MAYER | BROWN

APRIL 13, 2022

US SEC CYBER RISK MANAGEMENT PROPOSED RULES: ANALYSIS FOR INVESTMENT ADVISERS, INVESTMENT COMPANIES, BDCS AND BROADER IMPLICATIONS FOR PRIVATE SECTOR

AUTHORS: RAJESH DE, ADAM D. KANTER, LESLIE S. CRUZ, JENNIFER L. WEINBERG

On February 9, 2022, the Securities Exchange Commission ("SEC" or "Commission") voted 3-1 to propose rules, forms and amendments concerning cybersecurity risk management, as well as registered investment adviser and fund disclosures. As we have previously discussed, the proposal under the Investment Advisers Act of 1940 (Advisers Act) and the Investment Company Act of 1940 (Investment Company Act) seeks to set out specific requirements for cybersecurity risk management for registered investment advisers (RIAs), registered investment companies ("RICs," including mutual funds, exchange-traded funds (ETFs), unit investment trusts (UITs), and closed-end funds) and business development companies (BDCs)[1] and related amendments to certain rules and forms that govern RIA and fund disclosures.

The proposed rules would require registered advisers and funds to "adopt and implement written cybersecurity policies and procedures reasonably designed to address cybersecurity risks," report significant cybersecurity incidents to the SEC, and disclose cybersecurity risks and incidents occurring in the past two years in Form ADV, Part 2A and fund registration statements.[2] According to SEC Chair Gary Gensler, this proposal aims to "enhance cybersecurity preparedness and could improve investor confidence in the resiliency of advisers and funds against cybersecurity threats and attacks."[3] Additionally, the proposal's reporting requirements would seek to provide the SEC with key information about cybersecurity incidents and responses to enhance its examination and enforcement capabilities.

Although the proposed rules remain subject to comment, in many ways they reflect preexisting SEC expectations for how regulated entities should manage cybersecurity risks and report cybersecurity incidents.[4] For example, the SEC has repeatedly included information security among its examination priorities for RIAs and funds. In March 2021, the SEC announced that its 2021 exams would focus on a variety of information security measures, including "controls surrounding online and mobile application access to investor account information," and "policies and procedures to protect investor records and information," among others.[5] The SEC has highlighted cybersecurity risks arising out of its observations from such examinations. For example, in September 2020, the Office of Compliance Inspections and Examinations (OCIE) released a risk alert to highlight the threat of "credential stuffing," and encouraged firms and advisers to "review their customer account protection safeguards and identity theft prevention programs and consider whether updates to such programs or policies are warranted to address emergent risks."[6]

In addition to building on the Commission's long-established focus on cybersecurity, the proposal also

highlights the preexisting regulatory framework applicable to RIA and fund cybersecurity. For investment advisers, this includes fiduciary duties, the Advisers Act compliance rule,[7] and, for most investment advisers, Regulation S-P,[8] which requires the adoption of written policies and procedures to protect customer information, and Regulation S-ID,[9] which requires the implementation of an identity theft program. For funds, this includes the Investment Company compliance rule,[10] as well as, for many funds, Regulation S-P and Regulation S-ID.[11]

Taken together, under these and other rules, as well as based on SEC Risk Alerts, examination priorities and recent enforcement actions, most RIAs and funds currently consider and address cybersecurity risks. However, the Commission acknowledges that "there are no Commission rules that specifically require firms to adopt and implement comprehensive cybersecurity programs" and that, based on examinations, it appears that not all funds and advisers are taking the appropriate steps to mitigate cybersecurity risks.[12] This perspective is reflected in recent SEC enforcement actions premised on cybersecurity issues. Most notably, in August 2021, the SEC announced multiple actions sanctioning broker-dealers and/or investment advisory firms for deficiencies in their cybersecurity policies and procedures and disclosures following incidents.[13]

This Legal Update builds on our previous discussion of this proposal and discusses some of its major implications for registrants. Notably, the proposal imposes new cybersecurity incident reporting and related disclosure requirements on registered investment advisers and funds. In addition, the impact of the proposal would likely extend beyond the registered funds and advisers directly subject to them. Although funds and advisers generally do, and are expected to, oversee their service providers, including with respect to cybersecurity, the proposal imposes specific cybersecurity oversight responsibilities on registered advisers and funds for certain third parties they engage, including those that are not otherwise directly regulated by the SEC. If adopted in its current form, this proposal might trigger new pressures on service providers and vendors across the registered adviser and fund ecosystem to meet the cybersecurity expectations of advisers and funds. Because registered advisers and funds would be required to evaluate their existing vendor and service provider relationships and related cybersecurity risks, advisers and funds might choose to only work with service providers that are committed to proactive cybersecurity mitigation and otherwise meet the cybersecurity expectations of their adviser and fund business partners.

