Lowenstein Sandler

Investment Management

March 29, 2023

Investment Advisers, Broker-Dealers, and Other Financial Industry Participants Take Note: SEC Demonstrates Commitment to Cybersecurity With Three Simultaneous Rule Proposals

By Scott H. Moss and Michael J. Scales

On March 15, 2023, the Securities and Exchange Commission ("SEC") issued three releases proposing (i) amendments to Regulation S-P ("Regulation S-P Proposal")[1], (ii) amendments to Regulation SCI ("Regulation SCI Proposal")[2], and (iii) new Rule 10 under the Securities and Exchange Act of 1934 ("Exchange Act") (the rule, "Proposed Rule 10")[3], which would affect the compliance obligations of investment advisers, broker-dealers, and other financial industry participants in various ways.

The Regulation S-P Proposal would require brokers, dealers, investment companies, and SEC-registered investment advisers to adopt policies and procedures for incident response programs to address situations involving the unauthorized access of customer information. The Regulation SCI Proposal would recognize a broader array of institutions, including certain broker-dealers, as key participants in the U.S. securities markets infrastructure (by designating them as "SCI entities") and require them to implement policies and procedures designed to minimize the impact of any adverse cybersecurity events affecting their operational systems. Proposed Rule 10 would require certain broker-dealers and other institutions to address cybersecurity risks through policies and procedures and, in the event of significant cybersecurity incidents, make certain notices and disclosures to the SEC.

Background

Regulation S-P sets forth rules 248.30(a) ("Safeguards Rule") and 248.30(b) ("Disposal Rule"). The Safeguards Rule generally requires brokers, dealers, investment companies, and SEC-registered investment advisers to implement policies and procedures for safeguarding customer information by seeking to maintain the information's confidentiality and protect it against anticipated threats and unauthorized access. The Disposal Rule requires those entities, as well as registered transfer agents, to securely dispose of consumer report information. The Regulation S-P Proposal states that since the regulation was originally adopted, evolving digital communication and information storage tools have made it easier to obtain and share individuals' personal information, which increases the risk of unauthorized access.

Regulation SCI governs certain "SCI entities" (defined to include certain self-regulatory organizations, alternative trading systems, plan processors, exempt clearing agencies, and competing consolidators), which are entities the SEC has recognized as capable of interfering with the proper functioning of the securities markets in the event their computer information systems fail. Regulation SCI governs how SCI entities use various technology systems, including "SCI systems" (i.e., the technology systems that directly support certain enumerated securities market functions, such as trading, clearing, and settlement). Regulation SCI requires that SCI entities implement policies and procedures to ensure their SCI systems can operate properly and provide appropriate notices to the SEC and other market participants in the event of serious incidents affecting those systems. The Regulation SCI Proposal states that as technology changes, workforces become increasingly remote, and certain SCI entity functions are outsourced to vendors, new cybersecurity risks could threaten SCI systems.

In the release introducing Proposed Rule 10, the SEC recognizes that certain U.S. securities market participants (enumerated below) rely on an array

[1] The Regulation S-P Proposal is available here.
[2] The Regulation SCI Proposal is available here.
[3] Proposed Rule 10 is available here.

of electronic information, communication, and systems to operate. The SEC finds that significant cybersecurity incidents affecting those items could interfere with those participants' ability to perform their core functions, which could cause harm to investors and disrupt the overall operation of the markets.

The Proposals

Regulation S-P Proposal

The Regulation S-P Proposal seeks to make the following notable amendments, among others, to Regulation S-P.

Develop Incident Response Programs. The SEC recognizes that Regulation S-P currently does not require the institutions it covers (enumerated above) to implement policies and procedures for responding to data breach incidents or notify affected individuals in the event of a breach. The amendments would require covered institutions to incorporate "incident response programs" into their safeguards policies to respond to the unauthorized access of customer information. Those programs must be reasonably designed to detect, respond to, and recover from such an incident, assess the nature and scope of the incident, and take appropriate steps to contain and control it. The program must also include a clear and conspicuous notice to individuals whose customer information was compromised. That notice must be provided "as soon as practicable," but in no case later than 30 days after determining the breach occurred.

