February 18, 2022

SEC Proposes Cybersecurity Risk Management Rules for Registered Funds and Advisers

Attorneys
Fran Faircloth
Edward R. McNicholas
Jason E. Brown
Amanda N. Persaud

On February 9, 2022, the SEC published a release addressing Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies ("Release"). The Release contained proposed new rules under the Advisers Act (Rules 206(4)-9 and 204-6) and the Investment Company Act of 1940 (Rule 38a-2) and amendments (collectively, the "Proposals"), which would require registered investment advisers ("advisers") and registered investment companies ("registered funds") to implement cybersecurity risk management programs and new incident notification regimes. If adopted, the Proposals would:

- Require advisers and registered funds to disclose detailed information about their "cybersecurity risks" and "cybersecurity incidents" to current and prospective clients and shareholders;
- Require reporting of any "significant adviser cybersecurity incidents" (which may occur with respect to private funds or clients) and "significant fund cybersecurity incidents" (for registered funds) to the SEC within 48 hours of reasonably concluding an incident occurred; and
- Require advisers and registered funds to adopt and implement cybersecurity policies and procedures that are reasonably designed to address cybersecurity risks.

The proposed rules would not apply to private funds, which are exempt from the Investment Company Act of 1940 and thus are subject to the FTC's Safeguards Rule for cybersecurity. The proposed SEC rules would, however, apply to registered investment advisers who advise those private funds. Fortunately, the proposed rules appear to be largely consistent with the FTC's revised Safeguards Rule.

Some Early Thoughts:[1]

- Although the release suggests that advisers merely need to have appropriate policies and procedures, the SEC, as a practical matter, may be creating a regime of new cybersecurity requirements.
- The proposed "significant fund/adviser cybersecurity incidents" notification system, with initial confidential reporting to the SEC and then public disclosure to investors, may be particularly challenging given the overlap with state data breach laws that are generally not preempted.
- The Release does not propose changes to Regulation S-P, which requires cybersecurity policies and procedures to protect *customer* information from security threats and unauthorized access. Instead, the Proposals would amend the SEC's disclosure regime to require advisers and registered funds to establish policies and procedures that address a wide range of cybersecurity risks and incidents that go beyond customer information.
- While the Proposals require firms to establish written policies and procedures related to cybersecurity risk, they allow flexibility for firms to "tailor their cybersecurity policies and procedures to fit the nature and scope of their business and address their individual cybersecurity risks." The Proposals may be viewed as elaborating some of

[1] Terms that appear in quotation marks in this Alert are defined in the Release and are reproduced, with their respective definitions, in this Appendix.

the baseline expectations that have appeared in recent SEC enforcement actions and risk alerts. Some of these expectations could be difficult for smaller firms to meet. For example, the implementation of multifactor authentication ("MFA") and the incorporation of least-privilege concepts could present operational and compliance challenges for certain firms.

- While the Proposal's cybersecurity rules are generally consistent with the FTC Safeguards Rule—the SEC is working from a baseline of requirements similar to the rules the FTC recently promulgated for private funds exempt from the 1940 Act—the SEC's proposed requirements are less prescriptive, though may ultimately have the same practical impact through the disclosure regime.

Proposed New Rules and Amendments:

I. New Disclosure Requirements Regarding Cybersecurity Risks and Incidents

The Proposals would amend Form ADV for advisers and Forms N-1A, N-2, N-3, N-4, N-6, N-8B-2, and S-6 for registered funds to require the disclosure of cybersecurity risks and incidents.

Form ADV. The Proposals would add a new Item 20 "Cybersecurity Risks and Incidents" to Form ADV, or Part 2A, which currently requires disclosures related to business practices, fees, risks, and conflicts. In amended form, advisers would be required to describe cybersecurity risks that could materially affect the services they offer and disclose how they assess, prioritize, and address such risks.

- The Proposals would also require advisers to describe any "cybersecurity incidents" that occurred within the last two fiscal years that have significantly disrupted their 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 clients. This could be read to require reporting of a much broader set of incidents than most other state and federal cybersecurity reporting requirements.

- The Proposals would amend Rule 204-3(b) to require an adviser to promptly deliver interim brochure amendments to existing clients 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.

