The Investment Lawyer
Covering Legal and Regulatory Issues of Asset Management
VOL. 30, NO. 8 • AUGUST 2023

The SEC Proposes New Cybersecurity and Privacy Requirements

By Adam Aderton, Daniel K. Alvarez, Elizabeth P. Gray, Laura E. Jehl, A. Kristina Littman, Alexis Hassell, Kari Prochaska, Amelia Putnam, and Marc Lederer

In its March 15, 2023 Open Meeting, the US Securities and Exchange Commission (Commission or SEC) reopened the comment period for proposed cybersecurity risk management rules for registered investment advisers, and also approved three proposals to expand the Commission's privacy and data security requirements. One proposed rule would impose new requirements on a broad group of regulated entities, including broker-dealers, and the other two proposals would amend existing rules—Regulation S-P and Regulation SCI. The scope of these proposals is significant on three key vectors: (1) the companies to which the proposals would apply, (2) the types of information that would be subject to the rules, and (3) the new substantive requirements that would be imposed. If these proposals are ultimately adopted, covered companies will be subject to a number of new and potentially costly cybersecurity and privacy compliance obligations. If adopted, insufficient implementation of these requirements could also subject registrants to examination deficiency notifications and enforcement actions.

New Cybersecurity Risk Rules Proposed for Broker-Dealers, Others

By a 3-2 vote, the Commission proposed a set of new cybersecurity risk management rules[1] that would apply to Market Entities (for example, broker-dealers, broker-dealers that operate an alternative trading system (ATS), 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 (SBSDs), and transfer agents) and Covered Entities (a sub-set of Market Entities), which include certain broker-dealers,[2] the MSRB, and all clearing agencies, national securities associations, national securities exchanges, SBSDRs, SBS Entities, and transfer agents. The proposed rule attempts to address cybersecurity risks through (1) written policies and procedures; (2) immediate, detailed notification to the Commission of the occurrence of a significant cybersecurity incident; and (3) public disclosures intended to improve transparency with respect to cybersecurity risks and significant cybersecurity incidents.

Specifically, the proposal includes:

- *Written Cybersecurity Policies and Procedures.* The proposed cybersecurity risk rules would require all Market Entities to (i) establish, maintain, and enforce written policies and procedures that are reasonably designed to address their cybersecurity risks, and (ii) review

and assess the design and effectiveness of their cybersecurity policies and procedures—at least annually—including whether the policies and procedures reflect changes in cybersecurity risk over the time period covered by the review.[3] Covered Entities would be subject to *additional* requirements regarding the elements that must be included in their cybersecurity risk management policies and procedures, reporting, and public disclosures.[4] The Commission noted that the policies and procedures should be tailored to the nature and scope of that Covered Entity's particular business and designed with the flexibility to allow Covered Entities to update and modify their policies and procedures as needed to address cybersecurity risks over time.[5] A Covered Entity would also be required to review the design and effectiveness of the policies and procedures annually, prepare a written report that explains its assessment, discuss material changes, and document any cybersecurity incident that has occurred since the date of the last report.[6]

- *Notification of a Significant Cybersecurity Event*. Under the proposed cybersecurity risk rules, Covered Entities would be required to give the Commission immediate written electronic notice[7] of a significant cybersecurity incident upon having a "reasonable basis to conclude that the significant cybersecurity incident has occurred or is occurring."[8] The Covered Entity would also be required to report to the Commission—on a confidential basis (to the extent permitted by law) and promptly, but no later than 48 hours—by filing Form SCIR, Part 1 through the EDGAR system. The Commission would create a new Form SCIR, Part I for such a filing,[9] and the Covered Entity would be required to file amended Forms SCIR, Part I if any information previously reported to the Commission becomes materially inaccurate, if new material information pertaining to the significant cybersecurity incident is discovered, and after the significant cybersecurity event is resolved.[10]
- *Cybersecurity Disclosures*. Covered Entities would be required to provide summary descriptions of their cybersecurity risks and significant cybersecurity incidents they experienced during the current or previous calendar year via a new Form SCIR, Part II.[11] They would be required to publicly file the Form SCIR, Part II and post a copy of it on their business websites.[12] In addition, certain broker-dealer Covered Entities would be required to provide Form SCIR, Part II to customers during account onboarding, when information on the form is updated, and annually.[13]
- *Recordkeeping*. As with most recent SEC rule proposals, this proposal includes a recordkeeping obligation requiring all Market Entities to preserve prescribed records.

