Westlaw Today
powered by Reuters

Cybersecurity update for private fund managers: lessons from recent SEC enforcement actions

By Marc E. Elovitz, Esq., Kelly Koscuiszka, Esq., and Edward H. Sadtler, Esq., Schulte Roth & Zabel LLP*

OCTOBER 14, 2021

The Securities and Exchange Commission ("SEC") has highlighted cybersecurity risks to investment advisers for many years and routinely reminds firms of their obligations as fiduciaries and under other applicable laws. Cybersecurity is also a common part of exam staff sweeps and enforcement inquiries.

In June, the SEC Enforcement staff reached out to numerous companies, including private funds, in what it described on its website as a "confidential fact-finding investigation" of the December 2020 SolarWinds attack. While providing a response was voluntary, the SEC staff offered that it would not recommend charges against victims who agreed to provide information about the widely publicized attacks.[1] A recent trio of enforcement actions against investment advisory firms and broker-dealers shows how seriously the SEC takes cybersecurity risks and provides lessons for private fund managers on how to satisfy these obligations.

In its enforcement of the Safeguards Rule, the SEC staff has focused its attention on cybersecurity policies and procedures.

On Aug. 30, 2021, the SEC announced[2] the settlement of charges in three separate enforcement actions against investment advisers and broker-dealers for deficient cybersecurity procedures, where each firm had experienced breaches of cloud-based email accounts that exposed the personal information of thousands of investors of each firm.

The actions demonstrate the SEC's more aggressive enforcement of the Safeguards Rule of Regulation S-P at a time when financial institutions are increasingly targets of cyberattacks. The Safeguards Rule[3] requires advisers to adopt written policies and procedures reasonably designed to protect customer records and information.

In its enforcement of the Safeguards Rule, the SEC staff has focused its attention on cybersecurity policies and procedures, including in the context of cloud-based solutions.[4] The SEC also charged one of the advisory firms for violating the anti-fraud provision of the Investment Advisers Act of 1940 ("Advisers Act"), and the Compliance Rule (206(4)-7) thereunder, for failing to adopt sufficient written policies and procedures. The fines ranged from $200,000 to $300,000.

The enforcement actions each began with deficiencies identified by the exam staff and demonstrate the coordination between the exam staff and the Cyber Unit of the Enforcement Division on these issues.

This commentary discusses each of the actions and the lessons they provide for fund managers, including specific recommendations for cybersecurity compliance.

Overview of the actions

Cetera

The SEC found that between November 2017 and June 2020, cloud-based email accounts of 60 representatives of Cetera Advisor Networks LLC and four of its affiliates ("Cetera") were taken over through phishing,[5] credential stuffing[6] or other modes of attack, resulting in the exposure of personal information of at least 4,388 clients.

Cetera responded by amending its policies to require multifactor authentication ("MFA") to be turned on for "privileged or high-risk access." While Cetera activated MFA for its employees and certain other cloud-based email accounts, it did not activate MFA for independent contractors, including contractor accounts that had been breached as recently as the first half of 2020.

In finding Cetera violated the Safeguards Rule, the SEC observed that Cetera's policy of requiring MFA for "privileged or high risk access" was not reasonably designed; it did not apply to accounts of independent contractors, who had access to data that was no less high risk than the data to which employees had access.

The SEC also charged Cetera with violations of Section 206(4) of the Advisers Act and Rule 206(4)-7 thereunder, which require advisers to adopt and implement written compliance policies and procedures reasonably designed to prevent violations of the Advisers Act. Cetera engaged outside counsel to prepare breach notices that were sent to clients impacted by the breach.

Certain of these notices relied on template language that was misleading about the timing around the incident. In particular, certain breach notices stated that Cetera had learned of the breach

two months before the notification when, in fact, Cetera had learned of the breach at least six months earlier.

In finding a violation of the Advisers Act, the SEC noted that, while Cetera had a policy requiring that its personnel review all client communications before they were sent, Cetera failed to implement a reasonably designed policy because Cetera personnel failed to correct the template language that Cetera knew to be misleading at the time personnel conducted their review of the breach notices.

Cambridge

Between January 2018 and July 2021, cloud-based email accounts of 121 representatives of Cambridge Investment Research Inc. and Cambridge Investment Research Advisors Inc. ("Cambridge") were taken over through phishing, credential stuffing or other modes of attack, resulting in the exposure of personal information of at least 2,177 clients.

Investment managers must adopt and implement a robust written cybersecurity policy.

During that period, Cambridge's policies recommended, but did not require, individuals registered with FINRA as independent contractors, and associated with independent branch offices providing brokerage and investment advisory services, to implement enhanced security measures, such as MFA, on cloud-based email accounts.

