Davis Polk

SEC proposes sweeping new package of cybersecurity requirements for regulated market participants

March 21, 2023 | Client Update | 13-minute read

The SEC proposed a broad suite of new cybersecurity rules for many market participants, including policies and procedures to address cybersecurity risk, written incident response programs, public disclosure, new types of SEC filings, and extension of Regulation SCI to large broker-dealers and other types of firms. If adopted, the new requirements would impose significant new costs and enforcement risk for much of the securities industry.

The SEC proposed an array of new cybersecurity-related requirements in the form of: (1) an expansive new Rule 10, (2) extending the reach of Regulation SCI, and (3) expanding Regulation S-P, including to require incident response programs. The SEC also reopened the comment period for new cybersecurity rules for investment advisers and investment companies.

New requirements for market entities

On March 15, the SEC proposed a new Rule 10 under the Securities Exchange Act of 1934 (Exchange Act), which would impose new cybersecurity requirements on "Market Entities." That group includes many types of 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. Some of the requirements apply to a subset of Market Entities referred to as "Covered Entities." The proposal, which takes up more than 500 pages, defines "Covered Entities" and has four core requirements:

- **"Covered Entity."** Covered entities include:
  - Registered brokers or dealers that (a) maintain custody of cash and securities for customers or other broker-dealers; (b) introduce customer accounts to another broker or dealer that maintains 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 an 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;
  - Clearing agencies;
  - Registered major security-based swap participants;
  - The Municipal Securities Rulemaking Board;
  - FINRA;
  - National securities exchanges;

- Security-based swap data repositories;
- Registered security-based swap dealers; and
- Transfer agents that are registered or required to be registered.

— **Cybersecurity policies**: All Market Entities would be required to establish, maintain, and enforce written policies and procedures reasonably designed to address their cybersecurity risks. They also would be required to review and assess them annually, including whether they reflect changes in cybersecurity risk. Covered Entities would be required to prepare a report of the review, with other Market Entities preparing "a record" of it.

- Covered Entities would need to address the following elements in their policies and procedures: (i) periodic risk assessments; (ii) controls to minimize user-related risks and prevent unauthorized access to information systems; (iii) monitoring of information systems and oversee service providers whose work involves the entity's information systems; (iv) measures to detect, mitigate and remediate threats and vulnerabilities; and (v) measures to detect, respond to, and recover from a cybersecurity incident, including written documentation of the incident, response and recovery.

— **Notification and reporting**: Covered Entities would need to provide "immediate" written notice to the SEC of a significant cybersecurity incident. The requirement would be triggered by a "reasonable basis to conclude" that a significant cybersecurity incident has occurred or is occurring. Covered Entities also would be required to file Part I of proposed Form SCIR to report to the SEC detailed information about the significant cybersecurity incident and the entity's response to and recovery from the incident. This filing would be made on a confidential basis—the SEC would not make the filings public to the extent permitted by law—and must be made "promptly" but no later than within 48 hours upon having a reasonable basis to conclude that a significant cybersecurity incident has occurred or is occurring. The filing would also have to be updated, such as if new material information is discovered, upon resolution of the incident, or if the Covered Entity conducts an internal investigation of the incident.

- A "significant cybersecurity incident" would be defined as an incident that (1) significantly disrupts or degrades the ability of the entity to maintain critical operations; or (2) leads to unauthorized access or use of information where the access results in or is likely to result in substantial harm to the entity, a customer, a counterparty, a member, a registrant, a user of the market entity, or any other person that interacts with the market entity.

— **Public disclosure**: Covered Entities would be required to make two types of public disclosures through Part II of proposed Form SCIR, which would be posted on an "easily accessible" portion of the firm's website (for example, it could not be behind a paywall). The first requirement would be a plain English summary of the cybersecurity risks that could materially affect the entity's business and operations, and how the entity assesses, prioritizes, and addresses those risks. The second requirement would be a summary of each significant cybersecurity incident that occurred during the current or previous calendar year. This summary must include (i) the person or persons affected; (ii) the date the incident was discovered and whether it is ongoing; (iii) whether any data was stolen, altered, accessed or used for any unauthorized purpose; (iv) the effect of the incident on the entity's operations; and (v) whether the incident has been remediated or is currently being remediated.

- The SEC acknowledged that disclosing too much information could *increase* risk by assisting future attackers, and therefore said that it would require "only a summary description" and "high-level disclosures" of the risks and incidents.
- Covered Entities that are introducing broker-dealers and "carrying" broker-dealers—broker-dealers that maintain custody of securities and cash for customer or other broker-dealers—would need to provide the form to customers on account opening, when the form is updated, and annually.

— **Recordkeeping**: All Market Entities would need to preserve certain records, with the specific requirements depending on the type of Market Entity.