Below, we highlight some key takeaways from the SEC's proposal. We then examine specific elements of the proposal, which include: (1) cybersecurity risk management policies and procedures, (2) annual review and required written reports, (3) fund board oversight, (4) recordkeeping, (5) reporting of significant cybersecurity incidents to the SEC and (6) disclosure of cybersecurity risks and incidents. Finally, we consider the prospect for additional regulation of cybersecurity in the securities industry.

I. Major Takeaways from the Proposal

- ***Broad scope.*** The proposal has a broad scope, encompassing activities and operations central to an advisory business (including valuation, trading, issuer and other data access and importing)[14] as well as operations beyond the provision of advisory services. For example, the proposed rules appear to impose substantive cybersecurity requirements on *all* aspects of the adviser's business operations, including internal and non-client facing business activities, and potentially reach non-advisory lines of business conducted by the adviser, as well as the operations and systems of certain advisory affiliates.

- ***New confidential Form ADV-C requirements.*** The proposal would require registered advisers to adhere to strict incident reporting requirements. First, advisers must report a "significant cybersecurity incident" to the SEC within 48 hours of having a "reasonable basis" to conclude that an incident has occurred or is occurring. Second, advisers must amend any previously filed notice promptly but no later

than 48 hours after discovering new, material information, learning that information previously reported has become materially inaccurate, or resolving or closing an investigation regarding a previously reported incident. Responding to a cybersecurity incident is a fluid and time-sensitive process. Newly identified information can rapidly alter a firm's understanding of an incident's scope or impact. If adopted as proposed, advisers will need to consider how to actively and responsibly manage these new reporting requirements throughout the incident response process.

- ***Service provider oversight.*** The proposal highlights the risks posed by certain fund and adviser third-party service providers. Under the proposal, funds and advisers would be required to identify the service providers that receive, maintain or process fund or adviser information (as applicable), or are otherwise permitted to access fund or adviser information systems and any fund or adviser information residing therein (Service Providers), and assess the cybersecurity risks associated with the fund's/adviser's use of the Service Providers. [15] In addition, the proposed cybersecurity policy requirements would mandate that funds and advisers: (i) require oversight of Service Providers and, (ii) through that oversight, document that the Service Providers, *pursuant to a written contract between the fund/adviser and the Service Provider*, are required to implement and maintain "appropriate" measures that are designed to protect fund/adviser information and fund/adviser information systems, including certain specified practices described in the proposed cybersecurity policy rules. Thus, the risk assessments that would be required under the proposal must account for the potential impact of a cybersecurity incident impacting a Service Provider. This will require evaluation of the system access available to the Service Provider, the types of services it provides, and the type of data it possesses. Advisers and funds will be required to evaluate their exposure to Service Provider cybersecurity risk and consider what steps are needed to comply with the proposal's requirements regarding Service Providers.

- ***Increased costs.*** The proposed requirements are expected to result in increased costs for funds and advisers. For example, the proposal recognizes that advisers and funds may need to retain a cybersecurity expert or specialist to assist in the review of written cybersecurity protocols or to further educate the board of directors on these issues.

- ***Potential for overlapping regulatory regimes.*** The SEC's proposal appears to acknowledge that the regulatory framework it proposes to develop will create overlapping obligations for certain firms with other regulatory regimes, including those instituted by the federal banking agencies and the Federal Trade Commission. If the proposal is adopted, advisers should examine their preexisting obligations under such regulatory frameworks and consider how the new SEC requirements interact with them.

