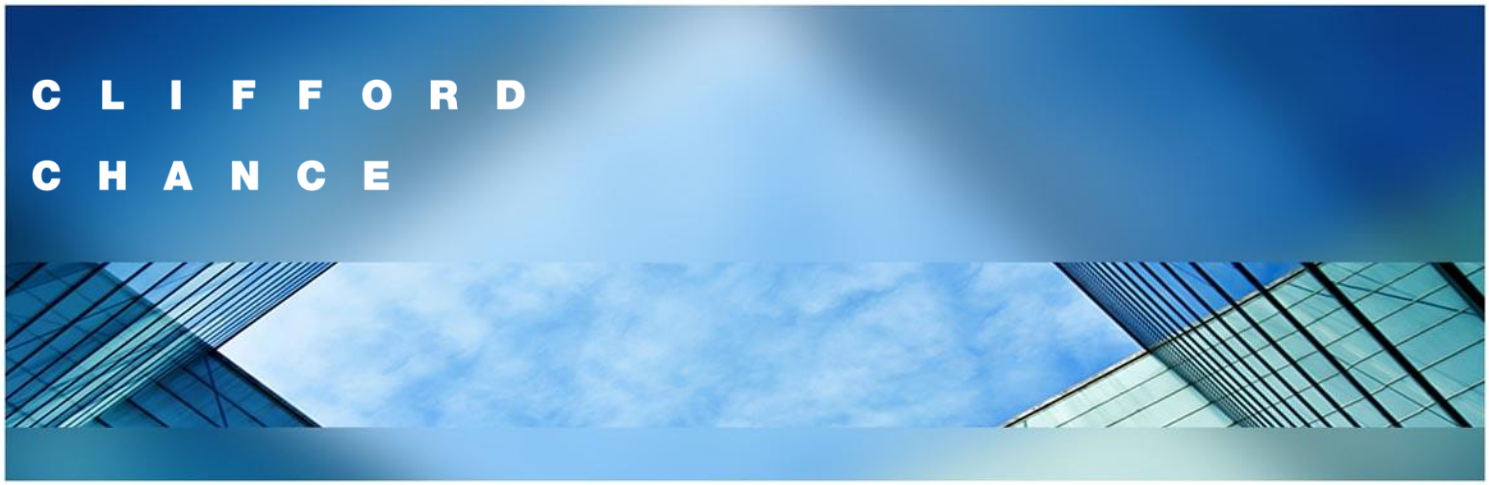

SEC PROPOSES SUBSTANTIAL NEW CYBERSECURITY REGULATIONS FOR REGISTERED INVESTMENT ADVISERS AND FUNDS

On February 9, 2022, the Securities and Exchange Commission voted 3-1 to propose rules and amendments that would require registered investment advisers and registered funds to confidentially report significant cybersecurity breaches to the SEC, disclose significant cybersecurity risks and incidents to clients, adopt written cybersecurity policies, and abide by new recordkeeping requirements. If enacted in similar form, these would be the first regulations to require investment advisers to disclose cybersecurity incidents.

There are no existing regulations that specifically require registered investment advisers ("advisers") and registered investment companies and business development companies ("registered funds") to report or disclose cybersecurity incidents or adopt comprehensive cybersecurity programs. Existing regulations, such as Regulation S-P and Regulation S-ID, indirectly address cybersecurity by requiring firms to adopt policies and procedures to protect investor data and guard against identify theft, but they do not mandate particular cybersecurity standards (such as conducting periodic risk assessments and implementing user access controls). In its discussion surrounding the proposed rules, the SEC observed that under the existing regulatory framework some advisers and registered funds lack sufficient cybersecurity preparedness, putting clients and investors at risk. Thus, the SEC concluded that mandating prescriptive cybersecurity policies and procedures is necessary. These proposed regulations represent a major development in the push by federal regulators to enhance cybersecurity protocols in the financial services industry. If enacted as proposed, these regulations would impose significant new regulatory requirements on advisers, including advisers to private funds, as well as enhanced disclosure requirements for registered funds.

Cybersecurity Incident Reporting

The proposed rules would require advisers to report significant cybersecurity incidents to the SEC. Importantly, advisers would be required to not only report their own significant incidents, but also those of their clients that are registered investment companies, registered business development companies, or private funds.

What Types of Incidents Would I Have to Report?

The proposed rules only require advisers to report "significant" cybersecurity incidents to the SEC. The proposed rules define a significant cybersecurity incident as an incident, or group of related incidents, that "significantly disrupts or degrades" a firm's ability to "maintain critical operations," or "leads to the unauthorized access or use of" firm information, which results in (1) substantial harm to the firm, or (2) substantial harm to a client or investor whose information was accessed. "Critical operations" include investment, trading, reporting, risk management, and operating in accordance with the federal securities laws. The SEC provided some examples of what it would consider significant cybersecurity incidents:

- A malware attack that shuts down a firm's internal computer, website, and email systems, leaving the firm's employees without the ability to make trades or manage a client's portfolio;
- A cyber attacker gaining access to a firm's systems and disclosing, modifying, or destroying firm or client data, or stealing intellectual property and client assets;
- A cyber attacker interfering with a firm’s ability to redeem investors, calculate NAV, or otherwise conduct its business.

This definition (if the rules are adopted) will likely be further refined through guidance.

When Would I Need to Report?

