
SEC Proposes Expanded Cybersecurity Disclosure Requirements for Broker-Dealers and Other Market Participants

On March 15, 2023, the Securities and Exchange Commission (“SEC”) proposed new requirements for market participants such as broker-dealers, swaps dealers, clearing agencies, national securities associations, transfer agents and others to address their cybersecurity risks.¹ The proposal follows the release of 2011 and 2018 interpretive guidance on the topic,² which the SEC had issued to assist public companies when considering, drafting, and issuing disclosures regarding cybersecurity risks and incidents. The SEC also previously issued a March 2022 proposed rule regarding certain cybersecurity disclosure requirements for public companies.³

The most recent proposal includes a new Rule 10 under the Securities Exchange Act of 1934 (“Rule 10” or the “proposed rule”) requiring that entities to which the rule applies establish, maintain, and enforce written policies and procedures reasonably designed to address their cybersecurity risks and periodically review the efficacy of those policies and procedures. Under the proposal, all entities subject to the rule must provide notice to, and update the SEC regarding significant cybersecurity incidents using a new Form SCIR. In addition, covered entities (as defined) would have to file Part II of new Form SCIR on the SEC’s Electronic Data Gathering, Analysis, and Retrieval system (“EDGAR”) and post it on a publicly available website.

Proposed Rule

Compared to other cybersecurity regulations, the SEC’s newly proposed cybersecurity risk management rule is fairly specific in establishing which entities are covered and what disclosure is required.⁴

Market Entities

The proposed rule would apply to the following registrants (collectively “Market Entities”):

¹ 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, Release No. 34-97142 (March 15, 2023). The comment period will be open for 60 days following publication of the proposed rule in the *Federal Register*.

² See CF Disclosure Guidance: Topic No. 2- Cybersecurity (Oct. 13, 2011) and Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Release No. 33-10459 (Feb. 26, 2018).

³ See Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Release Nos. 33-11038; 34-94382 (March 9, 2022).

⁴ See Cybersecurity Risk Management Rule, Release No. 34-97142 (March 15, 2023).

- 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; and
- Transfer agents.

Under Rule 10 as proposed, all Market Entities would be required to:

1. **Adopt Cybersecurity Policies and Procedures.** All Market Entities would be required to “establish, maintain, and enforce written policies and procedures that are reasonably designed to address their cybersecurity risks.” In addition, all Market Entities would be required to review and assess the design and efficacy of their policies and procedures at least annually to address changes in cybersecurity risks over time, and to keep records of each such review.
2. **Report Cybersecurity Incidents.** All Market Entities would be required to provide to the SEC “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.” The proposed rule defines a “significant cybersecurity incident” as one that (1) significantly disrupts or degrades the Market Entity’s ability to maintain its critical operations, or (2) results in unauthorized access to the Market Entity’s information systems and involves a reasonable likelihood of substantial harm to the Market Entity or any other party that interacts with the Market Entity.

Covered Entities

The proposed rule also seeks to impose more stringent requirements on a subgroup of Market Entities, “Covered Entities,” which are defined as the same entities that meet the definition of “Market Entity” (listed above) other than a narrow category of broker-dealers. Broker-dealers are included as Covered Entities if they fit any one of the following categories:

- Those that maintain custody of securities and cash for customers or other broker-dealers (“carrying broker-dealers”);
- Those that introduce their customer accounts to a carrying broker-dealer on a fully disclosed basis (“introducing broker-dealers”);
- Those with regulatory capital equal to or exceeding \$50 million;
- Those with total assets equal to or exceeding \$1 billion;
- Those that operate as market makers; and
- Those that operate an ATS.


