February 9, 2022

SEC Proposes Cybersecurity Rules for Registered Investment Advisers and Funds

Acknowledging the gravity of cybersecurity threats to investment advisers and funds, and by extension their tens of millions of clients and trillions of dollars of assets under management, the Securities and Exchange Commission today proposed rules under the Investment Advisers Act of 1940 and the Investment Company Act of 1940 pertaining to cybersecurity risk management by registered investment advisers ("RIAs") and investment companies ("funds"). The proposal complements the Biden administration's prioritization of cyber threats to economic security (as we have recently discussed) and, as a crystallization of the SEC's views on best practices for cybersecurity risk management, has significance beyond the investment industry. The proposal encompasses the following:

- *Cybersecurity Risk Management Policies and Procedures*. RIAs and funds would be required to formally implement written policies and procedures to address cybersecurity risks, which should be tailored based on the applicable business operations and cybersecurity risk profile, and should be reviewed and evaluated at least annually, with the evaluation summarized in a written report. Funds' boards of directors would also be required to approve the policies and procedures and review written reports of the evaluations. Mandatory elements of these policies and procedures would include periodic risk assessment and information systems assessment, implementation of controls designed to minimize user-related risks and prevent unauthorized access to information and systems, protocols for threat and vulnerability management, and plans for incident response and recovery.

- *Reporting of Significant Cybersecurity Incidents*. The SEC would establish a new reporting regime whereby RIAs would be required to confidentially report to the SEC significant cybersecurity incidents within 48 hours of discovery, on a new proposed Form ADV-C, with the twin objectives of helping the SEC assess the effects of the incident on the reporting RIA, and to help the SEC obtain enhanced visibility into systemic risks.

- *Enhanced Disclosure of Cybersecurity Risks and Incidents*. Proposed amendments to existing RIA and fund disclosure requirements would require enhanced disclosure regarding cybersecurity risks and incidents.

- *Recordkeeping Requirements*. RIAs and funds would be subject to new recordkeeping requirements for cybersecurity-related books and records, generally requiring maintenance for five years.

We have long highlighted the critical importance for public companies of maintaining effective disclosure controls concerning cybersecurity breaches and risks, and that boards of directors maintain focus on oversight of cybersecurity risks, including cultivating an understanding of the idiosyncratic risks companies face based on the systems they use and data they collect. We have also repeatedly stressed the need to maintain robust written policies and procedures with respect to cybersecurity protective measures, incident detection and response, and disclosure protocols. Apart from their direct applicability to RIAs and funds, the SEC's new proposed rules constitute a significant step toward formalization of national standards and regulatory expectations for corporate approaches to cybersecurity risk management, public disclosure of cyber-related risks, and timely regulatory and public notification of significant cyber incidents. As cybersecurity threats proliferate and become ever more sophisticated, companies both within and without the investment industry should carefully consider the SEC's prescriptions and consider whether any or all of these proposed components should be integrated into their existing cybersecurity risk management systems and procedures.

John F. Savarese
Sarah K. Eddy
David M. Adlerstein
Jeohn Salone Favors
Amanda M. Lee