The proposed rules would require advisers to report a significant cybersecurity incident *within* 48 hours of having "a reasonable basis to conclude" that an incident has occurred or is occurring. This means advisers must not wait until they have definitively concluded an incident has occurred nor immediately report as soon as they have an initial suspicion an event has occurred. For context, the New York State Department of Financial Services (NYDFS) Cybersecurity Regulation and EU General Data Protection Regulation (GDPR) both require notification of cyber incidents within 72 hours, and banking regulators recently issued a final rule requiring notification within 36 hours. For more on the banking notification rule, see our briefing here.

How Would I Report?

The rules would require advisers to file a new form, called Form ADV-C, electronically on the Investment Adviser Registration Depository ("IARD") platform to fulfil their reporting requirement. This form would include questions regarding the nature and scope of the incident, as well as whether any disclosure has been made to any clients and/or investors. This rule would also require advisers to

amend any previously filed Form ADV-C within 48 hours if information reported becomes materially inaccurate, new material is discovered, or the adviser closes an internal investigation of the incident.

Would My Reporting Be Public?

Recognizing that publicly disclosing certain information regarding cybersecurity incidents could adversely affect advisers and their clients, the current proposed rules would require the SEC to keep filed Form ADV-Cs confidential.

Disclosure Of Cybersecurity Risks And Incidents To Clients

The proposed rules and amendments would also require advisers and registered funds to disclose information regarding cybersecurity incidents and risks to existing and prospective clients.

What Would I Have to Disclose?

Currently, under Form ADV Part 2A, advisers are required to provide narrative brochures to clients and prospective clients with information regarding the adviser's business practices, fees, risks, conflicts of interest, and disciplinary events. Under the proposed amendments, advisers would also be required to include information regarding significant cybersecurity incidents that have occurred within the past two years and cybersecurity risks that "could *materially* affect the advisory relationship" in these brochures. A cybersecurity risk would be considered material if "there is a substantial likelihood that a reasonable client would consider the information important" based on the circumstances. Factors to consider when determining materiality include whether the risk could result in disruption of services, loss of adviser or client data, or other harm to clients.

Similarly, the SEC also proposed amendments that would require registered funds to disclose in required registration statements details of any significant cybersecurity incidents that have occurred within the past two years to prospective and current investors.

When Would I Have to Disclose?

The proposed amendments would require advisers and registered funds to promptly provide interim updates to existing clients. For advisers, this would entail delivering interim brochure amendments to existing clients, and for registered funds, this would require amending their prospectuses by filing a supplement with the SEC. In addition, registered funds would also be required to include a discussion of cybersecurity risks and significant cybersecurity incidents in their annual reports to investors if the incidents materially affected the firm's performance during the fiscal year.

What Information Would I Have to Disclose?

When disclosing incidents, advisers and registered funds would be required to identify, to the extent known, what entities were affected, when incidents were discovered or if they are ongoing, whether data was compromised, the effect of the incident on the firm's operations, and whether the firm or service provider has remediated or is currently remediating the incident.

Cybersecurity Risk Management Policies And Procedures

The proposed rules would also require advisers and registered funds to adopt and implement written cybersecurity policies and procedures. These policies and procedures would have to include the following elements:

- Periodic risk assessments;
- Controls to minimize user-related risks and prevent unauthorized access to systems;
- Monitoring and measures to protect information security, such as encryption and network segmentation;
- Threat and vulnerability management; and
- Incident response and recovery protocols.

The rules would also require advisers and registered funds to review their cybersecurity policies and procedures at least once a year and provide written reports summarizing the review process and results. For registered funds, the board of directors, including a majority of its independent directors, would be required to approve the fund's cybersecurity policies and procedures and review the fund's written reports.

In proposing the rules, the Commission recognized that cybersecurity is not a "one-size-fits-all approach," and stated that their proposal aims to provide firms with flexibility to implement the above elements in ways that best fit their business and individual cybersecurity risks. The proposed rules would also allow firms to outsource implementation and administration of their cybersecurity protocols to a third-party, so long as there is proper oversight, and the service provider is empowered to escalate issues to senior officers of the firm.

Recordkeeping

Finally, the proposed rules would impose recordkeeping requirements, under which advisers and registered funds would be required to keep, among other things, copies of their cybersecurity policies from the last five years, copies of documents regarding annual cybersecurity reviews, and records documenting cybersecurity incidents.

Takeaways

Although these regulations are only proposals at this time, and likely will generate robust industry comment, advisers, including advisers to private funds, and registered funds should consider taking steps now that are reasonably designed to ensure future compliance. These measures include taking inventory of existing cybersecurity policies and procedures and conducting risk assessments to identify significant vulnerabilities. These measures will not only provide a head start towards future compliance, but they will also help protect what is increasingly becoming one of an adviser or fund's most valuable assets: IT infrastructure and sensitive data (including personal data).

Public comment will remain open on these proposed regulations until April 11, 2022, or 30 days from when they are published in the Federal Register, whichever period is longer.

Clifford Chance has published a number of reports to help financial services firms and other companies protect themselves from cyber attacks and comply with international reporting requirements. For more information, see our Report on What Cyber Regulators Are Saying Around the World as well as our Ransomware Playbook.

CONTACTS

Daniel Silver
Partner

T +1 212 878 4919
E daniel.silver
@cliffordchance.com

Megan Gordon
Partner

T +1 202 912 5021
E megan.gordon
@cliffordchance.com

Steven Gatti
Partner

T +1 202 912 5095
E steven.gatti
@cliffordchance.com

Brian Yin
Associate

T +1 212 878 4980
E brian.yin
@cliffordchance.com

Shannon O'Brien
Law Clerk

T +1 212 880 5709
E shannon.obrien
@cliffordchance.com

www.cliffordchance.com

Clifford Chance, 31 West 52nd Street, New York, NY 10019-6131, USA