II. Proposal Analysis

1. Cybersecurity Risk Management Policies and Procedures

The proposal would require registered funds and advisers to adopt and implement cybersecurity policies and procedures addressing a range of specifically enumerated topics. The stated goal of this requirement is to require advisers and funds to appropriately "consider and mitigate cybersecurity risk." [16] The SEC acknowledges that "there is not a one-size-fits-all approach to addressing cybersecurity risks" and the proposal thus would allow firms to structure their policies and procedures to fit the "nature and scope of their business and address their individual cybersecurity risks." [17] While allowing for flexibility in specific protections, all registered advisers and funds would need to adopt policies that address the following specific issues: risk assessments, user security and access, information protection, threat and vulnerability management, and cybersecurity incident response and recovery. [18] The SEC also set out expectations for general administration of the policies.

A. Risk Assessment

Under the proposal, all registered advisers and funds would need to "periodically [] assess, categorize, prioritize, and draft written documentation of, the cybersecurity risks associated with their information systems and the information residing therein." The SEC specifies that compliant risk assessments would:

- "categorize and prioritize cybersecurity risks based on an inventory of the components of information systems and the data therein by analyzing the potential effect of cybersecurity incidents on the advisers and funds"; and
- "identify . . . service providers that receive, maintain or process adviser or fund information, or that are permitted to access their information systems . . . and identify the cybersecurity risks" related to the use of such providers.[19]

The risk assessment component is essential to ensuring that a firm's cybersecurity program is appropriately tailored to the specific risks it faces. The SEC also acknowledges that risks can evolve over time and would therefore require advisers and funds to "reassess and re-prioritize their cybersecurity risks periodically as changes that affect these risks occur."[20] Examples of developments that could prompt a firm to undertake such a reassessment include "changes to its business, online presence, or client web access, or external changes, such as changes in the evolving technology and cybersecurity threat landscape."[21] Notably, the proposal recommends that advisers and funds monitor and consider implementing updates and guidance from "private sector and governmental resources, such as the Financial Services Information Sharing and Analysis Center (FS-ISAC) and the Department of Homeland Security's CISA." [22]

B. User Security and Access

Another required cybersecurity risk management measure under the proposed rules would be the implementation of "controls designed to minimize user-related risks and prevent the unauthorized access to information and systems." The proposal would require these protocols to:

- "[r]equir[e] standards of behavior for individuals authorized to access adviser or fund information systems" (i.e., an acceptance use policy);
- "[i]dentify[] and authenticat[e] individual users" including via multi-factor authentication;
- "[e]stablish[] procedures for the timely distribution, replacement, and revocation of passwords or methods of authentication";
- "[r]estrict[] access to specific adviser or fund information systems or components thereof . . . solely to individuals requiring access to such systems and information as is necessary for them to perform their responsibilities and functions"; and
- "[s]ecur[e] remote access technologies used to interface with adviser or fund information systems." [23]

The SEC found that these controls were "necessary to prevent and detect unauthorized access to systems or client or investor data or information," especially in the increasingly hybrid, remote work environment prevailing at many financial institutions. The SEC does not identify specific technological solutions or requirements, but rather acknowledges that there are multiple approaches a firm could take based on its risk profile, including "issuance of user credentials, digital rights management with respect to proprietary hardware and copyrighted software, authentication and authorization methods (*e.g.*, multi-factor authentication and geolocation), and tiered access to sensitive information and network resources."[24] Moreover, this aspect of a firm's cybersecurity program must address not only employee access controls, but also access controls applicable to clients and investors. Many of the SEC enforcement actions noted above specifically related to user access issues. These enforcement actions further highlighted to the industry the

SEC's views regarding cybersecurity controls and what is necessary for compliance with Regulation S-P.

C. Information Protection

The proposed cybersecurity rules would also require an adviser or fund to implement procedures that enable it to "monitor information systems and protect information from unauthorized access or use." These procedures must consider:

- "[t]he sensitivity level and importance of adviser or fund information";
- "[w]hether any adviser or fund information is personal information";
- "[w]here and how adviser or fund information is accessed, stored and transmitted";
- "[a]dviser or fund information systems access controls and malware protection"; and
- "[t]he potential effect of a cybersecurity incident involving adviser or fund information . . . including the ability for the adviser to continue to provide investment advice or the fund to continue providing service."[25]

