SEC PROPOSES CYBERSECURITY RISK MANAGEMENT RULES FOR INVESTMENT ADVISERS AND FUNDS

Date: 9 March 2022

U.S. Asset Management and Investment Funds Alert

By: Abigail P. Hemnes, Marguerite W. Laurent, Keri E. Riemer, Cal J. Gilmartin, Haley E. Hohensee

Sections:

I. INTRODUCTION AND SUMMARY

On 9 February 2022, the U.S. Securities and Exchange Commission (the SEC) proposed new rules and amendments to existing rules (together, the Proposed Rules)[1] addressing cybersecurity risk management under the Investment Advisers Act of 1940, as amended (the Advisers Act) and the Investment Company Act of 1940, as amended (the 1940 Act).

The Proposed Rules would apply to investment advisers that are registered or required to be registered with the SEC (advisers) and registered investment companies and closed-end companies that elect to be treated as business development companies under the 1940 Act (BDCs, and, together with registered investment companies, registered funds) and would require:

- Policies and Procedures – Advisers and registered funds to adopt and implement written policies and procedures, including specific enumerated elements, reasonably designed to address cybersecurity risks;

- Reporting – Advisers to report certain cybersecurity incidents to the SEC on new Form ADV-C within 48 hours, including on behalf of any registered funds or private funds that experience such incidents; and
- Disclosure – Advisers and registered funds to disclose cybersecurity risks and incidents in their disclosure documents.

In addition, the SEC proposed corresponding amendments to certain recordkeeping rules that would obligate advisers and registered funds to maintain for five years copies of cybersecurity policies, reports of annual reviews, Form ADV-C filings, incident records, and risk assessments.

> Although the Proposed Rules apply specifically to registered funds and advisers that are registered or required to be registered with the SEC, private funds, non-U.S. investment funds and other investment products managed by such advisers will be indirectly impacted by the implementation of the compliance, reporting and disclosure requirements being applied to their advisers.

The Proposed Rules demonstrate the SEC's continued focus on cybersecurity risks, signaled through public statements by SEC Chairman Gary Gensler,[2] risk alerts published by the SEC's Division of Examinations,[3] and inclusion of the topic on recent SEC agendas.[4] The SEC's release (the Proposing Release) notes that advisers and registered funds are an integral part of the financial markets and "increasingly depend on technology for critical business operations,"[5] including substantial reliance on service providers to perform certain activities, such as custody and transfer agency services. The proposed reforms are intended to address the SEC's concerns for client and investor protection and transparency of information about cybersecurity incidents. In addition, the proposed new reporting requirements are intended to assist the SEC in its oversight role.

While the Proposed Rules could, if adopted, help to advance the SEC's objectives, they would also increase the burden, and potentially the liability, for advisers and registered funds, particularly when overseeing and contracting with service providers. Although advisers and registered funds currently engage in initial due diligence and ongoing oversight of their service providers' practices, the proposed rules would impose an explicit and substantial duty on advisers and registered funds to address risks directly faced by their respective service providers' systems and activities, which, in the event of a cybersecurity incident affecting such a service provider, could impact an adviser or registered fund. Registered fund boards would also need to consider the appropriate level of board oversight and review of these service provider cybersecurity concerns.

The public comment period will remain open until 11 April 2022.

II. CYBERSECURITY RISK MANAGEMENT POLICIES AND PROCEDURES

> The Proposed Rules would require advisers and registered funds to adopt and implement policies and procedures that are reasonably designed to address cybersecurity risks based on an ongoing analysis of specific elements.

