The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

MEMO# 35215

March 24, 2023

SEC Publishes Cybersecurity Proposal Affecting Transfer Agents

[35215]

March 24, 2023

TO: Operations Committee
SEC Rules Committee
Transfer Agent Advisory Committee RE: SEC Publishes Cybersecurity Proposal Affecting Transfer Agents

On March 15, 2023, the Securities and Exchange Commission (SEC) published a proposal that would establish new cybersecurity risk management rules for transfer agents, among other market entities.[1] The proposal seeks to address cybersecurity risks through policies and procedures, immediate SEC notification of significant cybersecurity incidents, and related reporting and disclosure obligations. The new rule would be labeled Rule 10 and establish a new reporting form: Form SCIR.[2] Comments on the proposal will be due 60 days after it is published in the Federal Register. While this memo will focus on the proposal's applicability to transfer agents, new Rule 10 would apply to many different market entities, including broker-dealers and security-based swap dealers.

Members with comments they would like the ICI to consider including in our comment letter on the proposal should send them to tamara@ici.org no later than Friday, April 7th.

The Proposed New Rule 10 Requirements

The proposed Rule 10 would impose several general requirements on market participants and impose more specific requirements on "covered entities." The general requirements are as follows:

- All market participants (both covered and noncovered entities) would be required to establish, maintain, and enforce written policies and procedures that are reasonably designed to address their cybersecurity risks;
- At least annually, all market participants must review and assess design and effectiveness of the policies and procedures;
- In conjunction with the annual review, all market participants would need to either prepare a written report (if a covered entity) or a record (if a noncovered entity); and
- All market entities must give the SEC "immediate" written electronic notice[3] of a "significant" cybersecurity incident upon having a reasonable basis[4] to conclude that such an event has occurred/is occurring.[5] These notices would be kept

nonpublic to the extent permitted by law.[6]

Specific Requirements for "Covered Entities"

The proposal would impose additional requirements for "covered entities" including Transfer agents which are defined as "covered entities" under the proposal.[7]

Covered entities would need to establish and maintain policies and procedures addressing cybersecurity risk management. The policies and procedures would need to include the following provisions:

- Periodic assessments of cybersecurity risks and written documentation of the risk assessments;
- Controls designed to minimize user-related risks and prevent unauthorized access to information systems;
- Measures designed to monitor information systems and protect information from unauthorized access or use, including periodic assessments; and oversee service providers that receive, maintain, or process information (or are otherwise allowed to access the covered entity's systems);
- Measures designed to detect, mitigate, and remediate any cybersecurity threats and vulnerabilities;
- Measures to detect, respond to, and recover from a cyber incident and written documentation of any cyber incident and the response to/recovery from the incident; and
- Impose recordkeeping requirements that refer to existing recordkeeping requirements that currently apply to each entity covered by the rule, which will be addressed separately below.

Notably, the policies and procedures would need to require the covered entity to identify service providers that "receive, maintain, or process information, or are otherwise permitted to access its information systems and the information residing on those systems," and assess the cyber risk associated with that activity.[11]

The proposal, in addition to imposing both general and specific requirements on covered entities, would also require compliance with modified versions of the general requirements under certain circumstances:

- Upon a "significant" cybersecurity incident (which triggers an "immediate" reporting requirement to the SEC), covered entities need to report and update information about the incident by filing Part 1 of proposed Form SCIR.
- If a covered entity is carrying or introducing broker-dealers, the covered entity would need to furnish the form to clients when an account is opened, when the form is updated, and annually.
- Public disclosures on Part 2 of proposed Form SCIR about cybersecurity risks and significant cyber incidents experienced during the current or previous calendar year.

The Proposal's Definition of "Significant Cybersecurity Incident"

The proposal defined "significant cybersecurity incident" as an incident of "unauthorized occurrence on or conducted through a Market Entity's information systems that jeopardizes the confidentiality, integrity, or availability of the information systems or any information residing on those systems."[12] In its definition, the SEC seeks to "encompass within the definition of 'cybersecurity incident' the various categories of unauthorized occurrences that can impact an information system (e.g., unauthorized access, use, disclosure,

downloading, disruption, modification, or destruction)."[13] The definition is intended to "include any unauthorized incident impacting an information system or the information residing on the system. An information system can experience an unauthorized occurrence without a threat actor itself directly obtaining unauthorized access to the system."[14] The Proposal clarifies the SEC's views by noting that "the occurrence must be one that jeopardizes (i.e., places at risk) the confidentiality, integrity, or availability of the information systems or any information residing on those systems."[15]

The Proposal adopts two approaches for evaluating whether a cybersecurity incident is "significant" under the proposed Rule 10. The first approach would define a "significant" incident as "a cybersecurity incident, or a group of related cybersecurity incidents, that significantly disrupts or degrades the ability of the Market Entity to maintain critical operations."[16] The second approach would define a "significant cybersecurity incident" as a "cybersecurity incident, or a group of related cybersecurity incidents, that leads to the unauthorized access or use of the information or information systems of the Market Entity, where the unauthorized access or use of such information or information systems results in or is reasonably likely to result in: (1) substantial harm to the Market Entity; or (2) substantial harm to a customer, counterparty, member, registrant, or user of the Market Entity, or to any other person that interacts with the Market Entity."[17]