The specific measures used to monitor for and prevent unauthorized information and system access should be tied to an evaluation of a firm's specific risks, but examples of measures could include, "encryption, network segmentation, and access controls to ensure that only authorized users have access to sensitive data or information or critical systems." In addition, firms may consider implementing measures designed to identify suspicious behavior, such as generating and reviewing user activity logs, identifying "potential anomalous activity," and escalating such issues to senior officers.[26]

In addition, firms also have the obligation to "oversee any service providers that receive, maintain, or process adviser or fund information, or are otherwise permitted to access their information systems" and associated data. In particular, firms must require service providers to agree via contract to implement their own cybersecurity policies and procedures. Advisers and funds should also employ "due diligence procedures or periodic contract review processes" to ensure proper oversight of Service Providers.[27]

D. Threat and Vulnerability Management

The proposal would also require advisers and funds to implement procedures "to detect, mitigate, and remediate cybersecurity threats and vulnerabilities with respect to" adviser or fund information and systems. The SEC highlights the importance of "ongoing monitoring" to detect threats and vulnerabilities. Specific examples of ongoing monitoring activities include "network, system, and application vulnerability assessments," such as "scans or reviews of internal systems, externally-facing systems, new systems, and systems used by service providers." The SEC also identifies certain mitigation measures firms could implement once such threats or vulnerabilities have been identified. These include "implementing a patch management program," "establish[ing] accountability for handling vulnerability reports," and developing "processes for intake, assignment, escalation, remediation, and remediation testing."[28]

E. Cybersecurity Incident Response and Recovery

The proposal would also require advisers and firms to have measures "to detect, respond to, and recover from a cybersecurity incident." Such measures would need to ensure:

- "[c]ontinued operations of the fund or adviser";
- "[t]he protection of adviser information systems and the fund or adviser information residing therein";

- "[e]xternal and internal cybersecurity incident information sharing and communications"; and
- "[r]eporting of significant cybersecurity incidents to the Commission." [29]

In addition, the proposal would require firms to document their response and recovery actions from any cybersecurity incident and to identify personnel responsible for specific roles in an incident response.

The SEC further encourages advisers and funds to take certain steps that could enhance the effectiveness of their incident response programs. These include: maintaining physical copies of response plans in case of system outages, backing up data, and testing their incident response plans through tabletop or full-scale exercises.

F. General Administration

According to the SEC, under the proposed cybersecurity risk management rules, an adviser or fund may choose to administer its cybersecurity policies and procedures using in-house resources with appropriate knowledge and expertise. The proposed framework also does not preclude an adviser or fund from using a third party's cybersecurity risk management services, subject to appropriate oversight. Similarly, subject to appropriate oversight, a fund's adviser or sub-adviser could administer any of the functions of the fund's required policies and procedures. 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 carry out the role effectively (*e.g.*, the policies and procedures could include an explicit escalation provision to the adviser's or fund's senior officers). 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 reporting to the Commission and disclosing to clients and investors certain incidents.

2. Annual Review and Required Written Reports

The proposal would require registered global advisers and funds to no less frequently than annually review and assess the design and effectiveness of the cybersecurity policies and procedures, including whether they reflect changes in cybersecurity risk over the time period covered by the review and prepare a written report reflecting this review. "The report would, at a minimum, describe the annual review, assessment, and any control tests performed, explain the results thereof, document any cybersecurity incident that occurred since the date of the last report, and discuss any material changes to the policies and procedures since the date of the last report." The stated purpose of the review and report requirement is to ensure that registrants' cybersecurity programs are working as designed and identify any necessary changes in response to changed conditions. The SEC acknowledges that this may require the expertise of additional internal and external expertise, including cybersecurity experts.[30]

3. Fund Board Oversight

The proposed rules would also require a fund's board of directors, including a majority of the independent directors, to both initially approve the fund's cybersecurity policies and procedures, and to review the written annual reports on the fund's procedures and incident reports. [31] Consistent with current practice under Rule 38a-1, directors may review and approve "summaries of the cybersecurity program prepared by persons who administer the fund's cybersecurity policies and procedures." The goal behind this requirement is to "assist directors in understanding a fund's cybersecurity risk management policies and procedures, as well as the risks they are designed to address."[32]

4. Recordkeeping

The proposed rules also impose new recordkeeping obligations on advisers and funds. Most notable amongst these is a requirement to retain "records documenting the occurrence of any cybersecurity incident, including records related to any response and recovery" from that incident from the past five years. [33] Depending on how this is interpreted, such documentation could be voluminous and include material that could qualify for legal privileges and protections. Also required are records documenting the adviser's/fund's cybersecurity risk assessment in the past five years. Compliance with these and other recordkeeping requirements might require advisers and funds, and by extension their Service Providers, to impose new administrative and technical protocols to ensure documentation is collected and maintained appropriately.

