FORsights

New Cyber Rules for Investment Funds & Advisers in 2024?

Cybersecurity threats pose an ongoing and escalating risk to investment companies, investors, and market participants. Cybersecurity incidents are becoming more sophisticated and frequent. On February 9, 2022, the SEC issued a proposal that would create new rules to enhance cybersecurity preparedness and improve the resilience of investment companies and advisers against cybersecurity threats and attacks as follows:

- **Require advisers and funds to adopt and implement written policies and procedures that are reasonably designed to address cybersecurity risks**
- **Require advisers to report significant cybersecurity incidents to the SEC on proposed Form ADV-C**
- **Enhance adviser and fund disclosures related to cybersecurity risks and incidents**
- **Require advisers and funds to maintain, make, and retain certain cybersecurity-related books and records**

The SEC's regulatory agenda indicates a final rule is planned before April 2024.

Background

An adviser's fiduciary obligations include steps to minimize operation and other risks that could lead to significant business disruptions or a loss or misuse of client information, which indirectly covers cybersecurity. Under the Investment Company compliance rule, many funds include cybersecurity when developing their compliance policies and procedures. Other rules cover the confidentiality of customer records and information and identity theft. While some funds and advisers have implemented cybersecurity programs under the existing regulatory framework, there are no SEC rules that specifically require firms to adopt and implement comprehensive cybersecurity programs.

Cybersecurity Risk Management Policies & Procedures

The proposal would require all advisers and funds to adopt and implement cybersecurity policies and procedures. Because the size and sophistication of funds and advisers vary widely, the SEC proposal provides flexibility to develop a program by listing required core elements. This process could be done in-house or outsourced to a third party subject to appropriate oversight. Whether the administrators of an adviser's or fund's cybersecurity policies and procedures are in-house or a third party, reasonably designed policies and procedures must empower these administrators to make decisions and escalate issues to senior officers as necessary for the administrator to effectively carry out the role. Reasonably designed cybersecurity policies and procedures generally should specify which groups, positions, or individuals, whether in-house or third party, are responsible for implementing and administering the policies and procedures, including specifying those responsible for communicating incidents internally and making decisions with respect to both SEC reporting and client and investor disclosures.

1. Required Elements

Risk Assessment

The risk assessment should be formally documented and should:

- Categorize and prioritize cybersecurity risks based on an inventory of the components of their information systems, the information residing therein, and the potential effect of a cybersecurity incident on the advisers and funds
- Identify service providers that receive, maintain or process adviser or fund information, or that are permitted to access information systems and identify the cybersecurity risks associated with the use of these service providers. An adviser or fund should consider if a cybersecurity incident at a service provider could lead to the unauthorized access or use of adviser or fund information or technology or process failures. The adviser should consider how the service provider will secure and maintain data and if the service provider has response and recovery procedures in place so that any compromised or lost data can be recovered and restored

User Security & Access

Controls should be designed to minimize user-related risk and prevent the unauthorized access to information systems and would generally include regularly monitored user security and access measures not only to provide access to authorized users, but also to remove access for users that are no longer authorized. Well-designed user access controls should assess the need to authenticate or investigate any unusual customer requests.

Information Protection

Advisers and funds would be required to monitor information systems and protect information from unauthorized access or use, based on a periodic assessment of their information systems and the information that resides on the systems.

Threat & Vulnerability Management

Cybersecurity vulnerabilities present weaknesses in adviser or fund information systems that attackers may exploit. Advisers and funds would be required to detect, mitigate, and remediate cybersecurity threats and vulnerabilities. Ongoing monitoring of vulnerabilities could include conducting network, system, and application vulnerability assessments. This could include scans or reviews of internal systems, externally facing systems, new systems, and systems used by service providers. An adviser or a fund should adopt policies and procedures that establish accountability for handling vulnerability reports, and processes for intake, assignment, escalation, remediation, and remediation testing.

Cybersecurity Incident Response & Recovery

Advisers and funds should have measures to detect, respond to, and recover from a cybersecurity incident. These include policies and procedures that are reasonably designed to ensure:

- Continued operations of the fund or adviser
- The protection of adviser information systems and the information residing therein
- External and internal cybersecurity incident information sharing and communications
- Reporting of significant cybersecurity incidents to the SEC

2. Annual Review & Oversite

Advisers and funds would be required to review their cybersecurity policies and procedures at least annually, which would include:

- Review and assess the design and effectiveness of the cybersecurity policies and procedures, including whether they reflect changes in cybersecurity risk during the year
- Prepare a written report which would—at a minimum—describe the annual review, assessment, and any control tests performed, explain the results, document any cybersecurity incident that occurred since the last report, and discuss any material changes to the policies and procedures since the last report

Proposed Rule 38a-2 would require a fund's board of directors, including a majority of its independent directors, initially to approve the fund's cybersecurity policies and procedures, as well as review the written report on cybersecurity incidents and material changes to the fund's annual cybersecurity policies and procedures.