Under the proposed new Rule 10, these “Covered Entities” would be required to meet the requirements for Market Entities (described above) and also the below:

1. *Adopt Cybersecurity Policies and Procedures (Additional Requirements)*. Covered Entities would need to implement written policies and procedures that address cybersecurity risks, as would all Market Entities, but Covered Entities would also need to implement policies and procedures that *specifically* address user security, information protection, vulnerability and threat detection, mitigation and remediation, as well as post-incident response and recovery operations. Additionally, Covered Entities would be required to review and assess these heightened policies and procedures annually, ensuring that they appropriately reflect changes in cybersecurity risk, and prepare a report of their review.
2. *Report Cybersecurity Incidents in Multiple Ways*. For example, Covered Entities would have to provide “immediate” written electronic notice of a significant cybersecurity incident to the SEC upon having a “reasonable basis” for concluding such an event has occurred, as would all Market Entities, but Covered Entities would also have to confidentially file Part I of proposed new Form SCIR “promptly, but no later than 48 hours,” after having such a basis to reach such a conclusion. Such filing would have to include detailed information about the incident and the entity’s response to and recovery from the incident. Note that this filing would also have to be updated, also within 48 hours, upon the discovery of new material information, upon resolution of the incident, or if the Covered Entity conducts an internal investigation of the incident.
3. *Publicly Disclose a Summary of their Cybersecurity Risks and the Significant Cybersecurity Incidents Experienced*. Covered Entities would be required to publicly file Part II of proposed Form SCIR with the SEC, as well as make “easily accessible” disclosures on their website. The disclosure would have to include a summary of cybersecurity risks that might materially affect the business and operations, as well as processes for assessment, prioritization and management of those risks. The proposed rule defines “materiality” in this context to mean that there is a substantial likelihood that a reasonable person would consider the information important based on the circumstances. The disclosure must also list any significant cybersecurity incidents experienced during the current or previous calendar year. The SEC acknowledged that revealing “too much information could assist future attackers as well as lead to loss of customers, reputational harm...” and therefore makes clear that Rule 10 would only require a “summary description” and “high-level disclosures” of an entity’s cybersecurity risks and incidents. Covered Entities that are considered carrying or introducing broker-dealers, as defined above, would need to also provide Part II of Form SCIR’s disclosures to customers at account opening, when the form is updated and on an annual basis.
4. *Keep Cybersecurity-Related Records*. Covered Entities would need to preserve certain records, such as policies and procedures to address cybersecurity risks, written documentation of any cybersecurity incident and the response to and recovery from the incident and electronic written notices to the SEC on significant cybersecurity incidents.

Conclusion

The proposed rule, advancing on a 3-2 vote of the SEC commissioners, has been criticized by at least one commissioner as following a “spaghetti on the wall” approach with “overlapping and potentially inconsistent regulatory regimes [that] can create confusion and conflicts, and could even weaken cybersecurity protections.”⁵

⁵ See SEC Commissioner Mark T. Uyeda’s “Statement on the Proposed Cybersecurity Risk Management Rule for Market Entities” (March 15, 2023).



Although it remains uncertain whether and in what form the SEC’s proposed cybersecurity risk management requirements for market participants will be adopted, a considerable amount of public comment is expected. It is also clear that cybersecurity disclosures will be heavily scrutinized in the event of a significant data breach or similar incident, and organizations that run afoul of the agency’s cybersecurity requirements may face harsh enforcement fines. For example, on March 9, 2023, the SEC announced a \$3 million fine against software company Blackbaud, Inc. for misleading disclosures concerning a 2020 ransomware attack that impacted 13,000 of the company’s customers. The proposed rules speak directly to that kind of incident and the disclosures concerning them in regard to market participants but also reflect the SEC’s expanding concern and focus on cybersecurity risks and its determined effort to provide additional requirements to protect investors. Market participants, as well as public companies, should take notice.

* * *

If you have any questions about the issues addressed in this memorandum, or if you would like a copy of any of the materials mentioned in it, please do not hesitate to call or email authors David Owen (Partner) at 212.701.3955 or dowen@cahill.com; Alexa Moses (Associate) at 212.701.3865 or amoses@cahill.com; or Ken Ritz (Associate) at 212.701.3661 or kritz@cahill.com; or email publications@cahill.com.

This memorandum is for general information purposes only and is not intended to advertise our services, solicit clients or represent our legal advice.