Summary of Key Comments

The comment period for the proposed cybersecurity risk rules closed on June 5, 2023. Commenters focused on, among other things, that: (1) the proposed cybersecurity policies and procedures requirements do not provide for adequate flexibility; (2) the proposed reporting of cybersecurity events should include a longer time period for notification in order to lessen operational impact; (3) certain proposed definitions (including, but not limited to, "cybersecurity incident" and "cybersecurity risk") are overly broad; and (4) requiring public disclosures of cybersecurity events may increase risk to Covered Entities due to the additional exposure during a state of vulnerability.

Commenters also provided recommendations with respect to the proposed rules, including: (1) calling for cybersecurity policies and procedures to be less prescriptive and more principles-based; (2) having defined terms be narrowed for reasonableness and materiality; (3) stating that the Commission should harmonize the proposed cybersecurity risk

rules with other notification requirement regimes, such as the longer 72-hour incident reporting requirement under the Cyber Incident Reporting for Critical Infrastructure Act; and (4) asking that the Commission address separate and duplicative requirements across other proposed rules and reporting structures.

Proposed Amendments to Regulation S-P, Regulation SCI Focus on Breach Preparation, Response, and Security

Regulation S-P

In addition to the new cybersecurity risk management rules for Market Entities, the Commission unanimously approved a proposal to amend *Privacy of Consumer Financial Information and Safeguarding Personal Information* (Regulation S-P), which currently requires "covered institutions" (brokers, dealers, investment companies, and registered investment advisers) to provide a "clear and conspicuous" privacy notice to certain consumers and customers, as well as adopt written policies and procedures to protect customer information and to dispose of information properly.[14] The proposal seeks to increase these obligations by requiring:

- *Written Incident Response Plans*. The proposed amendments would modify the Safeguards Rule[15] to require covered institutions to implement and maintain written incident response plans that are reasonably designed to detect, respond to, recover from, and prevent unauthorized access to and use of customer information, including procedures requiring notification to affected customers in the event of a security incident involving sensitive customer information, as discussed more fully below. The proposed amendments also would require covered institutions to execute contracts with service providers that require them to reasonably protect customer information and to notify the covered institution within 48 hours of a breach of such customer information; covered institutions must also address the risk of harm posed by service providers within their incident response programs.
- *New Notification Requirements*. Covered institutions would be required to notify customers (and customers of other financial institutions) whose sensitive customer information—defined as "any component of customer information alone or in conjunction with any other information, the compromise of which could create a reasonably likely risk of substantial harm or inconvenience to an individual identified with the information"[16]—has been or is reasonably likely to be, accessed or used by an unauthorized third party. However, notification would not be required where sensitive customer information has not been and is not likely to be used in a manner that would result in substantial harm to the customer. Notification would be required as soon as practicable, but no later than 30 days after discovery of the security incident. Unlike comparable state data breach notification laws, the proposed amendments generally do not permit a delay in notification even when requested by a law enforcement agency.[17]
- *"Customer Information" Subject to Safeguards Rule and Disposal Rule*. The proposed amendments would amend the Safeguards Rule and Disposal Rule[18] to broaden and align the types of personal information subject to the rules. The current rules apply to "customer records and information" or "consumer report information." The amendments would create a new category, "customer information," to mean any record containing nonpublic personal information of a customer of a financial institution, whether in paper, electronic or another form, maintained by or on behalf of the covered institution. As such, this would mean that the Safeguards Rule and Disposal Rule would now apply to both nonpublic personal information that a covered institution collects

about its own customers and to nonpublic personal information it receives from a third-party financial institution about that institution's customers.

