The SEC Expands Focus on Cybersecurity Risk to Include Registered Advisers, Broker-Dealers, and other Market Participants

14 Apr 2023

Investigations + White Collar Defense Securities Enforcement and **Securities Litigation**

Client Alert

Last month, the SEC took a big step toward strengthening the cybersecurity of financial systems by proposing regulations that, taken together, will require registered investments advisers, broker-dealers, and all national securities exchanges, among others, to implement additional measures to protect their systems.**[1]** Since these are proposed rules, there is time for affected companies to comment on them and prepare for their requirements.

Executive Summary

To date, investment advisers, broker-dealers, national securities exchanges, and other major participants in the securities markets have not been subject to specific cybersecurity regulations. Rather, attention to cybersecurity has been addressed in connection with general regulatory compliance obligations.**[2]** Recently, the SEC proposed several regulations that will impose upon these market participants a more specific obligation to take action to protect their clients and customers from cybersecurity risks.

Background

On March 15, 2023, the SEC released two rule proposals related to cybersecurity risk management. These proposals introduce heightened compliance obligations for various participants in the securities market. One proposal ("Exchange Act Cybersecurity Proposal") contemplates a new rule ("Proposed Rule 10") under the Securities Exchange Act of 1934 (the "Exchange Act") that would impose new cybersecurity risk management obligations on specific entities, including broker-dealers, who support the industry's operations.**[3]** A second proposal ("Regulation SCI Proposal") seeks to amend and expand Regulation Systems Compliance and Integrity ("Regulation SCI") under the Exchange Act to account for evolving risks to critical systems and infrastructure.**[4]**

In light of these regulatory developments, the SEC also reopened the public comment period for an earlier cybersecurity proposal from February 2022. This proposal (the "Investment Management Cybersecurity Proposal") contains proposed cybersecurity risk management rules (covered in greater detail in our **client alert**), for registered investment advisers ("RIAs") and investment companies under the Investment Advisers Act of 1940 and the Investment Company Act of 1940 (the "Investment Company Act"), respectively. The SEC is also soliciting feedback on the potential interplay between each of these three proposals (collectively, the "Proposals").**[5]**

Exchange Act Cybersecurity Proposal

The Exchange Act Cybersecurity Proposal introduces Proposed Rule 10 addressing cybersecurity risk management for entities who access or maintain information systems in order to support transactions or operations in the securities market.

- **Scope: Market Entities - Covered Entities vs. Non-Covered Entities.** Proposed Rule 10 would apply to all "Market Entities" consisting of broker-dealers, clearing agencies, major security-based swap participants, the Municipal Securities Rulemaking Board, national securities associations, and national securities exchanges. Proposed Rule 10

Contacts

Kelley Howes
khowes@mofo.com
(212) 336-4064
(303) 592-2237
(303) 592-1510
Kristen J. Mathews
kmathews@mofo.com
(212) 468-7900
(212) 336-4038
Haimavathi V. Marlier
hmarlier@mofo.com
(212) 468-7900
(212) 336-4409
Derek Steingarten
dsteingarten@mofo.com
(212) 336-4434
(212) 468-7900
Libby Strichartz
estrichartz@mofo.com
(415) 268-7522
(415) 268-7000

specifies a subset of Market Entities known as "Covered Entities" consisting of registered brokers or dealers that (a) maintain custody of cash and securities for customers or other broker-dealers; (b) introduce customer accounts to other brokers or dealers that maintain cash and securities; (c) have regulatory capital equal to or exceeding $50 million; (d) have total assets equal to or exceeding $1 billion; (e) are market makers under the Exchange Act, its rules, or the rules of a self-regulatory organization (SRO) of which the broker or dealer is a member; or (f) operate as an alternative trading system (ATS) or operate an NMS Stock ATS. Covered Entities would be subject to specific, additional requirements under Proposed Rule 10.

- **Written Cybersecurity Policies and Procedures.** Proposed Rule 10 would require all Market Entities to establish, maintain, and enforce policies and procedures "reasonably designed to address cybersecurity risks to their information systems." Covered Entities must specifically address the following topics in such policies and procedures: periodic cybersecurity risk assessments, controls to address user-risks to information systems, oversight of service providers with access to information systems, and measures to detect, mitigate, and remediate cyber threats and incidents.

