed rule provides that for purposes of calculating activity in transactions in NMS stocks "… effected otherwise than on a national securities exchange or on an alternative trading system, the broker-dealer shall exclude transactions for which it was not the executing party."[41] Does this mean that if a broker-dealer receives a customer order and routes the order directly to an exchange for execution, the broker-dealer would include the executed dollar volume in the numerator? Does this also mean that, if the broker-dealer on each side receives and routes a customer order to an exchange for execution, both broker-dealers would include the executed volume in their numerators? Assume that two dealers execute a trade on an exchange, would this be single or double counted for the denominator? Could the total numerators for all broker-dealers exceed the aggregate industry denominator?
- ***ATS crosses NMS stock transaction between two broker-dealers.*** Assume that two broker-dealers execute a trade on an ATS. If the broker-dealer that operates the ATS is not one of the counter-parties to the trade, which of the three broker-dealers (the counter-party broker-dealers and the broker-dealer that operates the ATS) would need to include the executed dollar volume in the numerator for the single execution? Now assume that the broker-dealer that operates the ATS is one of the counter-parties to the trade. Would the broker-dealer that operates the ATS be required to count the trade twice in its numerator?
- ***ATS crosses NMS stock transaction between broker-dealer and institution.*** Assume that an ATS crosses an NMS stock transaction between a broker-dealer and an institution. If the broker-dealer that operates the ATS is not the counter-party to the trade, would the counter-party broker-dealer and the ATS operator both include the executed volume in the numerator? If the broker-dealer that operates the ATS is the counter-party to the trade, would the broker-dealer that operates the ATS be required to count the trade twice in its numerator?
- ***Customer-facing broker-dealer routes customer NMS stock order to a routing broker; routing broker routes order to exchange for execution.*** Assume that a broker-dealer receives a

[40] Regulation SCI Proposing Release, at 8.
[41] Proposed Rule 1000.

customer order and routes the order to a routing broker. The routing broker, in turn, routes the order to an exchange for execution. Is the routing broker required to include the executed volume in its numerator? Is the customer-facing broker required to include the executed volume in its numerator? It would not seem appropriate for the customer-facing broker to include the executed volume in the numerator because the customer-facing broker is not one of the executing parties. In addition, requiring the routing broker and the customer-facing broker on the same side of a trade to include the same shares in their numerators would appear to be double-counting. While this double-counting does not seem like the correct result, the Commission's statement quoted in the first bullet above would imply that where a trade is executed on an exchange or ATS, a broker-dealer would include the trade in the numerator even where the broker-dealer is not an executing party. The Commission should clarify this point. More generally, the Commission should explicitly identify any scenario where a broker-dealer is not an executing party and would be required to include the executed dollar volume in its numerator. The Commission also should clarify for each execution scenario which party (or parties) is (or are) the executing party (or parties) for purposes of Regulation SCI. The Commission also should clarify why it would be appropriate to apply Regulation SCI to a broker-dealer that is not an executing party.

- ***Broker-dealer routes customer NMS stock order to market maker or wholesaler.*** If a broker-dealer routes a customer order to a market maker or wholesaler, and the market maker or wholesaler executes as a counter-party to the order, it appears that the market maker or wholesaler would include the executed shares in its numerator. Would the routing broker-dealer also include the executed shares in its numerator?
- ***Options transactions.*** For transactions in options, should the exchange members that are direct parties to a trade include the executed dollar volume in the numerator? Are there any other parties that would be required to include executed dollar volume in the numerator?
- ***Dealer routes Treasury or agency order to executing dealer.*** If a dealer routes an order for a Treasury or agency security to another dealer, and the second dealer executes the order, do both dealers include the execution in the numerator or does only the executing dealer include the execution in the numerator?
- ***Negotiated trade in Treasury or agency security.*** If two dealers negotiate a trade in a Treasury or agency security, do both dealers include the execution in the numerator or does only one of the dealers include the execution in the numerator?
- ***Trade between two dealers in a Treasury or agency security crossed on a system operated by a third broker-dealer.*** If a system operated by a dealer crosses a trade between two other dealers in a Treasury or agency security, which of these dealers would need to include the execution in the numerator? Would this calculation be impacted if the Commission adopts its current rule proposal to require ATS registration by certain systems that cross trades in Treasury and agency securities,[42] and the crossing system is an ATS?
- ***Trades in Treasury and agency securities that involve a bank dealer.*** How are trades in Treasury and agency securities that involve a bank dealer on either or both sides of the trade counted?

