LATHAM&WATKINS

Client Alert Commentary

Latham & Watkins Investment Funds Practice

May 6, 2022 | Number 2933

Analysis: SEC's Proposed Cyber Rules for RIAs, RICs, and BDCs

In another move related to strengthening its cybersecurity enforcement efforts, the SEC announced that it will nearly double the size of its cyber enforcement unit.

On May 3, 2022, the SEC announced that it will allocate 20 additional positions to the newly named Crypto Assets and Cyber Unit (formerly known as the Cyber Unit) in the Division of Enforcement, bringing the unit to 50 dedicated positions. In addition to carrying out its crypto mandate, the unit will investigate and bring actions against SEC registrants and public companies on critical cybersecurity issues, building on its record to date of cases focused on alleged failures to maintain adequate cybersecurity controls and to appropriately disclose cyber-related risks and incidents.

The announcement comes on the heels of several significant cybersecurity proposals. On February 9, 2022, the SEC voted 3-1 to propose rules that would significantly expand the risk management and reporting requirements concerning cybersecurity and related matters for registered investment companies (RICs), business development companies (BDCs), and investment advisers registered or required to be registered with the SEC (RIAs).

The comment period on these proposed rules has now closed. If enacted, the rules would:

- Require RICs and BDCs (collectively, Funds) and RIAs to adopt and implement written policies and procedures (Cybersecurity Policies) that are reasonably designed to address cybersecurity risks, including an annual review and assessment of such policies and procedures
- Require RIAs and Funds to report a "significant" cybersecurity incident[1] to the SEC within 48 hours of having a "reasonable basis" to conclude that it has occurred or is occurring
- Expand the disclosures concerning cybersecurity risks and incidents that RIAs must include on Form ADV and that Funds must include in various forms and filings with the SEC
- Impose new requirements on RIAs and Funds for maintaining books and records relating to cybersecurity matters

This Client Alert analyzes the proposed rules and advises SEC registrants on how to prepare for compliance.

Cybersecurity Risk Management

Elements of Cybersecurity Policies

The proposed rules would amend both the Investment Advisers Act of 1940 (Advisers Act) and the Investment Company Act of 1940 (Investment Company Act), by requiring RIAs and Funds to implement Cybersecurity Policies. Under the proposed rules, the Cybersecurity Policies would need to address operational and other risks that could cause financial, operational, legal, or reputational harm to an RIA's clients, investors in an RIA's private fund clients, or Fund investors, or which could result in the unauthorized access of information relating to the RIA or Fund, including with respect to the personal information of its respective clients or investors. The Cybersecurity Policies would need to be reasonably designed to ensure that the RIA or Fund's operations were able to continue following a cybersecurity incident, including with respect to the resiliency and capacity of information systems, regardless of whether such information systems were housed at a service provider or with the RIA or Fund.

In addition, the SEC has set out general elements to be incorporated in the Cybersecurity Policies, which the RIA or Fund would tailor to its particular operations, including:

- Periodic assessment of cybersecurity risks associated with the information systems of the RIA or Fund and the information contained therein (collectively, systems and information), including with respect to the categorization, prioritization, and documentation of such risks and the potential effect of a cybersecurity incident on the RIA or Fund

- Implementation of controls designed to minimize user-related risks and prevent unauthorized access to the RIA or Fund's systems and information, including:

  - Outlining standards of behavior for individuals authorized to access RIA or Fund information systems, such as an acceptable use policy

  - Identifying and authenticating individual users, including authentication measures that require two or more credentials for access verification

  - Implementing procedures for timely distribution, replacement, and revocation of passwords or authentication methods

  - Restricting access for specific RIA or Fund systems or information or components thereof solely to individuals on a need-to-know basis for the purpose of performing her or his responsibilities and functions on behalf of the RIA or Fund

  - Securing remote access technologies used to interface with RIA or Fund information systems

- Monitor information systems and protection of information from unauthorized access or use, based on periodic assessment of the RIA or Fund's systems and information, taking into account:

  - Level of sensitivity and importance of the information to business operations

  - Whether any such information is personal information

  - Where and how such information is accessed, stored, and transmitted, including monitoring information in transmission

