Katten

PRIVACY, DATA AND CYBERSECURITY AND
FINANCIAL MARKETS AND FUNDS ADVISORY

Client Alert: Proposed SEC Rules for Investment Advisers and Regulated Funds, and New FTC Safeguard Rule Applicable to Private Funds

March 3, 2022

On February 9, 2022, the Securities and Exchange Commission (SEC) voted to propose new rule 206(4)-9 under the Investment Advisers Act of 1940 (Advisers Act) and 38a-2 under the Investment Company Act of 1940 (collectively the "Proposed Rules") to address cybersecurity risks. The Proposed Rules would apply to registered investment advisers (RIAs), registered investment funds (funds) and business development companies (BDCs) (collectively "firms"). If adopted, the Proposed Rules will impose sweeping compliance obligations on firms by requiring them to:

1. Adopt and implement written cybersecurity policies and procedures reasonably designed to address cybersecurity risks;
2. Report cybersecurity incidents affecting the adviser, its funds or clients to the SEC on a proposed Form ADV-C and "significant" cybersecurity incidents within 48 hours to the SEC;
3. Disclose significant cybersecurity risks and incidents; and
4. Require new recordkeeping requirements pertaining to certain cybersecurity practices.

As described in more detail below, the Proposed Rules accentuate SEC Chairman Gary Gensler's continued prioritization and focus on cybersecurity, particularly in light of the hybrid workforce and firms' increasing dependencies on technology.

The Proposed Rules will be open for public comment for 60 days following the publication of the proposing release on the SEC's website or 30 days following the publication of the proposing release in the Federal Register, whichever period is longer.

Comprehensive Cybersecurity Program

The Proposed Rules would require firms to develop and implement written cybersecurity policies and procedures that are reasonably designed to address cybersecurity risks that could harm RIAs and the funds and BDCs that they manage, in accordance with fiduciary obligations imposed on RIAs pursuant to the Advisers Act (the Cybersecurity Program). For funds and BDCs, the Cybersecurity Program will need to be approved by the board and the board must ensure sufficient resources are committed to implementing the Cybersecurity Program.

The Cybersecurity Program must include, amongst other things, (1) a risk assessment of service providers and information systems handling client and fund information; (2) implementation of user security and access controls to protect confidential, fund or investor information; (3) a periodic assessment of information systems containing fund or adviser information; and (4) policies and procedures to address cybersecurity incidents, threats and vulnerabilities.

The Proposed Rules would require a firm to review its Cybersecurity Program no less than annually and draft a report detailing this assessment. The report must detail any cybersecurity incident that occurred during the reporting period and discuss any material changes to the Cybersecurity Program since the last annual report.

Reporting Significant Cybersecurity Incidents and Proposed Form ADV-C

The Proposed Rules would require RIAs to submit proposed Form ADV-C promptly, but in no event more than 48 hours, after having a reasonable basis to conclude that a significant adviser cybersecurity incident or a significant fund cybersecurity incident had occurred or is occurring.[1]

Proposed Amendments to Form ADV Part 2A and Disclosure of Cybersecurity Risks and Incidents

The Proposed Rules seek to amend the Form ADV narrative brochure, or Part 2A, by adding a new Item 20 entitled "Cybersecurity Risks and Incidents." RIAs would be required to provide disclosures to clients and prospective clients regarding cybersecurity risks and incidents that could materially affect the advisory services they offer and describe how they address such risks.

The Proposed Rules also would require a RIA to describe any cybersecurity incidents that occurred within the last two fiscal years that have significantly disrupted or degraded the adviser's ability to maintain critical operations, or that have led to the unauthorized access or use of adviser information, resulting in substantial harm to the adviser or its client. In addition, the SEC is also proposing amendments to funds' registration statements, requiring disclosure of any significant cybersecurity incident during the last two fiscal years.

Cybersecurity-Related Recordkeeping Requirements

The Proposed Rules contain new reporting and compliance requirements, requiring firms to maintain certain records for five years, including: (1) the Cybersecurity Program; (2) annual reviews thereof; (3) reports provided to a registered fund's or BDC's board regarding cybersecurity; (4) any Form ADV-C filed by a RIA; (5) regulatory filings related to cybersecurity incidents; (6) any cybersecurity incident; and (7) cybersecurity risk assessments.