5. Confidential Reporting of Significant Cybersecurity Incidents to the Commission

The proposal details new confidential reporting requirements for registered advisers, using new Form ADV-C to report significant cybersecurity incidents to the SEC. Advisers would also be required to report such incidents "on behalf of a client that is a registered investment company or business development company, or a private fund." Importantly, these reporting requirements cover not only material incidents regarding advisers, but also apply to incidents regarding private and registered fund clients, known in the proposal as "covered clients." [34]

Specifically, any adviser registered or required to register with the Commission would be required to submit proposed Form ADV-C within 48 hours after having a reasonable basis to conclude that a significant cybersecurity incident had occurred or is occurring. The Form ADV-C will provide this information through a series of check-the-box and fill-in-the-blank questions.

Importantly, this requirement also requires advisers to continuously update and amend any previously filed Form ADV-C as new material information becomes available. Such updates must be provided 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."[35]

6. Public Disclosure of Cybersecurity Risks and Incidents

The proposed rules also include requirements for registered advisers and funds to publicly disclose "cybersecurity risks and incidents to their investors and other market participants." Specifically, the Commission proposed amendments to Form ADV Part 2A for advisers and Forms N-1A, N-2, N-3, N-4, N-6, N-8B-2 and S-6 for funds.[36]

Form ADV Part 2A would require disclosure of cybersecurity risks and incidents to an adviser's clients and prospective clients. Advisers would be required to describe cybersecurity risks that could "materially" [37] affect the advisory services they offer and how they assess, prioritize and address cybersecurity risks created by the nature and scope of their business. In addition, the proposal would require advisers to disclose "cybersecurity incidents" [38] that occurred within the past two fiscal years and that have significantly disrupted or degraded the adviser's ability to maintain critical operations, or that have led to the unauthorized access or use of adviser information, resulting in substantial harm to the adviser or its clients. When describing these incidents in their brochures, 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. Also proposed is a requirement for advisers 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 such an incident.[39]

Registered funds also would be required to provide prospective and current investors with cybersecurity-related disclosures. Specifically, the proposal would require a description of any "significant fund cybersecurity incidents" that have occurred in the past two fiscal years in funds' registration statements. Regarding cybersecurity risks, the SEC reminded funds that they should consider cybersecurity risks when preparing risk disclosures in fund registration statements under the Investment Company Act and the Securities Act.

The goal of these required disclosures is to "enhance investor protection by ensuring cybersecurity risk or incident-related information is available to increase understanding and insight into an adviser's or fund's cybersecurity history and risks."[40]

III. *Next Steps*: Additional Regulation Likely

If implemented, the proposal would represent an important rulemaking action by the SEC with respect to cybersecurity risk management for regulated entities. Advisers and funds should carefully review the proposal; track related developments; consider existing policies, procedures and practices; and consider filing comments, which may be submitted through April 11, 2022.

This SEC proposal is another significant example of expanded cybersecurity expectations and requirements for SEC-regulated entities. The proposal would impose significant new reporting and disclosure obligations on registered advisers and funds and require that they adopt cybersecurity policies and procedures meeting new specific requirements. In addition, the new requirements will provide an enhanced source of subject matter for SEC examinations and enforcement actions. Overall, the proposal is another signal of a sea-change in the SEC's regulatory and enforcement posture, with SEC Chair Gensler at the helm. Registered funds and advisers should take heed.

Although the proposal itself would have broad impact on the registered adviser and fund landscape, it still leaves room for future regulatory action with respect to other regulated entities. For example, even though this proposal does not apply to broker-dealers or entities subject to Regulation SCI, these entities (and potentially other types of registrants in the SEC's jurisdiction) should take note. At the February Commission meeting during which the SEC voted to propose these rules for consideration, SEC Chair Gensler announced that he would like to see similar proposals that would extend to such entities in the near future. The SEC has also complemented the above described proposal for registered advisers and funds with a similar proposal for public companies, which was announced on March 9, 2022.[41]

Advisers, funds and other entities within the SEC's jurisdiction would be wise to review their current cybersecurity policies, procedures, approaches and controls and compare them with the proposal, not only to prepare for possible adoption of the same but also to determine whether revisions are appropriate at this time. Although only at the proposal stage, these proposed rules and related form and rule amendments are a clear indication of the SEC's current expectations regarding appropriate cybersecurity measures.