  - Information systems access controls and malware protection
  - Potential effect of a cybersecurity incident involving such information on the RIA or Fund and its clients or shareholders, including the RIA's ability to continue to provide investment advice or the Fund's to continue to provide services
- Identification and oversight of the service providers that receive, maintain, process, or access RIA or Fund systems and information and the cybersecurity risks presented by such service providers, which may include identifying alternative processes or vendors for certain services
- Documenting in a written agreement that service providers are required to implement and maintain appropriate measures designed to protect the RIA or Fund's information systems
- Detection, mitigation, and remediation of cybersecurity threats and vulnerabilities with respect to the RIA or the Fund's systems and information, which may include:
  - Undertaking assessments of network, system, and application vulnerability of the RIA, the Fund, and/or service providers
  - Surveying industry and government sources for information on new threats and vulnerabilities
  - Implementing patch management programs for hardware and software in connection with mitigation measures
  - Establishing a process for tracking and handling reports of vulnerabilities
  - Requiring cybersecurity threat, vulnerability, and response training specific to particular roles
- Implementation of measures to detect, respond to, recover from, and document a cybersecurity incident, including establishing an incident response plan, addressing:
  - How to continue operations
  - Protection of information systems and the information contained therein
  - External and internal cybersecurity incident information sharing and communications
  - Reporting of significant cybersecurity incidents to the SEC
  - The written documentation required for a cybersecurity incident, which would cover the response to and recovery from such incident
- Preparation of written documentation of the occurrence of, response to, and recovery from cybersecurity incidents

In addition, the SEC suggests that RIAs or Funds should:

- Reassess and revise their Cybersecurity Policies as cybersecurity risks arise
- Implement certain safeguards such as data backups

- With respect to incident response plans, ensure such plans:
  - Identify particular personnel to perform specific roles during a cybersecurity incident
  - Set out a clear escalation protocol to ensure that an adviser's and fund's senior officers, legal and compliance personnel, and board (as applicable) receive necessary information concerning cybersecurity incidents on a timely basis
- With respect to the risk assessment of a service provider, consider policies or procedures to assess the service provider's practices, the resiliency and capacity of its systems, its ability to protect information and systems, its response and recovery procedures and escalation protocols with respect to cybersecurity incidents, how the service provider will secure and maintain data, and/or the service provider's business continuity and disaster recovery protocols
- Hire personnel or third parties with cybersecurity and recovery experience
- Maintain physical copies of their Cybersecurity Policies and incident response plans to ensure such materials can be accessed during a cybersecurity or other incident
- Test incident response plans in order to evaluate their efficacy and determine what modifications, if any, are needed (for example, through tabletop or full-scale exercises)
- In connection with the annual review and assessment of the effectiveness of their policies and procedures, consider updates to the compliance program in order to correct any identified weaknesses in the design or effectiveness of their Cybersecurity Policies

Annual Review

Under the proposed rules, RIAs and Funds would be required to review and assess their Cybersecurity Policies at least annually. As part of an annual review, RIAs and Funds would need to review and assess the design and effectiveness of their Cybersecurity Policies and whether such policies and procedures reflect changes in cybersecurity risk over the time period covered by the review. In addition, the findings of the review would need to be captured in a written report (Annual Cyber Report) that:

- Describes the annual review, assessment, and control tests performed and explains the results of the review
- Documents each cybersecurity incident that occurred since the date of the previous report
- Discusses the material changes to the Cybersecurity Policies since the date of the previous report

The SEC suggests that the Annual Cyber Report should be prepared by the personnel that administer the Cybersecurity Policies and should address the risk assessments performed by the RIA or Fund.

Board Oversight for Funds

Under proposed Rule 38a-2 of the Investment Company Act, a Fund's board of directors (Board), including a majority of its independent directors, would initially approve the Fund's Cybersecurity Policies and would be required to review the Annual Cyber Report. According to the SEC, the Board is not intended to play a passive role in overseeing the Fund's cybersecurity program. Rather, in connection with its review of the Fund's Cybersecurity Policies and Annual Cyber Report, the Board should actively

follow up on weaknesses discovered in risk assessments, questions concerning service provider contracts, and the steps the Fund has taken to address overall cybersecurity risks.

Reporting "Significant" Cybersecurity Incidents: New Form ADV-C

In perhaps the most significant update, under the proposed rules, RIAs would be required to report to the SEC within 48 hours of the RIA having a "reasonable basis" to conclude that a "significant" cybersecurity incident[2] (concerning the RIA, a private fund client, or a Fund) is continuing or had occurred.

The proposed Form ADV-C contains a number of check-the-box and fill-in-the-blank questions, which capture information relating to the nature and scope of the significant cybersecurity incident and related disclosures made to clients and investors. Form ADV-C would be submitted to the SEC through the Investment Adviser Registration Depository platform, and the SEC's preliminary view is that Form ADV-C would be treated as a confidential filing. In addition to basic information regarding the RIA and the significant cybersecurity incident (e.g., name, address, and file number of the RIA; approximate date the incident occurred; approximate date the incident was discovered, whether the incident is related to the RIA, a Fund, or both; etc.), Form ADV-C would prompt the RIA to provide certain substantive and related information concerning the incident, including:

