Bond Case Briefs

Municipal Finance Law Since 1971

SEC Signals Heightened Scrutiny of Cybersecurity Practices.

On January 7, 2020, the U.S. Securities and Exchange Commission's (SEC) Office of Compliance Inspections and Examinations (OCIE) announced its 2020 Examination Priorities that included cybersecurity practices. Soon after the publication of the OCIE Examination Priorities, on January 27, 2020, OCIE followed-up with a report entitled Cybersecurity and Resiliency Observations. These two OCIE releases, along with prior SEC alerts and actions, provide strong indications that the SEC, in 2020, will be ramping up its focus on cybersecurity practices in the financial services industry. We expect increased examination and enforcement activities concerning cybersecurity practices, including vendor management and controls.

2020 Examination Priorities: Information Security

OCIE's 2020 Examination Priorities include information security practices for investment advisers, broker dealers, municipal advisers, and other registered entities that fall within the scope of OCIE's programs. As in previous years, OCIE is prioritizing information security practices in the industry to bolster investor and financial market confidence given the potential risk if massive data breaches were to occur. Information security examinations for 2020 will, therefore, include the following:

- Proper configuration of network storage devices
- Information security governance
- Retail trading information security
- Protection of registered investment advisers (including robo-advisers) clients' personal financial information, including: governance and risk management, access controls, data loss prevention, vendor management, training and incident response and resiliency
- Oversight practices of certain service providers and network solution, including firms leveraging cloud-based storage
- Compliance with Regulations S-P and S-ID
- Controls surrounding online access and mobile application to customer brokerage account information
- Safeguards regarding proper disposal of retired hardware possibly containing client or network information

OCIE also encourages market participants to engage with regulators and law enforcement to identify and address security risks like cyber-related attacks.

OCIE Cybersecurity and Resiliency Observations

This OCIE report, issued within the same month as the OCIE Priorities, discussed industry practices to manage and combat cybersecurity risk and to maintain operational resiliency that OCIE has observed through "thousands of examinations of broker-dealers, investment advisers, clearing agencies, national securities exchanges and other SEC registrants…" Here's our take:

- The observed industry practices covered areas of governance and risk management, access rights and controls, data loss prevention, mobile security, incident response and resiliency, vendor

management, and training and awareness.

- By putting all financial industry participants on notice regarding the availability of such practices, we believe the SEC is setting the stage to bring enforcement actions against financial industry participants that fail to adopt practices that are the equivalent to or reasonably meet the goals of the currently observed industry practices.
- Further, the report is yet another step toward creating a basis for future SEC enforcement cases related to deficient practices and controls of third party vendors that have access to client and customer data. The OCIE report devotes a separate section to vendor management, including cyber and privacy related due diligence, as well as robust contract language providing clear rights of the registrant to address a cyber incident arising out of a vendor relationship, monitoring and training. The SEC has historically not been shy about holding companies responsible for violations facilitated (or caused) by their third parties, and this would seem to be a logical extension of that approach.
- In 2015, the SEC brought its first ever enforcement action against an investment adviser in connection with a cyber breach. The action involved a breach of a third party-hosted web server that held personally identifiable information (PII) of the investment adviser's clients. The SEC faulted the investment adviser for failing to have any written policies to safeguard client PII. At the time, the SEC did not set forth any requirements to assess outside vendor's ability to safeguard client data.
- In May 23, 2019, OCIE issued a Risk Alert regarding the need to safeguard customers and information in network storage including the use of third party security features and cloud-based storage. Among other things, OCIE expressed concerns with inadequate oversight of vendor-provided network storage solutions.
- In the recent Report, OCIE specifically identified industry practices on vendor management that includes vendor monitoring and testing.

Recommended action

Given the prominence of information security in OCIE's 2020 Examination Priorities, registered firms should ensure that their policies and procedures appropriately account for risks to customer records and to IT systems in accordance with Regulation S-P Rule 30. With regard to broker-dealers specifically, FINRA will play an important part in this trend toward greater regulatory oversight. Indeed, FINRA expects all firms to implement policies and procedures related to cybersecurity, but expects that firms will approach these challenges in accordance with their scale and model.

Finally, in light of OCIE's report on industry practices, registered firms also should review their current procedures and processes to determine whether they are equivalent to or reasonably meet the goals of the practices described in the Report, and whether further enhancements are appropriate or necessary.

Baker McKenzie – Bernard (Brian) L. Hengesbaugh, Harry Valetk, Amy J. Greer, Jennifer L. Klass, A. Valerie Mirko, Peter K.M. Chan and Jerome Tomas

February 4 2020