3. Record-Keeping

Advisers

The proposal would update record-keeping requirements to require advisers to maintain:

- A copy of their cybersecurity policies and procedures that are currently in effect, or were in effect at any time within the past five years
- A copy of the adviser's written report documenting the annual review of its cybersecurity policies and procedures in the last five years
- A copy of any Form ADV-C filed by the adviser in the last five years
- Records documenting the occurrence of any cybersecurity incident, including any records related to any response and recovery from such an incident, in the last five years. This may include event or incident logs, as well as longer descriptions depending on the incident's nature and scope
- Records documenting an adviser's cybersecurity risk assessment in the last five years

Funds

Proposed Rule 38a-2 under the Investment Company Act would require that a fund maintain:

- A copy of its cybersecurity policies and procedures that are currently in effect, or were in effect at any time within the last five years
- Copies of written reports provided to the board
- Records documenting the fund's annual review of its cybersecurity policies and procedures
- Any report of a significant fund cybersecurity incident provided to the SEC by its adviser
- Records documenting the occurrence of any cybersecurity incident, including any records related to any response and recovery from such an incident
- Records documenting the fund's cybersecurity risk assessment

These records would have to be maintained for five years; the first two years in an easily accessible place.

Reporting

Any adviser registered or required to be registered with the SEC would be required to electronically submit new Form ADV-C within 48 hours after having a reasonable basis to conclude that a significant adviser or fund cybersecurity incident had occurred or is occurring. Form ADV-C would include both general and specific questions related to the significant cybersecurity incident, such as the nature and scope of the incident, as well as whether any disclosure has been made to any clients and/or investors. Details include:

- Date incident occurred, date incident was discovered, and whether the incident is ongoing
- Whether law enforcement or a government agency has been notified
- Any actions or planned actions to recover from the incident
- Whether any data was stolen or altered or accessed or used for any other unauthorized purpose
- How the incident affected critical operations, including which systems or services have been affected
- Whether the incident occurred at a service provider. If so, the adviser also should describe the service provided that experienced the incident and how any degradation in those services have affected the adviser's—or its registered and private fund clients'—operations.
- Whether the incident is covered by a cybersecurity insurance policy

Advisers would need to amend any previously filed Form ADV-C within 48 hours if information reported on the form becomes materially inaccurate, if new material information about a previously reported incident is discovered, and after resolving a previously reported incident or closing an internal investigation related to a previously disclosed incident.

> *The reporting trigger is based on the adviser having a **reasonable basis** to conclude that an incident has occurred or is occurring, and not after **definitively concluding** that an incident has occurred or is occurring.*

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

> *While most information on Form ADV-C is made publicly available, the SEC had concluded that public disclosure of cybersecurity incidents would adversely affect advisers and funds and this information would be kept confidential.*

Disclosure

While many advisers and funds already provide disclosure about cybersecurity risks, the proposal would update current reporting and disclosure requirements to address cybersecurity risks and incidents more directly. Under new Item 20 of publicly available Form ADV, advisers must describe, in plain English, cybersecurity risks that could materially affect the advisory services they offer and how they assess, prioritize, and address cybersecurity risks created by their business's nature and scope. A cybersecurity risk, regardless of whether it has led to a significant cybersecurity incident, would be material to an adviser's advisory relationship with its clients if there is a substantial likelihood that a reasonable client would consider the information important based on the total mix of facts and information. In assessing materiality, advisers should consider the likelihood and extent to which the cybersecurity risk or resulting incident:

- Could disrupt (or has disrupted) the adviser's ability to provide services, including the disruption duration
- Could result (or has resulted) in the loss of adviser or client data, including the nature and importance of the data and the circumstances and duration in which it was compromised
- Could harm (or has harmed) clients, *e.g.*, inability to access investments, illiquidity, or exposure of confidential or sensitive personal or business information

The proposal would require advisers to describe any cybersecurity incidents that occurred within the last two fiscal years that have significantly disrupted or degraded the adviser's ability to maintain critical operations, or that have

led to the unauthorized access/use of adviser information, resulting in substantial harm to the adviser or its clients. Advisers would be required to identify the entity or entities affected; when the incidents were discovered and whether they are ongoing; whether any data was stolen, altered, or accessed or used for any other unauthorized purpose; the effect of the incident on the adviser's operations; and whether the adviser or service provider has remediated or is currently remediating the incident.

In general, advisers are not required to deliver interim brochure amendments to existing clients unless the amendment includes certain disciplinary information. The proposal would add a requirement to deliver interim brochure amendments to existing clients promptly if the adviser adds disclosure of a cybersecurity incident to its brochure or materially revises information already disclosed in its brochure about a cybersecurity incident.

Fund Registration Statements

Funds would be required to provide prospective and current investors with a description of any significant fund cybersecurity incident that has occurred in its last two fiscal years and whether a significant fund cybersecurity incident has or is currently affecting the fund or its service providers.

The required disclosure is similar to the new information in Form ADV. A description of each significant fund cybersecurity incident is needed, including the following information to the extent known: the entity or entities affected; when the incident was discovered and whether it is ongoing; whether any data was stolen, altered, or accessed or used for any other unauthorized purpose; the effect of the incident on the fund's operations; and whether the fund or service provider has remediated or is currently remediating the incident.

Conclusion

The asset management team at Forvis Mazars has more than 50 years of experience providing accounting, tax, and consulting services to various types of investment holdings, including conventional debt and equity investments, loans, businesses, alternative investments, and other unique assets. As of June 2023, Convergence Optimal Performance ranked Forvis Mazars as a top 20 accounting and audit firm to registered investment advisers. Forvis Mazars also was ranked in the top 20 by AUM. We have experience providing services to funds ranging from emerging managers to $100-plus billion in AUM. Our knowledge allows us to provide tailored services to help meet your unique needs. We provide services to private, public, and Cayman funds. For more information, visit forvismazars.us.

Contributors

Brian Matlock

Partner/Financial Services

National Asset Management Leader

brian.matlock@us.forvismazars.com

FORsights

Anne Coughlan
Director
anne.coughlan@us.forvismazars.com