---

[1] For ease of reference, BDCs and registered investments companies are referenced herein as "registered funds."

[2] Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and

Business Development Companies, 87 Fed. Reg. 13524, 13561 (Mar. 9, 2022).

[3] SEC, Press Release, SEC Proposes Cybersecurity Risk Management Rules and Amendments for Registered Investment Advisers and Funds (Feb. 9, 2022), https://bit.ly/3DZOugM.

[4] For example, the SEC first issued staff guidance on cybersecurity disclosures for public companies in 2011, and issued a Commission Statement and Guidance on Public Company Cybersecurity Disclosures (the "2018 Guidance") in February 2018. The 2018 Guidance emphasized that public companies should "inform investors about material cybersecurity risks and incidents in a timely fashion." The guidance also clarified that companies are "required to disclose 'such further material information, if any, as may be necessary to make the required statements, in light of the circumstances under which they are made, not misleading.'" *See* Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg. 8166, 8166-68 (Feb. 26, 2018).

[5] *See* SEC Division of Examinations, 2021 Examination Priorities 24 (Mar. 3, 2021), https://bit.ly/378d82I. For additional information; Mayer Brown Legal Update, SEC's Division of Examinations 2021 Exam Priorities – Investment Advisers and Investment Companies (Mar. 12, 2021), https://bit.ly/3jsPlgu.

[6] SEC Office of Compliance Inspection and Examinations, Risk Alert, Cybersecurity: Safeguarding Client Accounts against Credential Compromise 4 (Sep. 15, 2020), https://bit.ly/3JIXUi5. Further, in January 2020, OCIE issued a 13-page report of observations from its examinations of market participants' cybersecurity and operational resiliency practices. *See* SEC Press Release, SEC Office of Compliance Inspections and Examinations Publishes Observations on Cybersecurity and Resiliency Practices (Jan. 27, 2020), https://bit.ly/3v725yN. For additional information, *see* Mayer Brown Legal Update, SEC's OCIE Publishes Observations on Cybersecurity and Resiliency Practices (Feb. 25, 2020), https://bit.ly/3xfaMd3.

[7] 17 C.F.R. § 275.206(4)-7.

[8] 17 C.F.R. §§ 248.1-248.31. Not all investment advisers are subject to Regulation S-P; however, there is a vast array of state and similar laws that could apply. In addition, other federal regulations could apply (*e.g.*, Federal Trade Commission regulations).

[9] 17 C.F.R. §§ 248.201-248.202.

[10] 17 C.F.R. § 270.38a-1.

[11] Not all funds are subject to these regulations. However, as with investment advisers, there are state and similar laws that could apply.

[12] 87 Fed. Reg. at 13527.

[13] *See* SEC, Press Release, SEC Charges Pearson plc for Misleading Investors About Cyber Breach (Aug. 16, 2021), https://bit.ly/3v6v2ek. For additional information, *see* Mayer Brown Legal Update, US Securities and Exchange Commission Increases Focus on Cybersecurity (Oct. 15, 2021), https://bit.ly/38wRCF4.

[14] The proposal is particularly impactful for "robo" and similar advisers, advisers that utilize "AI" or similar mechanisms, and advisers that utilize quantitative and similar investment strategies, as well as advisers utilizing "ESG" strategies.

[15] The proposal defines these important terms. "Adviser information" is defined as "any electronic information related to the adviser's business, including personal information, received, maintained, created, or processed by the adviser." "Adviser information systems" is defined as "the information resources owned or

used by the adviser, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of adviser information to maintain or support the adviser's operations." "Fund information" is defined as "any electronic information related to the fund's business, including personal information, received, maintained, created, or processed by the fund." "Fund information systems" is defined as "the information resources owned or used by the fund, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of fund information to maintain or support the fund's operations." 87 Fed. Reg. at 13589, 13593.