Fund Registration Statements.[2] The Proposals would require a registered fund to disclose in its registration statement whether a "significant fund cybersecurity incident" has affected or is currently affecting the registered fund or its service providers. Specifically, the Proposals would require a description of each incident, including the following information to the extent known:

- the entity or entities affected;

- when the incident was discovered and whether it is ongoing;

- whether any data was stolen, altered, or accessed or used for any other unauthorized purpose;

[2] The Release states that the proposed disclosure amendments would require registered funds to disclose significant fund cybersecurity incidents affecting insurance companies (for separate accounts that are management investment companies that offer variable annuity contracts registered on Form N-3) and depositors (for separate accounts that are unit investment trusts that offer variable annuity contracts on Form N-4; UITs that offer variable life insurance contracts on Form N-6; and UITs other than separate accounts that are currently issuing securities, including UITs that are issuers of periodic payment plan certificates and UITs of which a management investment company is the sponsor or depositor on Form N-8b-2 or Form S-6).

- 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.

A registered fund would be required to disclose this information regarding any significant fund cybersecurity incident if the incident occurred during the registered fund's last two fiscal years.

The Release provides further guidance on disclosing cybersecurity-related matters. It notes that, in order for registered funds to "make timely disclosures of cybersecurity risks and significant fund cybersecurity incidents, a fund would amend its prospectus by filing a supplement." Moreover, registered funds should include a discussion of such risks and incidents in annual reports to shareholders "to the extent that these were factors that materially affected performance of the fund over the past fiscal year." The Proposals would require all registered funds to tag information about significant fund cybersecurity incidents in a structured, machine-readable data language. The Proposals include conforming amendments to Rules 485 and 497 under the Securities Act.

Note: *The registered fund registration form amendments would require disclosure about whether the cybersecurity incident at issue has been or is being remediated, and the SEC staff may look to the support for such disclosure during exams.*

II. Mandatory Cybersecurity Incident Reporting

The Proposals include a new reporting obligation under proposed Rule 204-6 that would require advisers to report to the SEC on a confidential basis "significant adviser cybersecurity incidents" (which may be with respect to private funds or clients) and "significant fund cybersecurity incidents" (for registered funds) within 48 hours of having a reasonable basis to conclude that any such incident has occurred or is occurring. These reports would be transmitted by filing new Form ADV-C electronically on the Investment Adviser Registration Depository (the "IARD").

Rule 204-6 also would require each adviser to amend any previously filed Form ADV-C promptly, but in no event more than 48 hours after:

- Any information previously reported to the SEC on Form ADV-C concerning a "significant adviser cybersecurity incident" or a "significant fund cybersecurity incident" becoming materially inaccurate;
- Any new material information pertaining to a "significant adviser cybersecurity incident" or a "significant fund cybersecurity incident" previously reported to the SEC on Form ADV-C being discovered; or
- Any "significant adviser cybersecurity incident" or "significant fund cybersecurity incident" being resolved or any internal investigation pertaining to such an incident being closed.

Note: *Though the proposed reporting obligation distinguishes "significant adviser cybersecurity incident" from "significant fund cybersecurity incident," the definitions, as outlined in the Appendix, generally overlap. The Release defines a "significant cybersecurity incident" that triggers reporting as a "cybersecurity incident, or a group of related cybersecurity incidents, 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 (1) substantial harm to the adviser, or (2) substantial harm to a client, or an investor in a private fund, whose information was accessed." Relatedly, the Release broadly defines "cybersecurity incident" as an "unauthorized occurrence on or conducted through [an adviser's or a registered fund's] information systems that jeopardizes 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." This definition notably goes farther than state notification laws.

The proposed reporting obligation is one of a few notification requirements that has been recently adopted or proposed by federal regulators. The Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers ("Banking Rule"), issued by the Office of the Comptroller of Currency, Federal Deposit Insurance Corporation, and Board of Governors of the Federal Reserve, requires organizations to notify their primary federal regulator of significant "computer-security incidents," no later than 36 hours after the organization "determines" such an incident has occurred. The Banking Rule provides for confidential notification, unlike the proposed FTC Safeguards Rule amendment, which seeks public incident reporting. The proposed FTC Safeguards amendment requires institutions that experience a "security event," in which the misuse of customer information has occurred or is reasonably likely to occur, to provide notice of the event to the FTC no later than 30 days after "discovery" of the event if it affected or reasonably may have affected at least 1,000 consumers.