Proposed new Rule 206(4)-9 under the Advisers Act and proposed new Rule 38a-2 under the 1940 Act would require advisers to registered funds[6], separately managed accounts, and private funds (e.g., hedge funds), and registered funds, respectively, to adopt and implement policies and procedures reasonably designed to address "cybersecurity risks" (the Proposed Risk Management Rules). The Proposed Risk Management Rules would define a "cybersecurity risk" as the "financial, operational, legal, reputational, and other adverse consequences that could stem from cybersecurity incidents, threats, and vulnerabilities."[7]

The Proposing Release notes that reasonably designed cybersecurity policies and procedures should indicate which groups, positions, or individuals (whether in-house or third-party) are responsible for implementing and administering the policies and procedures, including communicating incidents internally and making decisions with respect to reporting to the SEC and disclosing to clients and investors certain incidents. Such policies and procedures must also be reasonably designed to protect against any anticipated threats or hazards, unauthorized access to, or use of customer records or information that could result in substantial harm or inconvenience to any customer.

As the SEC observed in the Proposing Release, the Proposed Risk Management Rules would not be the first regulations to require advisers and registered funds to consider cybersecurity and the risks presented by cybersecurity incidents in the context of developing their policies and procedures.[8]

It is worth noting that proposed Rule 206(4)-9 is grounded in the antifraud provision, Section 206, of the Advisers Act. Section 206 is an area of law that is at times applied broadly by the SEC in enforcement actions, and tying the new requirement to the antifraud provision may be intended to encourage advisers to prioritize cybersecurity.

a. Required Elements

Consistent with Rule 206(4)-7 under the Advisers Act and Rule 38a-1 under the 1940 Act regarding adviser and registered fund compliance policies and procedures, respectively, the SEC is proposing that the Proposed Risk Management Rules would permit advisers and registered funds to tailor their cybersecurity policies and procedures to the nature and scope of their business and their specific cybersecurity risks. However, the Proposed Risk Management Rules identify certain "core" areas that would be required when adopting, implementing, reassessing, and updating cybersecurity policies and procedures:

- Risk Assessment – Advisers and registered funds would be required "periodically" to assess, categorize, prioritize, and draft written documentation of the cybersecurity risks associated with their information systems and the information residing therein in light of the firm's particular operations.

The Proposing Release does not indicate what the SEC means by "periodic." The Proposed Risk Management Rules would require advisers and registered funds to review their cybersecurity policies and procedures no less frequently than annually and reassess and reprioritize their cybersecurity risks periodically as changes that affect these risks occur, rather than at specified intervals. Such changes might include internal changes relating to the online nature of the business or external changes driven by the evolution of cybersecurity threats.

This may imply that the SEC intends for this assessment to occur on a more frequent real-time basis dependent on the adviser's or registered fund's specific circumstances. The Proposing Release notes international operations, insider threats, or remote/travelling employees as examples of the different risks that may arise from a firm's specific operations. Specifically, when conducting this assessment, an adviser or registered fund would need to:

- Categorize and prioritize cybersecurity risks based on an inventory of their information systems, the information they contain, and the potential effect of a cybersecurity event on the adviser or registered fund; and
- Identify those of their service providers that receive, maintain, or process adviser or registered fund information or that are permitted to access their information systems.[9]

In addition, the proposed rule would require written documentation of any risk assessment.

- User Security and Access – Advisers and registered funds would be required to implement controls designed to minimize user-related risks and prevent the unauthorized access to information and systems. Specifically, policies and procedures must:
  - Require standards of behavior for individuals authorized to access adviser or registered fund information systems and any adviser or registered fund information residing therein, such as an acceptable use policy;
  - Identify and authenticate individual users, including by implementing authentication measures that require users to present a combination of two or more credentials for access verification;
  - Establish procedures for the timely distribution, replacement, and revocation of passwords or methods of authentication;
  - Restrict access to specific adviser or registered fund information systems or components thereof and adviser or registered fund information residing therein solely to individuals requiring access to such systems and information as is necessary for them to perform their responsibilities and functions on behalf of the adviser or registered fund; and
  - Secure remote access technologies used to interface with adviser or registered fund information systems.

In implementing the proposed controls, the Proposing Release notes that advisers and registered funds should consider what measures are necessary for clients and investors—not just their own adviser or registered fund personnel—that have access to information systems and information contained therein. The Proposing Release notes as an example that an adviser or registered fund may implement measures that monitor unauthorized login attempts, account lockouts, and the handling of customer requests (e.g., username and password changes). It also notes that advisers and registered funds should also consider their practices with respect to securing remote network access and teleworking when defining the network perimeter and take into account the types of technology through which its users access adviser or registered fund information systems (e.g., mobile devices or personal or employer-owned equipment).