- Contact information for an individual with respect to the incident
- Whether law enforcement or a government agency has been notified of the incident
- Whether actions have been taken or planned for recovery from the incident
- Whether data was stolen, altered, accessed, or used for any unauthorized purpose
- Whether the incident has been disclosed to the RIA's clients, investors in private fund clients, or Fund investors
- Whether and how the incident has affected the RIA or Fund's critical operations, and which systems or services have been affected
- If the incident occurred at or resulted from a cybersecurity incident at a service provider, a description of the services provided by the service provider to the RIA or Fund, and how any degradation in those services have affected the RIA or Fund's operations or the operations of the RIA's private fund clients
- Whether the incident is covered under a cybersecurity insurance policy

In addition, RIAs would be required to amend previously filed Form ADV-Cs within 48 hours of certain events, including one or more of the following:

- Information contained in a previously-filed Form ADV-C becomes materially inaccurate
- New material information is discovered relating to a significant cybersecurity incident that was reported to the SEC
- Resolution of a previously reported significant cybersecurity incident or the internal investigation into a previously reported significant cybersecurity incident has been closed

Under the proposed rules, the Cybersecurity Policies would be required to address the above reporting requirement, and in particular, the communications among the person(s) who administer the Cybersecurity Policies and the RIA regarding cybersecurity incidents affecting the RIA, the Fund, and/or their service providers.

Which Incidents Are "Significant"?

The proposed rules define a "significant" cybersecurity incident as "a cybersecurity incident, or a group of related cybersecurity incidents, that (a) significantly disrupts or degrades the fund's ability to maintain critical operations, or (b) leads to the unauthorized access or use of fund information, where the unauthorized access or use of such information results in substantial harm to the fund or to an investor whose information was accessed."

As further context for the foregoing definition, in Federal Register commentary, the SEC discusses the following guideposts and examples:

- With respect to significant disruption that could trigger the reporting rule:

  > *If an adviser were unable to maintain critical operations, such as the ability to implement its investment strategy, process or record transactions, or communicate with clients, there is potential for substantial loss to both the adviser and its clients. For example, if an adviser's internal computer systems, including its websites or email function, are shut down due to malware, it could have a significant effect on the ability for the adviser to continue to provide advisory services and for the adviser's clients to access their investments or communication with the adviser. In such a situation, it is possible that the adviser's employees would not be able to access the computer systems they need to make trades or manage a client's portfolio, and advisory clients may not be able to access their accounts through the adviser's webpage or other channels that were affected by the malware. Depending on the type of malware, this could lock up advisory client records, among other things, and affect an adviser's decision-making and investments for days, or even weeks. This in turn could potentially affect the market, particularly if other advisers are similarly targeted with the same malware.*

- With respect to unauthorized access to Fund information that might result in substantial harm to the fund or to an investor whose information was accessed:

  > *Substantial harm to an adviser as the result of a cybersecurity incident in which adviser information is compromised could include, among other things, significant monetary loss or theft of intellectual property. Substantial harm to a client or an investor in a private fund as the result of a cybersecurity incident in which adviser information is compromised could include, among other things, significant monetary loss or the theft of personally identifiable or proprietary information. After gaining access to an adviser's or a fund's systems, an attacker could use this access to disclose, modify, delete or destroy adviser, fund, or client data, as well as steal intellectual property and client assets. Any of these actions could result in substantial harm to the adviser and/or to the client.*

The proposed rules similarly define "significant adviser cybersecurity incidents" that would apply to an RIA, except that the definition also covers the ability of a private fund client to maintain critical operations and the harm to an investor in a private fund client as a result of the incident.

In this regard, the SEC provides the following example:

> *Significant fund cybersecurity incidents may include cyber intruders interfering with a fund's ability to redeem investors, calculate NAV or otherwise conduct its business. Other significant fund cybersecurity incidents may involve the theft of fund information, such as non-public portfolio holdings, or personally identifiable information of the fund's employees, directors or shareholders.*

Disclosure of Cybersecurity Risks and Incidents

The proposed rules would require RIAs to make additional cybersecurity-related disclosures in Form ADV Part 2A. In particular, the amended Form ADV would require each RIA to describe in narrative format:

- The cybersecurity risks that could materially affect the RIA's advisory services
- How the RIA assesses, prioritizes, and addresses cybersecurity risks in light of the nature and scope of its business
- Any cybersecurity incident in the last two fiscal years that significantly disrupted or degraded the RIA's ability to maintain critical operations or led to unauthorized access or use of certain information related to the RIA's business (including personal information received, maintained, created, or processed by the RIA)

Under the proposed rules, a cybersecurity risk (whether significant or not) would be "material" to an RIA's business if there is a "substantial likelihood that a reasonable client would consider the information important based on the total mix of facts and information." Relevant facts and circumstances for determining whether a cybersecurity risk is material to an RIA's business may include the likelihood and extent to which the risk or resulting cybersecurity incident could:

- Disrupt the RIA's ability to provide services and the duration of such disruption
- Result in loss of RIA or client data in light of the nature and importance of such data, the circumstances in which such data was compromised, and the duration during which such data was compromised
- Harm clients

In addition, the proposed rules would amend rule 204-3(b) under the Advisers Act, whereby RIAs would be required to deliver an other-than-annual brochure amendment to existing clients promptly if the amendment includes a new disclosure of a cybersecurity incident or materially modifies information already disclosed in its brochure about such an incident.