III. Cybersecurity Risk Management Policies and Procedures

The Proposals require advisers and registered funds to implement written policies and procedures that are reasonably designed to address cybersecurity risks and to update the board of directors no less often than annually. Each registered fund/adviser's cybersecurity policies and procedures would be required to include the following elements.

Risk Assessment. The cybersecurity policies and procedures would be required to provide for periodic assessments of cybersecurity risks associated with registered fund/adviser information systems and registered fund/adviser information within those systems, including policies and procedures requiring the registered fund/adviser to:

- Categorize and prioritize cybersecurity risks based on an inventory of the components of the registered fund/adviser information systems and the potential effect of a cybersecurity incident on the registered fund/adviser; and

- Identify the registered fund/adviser's service providers that receive, maintain or process registered fund/adviser information, or are otherwise permitted to access registered fund/adviser information systems, and assess the cybersecurity risks associated with the registered fund/adviser's use of these service providers.

The cybersecurity policies and procedures would be required to provide that any risk assessments must be documented in writing.

User Security and Access. The cybersecurity policies and procedures would be required to contain controls that are designed to minimize user-related risks and prevent the unauthorized access to registered fund/adviser information systems, including the following:

- Requiring standards of behavior for individuals authorized to access registered fund/adviser information systems, such as an acceptable use policy;

- Identifying and authenticating individual users, including implementing authentication measures that require users to present a combination of two or more credentials for access verification (otherwise known as MFA);

- Establishing procedures for the timely distribution, replacement, and revocation of passwords or methods of authentication;

- Restricting access to specific registered fund/adviser information systems 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 registered fund/adviser (principles of least privilege and zero trust); and

- Securing remote access technologies.

Information Protection. The cybersecurity policies and procedures would be required to include measures designed to monitor registered fund/adviser information systems and protect registered fund/adviser information from unauthorized access or use, based on a periodic assessment of the registered fund/adviser information systems and taking into account the following factors:

- The sensitivity level and importance of registered fund/adviser information to its business operations;

- Whether any registered fund/adviser information is "personal information";

- Where and how registered fund/adviser information is accessed, stored, and transmitted, including the monitoring of registered fund/adviser information in transmission;

- Registered fund/adviser information systems access controls and malware protection; and

- The potential effect a cybersecurity incident involving registered fund/adviser information could have on the registered fund/adviser, including the ability for the registered fund/adviser to continue to provide services/investment advice.

This would essentially require advisers and registered funds to maintain a detailed map of their data and systems that categorizes data by risk and tracks where data in different risk categories is stored, and how it is used and transferred.

The cybersecurity policies and procedures would also be required to provide for oversight of service providers that receive, maintain, or process registered fund/adviser information and, through that oversight, document that such service providers, pursuant to a written contract between the registered fund/adviser and any service provider, are required to implement and maintain appropriate measures (including the practices described in this Section II as required elements) that are designed to protect registered fund/adviser information and information systems.

Cybersecurity Threat and Vulnerability Management. The cybersecurity policies and procedures would be required to include measures to detect, mitigate and remediate any "cybersecurity threat" and "cybersecurity vulnerability" with respect to registered fund/adviser information systems.

Cybersecurity Incident Response and Recovery. The cybersecurity policies and procedures would be required to include measures to detect, respond to and recover from a cybersecurity incident, including policies and procedures that are reasonably designed to ensure:

- Continued operations of the registered fund/adviser;

- The protection of registered fund/adviser information systems;

- External and internal cybersecurity incident information sharing and communications; and

- Reporting of a "significant fund cybersecurity incident" (for registered funds) or a "significant adviser cybersecurity incident" (which may include private funds or clients).

The cybersecurity policies and procedures also would require written documentation of any cybersecurity incident, including the registered fund/adviser's response to and recovery from such an incident.