- Information Protection – Advisers and registered funds would be required to monitor information systems and protect information from unauthorized access or use based on a “periodic” assessment of the advisers' or registered funds' systems and the information residing therein to determine what methods to implement to prevent unauthorized access or use of the data. These assessments should consider:
  - The sensitivity level and importance of adviser or registered fund information to its business operations;

- Whether any adviser or registered fund information is personal information;
- Where and how adviser or registered fund information is accessed, stored, and transmitted, including the monitoring of information in transmission;
- Information system access controls and malware protection; and
- The potential effect of a cybersecurity incident involving adviser or registered fund information on the adviser or registered fund and its clients or shareholders (including, with respect to an adviser, the ability to continue providing investment advice or, with respect to a registered fund, the ability to continue providing services).

This element would also require advisers and registered funds to oversee any service providers that receive, maintain, or process adviser or registered fund information or are otherwise permitted to access their information systems and any information residing therein. In identifying cybersecurity risks, an adviser or registered fund should consider the service provider's cybersecurity practices, including whether any systems used have the resiliency and capacity to process transactions in an accurate, timely, and efficient manner and their capability to protect information and systems.[10]

An adviser or registered fund would also be required to document that it is requiring such service providers, pursuant to a written contract, to implement and maintain appropriate measures, including measures similar to the elements the adviser or registered fund must address in its own cybersecurity policies and procedures, designed to protect adviser or registered fund information and systems.

This could require advisers and registered funds to amend numerous existing contracts to modernize or add terms relating to cybersecurity, information protection, and business continuity and could potentially extend liability for service provider cybersecurity incidents to advisers and registered funds that have not adequately engaged in this required oversight.

- Threat and Vulnerability Management – Advisers and registered funds would be required to have measures to detect, mitigate, and remediate cybersecurity threats and vulnerabilities with respect to their information and systems.[11] The Proposed Risk Management Rules would define a “cybersecurity threat” as “any potential occurrence that may result in an unauthorized effort to adversely affect the confidentiality, integrity or availability of [an adviser's or a registered fund's] information systems or any [adviser or registered fund] information residing therein.”[12] A “cybersecurity vulnerability” is proposed to be defined as “a vulnerability in [an adviser's or a registered fund's] information systems, information system security procedures, or internal controls, including vulnerabilities in their design, maintenance, or implementation that, if exploited, could result in a cybersecurity incident.”[13]

In implementing this element, the Proposing Release notes that advisers and registered funds should monitor vulnerabilities on an ongoing basis, such as by conducting network, system, and application vulnerability reviews and considering new threat and vulnerability information from industry and government sources. The Proposing Release also notes that advisers and registered funds should adopt policies and procedures that establish accountability for handling vulnerability reports; establish processes for intake, assignment, escalation, remediation, and remediation testing; and consider role-specific cybersecurity threat and vulnerability response training.

- Cybersecurity Incident Response and Recovery – Advisers and registered funds would be required to have measures to detect, respond to, and recover from a cybersecurity incident, including policies and procedures reasonably designed to ensure:
  - Continued operations of the adviser or registered fund;
  - Protection of adviser or registered fund information systems and the adviser or registered fund information residing therein;
  - External and internal cybersecurity incident information sharing and communications; and
  - Reporting of significant cybersecurity incidents to the SEC.

As described in the Proposing Release, incident response plans should designate personnel to perform specific roles in the case of a cybersecurity incident and have a clear escalation protocol to ensure that senior officers, and for a registered fund, the board, receive necessary information regarding cybersecurity incidents on a timely basis.

