KPMG

Regulatory Alert

Regulatory Insights for Financial Services

March 2023

SEC Proposals on Cyber Risk Management for Market Entities, Investment Advisers and Funds

***KPMG Regulatory Insights**:*

- *In addition to the Cyber Risk Management proposal for Market Entities, the SEC reopened (on the same day) its February 2022 proposal on Cyber Risk Management for Investment Advisers and Funds.*
- *Key areas of focus for these rules, as well as the proposals released concurrently addressing Regulations S-P and SCI, include: i) written policies and procedures, ii) cyber risk assessments, iii) incident notification and disclosure, and iv) expanded coverage among market participants.*

As part of a comprehensive effort to enhance cybersecurity preparedness and resilience across all registrants of the Securities and Exchange Commission (SEC), the SEC has:

- Proposed Cybersecurity Risk Management Rule for "Market Entities"
- Reopened the February 2022 proposal on Cybersecurity Risk Management for Investment Advisers and Funds for comment (see KPMG's Regulatory Alert, here.)

The actions are outlined below.

Proposed Cybersecurity Risk Management for Market Entities

Applicability. The SEC's proposed rule for cybersecurity risk management would apply to the following types of registrants (collectively, "Market Entities"):

- Broker-dealers
- Clearing agencies
- Major security-based swap participants
- The Municipal Securities Rulemaking Board (MSRB)
- National securities associations
- National securities exchanges
- Security-based swap data repositories (SBSDRs)
- Security-based swap dealers
- Transfer agents

All Market Entities would be required to:

- **Adopt Policies and Procedures.** Proposed new Rule 10 would require Market Entities to establish, maintain, enforce, and annually review and assess written policies and procedures "reasonably" designed to address cybersecurity risks, including changes in cybersecurity risk over time. Further, they would be required to report on the annual review.
- **Report Cybersecurity Incidents.** Proposed new Rule 10 would also require all Market Entities to provide immediate written electronic notice to the SEC of a "significant cybersecurity incident" upon having a reasonable basis to conclude that the significant cybersecurity incident had occurred or is occurring.
  - A "significant cybersecurity incident" would be defined as a cyber incident, or group of related incidents, that:
    - Significantly disrupts or degrades the ability of the Market Entity to maintain critical operations, or
    - Leads to the unauthorized access or use of the information or systems of the Market Entity, where the unauthorized access or use results in or is reasonably likely to result in:

KPMG

© 2023 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

- Substantial harm to the Market Entity, or
- 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.

"Covered Entities"

Market Entities would be divided into two categories: "Covered Entities" and "Non-Covered Entities". "Covered Entities" would be defined to include the MSRB and all clearing agencies, national securities associates, national securities exchanges, SBSDRs, Security-Based Swap Entities, and transfer agents. "Covered Entities" would also include broker-dealers that fall under six categories: i) carrying broker-dealers; ii) introducing broker-dealers; iii) have regulatory capital of $50 million or more; iv) have total assets of $1 billion or more; v) operate as market makers; and vi) operate an ATS (Alternative Trading System).

Covered Entities would be subject to certain additional requirements as follows.

Policies and procedures. Covered Entities would be required to adopt policies and procedures that specifically include:

— **Risk assessments:** Periodic assessments of cybersecurity risks associated with the Covered Entity's information systems and written documentation of the risk assessments.

— **User security and access:** Controls designed to minimize user-related risks and prevent unauthorized access to the Covered Entity's information systems.

— **Information protection:** Measures designed to monitor the Covered Entity's information systems and protect the Covered Entity's information from unauthorized access or use, and oversee service providers that receive, maintain, or process information or are otherwise permitted to access the Covered Entity's information systems.

— **Threat and vulnerability management:** Measures to detect, mitigate, and remediate any cybersecurity threats and vulnerabilities with respect to the Covered Entity's information systems.

— **Cybersecurity incident response and recovery:** Measures to detect, respond to, and recover from a cybersecurity incident and procedures to create written documentation of any cybersecurity incident and the response to and recovery from the incident.