Note: *Under the Proposals, advisers and registered funds must adopt and implement written policies and procedures that are reasonably designed to address cybersecurity risks. This is particularly significant given that the SEC has held advisers liable for not implementing their own policies. In August 2021, for example, the SEC announced settlements with eight registered brokers and advisers related to alleged failures in cybersecurity safeguards that resulted in the exposure of customer information. The SEC noted that "it is not enough to write a policy requiring security measures if those requirements are not implemented or are only partially implemented," and reflected in the settlement orders a focus on the deployment of specific technical controls, including MFA. Notably, these settlements alleged violations of Regulation S-P. While Regulation S-P does not explicitly list required security measures, the SEC's "Cybersecurity and Resiliency Observations," published in January 2020, provides insight into what the Commission believes are "best practices" for cybersecurity, including data mapping, vulnerability scans, log retention, data encryption, and MFA.*

According to a statement on the Proposals released by Commissioner Hester M. Peirce, the only commissioner to oppose the new rules and amendments, detailed cybersecurity prescriptions could "become an easy hook for an enforcement action, even when a firm has made reasonable efforts to comply with the prescriptions."

IV. Board Oversight

For each registered fund,[3] the Proposals would require that the fund:

- Obtain the initial approval of the registered fund's board of directors, including a majority of the independent directors, of the fund's policies and procedures;
- Annually review and assess the design and effectiveness of its cybersecurity policies and procedures, including whether they reflect changes in cybersecurity risk over the time period covered by the review; and
- Provide, for review by the registered fund's board of directors, a written report prepared no less frequently than annually by the registered fund that describes the review, the assessment and any control tests performed, explains their results, documents any cybersecurity incident 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.

V. Annual Adviser Reviews

Similar requirements apply to advisers. Specifically, for each adviser, the Proposals would require the adviser to annually:

Review and assess the design and effectiveness of its 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 that describes the review, the assessment and any control tests performed, explains their results, documents any cybersecurity incident that has occurred since the adviser's last report, and discusses any material changes to the policies and procedures since the date of the last report.

VI. Recordkeeping

[3] The Proposals provide that, in the case of a unit investment trust (each, a "UIT"), the UIT's principal underwriter or depositor must (i) approve the fund's policies and procedures and (ii) receive all the written reports required in the case of a registered fund.

The Proposals would require that registered funds and advisers maintain various records related to their cybersecurity risk management programs. Under the new recordkeeping requirements, registered funds and advisers would be required to maintain records of (i) cybersecurity policies and procedures, (ii) annual reviews thereof,[4] (iii) documents related to the annual reviews, (iv) regulatory filings related to cybersecurity incidents required under the Proposals, (v) records documenting the occurrence of any cybersecurity incident, and (vi) cybersecurity risk assessments.

Looking Ahead

The Release requested comments on, among other things,

- Whether to exempt certain types of advisers or registered funds—including those with small staffs—from the proposed cybersecurity risk management rules
- Whether to scale the proposed requirements to the size of the adviser or registered fund
- Whether the proposed rules would require the right elements for cybersecurity policies and procedures
- Whether to include any other requirements, such as specific qualifications for certain employees
- Whether the proposed requirements and terms are clear
- Whether advisers and registered funds should be required to report cybersecurity incidents within a specific time frame
- Whether the annual review and report requirements are appropriate
- Whether a registered fund's board should be required to approve cybersecurity policies and procedures as part of their oversight
- Whether the "substantial harm" threshold for significant adviser cybersecurity incidents and significant fund cybersecurity incidents is appropriate
- Whether it is appropriate to require reporting 48 hours after having a reasonable basis to conclude there was a significant adviser cybersecurity incident or significant fund cybersecurity incident

We expect a significant number of comments on the Release and Proposals from various industry participants and other interested parties. Comments on the Proposals must be received by the SEC no later than April 11, 2022 or 30 days after the date of publication of the Release in the *Federal Register*, whichever is later.

While the Release does not set forth a compliance date or transition period (or explicitly request comments on timing), we expect comments to address the need to provide time for advisers and funds to comply.

* * *

If you would like to learn more about the issues in this Alert, please contact your usual Ropes & Gray attorney contacts.

[4] For registered funds, this would include the written reports provided to the fund's board of directors. In the case of UIT, this item would be the written reports provided to the UIT's principal underwriter or depositor.