In connection with this element, the SEC is requesting comment on whether advisers and registered funds should be required to respond to cybersecurity incidents within a specific timeframe.

b. Annual Reviews and Written Reports

The Proposed Risk Management Rules would also require advisers and registered funds to, at least annually:

- Review and assess the design and effectiveness of the cybersecurity policies and procedures, including whether they reflect changes in cybersecurity risks over the time period covered by the review; and
- Prepare a written report that, at a minimum, describes the annual review, assessment, and any control tests performed; explains the results thereof; documents any cybersecurity incidents that occurred since the date of the last report; and discusses any material changes to the policies and procedures since the date of the last report.

c. Registered Fund Board Oversight

> Registered fund boards would be required to actively engage in the oversight of a registered fund's cybersecurity policies and procedures.

Proposed Rule 38a-2 would require a registered fund's board of directors/trustees (directors), including a majority of its independent directors, to initially approve the registered fund's cybersecurity policies and procedures and review the written report on cybersecurity incidents and any material changes to the registered fund's cybersecurity policies and procedures described above. The Proposing Release states:

These requirements are designed both to facilitate the board's oversight of the [registered] fund's cybersecurity program and provide accountability for the administration of the program. These requirements also would be consistent with a board's duty to oversee other aspects of the management and operations of a [registered] fund. Board oversight should not be a passive activity, and the requirements for the board to initially approve the

[registered] fund's cybersecurity policies and procedures and thereafter to review the required written reports are designed to assist directors in understanding a [registered] fund's cybersecurity risk management policies and procedures, as well as the risks they are designed to address.

The Proposing Release also notes that, consistent with how directors may satisfy their obligations under Rule 38a-1 of the 1940 Act, directors may satisfy their obligation with respect to the initial approval of a registered fund's cybersecurity policies and procedures by reviewing summaries prepared by persons who administer them. In performing its oversight duties, a board should initially seek information to understand the potential cybersecurity risks and the salient features and operations of the program. The proposed ongoing board reporting should provide directors the information necessary to enable them to ask questions or seek additional information regarding the "effectiveness of the program and its implementation, and whether the [registered] fund has adequate resources with respect to cybersecurity matters, including access to cybersecurity expertise."[14]

The Proposing Release indicates that a board should consider whether, based on the registered fund's operations, the level of the board's oversight over the registered fund's service providers with regard to cybersecurity is appropriate. Notably, it also requests comment as to whether boards should be required to approve the cybersecurity policies and procedures of certain registered fund service providers, such as its investment adviser, principal underwriter, administrator, or transfer agent. Such a requirement would likely impose significant oversight responsibilities on registered fund boards.

The Proposing Release does not reference the standard of review that would apply for the various proposed board considerations, such as whether the business judgment rule would apply. With respect to board oversight, the Proposing Release seeks comment on whether the SEC should require boards to base their approval of the policies and procedures on any particular finding (e.g., that the policies and procedures are reasonably designed to prevent violations of the Federal securities laws or reasonably designed to address the registered fund's cybersecurity risks). It also seeks comment on whether a board, or some designee thereof (such as a subcommittee or cybersecurity expert), should have oversight over the registered fund's risk assessments of service providers. Such a requirement would also impose additional responsibility on registered fund boards.

Although the Proposing Release does not connect a board's oversight of cybersecurity risk management to the annual review of an advisory contract under Section 15(c) of the 1940 Act, a registered fund's board may consider whether to expand information requests relating to cybersecurity, business continuity, and disaster recovery as part of the Section 15(c) process in light of the Proposed Rules. Directors may also determine to oversee cybersecurity in a manner consistent with compliance program reviews performed pursuant to Rule 38a-1 of the 1940 Act.

III. REPORTING SIGNIFICANT CYBERSECURITY INCIDENTS TO THE SEC

> The Proposed Rules define "significant cybersecurity incidents" for advisers and funds that would need to be reported to the SEC.

Under proposed Rule 204-6 of the Advisers Act, advisers would be required to report significant cybersecurity incidents to the SEC on new Form ADV-C, including on behalf of any registered funds and private funds (defined

as issuers that would be investment companies as defined in the 1940 Act but for Section 3(c)(1) or 3(c)(7) of the 1940 Act) that experience such incidents. The reports would have to be made promptly but in no event later than 48 hours after having a reasonable basis to conclude that a "significant adviser cybersecurity incident" or "significant fund cybersecurity incident" has occurred or is occurring.[15] The new Form ADV-C would gather information regarding the nature and scope of the incident (e.g., actions to recover and whether information was stolen, altered, or accessed), whether shareholders/clients or law enforcement were notified, and whether the incident is covered under a cybersecurity insurance policy.