[42] Securities Exchange Act Release No. 94062 (Jan. 26, 2022), 87 FR 15496 (Mar. 8, 2022) (Amendments to Exchange Act Rule 3b-16 Regarding the Definition of "Exchange"; Regulation ATS for ATSs That Trade U.S. Government Securities, NMS Stocks, and Other Securities; Regulation SCI for ATSs That Trade U.S. Treasury Securities and Agency Securities) ("SEC Rule 3b-16 Proposal").

- ***Riskless principal transactions.*** For transactions in NMS stocks and Treasury and agency securities, how should riskless principal transactions be counted?
- ***Step-outs and CMTAs.*** Which broker-dealer would need to include a trade in the numerator for a step-out transaction or an options transaction that includes a Clearing Member Trade Agreement (CMTA)?

How the principal value of an execution should be calculated

- Is the dollar volume for an options transaction based on the total premium paid (or received) or based on another value?
- Is the dollar volume for a Treasury or agency transaction based on the trade price (i.e., principal value of bonds traded times the price relative to par) or based on another value?
- Should mark-ups, mark-downs, commissions and fees (either paid or received) be excluded?
- If a transaction is executed in a calendar month (Month 1) and cancelled in the following month (Month 2), does the broker-dealer reduce its numerator in Month 2 by the cancelled amount?

FIF members note that the Commission's guidance with respect to the questions above could dramatically impact the economic analysis of the Regulation SCI rule proposal.

* * * * *

The Commission writes in the Regulation SCI proposing release that it "… is proposing to include under the SCI broker-dealer threshold all trades for U.S. Treasury Securities and Agency Securities in which a broker-dealer may participate."[43] FIF members request that the Commission provide further clarification as to the meaning of this sentence.

* * * * *

While FIF members request that the Commission provide guidance on the questions above, these questions demonstrate the complexity of these calculations. It would be far more efficient for one entity (i.e., the Commission or FINRA) to perform these calculations instead of approximately 1,989 broker-dealers having to perform these calculations separately.

ATSs that do not operate a central limit order book

ATSs that do not operate a central limit order book (for example, systems that provide RFQ functionality and voluntarily register as ATSs or systems that provide RFQ functionality and could, as a result of the adoption of current Commission regulatory proposals, become subject to Regulation ATS[44]) should not be subject to Regulation SCI. These types of systems do not present the same risk to the technology infrastructure of the U.S. securities markets as compared to trading systems that operate a central limit order book.

[43] Regulation SCI Proposing Release, at 65.
[44] SEC Rule 3b-16 Proposal.

Service providers

The Commission's proposed amendments to Regulation SCI include additional requirements for SCI entities with respect to service providers.[45] The comments of FIF members relating to service providers set forth above in the discussion of the Commission's cybersecurity rule proposal also apply for the Commission's proposed amendments to Regulation SCI.

Testing with service providers

The Commission proposes to expand the business continuity and disaster recovery testing requirements for SCI entities to include designated third-party providers.[46] FIF members are concerned about the burden that would be imposed on a third-party provider if the provider were required to test separately with each SCI entity. FIF members support the mandate in the current Rule 1004(c) for each SCI entity to coordinate the testing of its business continuity and disaster recovery "… plans on an industry- or sector-wide basis with other SCI entities."[47] FIF members encourage the Commission to take further steps in support of this mandate, including the promotion of uniform test scripts across SCI entities, where appropriate.

FIF members also recommend that the Commission make explicit in Rule 1004 that SCI testing is only required with respect to SCI systems. The Commission also should make explicit in Rule 1004 that if an SCI entity qualifies as an SCI entity based on reaching one or more, but not all, of the transaction activity thresholds, the SCI entity would only be subject to SCI testing with respect to the asset class or classes for which it has exceeded the applicable Reg SCI transaction activity threshold.