- *Application of Regulation S-P to Transfer Agents*. Transfer agents are not currently subject to Regulation S-P, but the proposed amendments would include transfer agents registered with the SEC or with another "appropriate regulatory agency"[19] within the scope of "covered institutions" under Regulation S-P.
- *Recordkeeping*. The proposal's recordkeeping requirement would obligate covered institutions to make and maintain written records documenting their compliance with the rule.
- *Privacy Notices*. The proposal would also provide an exception to the delivery of annual privacy notices for covered institutions if they meet two conditions. First, covered institutions may only share nonpublic personal information with nonaffiliated third parties in accordance with the exceptions in the Gramm–Leach–Bliley Act (GLBA) that do not require opt-out consent to be provided. Second, a covered institution cannot have changed its policies and practices with regard to disclosing nonpublic personal information since the last time its privacy notice was delivered. This proposed exception is designed to be consistent with and comparable to that of the Commodity Futures Trading Commission, Consumer Financial Protection Bureau, and Federal Trade Commission.

Summary of Key Comments

The comment period for the proposed changes to Regulation S-P closed on June 5, 2023. Industry commenters focused on the need for the SEC to harmonize its proposals with existing federal and state cybersecurity and privacy frameworks to avoid a complicated patchwork of potentially conflicting regulations. Commenters also expressed concerns about the potential inability to delay notification to customers when in the midst of a law enforcement investigation.

Accordingly, they suggested the following changes to the proposal: (1) requiring notification only where the covered institution affirmatively finds a risk of harm to the affected individual, in order to avoid excessive notification when there is no or low likelihood of harm; (2) clearly defining the specific data elements that would constitute "sensitive customer information" that could trigger notification obligations; (3) eliminating the requirement to notify the customers of other financial institutions; and (4) increasing the amount of time that covered institutions would have to notify affected individuals, so as to provide more time to investigate and remediate the incident. There were also other commenters that argued that the Commission should actually strengthen the proposed amendments to Regulation S-P by, for example, requiring covered institutions to notify impacted individuals within 14 days after becoming aware of a cybersecurity incident, regardless of the risk of harm or inconvenience to the individual.

Regulation SCI

Finally, by a 3-2 vote, the Commission approved proposed amendments to *Regulation Systems Compliance and Integrity* (Regulation SCI).[20] Regulation SCI currently applies to certain entities (SCI entities) with respect to their automated and similar systems (SCI systems) that directly support any one of six key securities market functions—trading, clearance and settlement, order routing, market data, market regulation, or market surveillance—as well as systems (indirect SCI systems) that, if breached, would be reasonably likely to pose a security threat to SCI systems. These systems include those outsourced to third parties. The proposed amendments include, among other things:

- *Expanded Scope of SCI Entities*. SCI entities currently include, among others, self-regulatory organizations, such as national securities

exchanges, registered clearing agencies, registered securities associations, and the Municipal Securities Rulemaking Board, alternative trading systems meeting volume thresholds with respect to National Market System (NMS) stocks and non-NMS stocks, and certain exempt clearing agencies. The proposed amendments would expand that scope to include registered security-based swap data repositories; broker-dealers registered with the Commission under Section 15(b) that exceed a total assets threshold or a transaction activity threshold in NMS stocks, exchange-listed options, US Treasury securities or Agency securities; and *all* clearing agencies, including those exempted from registration.

- *SCI Entities' Oversight of Third-Party Providers*. The proposed amendments would require SCI Entities to adopt a program to manage and oversee third-party providers, including cloud service providers, that provide or support SCI or indirect SCI systems. This would include business continuity/disaster recovery plans that address the unavailability of any third-party provider without which there would be a material impact on critical SCI systems and a requirement that SCI entities include key third-party providers in annual business continuity/disaster recovery testing.
- *New Security Program, Notice, and Testing Requirements*. The proposed amendments would impose numerous additional prescriptive obligations on entities subject to Regulation SCI. Among other things, the amendments would require SCI entities to establish a program to prevent unauthorized access to SCI systems and information therein, amend the definition of "systems intrusion" to include additional types of cyber events and threats (for example, distributed denial-of-service attacks), require notification of systems intrusions to the Commission without delay, and update the SCI review requirement to specify that objective personnel assess the risks to covered systems, internal control design and operating effectiveness, and third-party provider management risks and controls, and require penetration testing at least annually (rather than every three years as under the current rule).