As proposed, the term "significant adviser cybersecurity incident" would mean a cybersecurity incident or group thereof 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 substantial harm to the adviser, or substantial harm to a client, or an investor in a private fund, whose information was accessed.

Similarly, the term "significant fund cybersecurity incident" would be defined in Rule 38a-2 under the 1940 Act as a cybersecurity incident or group thereof that significantly disrupts or degrades the registered fund's ability to maintain critical operations, or leads to the unauthorized access or use of registered fund information, where the unauthorized access or use of such information results in substantial harm to the registered fund or to an investor whose information was accessed.

Although the Proposed Rules do not define the term "substantial harm," the Proposing Release indicates that significant monetary loss; theft of intellectual property; theft of personally identifiable or proprietary information of personnel, directors, clients or investors; or disruptions to critical operations, such as the ability to implement investment strategies, process or record transactions, or communicate with clients or investors, would be some examples of substantial harm. The Proposing Release also notes that the SEC views critical operations as including investment, trading, reporting, and risk management of an adviser or fund, as well as operating in accordance with the Federal securities laws.

> Proposed new Form ADV-C would be a structured check-the-box and fill-in-the-blank format and include both general and specific questions related to the significant cybersecurity incident.

Although the Proposed Rules would require certain cybersecurity-related disclosures (as described below), the Form ADV-C reports would not be publicly available. Rather, they are intended to help the SEC monitor and evaluate the effects of a cybersecurity incident on an adviser or fund and its clients and investors and potentially market-wide events. However, in a request for comment, the SEC asked whether it should require public disclosure of some or all of the information included in Form ADV-C in a final rule.

In connection with this reporting requirement, the SEC has requested comment on, among other things, whether it should exclude incidents that affect private fund clients or registered funds; whether advisers should be required to report on significant cybersecurity incidents affecting additional investment products, such as pooled investment vehicles that rely on the exemption from the definition of "investment company" in Section 3(c)(5)(C) of the 1940 Act; and whether advisers should also account for "inconvenience" in the definition of significant adviser and fund cybersecurity incidents (which would arguably expand the reporting requirement).

IV. DISCLOSURE OF CYBERSECURITY RISKS AND INCIDENTS

a. Requirements for Advisers

> Advisers would be required to disclose in their Form ADV Part 2A brochures certain material cybersecurity risks and certain cybersecurity incidents that occurred within the last two fiscal years.

The Proposed Rules would amend Form ADV Part 2A to explicitly require advisers to describe in their brochures cybersecurity risks that could materially affect the advisory services they offer and how they assess, prioritize, and address cybersecurity risks created by the nature and scope of their business.[16] Advisers would also be required 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 led to the unauthorized access or use of adviser information, resulting in substantial harm to the adviser or its clients. In providing these disclosures, 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, 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. The SEC believes that such information would allow investors to make more informed decisions when deciding whether to initially engage - or remain with - an adviser.

Notably, although advisers are only currently required to deliver to existing clients interim brochure amendments in certain limited circumstances, the proposed rule amendments would require an adviser to deliver such amendments “promptly” if the adviser adds disclosure of a cybersecurity incident to its brochure or materially revises information already disclosed about such an incident.[17]

b. Requirements for Registered Funds

> Registered Funds will be required to disclose any principal cybersecurity risks and significant fund cybersecurity incidents that occurred in the last two fiscal years, as well as whether a significant fund cybersecurity incident has or is currently affecting the registered fund or its service providers.

