June 27, 2023

SEC Poised to Take Action on Cyber: Looking Ahead to Anticipated Cybersecurity and Privacy Rulemaking

The U.S. Securities and Exchange Commission (the "SEC") is poised to adopt several new rules on privacy and cybersecurity that will impact public companies, broker-dealers, investment companies and registered investment advisers, including the following proposed rules[1]:

- Proposed Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (applicable to public companies; adoption currently anticipated in October 2023)
- Proposed Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies (adoption currently anticipated in October 2023)
- Proposed Amendments to Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information (applicable to brokers and dealers, funds and advisers; adoption currently anticipated in April 2024)
- Proposed Cybersecurity Risk Management Rules for Broker-Dealers and Other Market Participants (adoption currently anticipated in April 2024)

Among other things, the proposed rules zero in on the intersection of cybersecurity and risk management matters, promote disclosure of certain privacy and cybersecurity risks and, in the case of the rules applicable to public companies, promote appropriate oversight of cybersecurity and privacy matters.

The SEC Staff previously issued guidance in 2011 and 2018 addressing public company disclosure and oversight of cyber risk, and has pursued a number of enforcement actions in connection with cybersecurity incidents.[2] As discussed in greater detail below, the proposed rules will present new challenges to businesses, in particular with respect to requirements to report cyber incidents to the SEC and to impacted individuals within prescribed time periods.

I. Public Company Cyber Disclosures

Recognizing that cybersecurity risks and incidents can impact a business's financial performance and position, the proposed "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure" seek "[c]onsistent, comparable, and decision-useful disclosures" relating to risk management and governance, as well as regarding "material cybersecurity incidents," in order to inform investors.

The key disclosure requirements of the proposed rules for public companies, if adopted, would include:

- **Incidents**: Disclosure within four business days after identifying a material cybersecurity incident (new Item 1.05 of Form 8-K); and disclosure of material changes, additions or updates to previously reported information (Form 10-Q and 10-K disclosures under Items 106(d) of Regulation S-K).
- **Risk Management and Governance:** Disclosure of cybersecurity risk management policies and procedures and governance practices (new Items 106(b) and (c) of Regulation S-K).
- **Board Expertise:** Disclosure of board members who possess cybersecurity expertise (new Item 407(j) of Regulation S-K).

Incident Disclosures

Of most immediate concern to many public companies is the requirement to provide detailed disclosures on Form 8-K about a cybersecurity incident within four business days after determining that such an incident is "material." In the proposing release, the SEC clarifies that the determination of whether an incident is material would be consistent with existing case law addressing materiality under the securities laws, including if there is a substantial likelihood that a reasonable shareholder would consider the information important in making an investment decision, or if the information significantly alters the "total mix" of information made available to investors. The SEC also emphasizes in the proposing release that doubts concerning materiality must be "'resolved in favor of those the statute is designed to protect,' namely investors." Under the proposed rule, incident-related disclosures would need to include information about when the cybersecurity incident was discovered and, if it is ongoing, a description of the nature and scope of the incident, whether data was stolen, altered, accessed or used for any unauthorized purpose, the effect of the incident on the operations of the business, and whether the incident has been remediated or is currently being remediated.

Risk Management and Governance Disclosures

Public companies would also be required to describe their cybersecurity risk management and strategy, and their governance and oversight of cybersecurity risks. Specifically, the proposed rules would require disclosure of the board's oversight of cybersecurity, including how and when the board is informed of cyber risks and how cyber risks are considered by the board in the company's strategy, as well as management's role and relevant expertise in assessing and managing cyber risk, including whether the company has a chief information security officer or similar position and information relating to management structure, as well as implementing policies and procedures used to identify and manage cyber risk.

Board Expertise

The proposed rules would require public companies to disclose whether any member of the board of directors has cybersecurity-related expertise.[3] Companies will need to assess information provided by directors with respect to their background, education, certifications and expertise, including as disclosed in their annual D&O questionnaires. Many companies have already begun to incorporate these practices and are highlighting cyber and technology skills in their annual meeting proxy statements.

II. Investment Adviser, Investment Company and Broker-Dealer Disclosures: Two Proposals

The SEC is also considering rulemaking that would impact broker-dealers, registered investment advisers, and investment companies. Proposed new rules under the Investment Advisers Act and the Investment Company Act would require registered investment advisers and investment companies to adopt written cybersecurity policies and procedures, and to report "significant" cybersecurity incidents to the SEC.[4] Recently-proposed revisions to Regulation S-P (which imposes certain privacy and cybersecurity requirements on financial institutions under the Gramm-Leach-Bliley Act ("GLBA")) would, among other things, require covered institutions to adopt written incident response plans and notify customers of certain types of cybersecurity incidents.[5]

Proposed rules under the Investment Advisers Act and Investment Company Act would apply to registered investment companies and business development companies ("funds") and investment advisers registered with the SEC ("advisers"). The proposed amendment to Regulation S-P would apply to financial institutions under the GLBA, which includes broker-dealers, funds and advisers.

