Harvard Law School Forum on Corporate Governance

SEC Cyber Enforcement Actions: Lessons for Private Fund Managers

Posted by Jason Daniel, Jenny Walters and Natasha Kohne, Akin Gump Strauss Hauer & Feld LLP, on Wednesday, September 22, 2021

Editor's note: Jason Daniel is partner, Jenny Walters is senior practice attorney and Natasha Kohne is partner at Akin Gump Strauss Hauer & Feld LLP. This post is based on their Akin Gump memorandum.

On August 30, 2021, the Securities and Exchange Commission announced three enforcement actions against registered investment advisers for alleged cybersecurity failures involving cloud-based email systems. All three actions (which were settled) imposed six-figure penalties on the advisers, despite the Staff's acknowledgement that none of the actions resulted in any unauthorized trades or fund transfers to unauthorized parties for any client accounts and despite the relatively small number of clients involved.

These three enforcement actions are just the latest example of the SEC's focus on cybersecurity for the past several years. Since 2015, the agency and its staff have issued risk alerts, brought enforcement actions and included cybersecurity as a stated priority examination area. These actions illustrate that cybersecurity responsibilities are, without doubt, part and parcel of an investment adviser's overall duties, including the obligations under Regulation S-P to adopt "written policies and procedures that address administrative, technical and physical safeguards for the protection of customer records and information."

Background

In each of the three enforcement actions, cloud-based email accounts of firm personnel were taken over by unauthorized third parties. The SEC found that these breaches compromised or potentially compromised the personally identifying information (PII) of thousands of clients.

As a general matter, the SEC alleged that the advisers, each of which had written cybersecurity policies and procedures, failed to design and enforce them in a sufficient manner as it related to cloud-based email accounts. For example, two of the firms recommended—but did not require—their independent contractors to use multi-factor authentication (MFA) for accessing sensitive data. Although the third firm's policies and procedures *did* require the use of MFA, several of its personnel accounts did not have MFA activated. Moreover, in the wake of the email breaches, the firms either did not activate MFA, or waited months or years to do so, resulting in the exposure and potential exposure of additional customer and client records and information. These allegations are consistent with the SEC's 2019 Risk Alert encouraging investment advisers to review the security settings and actively oversee vendors relating to third-party storage of electronic customer information (see our related alert here).

In addition, the orders allege that the firms failed to apply their policies for MFA to independent contractors and offshore contractors, whose systems and access to sensitive data were generally at the same or higher risk of compromise than the firms' employees.

The orders also allege failures to adopt written policies and procedures for additional firm-wide security measures in the wake of the email take-overs and even further delays in implementing these additional security measures, effectively allowing additional accounts to be breached and additional client PII to be exposed for up to three years.

Finally, in one of the actions, the SEC found that the firm sent clients breach notifications with misleading language suggesting that the notifications were issued much sooner than they actually had been after the incidents were discovered.

Violations

All three of the advisers were charged under Rule 30(a) of Regulation S-P,[1] known as the "Safeguards Rule." The Safeguards Rule requires every registered investment adviser to adopt written policies and procedures reasonably designed to:

1. Insure the security and confidentiality of customer records and information.
2. Protect against any anticipated threats or hazards to the security or integrity of the customer records and information.
3. Protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.

According to the orders, in all three cases, the cloud-based email accounts of the firms' employees and independent contractors were "taken over" by unauthorized third parties, resulting in exposure of PII. The orders allege that all three firms failed to take adequate steps to protect client data, either due to the failure to comply with their policies, or the failure to revise policies in response to cybersecurity breaches.

The SEC also found that the adviser that sent allegedly misleading breach notifications to clients violated Section 206(4) of the Investment Advisers Act of 1940 (which prohibits "fraudulent, deceptive, or manipulative" acts). There, the SEC found that the notifications contained misleading language regarding the date of the intrusion, which created the misimpression of a prompt response.

Without admitting or denying the SEC's findings, each firm agreed to cease and desist from future violations of the charged provisions, to be censured and to pay a penalty ranging from $200,000 to $300,000.

Lessons for Private Fund Managers

These enforcement actions send strong messages regarding compliance and implementation of cybersecurity policies and procedures, particularly related to cloud-based storage, the need to enable MFA on cloud-based email accounts, and the prohibition on making misleading statements in breach notices. As the Chief of the SEC Enforcement Division's Cyber Unit stated in the Release, "It is not enough to write a policy requiring enhanced security measures if those

requirements are not implemented or are only partially implemented, especially in the face of known attacks."

In particular, these actions provide several actionable lessons for private fund managers:

- ***More Work for the CCO***. The primary take-away for legal and compliance personnel is that the SEC deems cybersecurity to be within scope of a Chief Compliance Officer's responsibility. While one of these actions involved allegedly fraudulent statements about a cyber-breach, two did not—and those two firms received a cease and desist order, a censure, and a six-figure fine. Legal and compliance personnel who are relying on other departments to handle cybersecurity without Compliance oversight or, at the least, input and validation, should consider becoming more involved in the cybersecurity effort.
- ***Call out Regulation S-P in Policies, Reviews, and Training***. Private fund managers with strong cybersecurity programs often consider the elements of the program as a best practice, and not as a response to a specific regulatory mandate. While this approach may not cause concerns in most cases, when cyber-incidents occur, it would be useful to be able to demonstrate that the manager's policies and procedures were rigorous and that they specifically addressed the requirements of Regulation S-P to have written policies and procedures reasonably designed to: (1) insure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security or integrity of the customer records and information; and (3) protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer. A registered investment adviser should consider each of the above requirements in the annual compliance review, and—as with all material risk areas—consider targeted training in these areas.
- ***Know Your Coverage***. Many private fund managers have insurance coverage that could provide financial assistance in responding to a cyber-incident. A manager that expects to make a claim under an insurance policy will want to consider providing notice to the carrier in a timely manner.
- ***Don't Forget Your Other Regulators***. Fund managers that manage commodity pools and are National Futures Association members must also comply with NFA's Interpretive Notice 9070's cybersecurity-related compliance requirements, which includes – among other things – proactive planning requirements as well as obligations to establish an incident response plan that provides a framework for managing detected security events, analyzes potential impacts, and proposes appropriate measures to contain and mitigate breaches. NFA member firms must also notify the NFA of any cybersecurity incidents that result in the loss of customer or counterparty funds or the firm's own capital, or where the firm otherwise is required to notify its customers or counterparties pursuant to U.S. state or federal law. Managers regulated in non-U.S. jurisdictions also often have policy and notification obligations under local laws and regulations.
- ***Know Your Limitations***. Responding to a cyber-incident requires specific knowledge and experience. These SEC actions indicate that an honest but uninformed effort that does not satisfy the law could still expose a manager to liability, as would untimely and inadequate remediation of previously discovered compromises. Legal and compliance personnel should discuss these types of issues in advance with their counsel and also consider "table top" and similar exercises to map out responses to various cyber incidents.

- ***Know Your Lawyer***. One of these actions involved an allegedly misleading response, which triggered additional penalties. The manager's internal or external counsel, and not investor relations, needs to be in control of any response to ensure that partial or misleading statements do not add to a manager's problems. Allowing counsel to direct the investigation and manage the response also allows more communications to fall within the attorney-client (or a similar) privilege.