Extend Safeguards Rule to Transfer Agents. The SEC recognizes that while the Disposal Rule under Regulation S-P applies to transfer agents, the Safeguards Rule does not, even though transfer agents – like broker-dealers, investment companies, and SEC-registered investment advisers – also maintain and share the personal information of securityholders. Therefore, the amendments would extend the Safeguards Rule to also apply to transfer agents registered with the SEC or another appropriate regulatory agency as defined by Section 3(a)(34)(B) of the Exchange Act.

Broaden Protections to More Customer Information. The SEC recognizes that the current Safeguards Rule only protects the information of the covered institutions' own customers, which overlooks that a covered institution may receive sensitive information about other institutions' customers. For example, a covered institution may receive nonpublic personal information from an introducing broker or dealer that clears transactions for its customers through a clearing broker on a fully-disclosed basis. The current Safeguards Rule would not specifically require the covered institution to protect that information. As such, the amendments would state that the Safeguards Rule and Disposal Rule apply to all customer information in the covered institution's possession and all consumer information that a covered institution possesses for a business purpose, which would protect both the covered institution's own customers' information and the customer information the covered institution receives from other financial institutions.

Regulation SCI Proposal

The Regulation SCI Proposal seeks to make the following notable amendments, among others, to Regulation SCI.

Expand Definition of "SCI Entity." While Rule 1000 under Regulation SCI currently defines "SCI entity" to include certain self-regulatory organizations, alternative trading systems, plan processors, exempt clearing agencies, and competing consolidators, the amendments would expand that definition to include certain registered security-based swap data repositories, registered broker-dealers exceeding an asset or transaction activity threshold, and additional clearing agencies exempted from registration.

Further Specify Policies and Procedures. Rule 1001 requires SCI entities to establish and maintain policies and procedures reasonably designed to ensure that their SCI systems can maintain their operational capacity by requiring, among other things, the establishment of technological infrastructure capacity planning estimates, periodic capacity stress tests of systems, and programs to keep current the systems development and testing methodology of such systems. The amendments would further state that those policies must require, among other things, the maintenance of a written inventory and classification of the entity's SCI systems and a program to manage and oversee outside parties that provide services to the SCI systems.

Proposed Rule 10

Proposed Rule 10 would apply to broker-dealers, clearing agencies, major securities-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 who each meet specific enumerated requirements (collectively, "market entities").

Such market entities would be required to establish, maintain, and enforce written policies and procedures that are reasonably designed to address the cybersecurity risks specific to their businesses. They would also be required to annually review and assess the design and effectiveness of their policies to reflect changes in those risks, document those reviews, and provide immediate written notice to the SEC of any significant cybersecurity incidents.

Additionally, market entities that meet the heightened definition of "covered entities" under the rule must have more complex policies and procedures that address certain specific elements. Though the requirements for being considered a covered entity are different for each of the above types of market

entities, broker-dealers in particular will only be covered entities if they (1) maintain custody of securities and cash for customers or other broker-dealers, (2) introduce their customers' accounts to a carrying broker-dealer on a fully-disclosed basis, (3) have regulatory capital equal to or exceeding $50 million, (4) have total assets equal to or exceeding $1 billion, (5) operate as market makers, and (6) operate on an alternative trading system.

A covered entity's policies and procedures must specifically address the following elements.

Risk Assessment. The policies must require the covered entity to conduct a periodic assessment of cybersecurity risks relevant to its particular information systems and information residing on those systems. The periodic assessment portion of the policies must require the covered entity to (1) categorize and prioritize cyber risks based on an inventory of the components of its information systems and information and (2) identify its outside service providers that receive, maintain, or process information or are otherwise permitted to access its information systems and information on those systems and then assess the risks associated with those service providers. These risk assessments must be documented.

User Security and Access. The policies must also include controls designed to minimize user-related risks and prevent unauthorized access to the covered entity's information systems and the information residing on them. Additionally, they must include controls addressing certain enumerated aspects of user security and access.

Information Protection. The policies must also seek to protect information that the covered entities maintain in two ways: by (1) including measures designed to protect the covered entity's information systems and the information residing on them from unauthorized access and (2) requiring oversight of service providers that receive, maintain, or process the covered entity's information or are otherwise permitted to access the covered entity's information systems (pursuant to a written contract between the covered entity and the service provider).