Cybersecurity Risk Management for Registered Investment Advisers, Registered Investment Companies, and Business Development Companies (the "Fund and Adviser Cyber Rules")

The proposed Fund and Adviser Cyber Rules would impose requirements on both funds and advisers – some proposed requirements are shared, and certain requirements related to reporting and retention have nuances that are specific to either funds or advisers.

Most notably, advisers would be required to report a "significant" adviser or fund cybersecurity incident to the SEC by submitting a Form ADV-C no later than 48 hours after having a reasonable basis to conclude that a significant adviser or fund cybersecurity incident had occurred or is occurring.[6] The proposal defines a reportable "significant adviser cybersecurity incident" as "a cybersecurity incident, or a group of related cybersecurity incidents, that significantly disrupts or degrades the adviser's ability, or the ability of a private fund client of the adviser, to maintain critical operations, or leads to the unauthorized access or use of adviser information, where the unauthorized access or use of such information results in: (i) substantial harm to the adviser, or (ii) substantial harm to a client, or an investor in a private fund, whose information was accessed."[7]

In addition to incident reporting, funds and advisers would be required to implement, and to review annually, written policies and procedures reasonably designed to address cybersecurity risks, including with respect to: risk assessment, systems monitoring and threat and vulnerability management; the implementation of security and access controls to prevent unauthorized access to information and systems; and cybersecurity incident response and recovery. Funds and advisers would also be required to include information regarding cybersecurity risks and incidents on annually updated registration forms (for funds) and the Form ADV (for advisers).

Advisers and funds would be required to maintain copies of certain cybersecurity-related documentation (each for five years):

Advisers	Funds
• Cybersecurity policies and procedures; • Written report documenting annual review of cybersecurity policies and procedures; • Any form ADV-C filed; • Records documenting any cybersecurity incident (including response and recovery records); and • Documentation of cybersecurity risk assessments.	• Cybersecurity policies and procedures; • Written reports provided to board and records documenting annual review of cybersecurity policies and procedures; • Report of a significant fund cybersecurity incident provided to the SEC; • Records documenting any cybersecurity incident (including response and recovery records); and • Documentation of cybersecurity risk assessments.

Proposed Amendment to Regulation S-P

Proposed amendment to Regulation S-P would impose requirements on brokers and dealers, funds and advisers (collectively, "covered institutions").

The proposed amendment introduces a notification requirement in connection with security incidents. Covered institutions would be required to provide "clear and conspicuous notice"[8] in writing to each affected individual whose sensitive customer information was, or was reasonably likely to have been, accessed or used without authorization. Notification must be made as soon as possible but no later than thirty days after the covered institution becomes aware of the incident, unless a "reasonable investigation" determines that the sensitive customer information has not been and is not reasonably likely to be used in a manner that would result in "substantial harm or inconvenience."[9] The proposed rule defines "customer information" as nonpublic personal information about a customer of a covered institution maintained by the covered institution or on its behalf,[10] and "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."[11] The proposed rule defines "substantial harm or inconvenience" as "personal injury, or financial loss, expenditure of effort or loss of time that is more than trivial."[12] If the covered institution cannot identify the specific impacted individual/s, it would be required to provide notice to all individuals whose sensitive customer information resides in the affected system.

In addition to incident reporting, the proposed amendment would update Safeguards and Disposal Rules that are part of Regulation S-P. Covered institutions would be required to implement and maintain written policies and procedures reasonably designed to protect the confidentiality and integrity of customer information under the Safeguards Rule, including an incident response program. Covered institutions other than notice-registered broker-dealers would have to additionally implement policies and procedures addressing the proper disposal of consumer and customer information under the Disposal Rule.[13] The proposed amendment would also make applicable the Safeguards and Disposal Rule to all customer and consumer information that a covered institution possesses, maintains or receives, regardless of whether such information relates to the covered institution's own customers or to customers of other financial institutions, and would expand the applicability of the rules to transfer agents registered with the SEC (or an analogous agency). Finally, covered institutions and transfer agents would be required to maintain copies of certain documentation to demonstrate compliance with the Safeguards and Disposal Rules.

III. Next Steps

Taken together, and in the context of recent enforcement actions, this series of proposed rules demonstrate the SEC's keen focus on privacy and cybersecurity hygiene for companies that come within its regulatory scope. Even absent implementation of these rules, the concepts addressed in the proposals set out a foundation of best practices for SEC-regulated companies. As a matter of good practice, companies should consider the following:

- **Implement cybersecurity risk management policies and procedures.** Implement and review regularly (e.g., at least annually) written policies and procedures that address known vectors of cybersecurity risk and procedures for risk management, which should include: testing and auditing; threat and vulnerability management; and incident response and breach notification. Emphasis should be placed on internal and external reporting. There must be clear requirements regarding timely reporting of risks and incidents to executive management and the board of directors to avoid unpleasant surprises for directors, even if they are still under investigation internally and being evaluated for materiality.
- **Re-examine cyber-related disclosures and related controls and procedures; focus on internal information flow and alert system.** In light of proposed rules and in consideration of the SEC's heightened focus on cybersecurity disclosures through comment letters and other review processes, public companies, broker-dealers, funds and others should review or establish, as applicable, a process for timely escalation of cyber incidents to appropriate decision-makers. Further, they should also review their disclosure controls and information flow through the company relating to the evaluation of potentially material or otherwise reportable cyber incidents, including those company officers or other personnel who will determine incidents need to be disclosed or reported, as applicable, and approve disclosures). Companies should also consider whether their existing cybersecurity and privacy disclosures (e.g., risk factors and, if applicable, incident or remediation disclosures) are sufficient or whether changes should be implemented in anticipation – or upon adoption – of the proposed rules.
- **Ensure adequate processes for scoping applicable disclosure and reporting standards.** As indicated above, the proposed rules include varying standards for assessing cyber incidents and required disclosures. As such, companies should proactively consider the standard(s) applicable to them under particular situations – i.e., "material" for public companies under Regulation S-K, "significant" for broker-dealers, registered investment advisers and investment companies under the GLBA and "substantial harm or inconvenience" for brokers and dealers, funds and advisers under Regulation S-P. Companies need to be ready to evaluate cyber incidents based on the relevant standard if and when adopted by the SEC and should review their practices of scoping cybersecurity risks and incidents for potential disclosure and consider what updates may be needed in connection with the anticipated adoption of the new cybersecurity rules.
- **Board oversight and engagement.** Boards have responsibility for overseeing material company risks and therefore should be engaged in the oversight of cyber risk and its intersection with company strategy. It is also increasingly common for boards, directly or through the board committee responsible for cyber risk, to receive regular reports from a business's Chief Information Security Officer, or equivalent.
- **Board expertise.** Although there is no requirement for directors to have specific cybersecurity expertise, the proposed rules would require companies to identify directors who do have such expertise in proxy statements, including the name of the board member(s) and such detail necessary to fully describe the expertise. Therefore, companies should begin to gather relevant skills information for their directors and consider whether a search should be conducted for a director with the technology and/or cyber skills to fill any gaps. Public companies should consider adding a question

regarding cyber qualifications to their D&O questionnaires to support the disclosures and determinations regarding their expertise.

* * *

[1] Timing reflects the Securities and Exchange Commission Agency Rule List for Spring 2023 made available during the week of June 12, 2023. See prior Weil blog here for more detail.

[2] The SEC's recent focus on cybersecurity in enforcement include, but are not limited to, recent actions involving the following companies: Blackbaud Inc. (cyber disclosure); J.P. Morgan Securities LLC, UBS Financial Services Inc., and TradeStation Securities, Inc. (insufficient policies and procedures to protect investors from identity theft, in violation of the SEC's Identity Theft Red Flags Rule (Regulation S-ID)); and Morgan Stanley Smith Barney (extensive failures, over a five-year period, to protect the personal identifying information of approximately 15 million customers).

[3] A safe harbor clause clarifies that this disclosure would not impose greater duties, obligations, or liabilities on this person as opposed to a member who does not have cybersecurity expertise.

[4] Another proposed rule, *Outsourcing by Investment Advisers*, would, among other things, require registered investment advisers to conduct diligence, including related to cybersecurity, before onboarding third-party service providers, and monitor such service providers on an ongoing basis. RIN 3235-AN18.

[5] Certain entities subject to Regulation S-P could be impacted by two additional proposals. A proposed amendment to Regulation SCI would expand the scope of that Regulation to additional entities and update requirements including related to cybersecurity, systems management and vendor management. RIN 3235-AN25. A new Cybersecurity Risk Management Rule for broker-dealers, transfer agents, clearing agencies, and several securities-based entities would also require disclosures of cybersecurity risks and incidents. RIN 3235-AN15.

[6] Proposed Rule 204-6.

[7] Proposed Rule 204-6(b). This could include malware that shuts down a company's computer systems, or an incident resulting in significant monetary loss or the theft of personal information.

[8] Proposed Rule 248.30(b)(4)(i).

[9] Proposed Rule 248.30(b).

[10] Proposed Rule 248.30(e)(5)(i).

[11] Proposed Rule 248.30(e)(9)(i).

[12] Proposed Rule 248.30(e)(11).

[13] Under Regulation S-P, a "consumer" is "an individual who obtains or has obtained a financial product or service from you that is to be used primarily for personal, family, or household purposes, or that individual's legal representative," while a customer is a subset of consumers who maintains a continuing customer relationship with the financial institution. 17 C.F.R. § 248.3.

If you have questions concerning the contents of this alert, or would like more information, please speak to your regular contact at Weil or to any of the following:

Authors

Olivia J. Greer	View Bio	olivia.greer@weil.com	+1 212 310 8815
Kaitlin Descovich	View Bio	kaitlin.descovich@weil.com	+1 202 682 7154

Editors

Lyuba Goltser	View Bio	lyuba.goltser@weil.com	+1 212 310 8048
P.J. Himelfarb	View Bio	pj.himelfarb@weil.com	+1 202 682 7208
David Wohl	View Bio	david.wohl@weil.com	+1 212 310 8933