Client Update

SEC Issues Cybersecurity Guidance for Registered Investment Advisers and Funds

NEW YORK
Jeremy Feigelson
jfeigelson@debevoise.com

James J. Pastore, Jr.
jjpastore@debevoise.com

Christopher S. Ford
csford@debevoise.com

WASHINGTON, D.C.
Kenneth J. Berman
kjberman@debevoise.com

Jeffrey P. Cunard
jpcunard@debevoise.com

Robert B. Kaplan
rbkaplan@debevoise.com

David A. O'Neil
daoneil@debevoise.com

The SEC's Division of Investment Management has issued an IM Guidance Update addressing cybersecurity issues faced by registered investment advisers (including private fund managers) and registered investment companies (in plain English, "funds"). The IM Guidance Update makes plain that registered investment advisers and funds need to actively manage their cybersecurity risks — and be prepared to respond in the event of a cyberattack or data breach — or risk running afoul of the U.S. federal securities laws.[1]

In the Division's view, for example, failure to mitigate exposure to compliance risks associated with cyber threats through compliance policies and procedures could violate the rules under the U.S. Investment Advisers Act of 1940 and the U.S. Investment Company Act of 1940 that require registered investment advisers and funds to adopt and maintain written policies and procedures designed to assure compliance with federal securities laws. These rules also require annual reviews to ensure that the policies are adequate and effectively implemented. Similarly, the IM Guidance Update states that failure to mitigate harm from cyberattacks that expose personal identification information, or that prevent investors from exercising their legal rights (*e.g.*, where a shareholder in an open-ended fund is prevented from redeeming shares due to disruption from a cyberattack), could be construed as violations of the SEC's identity theft red flag rules or Section 22(e) of the Investment Company Act (in the event that a cyberattack prevents a fund from meeting redemption requests).

[1] The full text of the guidance is available through the Investment Management Division webpage, http://www.sec.gov/investment, or in PDF format at http://www.sec.gov/investment/im-guidance-2015-02.pdf.

The IM Guidance Update thus reinforces a clear regulatory trend: cybersecurity standards that might previously have been seen simply as common sense or best IT practice can now, in effect, have the force of law.

RISK MITIGATION

The Division's views with respect to risk mitigation closely mirrors other leading cybersecurity standards, like the Framework issued by the National Institute of Standards and Technology. Specifically, the Division recommends that funds and investment advisers conduct periodic assessments of:

- where they store sensitive information (like Social Security numbers, bank account details, or passport information), and how they secure that information;
- what cybersecurity threats the firm faces, including both insiders (*e.g.*, the disgruntled employee) and outsiders (*e.g.*, hackers and other cybercriminals);
- how the firm's IT infrastructure may be vulnerable to those threats;
- what security controls and processes the firm has — or should — put into place to mitigate those threats;
- what impact a breach or disruption would have on the firm's systems, and what backups are in place to mitigate those effects; and
- how the firm's governance structure addresses and manages cybersecurity risk.

BREACH DETECTION AND RESPONSE

In addition to mitigating risks, the IM Guidance Update recognizes it is simply not possible to prevent every cyberattack. The Division's guidance indicates that registered funds and advisers should:

- Control access to firm systems, especially those that contain sensitive data, using both technical means (firewalls, strong user credentials like two-factor authentication) and employee training that reduces the possibility of insider attacks;
- Encrypt sensitive data wherever it exists on the firm's network, back up that data, and restrict the use of removable storage media (like USB thumb drives) that could lead to sensitive data moving outside the firm's control;
- Deploy software that monitors for unauthorized activity and other unusual events — and be sure to regularly update that software and the firm's

knowledge base of what cyber threats are facing the financial services sector (*e.g.* through participating in information-sharing groups like FS-ISAC);

- Develop a detailed incident response plan and test that plan regularly to ensure that it will be effective when a breach actually occurs; and
- Implement policies and procedures, and conduct regular training, to ensure that fund officers and employees understand cybersecurity risks and how to respond to incidents.

Good breach detection works best when good risk mitigation is already in place. Understanding where the adviser or fund stores sensitive information (mitigation) is a necessary step before securing that information and identifying intrusions (detection) is possible.

The IM Guidance Update notes that a firm's obligations in this regard don't stop at the front door. Nearly all registered funds and investment advisers rely on third-party vendors and service providers to carry out their day-to-day operations — meaning a cyberattack on one of those third parties may have the same impact as an attack on the firm itself. The IM Guidance Update specifically highlights the importance of assessing vendors' cybersecurity policies and procedures, including by using contractual provisions to ensure a minimum level of compliance.

The IM Guidance Update, coupled with the recent report by the SEC's Office of Compliance Inspections and Examinations concerning its cybersecurity examination sweep, provides a roadmap for the policies and practices that funds and investment advisers should already be implementing with respect to cybersecurity mitigation and breach response.[2] Firms of every size and prominence are targets, although the nature of their risks may vary. While acknowledging that it is not possible for a fund or adviser to anticipate and prevent every cyberattack, the Division now has clearly communicated its expectations that firms will conduct thorough, thoughtful, and repeated assessments of what risks the firm faces, how to reduce those risks, and how to respond in the event of a breach or attack. By highlighting the risk that a firm could violate U.S. federal law if it fails to do so, the IM Guidance Update makes it clear that cybersecurity is not only an IT issue, it is also a compliance issue that

---

[2] *See* OCIE Cybersecurity Examination Sweep Summary, National Exam Program Risk Alert, Vol. IV, Issue 4 (Feb. 3, 2015), http://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf. We have also previously written about OCIE's priorities for 2015, in an update available at http://www.debevoise.com/insights/publications/2015/02/what-will-the-eyes-and-ears-of-the-sec-choose.

should be on the minds of every officer and employee. Registered investment advisers, including private fund sponsors, should be proactive in identifying the cybersecurity risks of their business and reviewing their compliance policies and procedures to confirm that these risks are addressed.

* * *

Please do not hesitate to contact us with any questions.