Under the Proposed Rules, registered funds would also be required to provide prospective and current investors with disclosure about significant cybersecurity incidents. The Proposed Rules include amendments to registered funds' registration statement forms (e.g., Form N-1A, Form N-2) that would require a description of any significant fund cybersecurity incident that has occurred in its last two fiscal years, as well as whether a significant fund cybersecurity incident has or is currently affecting the registered fund or its service providers.[18] Registered funds would be required to disclose, 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 registered fund's operations; and whether the registered fund or service provider has remediated or is currently remediating the incident. The Proposing Release notes that a registered fund should also consider cybersecurity risk disclosure, and whether such disclosure should be included in its prospectus as a principal risk of investing in the registered fund.

Registered funds would also be required to supplement their prospectuses to disclose any cybersecurity risks and significant fund cybersecurity incidents. In addition, the Proposing Release states that registered funds should generally include in their annual reports to shareholders a discussion of cybersecurity risks and significant fund cybersecurity incidents, to the extent that these were factors that materially affected performance of the registered fund during the past fiscal year.

V. RECORDKEEPING

Under the Proposed Rules, an adviser would be required to maintain for a prescribed period of time copies of the proposed new cybersecurity policies and procedures that are in effect (or at any time within the past five years were in effect), the adviser's written report documenting the annual review of its cybersecurity policies and procedures, 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, and records documenting the adviser's cybersecurity risk assessment in the last five years.

Similarly, a registered fund would be required to maintain for a prescribed period of time copies of its cybersecurity policies and procedures that are in effect (or at any time within the last five years were in effect), written reports provided to its board, records documenting the registered 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, and records documenting the occurrence of any cybersecurity incident (including any records related to any response and recovery from such an incident), and records documenting the registered fund's cybersecurity risk assessment.

VI. SUMMARY AND KEY DATES

Although the final rules may vary from the Proposed Rules, advisers and registered funds should prepare for an increased risk of enforcement action related to cybersecurity governance and risk management in light of the SEC's focus in this area. As noted above, proposed Rule 206(4)-9 is grounded in Section 206 of the Advisers Act, which applies to fraudulent, deceptive, or manipulative acts by an adviser, thus increasing the risk of monetary penalties and other sanctions for cybersecurity related incidents or matters. Additionally, registered funds and their directors will need to reconsider the manner in which they exercise their oversight responsibilities with respect to the cybersecurity governance and risk management programs of advisers and other service providers. While the SEC has recognized that each registered fund and adviser must consider the cybersecurity risks unique to their particular circumstances, the Proposed Rules outline specific required elements and demonstrate the SEC's intention to hold all regulated entities accountable for cybersecurity compliance to a heightened degree.

FOOTNOTES

[1] See U.S. SEC. & EXCH. COMM'N, CYBERSECURITY RISK MANAGEMENT FOR INVESTMENT ADVISERS, REGISTERED INVESTMENT COMPANIES, AND BUSINESS DEVELOPMENT COMPANIES (Feb. 9, 2022), https://www.sec.gov/rules/proposed/2022/33-11028.pdf [hereinafter Proposing Release].

[2] U.S. Sec. & Exch. Comm'n Chair Gary Gensler, *Testimony Before the United States Senate Committee on Banking, Housing, and Urban Affairs* (Sept. 14, 2021), https://www.sec.gov/news/testimony/gensler-2021-09-14;

U.S. Sec. & Exch. Comm'n Chair Gary Gensler, Remarks at the Northwestern Pritzker School of Law's Annual Securities Regulation Institute (Jan. 24, 2022), https://www.sec.gov/news/speech/gensler-cybersecurity-and-securities-laws-20220124.

[3] U.S. SEC. & EXCH. COMM'N, RISK ALERT: CYBERSECURITY: RANSOMWARE ALERT (July 10, 2020), https://www.sec.gov/files/Risk%20Alert%20-%20Ransomware.pdf; U.S. SEC. & EXCH. COMM'N, RISK ALERT: CYBERSECURITY: SAFEGUARDING CLIENT ACCOUNTS AGAINST CREDENTIAL COMPROMISE (Sept. 15, 2020), https://www.sec.gov/files/Risk%20Alert%20-%20Credential%20Compromise.pdf.