Cybersecurity Threat and Vulnerability Management. The policies and procedures must include measures designed to detect, mitigate, and remediate any cybersecurity threats and vulnerabilities with respect to the covered entity's information systems and information residing on those systems.

Cybersecurity Incident Response and Recovery. The policies must include measures designed to detect, respond to, and recover from a cybersecurity incident. These policies must be reasonably designed to ensure (1) the continued operations of the covered entity, (2) the protection of the covered entity's information systems and the information residing on those systems, (3) external and internal cybersecurity incident information sharing and communications, and (4) the reporting of significant cybersecurity incidents to the SEC.

In addition to requiring the above policies and procedures, Proposed Rule 10 would require the covered entity to provide immediate written notice to the SEC of a significant cybersecurity incident upon having a reasonable basis to conclude that the incident has occurred or is occurring. The covered entity would also be required to report detailed information about the incident by confidentially filing Part I of proposed Form SCIR with the SEC.

Our Thoughts

These rule proposals demonstrate that the SEC recognizes the devastating effects cyber incidents could have on the proper functioning of the U.S. securities markets and is committed to ensuring all entities subject to its jurisdiction implement robust policies and procedures to minimize those potential effects. The proposals are each notable in their own ways.

The Regulation S-P Proposal is particularly focused on the adverse effects of data breaches and emphasizes the importance of robust policies and procedures regarding how to respond to them. While most broker-dealers, investment companies, and SEC-registered investment advisers likely already have policies in place to try to protect confidential information, firms should take note of the particular features that these amendments would require as part of those policies and be prepared to update them to ensure full compliance with Regulation S-P. In particular, firms should be prepared to revise their policies to establish an appropriate plan for responding to data breaches and to protect the sensitive information they receive regarding the customers of other institutions, as these amendments would require. With particular respect to data breaches, firms should consider both the requirements sought to be imposed by these proposed amendments and any requirements imposed by applicable state law. As the Regulation S-P Proposal recognizes, all 50 states have enacted laws requiring firms to notify individuals of data breaches, with some states imposing more comprehensive requirements.

The Regulation SCI Proposal is notable because it would expand the regulation's various requirements to certain broker-dealers who did not previously need to consider the regulation's requirements. It is also notable that the policies and procedures required by these proposed amendments would need to be consistent with "industry standards." This will likely prove problematic as this term could be subject to various interpretations, technology changes, and each entity has unique risks that may make it desire policies and procedures quite different from those of its peers.

Proposed Rule 10 is also notable for its distinction between covered entity broker-dealers and other

broker-dealers. If the broker-dealer does not satisfy the conditions above to qualify it as a covered entity, the broker-dealer would still be a market entity under the rule and thus still subject to various requirements. As the release introducing Proposed Rule 10 specifically recognizes, such "non-covered broker-dealers" would be required to establish, maintain, and enforce written policies and procedures that are reasonably designed to address their unique cybersecurity risks, periodically review and assess the design and effectiveness of those policies, make records of those periodic reviews and previous versions of their policies and procedures, and provide the SEC with immediate written notice of significant cybersecurity incidents. However, non-covered broker-dealers need not address in their policies the specific elements that the rule requires covered entities to address, file confidential reports about significant cybersecurity incidents with the SEC, or make public disclosures about their cybersecurity risks and incidents they experienced. As such, broker-dealers should consider whether the elements of covered entities specific to broker-dealers (discussed above) apply, and then tailor their policies and procedures accordingly.

Next Steps

The comment periods for the Regulation S-P Proposal, the Regulation SCI Proposal, and Proposed Rule 10 are each open until 60 days after their respective dates of publication in the Federal Register. Lowenstein Sandler will monitor the status of the proposals and provide additional updates and analysis in future Client Alerts so that clients can determine whether changes are required to their existing compliance policies and procedures. Please contact one of the listed authors of this Client Alert or your regular Lowenstein Sandler contact if you have any questions regarding these proposals.

Contacts

Please contact the listed attorneys for further information on the matters discussed herein.

SCOTT H. MOSS
Partner
Chair, Fund Regulatory & Compliance
T: 646.414.6874
smoss@lowenstein.com

MICHAEL J. SCALES
Associate
T: 973.422.6770
mscales@lowenstein.com