

A Late Winter Blizzard of SEC Cybersecurity Rulemaking: the Proposed BD Cybersecurity Rules and Expanded Reg S-P and Reg SCI Obligations

March 20, 2023

On March 15, 2023, the U.S. Securities and Exchange Commission (the “SEC”) released a suite of proposed new rules (the “Proposed Rules”) that include:

- [Proposed new cybersecurity rules](#) for broker-dealers, security-based swap dealers, major security-based swap participants, transfer agents, a variety of market infrastructure providers (national securities exchanges, clearing agencies, and security-based swap data repositories), and securities SROs (collectively, “Market Entities”) that would impose new policies and procedures requirements and incident notification obligations (“BD Cyber Proposal”);
- [Amendments to Regulation S-P \(“Reg S-P”\)](#) that would require the implementation of an incident response program, including a new customer notification obligation; expand the scope of the existing requirements relating to the safeguarding of “customer” information and the disposal of “consumer” information relating to individuals (the “Safeguards and Disposal Rules”); and impose new recordkeeping requirements (“Reg S-P Proposal”); and
- [Amendments to Regulation SCI \(“Reg SCI”\)](#) to expand the scope of covered entities to cover certain broker-dealers without an ATS and security-based swap data repositories and to update requirements relating to policies and procedures, incident notification, and other compliance obligations (“Reg SCI Proposal”).

The Proposed Rules follow the SEC’s February 9, 2022 proposed cybersecurity rules for [registered investment advisers and registered funds](#) (“IM Cyber Proposal”) and March 9, 2022 cybersecurity rules for [issuers](#) (“Issuer Cyber Proposal”). The SEC also [reopened the public comment](#) period for the IM Cyber Rules in light of potentially overlapping obligations with these proposed new rules relating to policies and procedures, incident response, SEC notification, public disclosure, and recordkeeping.

Because the SEC’s proposed rules have overlapping requirements, it will be important for firms to assess how these competing requirements would interact and impact their

incident response and compliance programs, as well as their regulatory notification and disclosure obligations.

In this Data Blog post, we outline the key requirements of the Proposed Rules and offer key takeaways to help firms navigate and prepare for the likely adoption of a version of these complex regulations. We will also be discussing these issues during our [live webcast on March 21, 2023, as well as in subsequent blog posts](#).

Key Requirements under the BD Cyber Proposal

The BD Cyber Proposal would create new cybersecurity obligations for sell-side financial institutions and various market infrastructure providers. For broker-dealers, the BD Cyber Proposal differentiates between (i) those for which a significant cyber event might pose higher risk to the market, which—along with all of the other types of covered institutions—would be defined as “Covered Entities” and (ii) more limited broker-dealers that would be subject to a smaller set of requirements. “Covered Entities” would include all (1) carrying broker-dealers; (2) introducing broker-dealers; (3) broker-dealers with regulatory capital equal to or exceeding \$50 million; (4) broker-dealers with assets equal to or exceeding \$1 billion; (5) broker-dealers that operate as market makers; and (6) entities that operate an alternative trading system (“ATS”). All other broker-dealers are excluded from this “Covered Entities” category (collectively, “Other Broker-Dealers”) and would be subject to fewer requirements.

The BD Cyber Proposal would create requirements for Covered Entities and Other Broker-Dealers related to incident response and notification, disclosure, and policies and procedures, including:

- **Immediate Incident Notification:** All Covered Entities and Other Broker-Dealers would be required to provide immediate written electronic notification to the SEC upon having a “reasonable basis to conclude that a significant cybersecurity incident has occurred or is occurring.” For this purpose, a “significant” incident would be one that significantly disrupts or degrades critical operations of the target or leads to unauthorized access that results, or is reasonably likely to result, in substantial harm to the target or any other person that interacts with the target.

Covered Entities would also be required to report additional information about the incident by filing Part I of proposed Form SCIR on EDGAR “promptly, but no later than 48 hours” after having a reasonable basis to conclude that a significant cybersecurity incident has occurred or is occurring. Covered Entities would also need to amend Part I of proposed Form SCIR no later than 48 hours after (1) determining

that previously reported information has become materially inaccurate; (2) learning new material information related to the previously reported incident; (3) resolution of the significant cybersecurity incident; or (4) conclusion of an internal investigation relating to the significant cybersecurity incident. Part I would not be public.