Significant unauthorized intrusion

The Commission proposes to amend the definition of "system intrusion" 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."[48] One impact of an attempted unauthorized entry being defined as a "system intrusion" is that an SCI entity would need to report the incident to the Commission.[49] A second impact is that the SCI entity, absent an applicable exception under Regulation SCI, would need to disseminate information about the event to its participants, members or customers, as applicable.[50] FIF members disagree with requiring notification and dissemination of information about unsuccessful attacks. As noted above in the discussion of the cybersecurity rule proposal, the ratio of unsuccessful to successful attacks (including, for example, denial of service attacks) is high. Requiring SCI entities to review and classify every unsuccessful attack as

[45] Ibid.
[46] Proposed Rule 1004.
[47] 17 CFR §242.1004(c).
[48] Proposed Rule 1000.
[49] 17 CFR §242.1002(b).
[50] 17 CFR §242.1002(c).

significant or not significant, and to provide notification of unsuccessful attacks, would distract SCI entities and the Commission from focusing on the highest risk threats and incidents.

Compliance period

As proposed by the Commission, a broker-dealer would become subject to the requirements of Regulation SCI six months after the end of the quarter in which the broker-dealer satisfies the total assets threshold for the first time or six months after the end of the month in which the broker-dealer satisfies one of the transaction activity thresholds for the first time.[51] FIF members believe that a six-month period is too short and recommend that a minimum period of two years be provided. As one example, a six-month compliance period would not be sufficient for implementing the proposed requirements with respect to third-party providers, including potential contract amendments.[52]

C. Proposed amendments to Regulation S-P

Compliance period

The Commission proposes a compliance period of twelve months for a covered institution to comply with the Commission's proposed amendments to Regulation S-P.[53] FIF members do not consider this to be a sufficient implementation period given the changes to service provider contracts that would be required in certain cases[54] and the need to conform the new Commission data breach notification requirements with state data breach notification requirements. FIF members recommend a minimum implementation period of two years.

Potential inconsistencies with state data breach notification laws

The Commission should amend the proposing release to discuss potential inconsistencies between the Commission's proposed amendments to Regulation S-P and state data breach notification laws, and potential approaches for addressing these conflicts. For example, various state data breach notification laws require that notifications be delayed if a law enforcement agency determines that the notifications will impede a criminal or civil investigation and the law enforcement agency has made a request that the notifications be delayed.[55] These state laws do not provide for a time limitation. In contrast, the Commission's proposed amendments to Regulation S-P would only permit a delay upon a request from the Attorney General of the United States, and the delay has a time limitation. For customers in these states, if a law enforcement agency has requested that a notification be delayed (and absent further regulatory clarification), an entity most likely would need to provide a Regulation S-P notification to those customers and then provide a subsequent state-mandated notice at a later date to the same

[51] Proposed Rule 1000.
[52] Proposed Rule 1001(a)(2)(ix).
[53] Regulation S-P Proposing Release, at 131.
[54] Proposed Rule 248.30(b)(5).
[55] See, for example: Fla. Stat. §501.171(4)(b); H.R.S. §487N-2(c); N.J. Stat. §56:8-163.c.(2); and N.C. Gen. Stat. §75-65(c).

customers for the same incident. It is not clear what is the best approach for addressing this type of situation, but it is important for the Commission to consider these types of scenarios.

* * * * *

FIF appreciates the opportunity to comment on these rules rule proposals from the Commission. If you would like clarification on any of the items discussed in this letter or would like to discuss further, please contact me at howard.meyerson@fif.com.

Very truly yours,

/s/ Howard Meyerson

Howard Meyerson
Managing Director, Financial Information Forum

Attachment I
Additional Concerns About the EDGAR Filing Process

Technical and operational challenges with the EDGAR filing system

As proposed by the Commission, a covered entity would have the option to submit the Form SCIR filing "… directly to the EDGAR system in the relevant custom XML data language, or to manually input the information into a fillable web-based form developed by the Commission that converts the completed form into a custom XML document."[56] Both approaches would be problematic. We start with a discussion of the option to use a fillable web-based form that would be provided by the Commission.

Challenges with using a fillable web-based EDGAR form

The EDGAR system is decades behind current technology. Alternative Trading System ("ATS") operators that are required to submit Form ATS-N through the EDGAR system for filing have experienced significant and ongoing challenges with EDGAR, including the EDGAR system rejecting filings that are in proper format, the EDGAR system not properly communicating to a filer why a filing is not in proper format, Level 1 support personnel not being available on a timely basis, Level 1 support personnel not being familiar with the Form ATS-N given the fact that they are required to provide support for many Commission filing forms, delays in responses from higher-level support when EDGAR system issues are escalated, instances where higher-level support are unable to replicate the rejections experienced by filers, and instances where higher-level support are able to replicate rejections but indicate that these are known issues with the EDGAR system.