Summary of Key Comments

The comment period for the proposed changes to Regulation SCI closed on June 13, 2023. Among other things, industry commenters noted that: (1) it would become overly burdensome to expand the definition of a systems intrusion event; (2) expanding Regulation SCI to broker-dealers with trading volume at or above a 10 percent threshold would arbitrarily increase the regulatory burdens of larger, diversified broker-dealers; (3) the Commission underestimates the costs of expanding Regulation SCI to broker-dealers; and (4) the scope of third-party providers required to be monitored by SCI entities is ambiguous, overly broad, and overly burdensome. Commenters provided several recommendations to the proposal. Some of those recommendations proposed that: (1) the Commission to allow for an extended implementation period if the SEC's final modifications include any new requirements that will necessitate modified contractual terms with third-party providers; (2) Regulation SCI requirements be less prescriptive and more principles-based; (3) certain defined terms be narrowed and clarified; and (4) the Commission harmonize the proposed rules with other rule regimes, such as the CFTC rules.

Implications of the Proposed Rules

The proposed rules evince a clear desire for the SEC to play a role in major privacy and data security issues, but they present a number of issues that were raised in the public comment period. As highlighted by commenters, the Commission will need to grapple with challenging issues, including:

- While many existing rules in the financial and other sectors establish requirements based on a risk assessment, the proposed rules skip the risk assessment and impose highly prescriptive cybersecurity and privacy measures. This one-size-fits-all approach runs counter to years of existing policy precedent on cybersecurity and data security. Commissioner Peirce objected to the proposed Regulation SCI amendments as "micromanagement."[21] She feared it would "pad future enforcement actions with additional charges while undermining the integrity of the systems it aims to protect."[22]
- The new notification obligations may overlap—and potentially conflict, especially with respect to law enforcement delays of notification—with notification obligations under state law or other SEC rules or proposed rules, and may impede an entity's ability to devote essential time and resources to mitigating a significant cybersecurity incident. Commissioner Uyeda also emphasized that onerous notification obligations may cause entities to err on the side of over-notification, leading to notification fatigue for customers. Commissioners Lizarraga and Crenshaw expressed their views that these proposed amendments allow for consistent notification obligations throughout the country to the benefit of customers.
- The proposed amendments would expand Regulation SCI's scope to include new entities, such as registered security-based swap data repositories that are already subject to separate regulatory regimes that have many of the same requirements as Regulation SCI. This may cause unnecessary costs for entities already subject to overlapping regulatory frameworks.[23]
- The proposed amendments to Regulation SCI overlap with other rules. The proposed amendments coexist with many similar—but not identical—obligations in other SEC rules, including Regulation S-P, Regulation S-ID and the cybersecurity risk management rule proposals. The proposed amendments note that compliance with one set of rules would "largely" constitute compliance with another, but the SEC typically does not find it persuasive when a respondent to an enforcement action indicates that is has "largely" complied with rules, and the complex overlaps presented by the various rules may make it difficult for SCI entities to determine how the rules fit together.[24]
- The proposed amendments to Regulation SCI could lead to decreased service provider quality. The proposed amendments may be expected to make it more difficult for SCI entities to find high-quality third-party service providers to assist in performing critical functions, such as cloud computing services. In this regard, if third-party service providers face increased legal liability by, for example, not appropriately managing the relationship according to Regulation SCI, third-party service providers may be less likely to provide services to SCI entities. Ultimately, this could lead to fewer and/or lower quality third-party service providers available to SCI entities.[25]

Mr. Aderton is a partner, **Mr. Alvarez** and **Ms. Jehl** are partners and Co-Chairs of the Privacy, Cybersecurity & Data Strategy Practice Group, **Ms. Gray** is a partner and Co-Chair of the Securities Enforcement Practice Group, **Ms. Littman** is a partner and Co-Chair of the Willkie Digital Works Practice Group, and **Ms. Hassell** and **Ms. Putnam** are associates in the Washington, DC office of Willkie Farr & Gallagher LLP. **Ms. Prochaska** is an associate in the firm's Chicago office, and **Mr. Lederer** is a staff attorney in the firm's New York office.