- **Annual Review and Required Written Reports.** All Market Entities must annually review their policies and procedures to ensure they adequately address changes to their cybersecurity risks. While Non-Covered Entities need only prepare a "record" of this assessment, Covered Entities must prepare a more extensive "report" of the assessment.

- **Reporting of Significant Cybersecurity Incident.**

  - **Reportable incidents**: Proposed Rule 10 would require all Market Entities to report "significant cybersecurity incidents" to the SEC. A "significant cybersecurity incident" would include a cybersecurity incident, or a group of related cybersecurity incidents, that significantly disrupts or degrades a Market Entity's ability to maintain critical operations. Under Proposed Rule 10, a "cybersecurity incident" would include any "unauthorized incident" that jeopardizes the confidentiality, integrity, or availability of an information system or the information residing on it.

  - **Timing**: Whereas all Market Entities would need to provide the SEC with "immediate written notice" of a significant cybersecurity incident, Covered Entities would also need to confidentially file detailed information with the SEC within 48 hours, using Part I of new Form SCIR, and to continually update the SEC of any material developments.

- **Cyber-specific Disclosures.** Proposed Rule 10 would require Covered Entities specifically (*not* all Market Entities), to publicly disclose "summary descriptions" of their cybersecurity risks and significant cybersecurity incidents from the prior calendar year by filing Part II of the new Form SCIR publicly, and by posting a copy to their websites. Certain Covered Entities would need to provide the recently filed version of the form to certain customers as well.

- **Cybersecurity-Related Recordkeeping.** Proposed Rule 10 would require both Covered and Non-Covered Entities to address their Proposed Rule 10 compliance efforts as part of their current recordkeeping obligations.

Back to Top

Regulation SCI Proposal

Regulation SCI focuses on technology-related risks to critical systems and infrastructure in the securities market. Regulation SCI currently applies to major market players like national securities exchanges (e.g., NASDAQ or NYSE), SROs (e.g., FINRA), ATSs, and certain registered or exempt clearing agencies (collectively, "SCI entities"). The Regulation SCI Proposal targets cybersecurity risk management more directly and aggressively by introducing new requirements and expanding the scope of the regulation itself.

- **Expanded Scope.** The Regulation SCI Proposal would expand the definition of SCI entities to include security-based swap data repositories ("SBSDRs"), registered broker-dealers above a size threshold, and certain exempt clearing agencies.

- **Written Policies and Procedures and Amended Safe Harbor.** The Regulation SCI Proposal would require SCI entities to establish policies and procedures "reasonably

designed to ensure" adequate capacity, integrity, resiliency, availability, and security of SCI systems. The Regulation SCI Proposal also identifies specific topics that must be addressed, including a written inventory of an SCI entity's systems and their designated classifications, an SCI entity's life cycle management, and an SCI entity's third-party oversight measures. Additionally, SCI entities must document programs protecting against unauthorized access to SCI systems in their policies and procedures.

- **Safe Harbor for "SCI Industry Standards."** The Regulation SCI Proposal provides a safe harbor against liability for failing to comply with the specifications for written policies and procedures, so long as the SCI entity utilizes consistent, current SCI standards as policies and procedures.

- **Enhanced Incident Reporting.**

  - **Reportable incidents**: The definition for reportable incidents ("SCI events") under Regulation SCI is currently limited to instances of unauthorized "entry" into an SCI system. The Regulation SCI Proposal would broaden this definition to include incidents that "significantly disrupt or degrade" an SCI system, or incidents involving "significant *attempted* unauthorized entry," even if they do not lead to an actual unauthorized "entry" into the system.

  - **Timeline**: SCI entities would be required to notify the SEC immediately, and to provide the SEC with specific information contained on Form SCI within 24 hours, and provide a final detailed report to the SEC. SCI entities must also promptly notify any impacted members or participants once there is a reasonable basis to conclude an SCI event has occurred.

- **Amended Annual Review and Written Reports Requirements.** The Regulation SCI Proposal would obligate SCI entities to have "objective personnel" annually review their SCI systems according to the specific process set forth in the proposal. SCI entities would also need to perform subsequent penetration testing to test vulnerabilities identified during the initial annual review. The frequency with which SCI entities must conduct penetration testing would increase from the currently required three-year cadence to annually. SCI Entities would need to report to the SEC any identified "systems changes," or planned material changes, to their SCI systems on a quarterly basis.