The FTC's Recent Amendments to the Standards for Safeguarding Nonpublic Personal Information

On October 27, 2021, the Federal Trade Commission (FTC) announced revisions to the Gramm-Leach-Bliley Act (GLBA) by amending the standards for safeguarding nonpublic personal information (NPI) under the GLBA's "Safeguards Rule" (the Final Rule). The FTC announced that the Final Rule was required due to significant harm caused to consumers, including monetary loss, identity theft and other forms of financial distress, as a result of data breaches and other cybersecurity concerns. The Final Rule was published in the Federal Register on December 9, 2021. The Final Rule is effective on January 10, 2022, however, most of the substantive provisions of the Final Rule take effect a year from the publication date.

The Final Rule requires non-banking financial institutions subject to the FTC's jurisdiction under the GLBA to develop, implement and maintain a comprehensive security system to protect NPI. Private investment funds are generally subject to the FTC's Safeguards Rule. Although the Final Rule currently does not include the disclosure, regulatory reporting and recordkeeping requirements of the SEC's Proposed Rules, the Final Rule's requirements with respect to protecting against cybersecurity breaches are more prescriptive than the Proposed Rules. Specifically, the Final Rule:

[1] The Proposed Rules define a "significant" cybersecurity incident as "a cybersecurity incident, or a group of related incidents, that significantly disrupts or degrades the adviser's ability . . . 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 . . . whose information was accessed."

1. Implements more detailed requirements for the development and establishment of an information security program, including conducting a risk assessment and incorporating written provisions related to access controls, data mapping, authentication, encryption, information disposal protocols, incident response management, change management, employee training and vendor management; and
2. Requires financial institutions to designate a single qualified individual to oversee the information security program, and further requires such qualified individual to provide periodic written reports to an institution's board of directors or governing body.[2]

Both the Final Rule and the SEC's Proposed Rules require oversight of service providers to private funds and RIAs, including requiring service providers to agree by contract to implement appropriate cybersecurity safeguards.

In addition to the Final Rule, the FTC is also seeking public comment on whether to further amend the Safeguards Rule to require covered financial institutions to report certain data breaches and other security events to the FTC.[3] The FTC has announced that it soon will publish a supplemental Notice of Proposed Rulemaking, after which the public will have 60 days to submit comments.

To the extent that a private fund is managed by an adviser that is registered with the SEC, the RIA to the private fund will need to be cognizant of addressing both the requirements of the Final Rule and the SEC's Proposed Rules as adopted. In regard to this, the SEC stresses that the Proposed Rules are designed to address the cybersecurity risks created as a result of a RIA's operations and are not limited to the protection of customer financial information by private funds as in the case of the Final Rule.

Conclusion

Navigating through the complex regulatory landscape can be challenging for investment advisers, funds and BDCs. Developing a dynamic cybersecurity program to address the evolving cybersecurity threat landscape in the digital world can be overwhelming. If you have any questions regarding these proposed rules and amendments to the Investment Advisers Act, Investment Company Act and Form ADV, the GLBA, or questions otherwise relating to the above alert, please contact us.

[2] The Final Rule provides an exemption from requirements related to written risk assessments, incident response plans and annual reporting to the board of directors, for financial institutions that collect information on fewer than 5,000 consumers.

[3] The proposed amendment would require covered financial institutions to report a data breach affecting or reasonably likely to affect at least 1,000 consumers through a form on the FTC's website within 30 days of discovery of the breach and would require certain specified disclosures.

CONTACTS

For more information, contact your Katten attorney or any of the following:

Trisha Sircar
Privacy, Data and Cybersecurity
+1.212.940.8532
trisha.sircar@katten.com

David Y. Dickstein
Financial Markets and Funds
+1.212.940.8506
david.dickstein@katten.com

Richard D. Marshall
Financial Markets and Funds
+1.212.940.8765
richard.marshall@katten.com

Vlad M. Bulkin
Financial Markets and Funds
+1.202.625.3838
vlad.bulkin@katten.com

Katten katten.com

CENTURY CITY | CHARLOTTE | CHICAGO | DALLAS | LONDON | LOS ANGELES | NEW YORK | ORANGE COUNTY | SHANGHAI | WASHINGTON, DC

3/1/22