With respect to RICs and BDCs, the proposed rules would amend Forms N-1A, N-2, N-3, N-4, N-6, N-8B-2, and S-6, and require RICs and BDCs to describe any significant fund cybersecurity incidents that have occurred in the last two fiscal years in registration statements, such disclosures to be tagged in a structured, machine-readable data language.

Recordkeeping

The proposed rules would amend Rule 204-2 under the Advisers Act and Rule 38a-2 under the Investment Company Act, which set forth recordkeeping requirements for RIAs, RICs, and BDCs, as

applicable. Under the amended rules, RIAs would be required to maintain records related to cybersecurity incidents and risk management, including without limitation:

- A copy of the Cybersecurity Policies currently in effect, or that were in effect at any time within the past five years
- A copy of each Annual Cyber Report completed in the previous five years
- A copy of any Form ADV-C filed in the previous five years
- Records documenting each cybersecurity incident (including without limitation those relating to the response to and recovery from each such incident) that has occurred in the previous five years
- Records documenting each cybersecurity risk assessment carried out by the RIA in the previous five years

The amendments to Rule 38a-2 under the Investment Company Act impose similar recordkeeping requirements on RICs and BDCs.

Takeaways

The issue of how to address cybersecurity risks is not a new one and many RIAs and other advisers, as well as the Funds they advise, have already implemented cybersecurity and related policies and procedures of varying degrees of robustness. Consequently, the proposed requirements concerning the adoption and implementation of Cybersecurity Policies and procedures may in many ways formalize the steps previously taken to mitigate cybersecurity risks by RIAs and Funds. However, if implemented, the proposed rules could significantly increase the reporting and recordkeeping burden of RIAs and Funds with respect to cybersecurity risks and incidents.

SEC registrants should revisit their enterprise information security programs, disclosure practices, and incident response plans. In particular, SEC registrants should:

- Undertake a review and risk assessment of the current and desired cybersecurity controls (e.g., access controls, monitoring and detection, credentials and password management) to identify areas that require updating to better align with the proposed requirements
- Plan and document a process to enable periodic (e.g., annual) review and reporting to senior leadership (e.g., a fund's board of directors) and sound recordkeeping, including in relation to cybersecurity incidents (which may require thoughtful approaches to addressing the presence of potential attorney-client privileged information)
- Ensure that critical service providers (including those that receive, maintain, or process fund or adviser information) are identified and governed by sound third-party cybersecurity management (e.g., diligence, contracting, monitoring) protocols.
- Implement protocols into incident response plans to incorporate tight-timing (e.g., 48 hour) deadlines for rendering internal analyses and conclusions on whether detected incidents are "significant" and therefore subject to Form ADV-C requirements.

If you have questions about this Client Alert, please contact one of the authors listed below or the Latham lawyer with whom you normally consult:

Laura N. Ferrell
laura.ferrell@lw.com
+1.312.876.7616
Chicago

Tony Kim
antony.kim@lw.com
+1.202.637.3394
Washington, D.C.

Daniel A. Filstrup
daniel.filstrup@lw.com
+1.312.876.6511
Chicago

You Might Also Be Interested In

SEC Proposes Significant Rule Changes for Private Fund Advisers

SEC Proposes Changes to Form PF for Private Equity and Large Hedge Fund Advisers

SEC Staff Issues Key Considerations on LIBOR Transition

Endnotes

[1] The proposed rules define "cybersecurity incident" as "an unauthorized occurrence on or conducted through [an RIA's or Fund's] information systems that jeopardizes the confidentiality, integrity, or availability of [an RIA's or Fund's] information systems or any adviser [or fund] information residing therein."

[2] The proposed rules define a "significant fund cybersecurity incident" as "a cybersecurity incident, or a group of related cybersecurity incidents, that significantly disrupts or degrades the fund's ability to maintain critical operations, or leads to the unauthorized access or use of fund information, where the unauthorized access or use of such information results in substantial harm to the fund or to an investor whose information was accessed." The proposed rules similarly define "significant adviser cybersecurity incident" as would apply to an RIA, provided that such definition also covers the ability of a private fund client to maintain critical operations and the harm to an investor in a private fund client as a result of the incident. For purposes of this client alert, "significant cybersecurity incident" refers to a significant fund cybersecurity incident and/or a significant adviser cybersecurity incident, as applicable.