KPMG

Regulatory Alert

Regulatory Insights for Financial Services

February 2022

Cybersecurity: SEC Proposal for Adviser/Fund Risk Management

As SEC Chair Gensler has previously indicated, the SEC is considering several rule changes to strengthen the "cyber hygiene" of SEC registrants. These current proposals, focused on SEC-registered investment advisers and funds, seek to improve business practices around cybersecurity and cyber risks, specifically maintaining the security of data, IT systems, and networks, promoting resiliency and incident response, and addressing the timeliness and materiality of cybersecurity incident notifications and disclosures. Registered investment advisers, investment companies, and investment funds should consider how these proposals will impact their current operations and risk management strategies, as well as reporting and disclosures activities.

The SEC has proposed rules related to cybersecurity risk management that are intended to promote cybersecurity preparedness and resilience for registered investment advisers (advisers) and investment companies (funds). As proposed, the rules would establish several new requirements, as outlined below.

Cybersecurity Risk Management Policies and Procedures

The proposal presents two new rules, Rule 206(4)-9 under the Investment Advisers Act and Rule 38a-2 under the Investment Company Act, that would require both advisers and funds to adopt and implement written policies and procedures "reasonably" designed to address cybersecurity risks. These policies and procedures would be required to address the following general elements:

- **Risk assessments.** Periodic assessment, categorization, prioritization, and documentation of cybersecurity risks related to data and information, IT systems, and service providers.
- **User security and access.** Controls to minimize user-related risks and prevent unauthorized access to information and systems, including consideration of acceptable use policies, multi-factor authentication, tiered access, and remote access controls.
- **Information protection.** Periodic assessment of IT systems and data to protect from unauthorized access or use, including assessing the sensitivity and importance of information to adviser or fund operations, whether certain information is personal information, where and how the information is accessed, controls and malware protections, and the potential impact of a cybersecurity incident on business continuity.
- **Threat and vulnerability management.** Proactive and ongoing detection, mitigation, and remediation of cybersecurity threats and vulnerabilities with respect to information and IT systems, including policies to establish accountability, threat intake processing, assignments, escalations, remediations, and remediation testing.
- **Cybersecurity incident response and recovery.** Measures to detect, respond to, and recover from cybersecurity incidents, including policies and procedures for business continuity, protection of IT systems and information, and cybersecurity incident

communications, both internal and external, to both the SEC and clients.

In addition, the rules would require:

— **Annual Review and Written Reports.** Advisers and funds would be required to review and assess the design and effectiveness of their cybersecurity risk management policies and procedures at least once annually, and prepare a written report noting changes in cybersecurity risk over time.

— **Fund Board Oversight.** Rule 38a-2 would require a fund's board to initially approve a fund's cybersecurity risk management policies and procedures, and to review the annual written report.

— **Recordkeeping.** Proposed amendments to Rule 204-2 would require investment advisers to maintain certain records of their cybersecurity risk management policies and procedures and cybersecurity incidents for a period of five years. Proposed Rule 38a-2 would similarly require investment funds to maintain records of their cybersecurity policies and procedures, and other related records.

Cybersecurity Incident Reporting

Proposed Rule 204-6 would require advisers to report "significant cybersecurity incidents" to the SEC, including on behalf of a client that is a registered investment company or business development company, or a private fund.

— A "significant cybersecurity incident" would be defined as an incident, or group of related incidents, that significantly disrupts or degrades the ability of an adviser, or a private fund client of the adviser, to maintain critical operations or leads to the unauthorized access or use of information and results in substantial harm to the adviser or client or investor in a private fund whose information was accessed.

— A "significant cybersecurity incident" for a fund would be defined similarly and could include cyber events that impact a fund's ability to redeem investors, calculate NAV or otherwise conduct its business.

— "Substantial harm" would be defined to include, but would not be limited to, significant monetary losses, thefts of intellectual property of the adviser, or thefts of personal or proprietary information of the client.

If advisers experience a significant cybersecurity incident, the proposed rules would require them to report the incident by confidentially submitting the proposed new Form ADV-C within 48 hours of recognizing the incident has occurred or is occurring. Additionally, advisers would be required to amend Form ADV-C submissions within 48 hours of recognizing that previous reports are materially inaccurate.

Cybersecurity Risk and Incident Disclosures

The proposal would also amend the advisers' Form ADV Part 2A to require disclosure of both cybersecurity risks and incidents (including incidents other than significant incidents) to current and prospective clients that could materially affect the advisory relationship. "Materiality" in this instance would be based on whether there is a "substantial likelihood" that a reasonable client would consider the information important based on the total mix of facts and information (e.g., disrupt services, compromise data, client harm). Amendments to Rule 204-3(b) would require advisers to deliver interim disclosure amendments to existing clients promptly if the adviser adds or materially revises disclosure of a cybersecurity incident.

Similarly, the proposal amends several forms for funds' disclosure of cybersecurity risks and incidents, including description of any significant cybersecurity incidents that have occurred in the last two fiscal years. These proposals affect Form N-1A, Form N-2, Form N-3, Form N-4, Form N-6, Form N-8B-2, and Form S-6.

The SEC is seeking public comments on the proposed rules. The SEC states the public comment period will remain open for 60 days following the publication of the proposing release on the SEC's website or 30 days following the publication of the proposing release in the Federal Register, whichever period is longer.

For additional information, please contact Matt Miller or Mike Sullivan.

Please refer to:

— Press Release: SEC Proposes Cybersecurity Risk Management Rules and Amendments for Registered Investment Advisers and Funds

— Proposed Rule: Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies

— KPMG Regulatory Alert | SEC Reg SCI Proposal, Future Considerations

— KPMG Regulatory Alert | Cyber incident notifications

Contact the author:

Amy Matsuo
Principal and Leader
Regulatory and ESG Insights
amatsuo@kpmg.com

kpmg.com/socialmedia