Recordkeeping Provision of Proposed Rule 10

Proposed Rule 10 would amend current recordkeeping rules that govern transfer agents. The proposal would require transfer agents to retain Rule 10 records for three years. Written cybersecurity policies and procedures would need to be maintained for three years after their use terminates. More generally, Rule 10 records would be subjected to the record maintenance requirements of Rule 17ad-7, including applicable requirements for electronic records. Finally, transfer agents (both SEC-registered and those registered with another appropriate regulatory agency defined by 15 U.S.C. 78c(34)(B)) would be subject to the Regulation S-P Safeguards Rule and the Disposal Rule.[18]

Relevant Requests for Comment

Request for Comment #43 asks whether the immediate written electronic notice requirement timeline of 48 hours is proper, and whether an alternative timeline (such as a same-day or 24-hour timeline) would be more appropriate. See Proposing Release at 163.

Request for Comment #29, on page 129 of the Proposing Release, asks whether, and in what ways, the service provider oversight requirements should be modified.

Thomas Archer
Legal Intern

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 (March 15, 2023), available at https://www.sec.gov/rules/proposed/2023/34-97142.pdf.

[2] While transfer agents are considered "covered entities" under the proposal, no section

of the new Form SCIR is unique to transfer agents, although transfer agents would be required to designate their status as such on the Form.

[3] Transfer agents would need to provide written notice to its Appropriate Regulatory Agency (ARA). See Proposing Release at 142 and paragraphs (c)(1)(i)-(ii) of proposed Rule 10.

[4] The Proposing Release notes that "reasonable basis" does not mean that a covered entity can "wait until it definitively concludes that a significant cybersecurity incident has occurred or is occurring." The Proposing Release explains that the "reasonable basis" term reflects the reality that in the beginning stages of uncovering a cyber incident, it is difficult to conclude the extent of the incident's severity.

[5] The Proposing Release at 141 elaborates slightly on what "immediate" means in the context of the proposed new Rule 10. The "immediate written notification requirement is modelled on other notification requirements that apply to broker-dealers and SBSDs pursuant to other Exchange Act rules. Under these existing requirements, broker-dealers and certain SBSDs must provide the Commission with same-day written notification if they undergo certain adverse events…" [emphasis added].

Further clarification about the "immediate" standard is found on page 122 of the Proposing Release, which states "the Covered Entity would need to report information about the significant cybersecurity incident promptly, but no later than 48 hours, after having a reasonable basis to conclude that the incident has occurred or is occurring by filing Part I of proposed Form SCIR with the Commission." See paragraph (c)(2) of proposed Rule 10. The proposed Rule 10 would also impose follow-on disclosure obligations under certain circumstances.

Finally, note that the immediate reporting requirement is intended to "alert the Commission on a confidential basis as to the existence of a significant cybersecurity incident. . . [i]t is not intended as a means to report information about the. . . incident." More detailed information would be reported on proposed Form SCIR. See Proposing Release at 142-43. Both the immediate written notice and the Form SCIR filing would have the same trigger event - a reasonable basis for concluding that a significant cyber event is occurring or has occurred. The Form SCIR filing would also be required to be filed "promptly, but no later than 48 hours" after forming the reasonable basis for concluding that a significant cyber event has occurred. See Proposing Release at 143.

[6] See Proposing Release at 140.

[7] The proposed rule refers to the definition of "transfer agent as defined in Section 3(a)(25) of the Exchange Act that is registered or required to be registered with an appropriate regulatory agency ("ARA") as defined in Section 3(a)(34)(B) of the Exchange Act." See Proposing Release at 73; see also paragraph (a)(1)(ix) of proposed Rule 10. See also 15 U.S.C. 78q-1(c)(1) (registration requirements for transfer agents); 15 U.S.C. 78c(a)(25) (definition of transfer agent) and (a)(34)(B) (definition of appropriate regulatory agency).

[8] Relevant controls may include an acceptable use policy, authentication procedures for access verification, password management procedures, access restriction procedures, and procedures governing remote access technology. See Proposing Release at 109-110.

[9] The covered entity's policies and procedures would need to require oversight to be imposed pursuant to a written contract between the covered entity and the service provider. The proposed new Rule 10 would impose mandatory terms in those contracts relating to implementation and maintenance of appropriate measures, including those in sections (b)(1)(i), (b)(1)(ii), (b)(1)(iii), (b)(1)(iv), and (b)(1)(v) of the proposed rule. See Proposing Release at 115.

[10] Periodic assessments would need to consider the sensitivity level of the covered entity's business operations, the presence of any personal information, where and how information is accessed, stored, and transmitted, the information system's access controls and malware protection, and the potential effect a cyber incident would have on the covered entity. See Proposing Release at 113-14.

[11] See Proposing Release at 107. Relevant considerations for assessing the cyber risk identified would include the service provider's level of protection against its own cyber risk and its ability to respond to and recover from cyber incidents.

[12] See paragraph (a)(2) of proposed Rule 10.

[13] See Proposing Release at 77.

[14] Id.

[15] See Proposing Release at 78.

[16] See paragraph a(10)(i) of Proposed Rule 10.

[17] See Paragraph a(10)(ii) of Proposed Rule 10.

[18] See Proposing Release at note 475.