Regulation SCI amendments

The SEC proposed amendments to Regulation Systems Compliance and Integrity (Reg SCI). Reg SCI currently imposes a number of requirements concerning system operations and compliance, including: having comprehensive policies and procedures reasonably designed to ensure that certain systems maintain operational capability and promote the maintenance of fair and orderly markets; having policies and procedures reasonably designed to insure certain systems operate in a manner that is compliant with the Exchange Act and the entity's own rules and governing documents; taking corrective action in response to system issues; providing notice to the Commission; and conducting annual compliance reviews.

The proposed amendments would expand the scope of SCI entities covered by the rule. Currently, SCI entities are self-regulatory organizations (SROs), certain large ATSs, plan processors, certain clearing agencies, and SCI competing consolidators (if and when they come into existence). Under the proposed amendments, the reach of the rule would be extended to:

- Registered broker-dealers that exceed certain asset or activity thresholds;
- Registered security-based swap data repositories; and
- Clearing agencies exempted from registration.

This change would bring the largest broker-dealers, along with swap data repositories and certain exempt clearing agencies under the umbrella of Reg SCI.

The amendments would also add new requirements, including:

- Maintenance of a written inventory of systems and classification of those systems;
- A program to manage and oversee third-party providers that provide functionality, support or service, directly or indirectly, for SCI systems;
- Expansion of business continuity/disaster recovery plans to address the unavailability of any third-party provider that provides functionality, support, or service to the SCI entity without which there would be a material impact on any critical SCI system;
- Expansion of required policies and procedures to include a program to prevent unauthorized access of SCI systems;
- Increased frequency of penetration testing from every three years to annually;
- An expanded definition of "systems intrusion" to include any event that disrupts, or significantly degrades, the normal operation of an SCI system, such as distributed denial-of-service (DDoS) attacks, and *attempted*, *unsuccessful* but significant unauthorized system entries;
- A requirement to notify the Commission of systems intrusion without delay;
- A requirement that objective personnel assess the risks to covered systems, internal control design and operating effectiveness, and third-party provider management risks and controls;
- Revisions to the requirements for SCI reviews and reports, such as to detail what an SCI review would be required to include;
- Clarifying that following current industry standards operates as a safe harbor by adding the words "safe harbor" to the rule;
- Listing minimum requirements that an SCI entity's Rule 1001(a) policies and procedures must include;
- Dissemination information about an event to an SCI entity's customers;
- Updated recordkeeping provisions and Form SCI consistent with the amendments; and

  Recordkeeping requirements for entities that cease to qualify as an SCI entity.

In a statement, Commissioner Hester Peirce objected to the proposed amendments as overly prescriptive. She argued that the updates to Reg SCI would create "micromanagement" of the covered entities' operations, many of which already have market, reputation, and regulatory incentives to adequately maintain their systems in order to perform key market functions. Commissioner Peirce noted that the Reg SCI amendments overlap significantly—but not entirely—with the Commission's proposed Regulation S-P and Cybersecurity Risk Management Rule without rationalizing whether, and where, deltas exist between these rules.

Regulation S-P amendments

Regulation S-P, adopted in 2000 and known as the "Safeguards Rule," requires brokers, dealers, investment companies, and registered investment advisers (the "covered institutions") to adopt written policies and procedures for safeguards to protect customer records and information. The regulation also requires proper disposal of information, both by covered institutions as well as transfer agents registered with the SEC. The SEC's proposal would expand the rule by adding a requirement for an incident response program and also a requirement to notify affected individuals in the event of a data breach. Specifically, the proposal includes:

- **Incident response program:** Covered institutions would be required to adopt written policies and procedures for an incident response program that is reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information. The program would be required to assess the nature and scope of any incident and take appropriate steps to contain and control the incident. Any instance of unauthorized access to or use of customer information would trigger the incident response protocol. The SEC said that the proposed rules would be flexible by not prescribing specific steps to be taken because institutions would need to tailor their programs to the individual facts and circumstances.
- **Customer notification:** Institutions would be required to notify individuals, as soon as practicable but at least within 30 days, if their sensitive customer information was, or reasonably likely to have been, accessed or used. However, notice would *not* be required if, after a reasonable investigation, the institution determined that sensitive customer information had not been, and was not reasonably likely to be, used in a manner that would result in substantial harm or inconvenience. Such an investigation would have to provide a sufficient basis for the determination that notice is not required, the firm should maintain a record of the investigation and its determination, and the SEC identified scenarios that do not require notice as "limited circumstances."
  - The proposal defines "sensitive customer information" 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." Explaining the focus on "substantial harm or inconvenience," the SEC noted the risk that a large volume of notices could erode their efficacy. The SEC defined the phrase as meaning "personal injury, or financial loss, expenditure of effort or loss of time that is more than trivial," saying that trivial effects are those that would not likely be of concern to the individual or that would prompt further action. In responding to requests for comment, firms might wish to highlight the seeming definition of "substantial" as "more than trivial."
  - If notice also is required under state law, which often will be the case, the SEC rule would require a single notice that would include all information required by the SEC rule and state law.
- **Scope of information:** Current rules on the safeguarding and proper disposal of customer information would be expanded to apply to all "customer information," a newly defined term that would include any record containing nonpublic personal information in any form about a customer of a financial institution. The amendment extends to both nonpublic personal information that a covered institution collects about its own customers and that it receives about customers of other financial institutions.
- **Transfer agents:** The proposal would extend its incident response and safeguarding and disposal rules to any

transfer agent registered with the Commission or another appropriate regulatory agency.