The EDGAR ATS-N application does not allow filers to cut and paste entries into a Form ATS-N filing if the text includes any special characters, which include such common characters as a colon or semi-colon, an apostrophe, or a quotation mark. As a result of this system deficiency, filers must first either strip out all special characters in the text, paste the stripped text into EDGAR, and then re-add the special characters manually, or type the entire submission manually into EDGAR. In addition, Form ATS-N filers are required to attach several PDF documents to each of their Form ATS-N filings, including a PDF of the "redline" of a proposed amendment showing the additions and deletions, as well as PDFs of other documents including, but not limited to, schedules documenting the filer's ownership and its officers and directors. FIF members that file Form ATS-Ns have experienced PDF attachments that are rejected by EDGAR because, while they are indeed PDF documents, they are not in a specific PDF *type,* causing a validation error. In many cases, firm personnel are required to spend as much time working through technical issues with the EDGAR system as they do on the substantive aspects of a Form ATS-N filing. These technical issues often cause delays in filings.

Challenges with the alternative for Covered Entities to submit directly in XML

The alternative for Covered Entities to submit directly in XML format is also problematic. Many Covered Entities that seek to utilize this alternative would need to engage a vendor for their Form SCIR filings

[56] Cybersecurity Proposing Release, at 176.

and/or license third-party software. This vendor cost, which would most likely be significant (especially for smaller firms), is not included in the cybersecurity proposing release and should be included in any re-proposal. Engagement of a vendor also could involve disclosure of confidential information to the vendor relating to cybersecurity incidents to be reported to the Commission. The Commission also should consider how the additional time required for Covered Entities to apply XML formatting to their Form SCIR filings would impact the ability of Covered Entities to comply with the Form SCIR filing timeframes. It is also unclear whether the challenges described above with using an EDGAR web-based form would continue to apply for Covered Entities that submit directly in XML, or whether XML formatting would address some or all of these challenges. The Commission should provide clarification on this point. Presumably, the Commission would need to publish the details of this XML formatting before the implementation period for the proposed cybersecurity Rule 10 could commence.

Given the concerns above, the Commission should not add any new uses for EDGAR at this time

Given the technical and operational challenges described above, the Commission's proposal to expand EDGAR to approximately 1,989 Covered Entities[57] would be problematic. The proposal to use the EDGAR system for Form SCIR filings also appears to be inconsistent with the Commission's proposed expedited timeframes for Form SCIR filings. The Commission should not add any new uses for the EDGAR system until the application is enhanced to become easier for filers to use and until the usage and support issues highlighted above are resolved. One potential alternative the Commission could consider would be to require filing with the Commission via secure email (as currently used by the Commission to accept Form ATS-R filings from ATS operators), subject to implementation of appropriate security controls, as discussed above.

Limited time periods during which the EDGAR system is available

The Commission notes in the cybersecurity proposing release that "[T]he Commission accepts electronic submissions through the EDGAR system Monday through Friday, except federal holidays, from 6:00 a.m. to 10:00 p.m. Eastern Time."[58] If a firm, on a Friday at 9:30 p.m. Eastern Time, has a reasonable basis to conclude that a significant cybersecurity incident has occurred or is occurring, is the firm required to submit its Form SCIR within 30 minutes? Given the Commission's proposed requirements for expedited Form SCIR filings, it would be appropriate for the Commission to provide a reporting system that is available on a 24 x 7 x 365 basis.

Date and time of filing

The Commission indicates in the cybersecurity proposing release that

> … filings submitted by direct transmission commencing on or before 5:30 p.m. Eastern Standard Time or Eastern Daylight Saving Time, whichever is currently in effect, shall be deemed filed on the same business day, and all filings submitted by direct transmission

[57] Cybersecurity Proposing Rule, at 132.
[58] Id. at 156.

> commencing after 5:30 p.m. Eastern Standard Time or Eastern Daylight Saving Time, whichever is currently in effect, shall be deemed filed as of the next business day.[59]

Given that filing is required within 48 hours, a Form SCIR filing should be deemed filed as of the date and time of filing and not as of the following business day. The Commission also should make available a documented process for a firm to communicate to the Commission that the firm was prepared to submit its Form SCIR to the Commission within the required time period but was prevented from doing so because of technical issues with the Commission's reporting system.

[59] Ibid.