NOTES

1 *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, U.S. Securities and Exchange Commission (Mar. 15, 2023), *https://www.sec.gov/rules/proposed/2023/34-97142.pdf*. The Commission proposes to add the following new rule and form under the Securities Exchange Act of 1934: (1) 17 CFR 242.10 (Rule 10) and (2) 17 CFR 249.642 (Form SCIR). The Commission also is proposing amendments to the following rules: (1) 17 CFR 232.101; (2) 17 CFR 240.3a71-6; (3) 17 CFR 240.17a-4; (4) 17 CFR 240.17Ad-7; (5) 17 CFR 240.18a-6; and (6) 17 CFR 240.18a-10.

2 Covered Entities includes broker-dealers that are: (1) carrying broker-dealers; (2) introducing broker-dealers; (3) broker-dealers with regulatory capital equal to or exceeding $50 million; (4) broker-dealers with total assets equal to or exceeding $1 billion; and (5) broker-dealers that operate an ATS.

3 *Id.* at 55–56.

4 *Id.* at 76. The additional requirements include, among other things, periodic assessments of cybersecurity risks associated with the Covered Entity's information systems and written documentation of the risk assessments, controls designed to minimize user-related risks and prevent unauthorized access to the Covered Entity's information systems, and measures designed (i) to monitor the Covered Entity's information systems, (ii) to detect, mitigate, and remediate any cybersecurity threats and vulnerabilities with respect to the Covered Entity's information systems, and (iii) to detect, respond to, and recover from a cybersecurity incident and written documentation of any cybersecurity incident and response to and recovery from the incident. *Id.* at 56–57 (setting forth the requirements for Covered Entities).

5 *Id*. at 103.

6 *Id.* at 515.

7 *Id.* at 140. A Covered Entity would provide notification and state that the notice is being given to alert the Commission of a significant cybersecurity incident and provide the name and contact information of an employee of the Covered Entity who can provide further details about the nature and scope of the significant cybersecurity incident.

8 Paragraph (e)(2) of proposed Rule 10 also requires that a broker or dealer that is not a "covered entity" must give the Commission immediate written electronic notice of a significant cybersecurity incidents upon having a reasonable basis to conclude that the significant cybersecurity incident has occurred or is occurring. *Id*. at 519.

9 *Id.* at 140,143.

10 *Id.* at 144.

11 *Id*. at 57.

12 *Id.* at 490–491.

13 *Id.*

14 *Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information*, Release Nos. 34-97141; IA-6262; IC-34854, U.S. Securities and Exchange Commission (Mar. 15, 2023), *https://www.sec.gov/rules/proposed/2023/34-97141.pdf*.

15 17 CFR § 248.30(a).

16 SSNs and certain biometric records would be considered sensitive customer information along with certain combinations of identifying information and authenticating information.

17 The proposed amendments permit a 15-day delay of notification (which can be extended an additional 15-days) where there is a written request from the Attorney General of the United States to delay notification that would pose a substantial risk to national security.

18 17 CFR § 248.30(b).

19 This term is defined in Section 3(a)(34)(B) of the Securities Exchange Act of 1934.

20 *Regulation Systems Compliance and Integrity*, Securities and Exchange Commission, Release Nos. 33-11167; 34-97144; IA-6263; IC-34855, U.S. Securities and Exchange Commission (Mar. 15, 2023), *https://www.sec.gov/rules/proposed/2023/34-97143.pdf*.

21 *See* Commissioner Hester M. Peirce, *Comments on Proposed Expansion of Regulation SCI*, U.S. Securities

and Exchange Commission (Mar. 15, 2023), *https://www.sec.gov/news/statement/peirce-statement-regulation-sci-031523*.

22 *Id.*

23 *See* Commissioner Mark T. Uyeda, *Statement on the Proposed Amendments to Regulation Systems Compliance and Integrity*, U.S. Securities and Exchange Commission (Mar. 15, 2023), *https://www.sec.gov/news/statement/uyeda-statement-regulation-sci-031523*.

24 *See* Commissioner Hester M. Peirce, *Comments on Proposed Expansion of Regulation SCI*, U.S. Securities and Exchange Commission (Mar. 15, 2023), *https://www.sec.gov/news/statement/peirce-statement-regulation-sci-031523*.

25 *Id.*