- **Recordkeeping**: Covered institutions would be required to make and maintain written records documenting their compliance with the safeguards and disposal rules.

Cybersecurity risk management for registered investment advisers and funds

The SEC also reopened the comment period for proposed rules that would impose significant new cybersecurity requirements for registered investment advisers and investment companies (summarized in our prior client update). The proposed rules, written to cover all registered funds, would require policies and procedures, annual reviews, reporting to the SEC, disclosures to investors, and recordkeeping. The reopened comment period allows firms to evaluate the proposed rule for registered investment advisers and investment companies in connection with the new proposed requirements for Market Entities and amendments to Regulation SCI and Regulation S-P.

Takeaways

These sweeping new requirements would greatly increase the SEC's management of regulated entities' approach to cybersecurity and system integrity. Current SEC regulation is targeted at certain risks, such as protecting customer information under Regulation S-P or preventing identity theft under Regulation S-ID. It also is focused on select market participants of significant market importance, such as the entities currently covered by Regulation SCI. The proposed rules would put the SEC in the business of dictating the elements of comprehensive cybersecurity programs across a wide swath of market participants including, for the first time, SEC-mandated incident response requirements. Although the SEC said that the proposed Rule 10 is not meant to be a one-size-fits-all approach, it contains multiple parts and sub-parts of detailed requirements, defines many new terms and concepts to be learned and followed, and imposes standardized notice and disclosure through new forms that must be filed with the SEC.

Commissioner Peirce expressed concerns about the Commission's proposed approach in her statement opposing the proposed new Rule 10, including these comments:

> Unfortunately, with this proposal, the Commission has apparently decided its role is to be an enforcer demanding that a firm dealing with a cybersecurity attack first and repeatedly attend to the Commission's voracious hunger for data. The Commission stands ready, not with assistance but with a cudgel to wield if the firm fails to comply with a complicated reporting regime, even if the firm resolves the incident by avoiding significant harm to the firm or its customers… .
>
> When we engage with a regulated entity that has suffered a cyberattack, we deal with a victim. We typically deal with a victim who has made great effort to protect its systems and its customers' data and is devoting significant resources to mitigate the harm from such an attack. Our priority should be to provide what support and information we can to assist the firm in this effort and, following resolution, to gather information that will help other firms in the future. Instead, this proposal demonstrates that our priority is to create even more legal peril for a firm in this situation, legal peril that will distract employees of the firm from mitigating the immediate threat to the firm and its customers as they navigate the aggressive deadlines and open-ended information demands of the Commission.

On their face, the proposals would seem to impose substantial new costs across the industry, especially considering the nearly 1,200 total pages of new guidance and explanation. The SEC concluded otherwise, estimating, for example, that the average internal costs per Covered Entity for the new policy and procedure and annual review requirements of Rule

10 would be only $14,531.54 per Covered Entity and $29.1 million in total (in addition to external costs of $3,472 per Covered Entity and $6.9 million in total external costs). The SEC estimated that a compliance attorney and assistant general counsel would require a total of 31.67 hours—four working days—to comply with the rules. It is difficult to square these estimates with the expansive new requirements; one wonders whether a firm could even read the three proposals and respond to the SEC's many requests for comment in that amount of time. The accuracy of the cost estimate may provide a basis to challenge the rules if they are adopted.

The proposal also would create new hindsight enforcement risk. The SEC frequently brings enforcement cases involving policy and procedure requirements, such policies and procedures to prevent the misuse of material, nonpublic information under Exchange Act Section 15(g) and Investment Advisers Act Section 204A. Cybersecurity-related enforcement actions have been on the rise in recent years, a trend that is sure to continue if the proposed suite of new requirements is adopted.

If you have any questions regarding the matters covered in this publication, please reach out to any of the lawyers listed below or your usual Davis Polk contact.

Greg D. Andres
+1 212 450 4724
greg.andres@davispolk.com

Matthew J. Bacal
+1 212 450 4790
matthew.bacal@davispolk.com

Martine M. Beamon
+1 212 450 4262
martine.beamon@davispolk.com

Micah G. Block
+1 650 752 2023
micah.block@davispolk.com

Robert A. Cohen
+1 202 962 7047
robert.cohen@davispolk.com

James W. Haldin
+1 212 450 4059
james.haldin@davispolk.com

Paul J. Nathanson
+1 202 962 7055
+1 212 450 3133
paul.nathanson@davispolk.com

Gabriel D. Rosenberg
+1 212 450 4537
gabriel.rosenberg@davispolk.com

Margaret E. Tahyar
+1 212 450 4379
margaret.tahyar@davispolk.com

Zachary J. Zweihorn
+1 202 962 7136
zachary.zweihorn@davispolk.com