- **Public Disclosure of Risks and Incidents:** A Covered Entity would be required to make (and update in the case of material changes) two categories of cybersecurity disclosures on Part II of proposed Form SCIR (filed on EDGAR), as well as on an easily accessible section of its public website: (1) a summary description of cybersecurity risks that could materially affect the Covered Entity's business and operations (including how the Covered Entity "assesses, prioritizes, and addresses those cybersecurity risks"); and (2) "a summary description of each significant cybersecurity incident that occurred during the current or previous calendar year."
- **Cybersecurity Program:** Both Covered Entities and Other Broker-Dealers would be required to implement written policies and procedures that are reasonably designed to address their cybersecurity risks taking into account the size, business, and operations of the firm. These policies and procedures would need to be reviewed annually to "assess the design and effectiveness of the cybersecurity policies and procedures," including to address evolving cybersecurity risk. Covered Entities would need to document the annual review in a written report and would also be subject to more specific policies and procedures requirements, which would need to address "(1) risk assessments; (2) user security and access; (3) information protection; (4) cybersecurity threat and vulnerability management; and (5) cybersecurity incident response and recovery."
- **Books and Records:** New recordkeeping requirements would also be introduced for Covered Entities and Other Broker-Dealers that would cover, as applicable, the required policies and procedures, incident notification, Form SCIR disclosures, risk assessments, and annual reviews.

Proposed Amendments to Regulation S-P

As we've discussed in our prior Data Blog posts ([here](#) and [here](#)), Reg S-P has been an active area for SEC enforcement activity. Key proposed amendments in the Reg S-P Proposal include:

- **Incident Response Program:** Would require broker-dealers, registered investment advisers, registered funds, and transfer agents (collectively, "Covered Institutions")

to implement 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 need to cover the risk of harm posed by security compromises at third-party service providers, as well as the Covered Institution itself.

- **Customer Notification:** Would generally require Covered Institutions to notify affected customers as soon as practicable, but no later than 30 days, of becoming aware that an incident involving unauthorized access to or use of “sensitive customer information” has occurred or is reasonably likely to have occurred. “Sensitive customer information” would be defined to mean any 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 the individual identified. The Reg S-P Proposal contains an “affirmative presumption” of customer notice: notice would be required, unless the Covered Institution determines after a “reasonable investigation” of the incident that the sensitive customer information has not been or is reasonably unlikely to be used to cause substantial harm or inconvenience.
- **Expansion of Safeguards and Disposal Rules:** Would expand the Safeguards and Disposal Rules to cover all “customer information” in the possession of the Covered Institution regardless of whether it has a customer relationship with the relevant individual(s) and extends the applicability of the preexisting Safeguards and Disposal Rules to all transfer agents, including *both* those registered with the SEC and those registered with another regulatory agency.
- **Recordkeeping:** Would require the maintenance of written records documenting compliance with the Safeguards and Disposal Rules; amend recordkeeping provisions under the Investment Company Act of 1940, Investment Advisers Act of 1940, and the Securities Exchange Act of 1934; and add a recordkeeping requirement for investment companies not registered under the Investment Company Act.
- **Exception for Annual Privacy Notice:** Would conform Reg S-P’s existing annual privacy notice requirement to be consistent with the GLBA exception to the annual notice delivery requirements for financial institutions that meet certain requirements.

Reg S-P does not apply to private funds (either directly or as institutional clients of registered investment advisers) that rely on an exemption from registration under Sections 3(c)(1) or 3(c)(7) of the Investment Company Act of 1940, and the Reg S-P proposal does not suggest any change to this approach. The Reg S-P proposal provides a proposed compliance date 12 months after the effective date of the final amendments.

Proposed Amendments to Regulation SCI

The Reg SCI Proposal includes amendments relating to (1) scope of covered entities subject to the regulation; (2) systems classification and lifecycle management; (3) third-party/vendor management; (4) cybersecurity; (5) the SCI review; (6) the role of current SCI industry standards; and (7) recordkeeping and related matters. Key proposals include:

- **Expansion of the Definition of “SCI Entities”:** The definition of SCI entity would be expanded to include certain large broker-dealers, registered security-based swap data repositories; and exempt clearing agencies. Broker-dealers would become subject to the full set of requirements if (i) their total assets in at least two of the previous four calendar quarters exceed 5% of the “total assets of all security broker-dealers” (as reported by the FRB); or (ii) their transaction volume over a slightly longer quarterly look-back period in any of four categories (NMS stocks, listed options, U.S. Treasuries, or U.S. Agency securities) exceeds 10% relative to the reported market.
- **Enhanced Policies and Procedures Requirements (with a focus on third-party providers):** An SCI entity’s policies and procedures would be required to include programs that address inventory, classification, and lifecycle management for SCI systems and indirect SCI systems; management and oversight of third-party providers (including cloud service providers) that provide or support SCI or indirect SCI systems; BC/DR plans that address the unavailability of certain third-party providers (and any resulting material impact); unauthorized access to SCI systems and information therein; and identification of current SCI industry standards with which each such policy and procedure is consistent.
- **More Frequent Penetration Testing:** Would increase the scope and the required frequency of penetration testing by SCI entities to at least annually, rather than once every three years.
- **Expanded Definition of “Systems Intrusion”:** Would amend the definition of “systems intrusion” to include two more cyber events: (1) any cybersecurity event that disrupts, or significantly degrades, the normal operation of an SCI system (e.g., DDOS attacks, remote command-and-control attacks, supply-chain attacks); and (2) any significant attempted unauthorized entry into the SCI systems or indirect systems of an SCI entity as determined by the SCI entity pursuant to established reasonable written criteria. Such events would also require SEC notification under Reg SCI’s existing notification framework.

Key Takeaways

- **The SEC's Comment Process.** Given the number of overlapping and significant proposed regulatory obligations, consider submitting comments to the Proposed Rules.
- **Cross-Functional Risk Assessment Mapped to the Rules.** Consider a risk assessment that assesses both policies and procedures, as well as technical cybersecurity controls, and that maps onto the proposed rules (as well as other applicable regulatory frameworks). Cross-enterprise teams or committees that include members of the business, internal audit, and compliance can ensure that compliance obligations are not missed by working with security teams on these assessments. While the applicability of privilege for such assessments is subject to debate, some of our clients have found it helpful to use outside counsel together with a technical vendor to assist with these.
- **Review Applicability of Each Rule under Expanded Scope and Definitions.** As the SEC itself recognizes, the Proposed Rules have overlapping requirements because a single entity will potentially be bound by multiple sets of rules. For instance, certain SCI entities are also "Covered Entities" under the BD Cyber Proposal and would separately also be subject to requirements under Reg S-P. Likewise, registered investment advisers (which are already subject to Reg S-P) would also be subject to the IM Cyber Proposal. A first step for registrants to consider is identifying and assessing the full range of potentially new or heightened obligations. For some firms that are covered by the Proposed Rules, it may take significant time and resources to fully implement these requirements, and accordingly, they may want to start early.
- **An Integrated Approach.** The SEC also recognizes that registrants can likely comply with the proposed new obligations through a global framework for policies and procedures and incident response. Consider taking a holistic view of covered areas such as incident response, policies and procedures, notification, and recordkeeping.

Compliance with Notification and Reporting Obligations. The different proposed regulatory frameworks have different notification timelines, obligations, and formats for notification. Consider preparing a decision matrix for assessing cybersecurity events under each notification trigger, including the factors to consider when determining whether a particular cybersecurity event would qualify as "significant" for reporting purposes.

* * *

Please do not hesitate to contact us with any questions.

To subscribe to the Data Blog, please click [here](#).

The [Debevoise Data Portal](#) is now available for clients to help them quickly assess and comply with their various state, federal, and international breach notification obligations.

NEW YORK



Avi Gesser
agesser@debevoise.com



Erez Liebermann
eliebermann@debevoise.com



Jeff Robins
jlrobin@debevoise.com



Charu A. Chandrasekhar
cchandrasekhar@debevoise.com



Sheena Paul
spaul@debevoise.com



Suchita Mandavilli Brundage
smbrunda@debevoise.com



Michael R. Roberts
mrroberts@debevoise.com



Ned Terrace
jkterrace@debevoise.com



Luke Dembosky
ldembosky@debevoise.com

WASHINGTON, D.C.



Marc Ponchione
mponchione@debevoise.com



Julie M. Riewe
jriewe@debevoise.com



Kristin A. Snyder
kasnyder@debevoise.com

SAN FRANCISCO

SAN FRANCISCO



Mengyi Xu
email@debevoise.com