- **Disaster Recovery and Business Continuity Testing.** SCI entities must maintain disaster recovery and business continuity standards that address the unavailability of third-party providers whose services have a material impact on critical SCI systems.

- **Cybersecurity-specific Disclosures.** SCI entities must notify their members or participants estimated to have been affected by an SCI event. For "major" SCI events, SCI entities must notify all members and participants. Since there could be overlap between required disclosures under the Regulation SCI Proposal and the Exchange Act Cybersecurity Proposal, the SEC notes that these disclosures, in some instances, may be effectuated through the Form SCIR.

- **Recordkeeping.** The Regulation SCI Proposal updates SCI entities' recordkeeping obligations to incorporate recordkeeping of the updated requirements. Additionally, entities who no longer qualify as SCI entities because they do not meet the volume thresholds would still be required to comply with recordkeeping requirements.

Back to top

Investment Management Cybersecurity Proposal

The Investment Management Cybersecurity Proposal introduces cybersecurity risk management rules for RIAs and registered investment companies and closed-end companies that have elected to be treated as business development companies ("BDCs" and, together with registered funds, "funds") under the Investment Company Act.

- **Scope: Covered Entities vs. Non-Covered Entities.** The Investment Management Cybersecurity Proposal identifies a new category of "Market Entities" who provide financial support services and thus have access and/or maintain information systems containing financial information and/or proprietary information about financial assets and transactions.

- **Written Policies and Procedures.** The Investment Management Cybersecurity Proposal would require RIAs and funds to adopt and implement policies and procedures that are reasonably designed to address cybersecurity risks. These policies and procedures would be required to include: (1) a risk assessment based on an inventory of information systems; (2) controls designed to minimize user-related risks by implementing standards for user security and access; (3) a periodic assessment of information systems to ensure information protection; (4) procedures for threat and vulnerability management, including mitigation, remediation, and training; and (5) cybersecurity incident response and recovery measures. An RIA or fund would be able to either administer its cybersecurity policies and procedures using in-house resources with appropriate knowledge and expertise, or utilize a third-party cybersecurity risk management service, subject to appropriate oversight.

- **Significant Cybersecurity Incident Reporting.** The Investment Management Cybersecurity Proposal would require RIAs to report significant cybersecurity incidents to the SEC, including on behalf of clients that are registered funds, BDCs, or private funds. Advisers would be required to submit proposed Form ADV-C "promptly" after having a reasonable basis to determine that a significant cybersecurity incident (as defined by the proposed rules) has occurred, but in any event to file within 48 hours of such determination.

- **Cybersecurity-Related Disclosures.** The Investment Management Cybersecurity Proposal would amend Form ADV Part 2A to require RIAs to disclose cybersecurity risks and incidents to their clients, investors, and other market participants.

- **Cybersecurity-Related Recordkeeping.** The Investment Management Cybersecurity Proposal contains new recordkeeping requirements, requiring advisers and funds to maintain certain records for five years including: (1) cybersecurity policies and procedures; (2) annual reviews thereof; (3) documents related to the annual reviews; (4) regulatory filings related to cybersecurity incidents required under the proposed amendments; (5) any cybersecurity incident; and (6) cybersecurity risk assessments.

Back to Top

Key Takeaways

The SEC is doubling down on the need for documented, internal risk management measures focusing specifically on risks to cybersecurity and system availability. The SEC is also enhancing its own regulatory authority and oversight capabilities on each of these topics through a series of time-sensitive incident reporting requirements, as well as broader compliance and risk reporting requirements.

---

[1] On the same day, the SEC also proposed a rule addressing Regulation S-P (the "Reg S-P Proposal"), which primarily addresses privacy, rather than cybersecurity, concerns. The Reg S-P proposal would obligate covered entities to develop, implement, and maintain written incident response policies and procedures, which could implicate an organization's cybersecurity posture.

[2] See, e.g., Rule 206(4)-7 under the Investment Advisers Act.

[3] See Securities Exchange Release No. 97142 (Mar. 15, 2023) (File No. S7-06-23) (proposing 17 CFR 242.10).

[4] See Securities Exchange Release No. 97143 (Mar. 15, 2023) (File No. S7-07-23) (proposing amendments to 17 CFR 242.1000 – 17 CFR 242.1005).

[5] The SEC has also proposed cybersecurity disclosure rules for public companies, as discussed in greater detail in our earlier **Client Alert**.