[16] 87 Fed. Reg. at 13527. Cybersecurity risk is defined as "financial, operational, legal, reputational, and other adverse consequences that could result from cybersecurity incidents, threats, and vulnerabilities." *Id*. at 13589.

[17] 87 Fed. Reg. at 13527.

[18] In order to assist the adviser in reporting a significant fund cybersecurity incident on new Form ADV-C (see below), a registered fund's cybersecurity policies and procedures must address the proposed notification requirement to the SEC on Form ADV-C. Generally, these provisions of the policies and procedures should address communications between the person(s) who administer the fund's cybersecurity policies and procedures and the adviser about cybersecurity incidents, including those affecting the fund's Service Providers.

[19] 87 Fed. Reg. at 13529.

[20] *Id. See also* Section 2: Annual Review and Required Written Reports, *infra*.

[21] 87 Fed. Reg. at 13529.

[22] 87 Fed. Reg. at 13529-13530.

[23] 87 Fed. Reg. at 13530.

[24] *Id.*

[25] 87 Fed. Reg. at 13531.

[26] *Id.*

[27] *Id.*

[28] 87 Fed. Reg. at 13532.

[29] *Id.*

[30] 87 Fed. Reg. at 13534.

[31] As unit investment trusts do not have boards of directors, the proposal would require the trust's principal underwriter or depositor to approve the policies and procedures.

[32] 87 Fed. Reg. at 13534.

[33] 87 Fed. Reg. at 13535. Specifically, under the proposed rule, advisers must "maintain: (1) a copy of their

cybersecurity policies and procedures formulated pursuant to proposed rule 206(4)-9 that are in effect, or at any time within the past five years were in effect; (2) a copy of the adviser's written report documenting the annual review of its cybersecurity policies and procedures pursuant to proposed rule 206(4)-9 in the last five years; (3) a copy of any Form ADV-C filed by the adviser under rule 204-6 in the last five years; (4) 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 (5) records documenting an adviser's cybersecurity risk assessment in the last five years." *Id.* Similarly, a fund must "maintain: (1) a copy of its cybersecurity policies and procedures that are in effect, or at any time within the last five years were in effect; (2) copies of written reports provided to its board; (3) records documenting the fund's annual review of its cybersecurity policies and procedures; (4) any report of a significant fund cybersecurity incident provided to the Commission by its adviser; (5) records documenting the occurrence of any cybersecurity incident, including any records related to any response and recovery from such an incident; and (6) 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." *Id.*

[34] 87 Fed. Reg. at 13536.

[35] *Id.*

[36] 87 Fed. Reg. at 13539.

[37] According to the proposal, "[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: (1) [c]ould disrupt (or has disrupted) the adviser's ability to provide services, including the duration of such a disruption; (2) 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; and/or (3) could harm (or has harmed) clients (*e.g.*, inability to access investments, illiquidity, or exposure of confidential or sensitive personal or business information)." 87 Fed. Reg. at 13540.

[38] As proposed, this term means an unauthorized occurrence on or conducted through an adviser's information systems that jeopardizes the confidentiality, integrity, or availability of an adviser's information systems or any adviser information residing therein.

[39] 87 Fed. Reg. at 13540.

[40] 87 Fed. Reg. at 13539.

[41] *See* Mayer Brown Legal Update, SEC Proposes Amendments That Would Place New Cybersecurity Reporting and Disclosure Requirements on Public Companies (Mar. 10, 2022), https://bit.ly/3reuVfC; Mayer Brown Legal Update, SEC Proposes New Rules on Public Company Cybersecurity Disclosures (Mar. 14, 2022), https://bit.ly/3M1nkZP.

AUTHORS

COUNSEL

LESLIE S. CRUZ

WASHINGTON DC +1 202 263 3337

LCRUZ@MAYERBROWN.COM

PARTNER

RAJESH DE

WASHINGTON DC +1 202 263 3366

RDE@MAYERBROWN.COM

PARTNER

ADAM D. KANTER

WASHINGTON DC +1 202 263 3164

AKANTER@MAYERBROWN.COM

ASSOCIATE

JENNIFER L. WEINBERG

WASHINGTON DC +1 202 263 3499

JLWEINBERG@MAYERBROWN.COM