[4] U.S. SEC. & EXCH. COMM'N, UNIFIED AGENDA OF REGULATORY AND DEREGULATORY ACTIONS (June 11, 2021), https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202110&RIN=3235-AM89.

[5] Proposing Release, supra note 1, at 6.

[6] This requirement applies to advisers to all funds registered under the 1940 Act, including, but not limited to exchange-traded funds, unit investment trusts, and BDCs.

[7] Proposing Release, *supra note* 1, at 20 n.28.

[8] For example, Regulation S-P requires applicable advisers and registered funds to adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information. Regulation S-ID requires applicable advisers and registered funds to develop and implement written identity theft programs. However, the SEC has not yet adopted specific rules that require advisers or registered funds to adopt and implement comprehensive cybersecurity programs. In introducing the Proposed Risk Management Rules, the SEC seems to be indicating its concern that this gap may expose clients and investors to risks that could potentially be mitigated by the implementation of robust cybersecurity programs.

[9] The SEC notes that because many advisers and registered funds are exposed to cybersecurity risks through such service providers' technology, the risk assessment must also consider the cybersecurity risks relating to those arrangements. For example, advisers that use service providers for trade order management systems that allow the adviser to automate all or some of the adviser's trading should consider any cybersecurity risks presented by these services

[10] The Proposing Release notes that such policies and procedures generally should also include other oversight measures, such as due diligence procedures or periodic contract review processes, that allow advisers and registered funds to assess whether, and help to ensure that, their agreements with service providers contain provisions requiring service providers to implement and maintain appropriate measures designed to protect adviser or registered fund information and systems (e.g., notifying the adviser or registered fund of cybersecurity incidents that adversely affect the adviser's or registered fund's information, systems, or operations).

[11] Once identified, advisers and registered funds would need to mitigate and remediate any identified threat or vulnerability with a particular focus on minimizing the window of opportunity for attackers to exploit vulnerable hardware and software, such as by implementing a patch management program to ensure timely patching of hardware and software vulnerabilities and maintaining a process that tracks and addresses reports of vulnerabilities.

[12] Proposing Release, *supra note* 1, at 21 n.32.

[13] *Id.* at 30 n.42.

[14] *Id.* at 42.

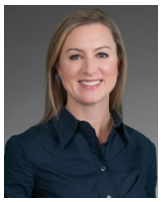
[15] Proposed rule 204-6 would also require advisers to amend any previously filed Form ADV-C promptly, but in no event more than 48 hours, after information reported on the form becomes materially inaccurate; if new material information about a previously reported incident is discovered; and after resolving a previously reported incident or closing an internal investigation pertaining to a previously disclosed incident. The filing of Form ADV-C reports should be addressed in the policies and procedures discussed above.

[16] 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. The facts and circumstances relevant to determining materiality in this context may include, among other things, 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 duration of such a disruption; 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; or could harm (or has harmed) clients.

[17] Given the potential effect that significant cybersecurity incidents could have on an adviser's clients—such as exposing their personal or other confidential information or resulting in losses in their accounts—the SEC believes that requiring an adviser to promptly deliver the brochure amendment would enhance investor protection by enabling clients to take protective or remedial measures to the extent appropriate.

[18] Registered funds would be required to tag this information in Inline eXtensible Business Reporting Language (Inline XBRL).

KEY CONTACTS



ABIGAIL P. HEMNES
PARTNER

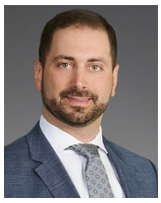
BOSTON
+1.617.951.9053
ABIGAIL.HEMNES@KLGATES.COM

MARGUERITE W. LAURENT
PARTNER

WASHINGTON DC
+1.202.778.9403
MARGUERITE.LAURENT@KLGATES.COM

KERI E. RIEMER
OF COUNSEL

NEW YORK
+1.212.536.4809
KERI.RIEMER@KLGATES.COM



CAL J. GILMARTIN
PARTNER

BOSTON
+1.617.951.9103
CAL.GILMARTIN@KLGATES.COM

