SEC Proposed Rules on Cybersecurity.

Background

The Securities and Exchange Commission (SEC) is proposing new rules to require registered funds (RFs) and registered investment advisers (RIAs) to implement comprehensive cybersecurity programs.

Timings

The comment period will run for the longer of either 60 days from February 9, 2022, or 30 days after publication of the proposal in the Federal Register.

Scope of application

The proposed rules will apply to RFs and RIAs; private funds will not be subject to the rule, however the RIAs that advise them will be.

Distinctions

Existing rules, such as Regulation S-P and S-ID, are mainly focused on protecting customer data; the proposed rules center on protecting systems, the data within them, and improving overall cybersecurity practices.

Rationale – Cybersecurity risk management

RFs and RIAs face numerous cybersecurity risks and may experience cybersecurity incidents that can cause, or be exacerbated by, critical system or process failures.

Objective

To address cybersecurity risks faced by RFs and RIAs to better protect clients and investors.

Proposal

Under the proposed rules, RFs and RIAs would be required to maintain and implement written cybersecurity policies and procedures, adopt new recordkeeping standards, report certain incidents to the SEC, and disclose cybersecurity risks and incidents to clients and investors.

Policies and Procedures

RFs and RIAs will be required to maintain and implement written policies and procedures that are reasonably designed to address the following elements:

- risk assessment;
- user security and access control;
- information protection;
- threat and vulnerability management; and
- incident response and recovery.

RFs and RIAs will need to conduct an annual review of cybersecurity policies and procedures, and produce a written report of such review.

Recordkeeping

RFs and RIAs will be required to maintain records of and related to:

- cybersecurity policies and procedures;
- annual reviews of cybersecurity policies and procedures;
- cybersecurity incident filings provided to the Commission;
- the occurrence of any cybersecurity incident, including any records related to any response and recovery from such an incident; and
- cybersecurity risk assessments.

Incident reporting

RIAs will be required to submit a form electronically to the SEC promptly (but in no event more than 48 hours) where they reasonably believe that a Significant Adviser/Fund Cybersecurity Incident has occurred or is occurring. The form asks questions about the Significant Adviser/Fund Cybersecurity Incident, such as its nature and scope as well as whether any disclosure has been made to any clients and/or investors.

Significant Adviser/Fund Cybersecurity Incident

Defined as a cybersecurity incident (group of related incidents) that:

- significantly disrupt(s) or degrade(s) the RIA/RF's ability (or the ability of a private fund client of an RIA) to maintain critical operations; or
- leads to the unauthorized access or use of RIA/RF information, resulting in substantial harm to the RIA/RF, a client, or an investor in a private fund, whose information was accessed.

RIA Disclosure

In disclosure brochures, RIAs will be required to describe:

- cybersecurity risks that could materially affect the advisory services they offer and how they assess, prioritize, and address cybersecurity risks created by the nature and scope of their business; and
- 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 clients.

RF Disclosure

On registration statement forms, RFs will be required to:

- describe any significant fund cybersecurity incident that has occurred in its last two fiscal years;
- disclose to investors in its registration statement whether a significant fund cybersecurity incident has or is currently affecting the fund or its service providers; and
- describe cybersecurity risks determined to be "principal risks."

Supplemental Disclosure

RIAs will be required to deliver interim brochure amendments to existing clients promptly if the RIA adds disclosure of a cybersecurity incident to its brochure or materially revises information already disclosed in its brochure about such an incident. RFs will be required to include cybersecurity risks and significant fund cybersecurity incidents in annual reports to shareholders

WHAT WE CAN DO FOR YOU

The new rules are very likely to come into force during the course of this year (2022). We therefore recommend that RFs and RIAs start to make preparations for the implementation of the new rules through internal testing and by reviewing their existing policies, procedures, and practices.

Any aspects of the proposed rules that are unable to be complied with should be raised during the comment period.

Please let us know if you would like to discuss the new rules and the preparations that should be made:

Key contacts

Gerard Stegmaier
Partner, Washington D.C.
+1 202 414 9228
gstegmaier@reedsmith.com

Howard Womersley Smith
Partner, London
+44 (0)20 3116 3498
hwsmith@reedsmith.com