Cybersecurity Incident Reporting. Covered Entities, upon providing written notice of a significant cybersecurity incident, would also be required to confidentially file Part I of proposed new Form SCIR (covering information about the incident and response and recovery efforts) with the SEC within 48 hours. Likewise, Covered Entities would be required to file amendments to Part I of Form SCIR within 48 hours under four circumstances:

— If any information previously reported pertaining to the significant cybersecurity incident becomes materially inaccurate.

— If any new material information pertaining to the significant cybersecurity incident previously reported is discovered.

— After the significant cybersecurity incident is resolved.

— If an internal investigation pertaining to the significant cybersecurity incident is closed.

Cybersecurity Risk and Incident Disclosures. Covered Entities would be required to file Part II of proposed Form SCIR with the SEC and to post it on its website, publicly disclosing two types of information relating to cybersecurity:

— Summary descriptions of cybersecurity risks that could materially affect the business and operations, as well as processes for assessment, prioritization, and management of those risks.
  - "Materiality" of cybersecurity risks would be based on whether there is a substantial likelihood that a reasonable person would consider the information important based on the total mix of facts and information (e.g., disrupt or degrade the ability to maintain critical operations, adversely affect confidentiality, integrity, or availability of (personal, confidential, or proprietary) information residing on information systems, and/or harm a covered entity, customers, counterparties, members, registrants, users, or other persons).
  - Significant cybersecurity incidents experienced during the current or previous calendar year.

Covered Entities that are carrying or introducing broker-dealers would also need to provide Part II of Form SCIR's disclosures to customers at account opening, when the form is updated, and annually.

The SEC notes that both Part I and II of Form SCIR must be filed in EDGAR using structured data language.

Record Retention and Reporting. Proposed new Rule 10 would require Covered Entities to "make several different types of records" (collectively, "Rule 10 Records"), based on the different requirements of the rule, including:

— Policies and procedures to address cybersecurity risks.

— Written documentation of risk assessments.

— Written documentation of any cybersecurity incident, including response and recovery efforts.

— Annual written reports on reviews of policies and procedures to address cybersecurity risks.

© 2023 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

— Electronic written notices to the SEC of significant cybersecurity incidents.
— Reports to the SEC of significant cybersecurity incidents.
— Written summary disclosures of cybersecurity risks, assessment, prioritization, and management.

The proposal does not include explicit retention requirements for Rule 10 Records, but rather states that preservation and maintenance requirements would be imposed through proposed amendments, as necessary, to existing record requirements applicable to the Covered Entities. For example, the SEC would propose to:

— Amend Rules 17a-4, 17ad-7, and 18a-6 to include Rule 10 Records under the existing maintenance requirements for broker-dealers, transfer agents, and security-based swap entities, as well as a three (3) year retention period for the records.
— Retain, without change, existing Rules 17a-1 and 13n-7, for clearing agencies, the MSRB, national securities associations and exchanges, and SBSDRs, which would currently require the maintenance and preservation of Rule 10 Records as well as a retention period of at least five (5) years.

Proposed Cyber Risk Management for Investment Advisers and Funds – Reopened Comment Period

Concurrent to the release of its proposal for Market Entities, the SEC also reopened the comment period on its previously proposed rules and amendments for cybersecurity risk management and disclosure for registered investment advisers and funds.

The SEC states the reopened comment period is intended to allow interested parties additional time to analyze the issues and prepare comments in light of other regulatory developments, including whether there would be any effects of other SEC proposals related to cybersecurity risk management and disclosure that should be considered.

Comment Period

For each of these proposals, the comment period will remain open for a period of 60 days following publication in the Federal Register.

For more information, please contact Matt Miller, Steve Stein, or Mike Sullivan.

Contact the author:

Amy Matsuo
Principal and National Leader
Regulatory Insights
amatsuo@kpmg.com

kpmg.com/socialmedia

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

All information provided here is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the facts of the particular situation.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

© 2023 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.