After discovering the email account breaches, Cambridge suspended and reset the passwords for the accounts of the affected independent representatives. Cambridge also recommended, but did not require, these representatives to implement MFA or other enhanced security measures to prevent future breaches of cloud-based accounts.

Some, but not all, representatives followed Cambridge's recommendations, and takeovers of independent contractor email accounts persisted. Not until April 2021 did Cambridge revise its policy to require MFA for all cloud-based accounts. The SEC found that Cambridge's failure to timely adopt and implement a firmwide policy requiring enhanced security measures for cloud-based email accounts violated the Safeguards Rule.

KMS

Between September 2018 and December 2019, cloud-based email accounts of 15 independent financial advisers of KMS Financial Services Inc. ("KMS") were taken over through phishing and other modes of attack, resulting in the exposure of personal information of approximately 4,900 clients. During this period, KMS maintained a policy manual that required its financial advisers to

(1) "[c]onduct [their] business practices in a way that safeguards the confidentiality of [their] client's identity, including protecting all sensitive client information" and

(2) "[p]eriodically review [their] internal business policies to make sure they are adequately designed to protect sensitive client information."

The policy manual also required advisers to comply with KMS's Computer Network and Security Policies, which contained detailed technical security requirements,[7] but did not require the use of MFA for accessing sensitive data.

After discovering the email account breaches, KMS reset passwords, removed email forwarding rules and enabled MFA for the accounts of the affected financial advisers. However, KMS did not implement these security measures for all independent advisers until approximately 21 months after the discovery of the first breach, a period during which approximately 2,700 emails of one KMS financial advisor were exposed and forwarded outside the firm.

The SEC's order also notes that KMS failed to adopt enhanced security measures firmwide, despite several of the incident reports prepared by the forensic firms KMS hired to investigate the breach recommending that KMS expedite the enabling of MFA for all independent contractor email addresses.

As in the Cambridge action, the SEC found that KMS's delay in adopting and implementing a firmwide policy requiring enhanced security measures for cloud-based email accounts violated the Safeguards Rule.

Compliance lessons and recommendations for private fund managers

These enforcement actions serve as an important reminder that, to comply with the Safeguards Rule and the Advisers Act, investment managers must

(1) adopt and implement a robust written cybersecurity policy,

(2) regularly update the policy to account for risks introduced by the use of new technologies and in response to known cybersecurity incidents and

(3) regularly test the policy to ensure the security measures it mandates have been properly implemented.

The SEC staff continues to be focused on risks presented by the use of new technologies.

In the SEC's announcement, the Chief of the SEC Enforcement Division's Cyber Unit remarked: "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."

The involvement of the SEC's examination staff in pursuing these actions also serves as a reminder to managers to keep good records of their compliance, as questions about cybersecurity compliance are likely to come up on exams.

The three actions brought by the SEC share common themes that underscore the importance of the following cybersecurity considerations for fund managers:

- *Use of Cloud Solutions.* The SEC staff continues to be focused on risks presented by the use of new technologies, in particular the use of cloud-based email and other cloud-based solutions. In making IT infrastructure changes that impact how client records are handled, including what third parties have access to client records and how client records are stored, managers should review and update their cybersecurity policies to account for the risks that have been introduced. Managers are also reminded to conduct, and document the findings of, cybersecurity due diligence on vendors, both at the time of engagement and periodically thereafter.
- *Application of Policies to Contractors Where Appropriate.* Cybersecurity policies should be written, implemented and updated on a firmwide basis, including to properly account for the role of any independent contractors who have access to personal or other sensitive information. In some cases that will require application of the firm's policies to those contractors, while in other cases the firm may be able to rely on contractors following their own policies, provided these policies pass muster in the vendor due diligence process.
- *Implementation and Testing.* Managers should periodically test the effectiveness of their cybersecurity policies and procedures to determine if they are reasonably designed in light of current developments, including any recent cyberattacks, and whether they are being effectively implemented. As part of this review, Managers should also consider whether measures that are recommended in their policies should be changed to requirements.
- *Multi-Factor Authentication.* The SEC's recent enforcement actions and risk alerts signal that the SEC staff views MFA as a valuable tool for safeguarding email accounts and other electronic systems containing sensitive client information. Managers should, in consultation with their outside IT advisers, review their cybersecurity policies to ensure that MFA is required where appropriate and, where it is required, has in fact been implemented.
- *Training on Phishing and Credential-Stuffing.* Phishing and credential stuffing continue to be the most common modes through which threat actors are able to breach systems. In addition to implementing MFA, managers should conduct training on these tactics for all personnel (including independent contractors) that is targeted to the types of threats the firm is facing. Training should be conducted no less than annually, as well as promptly after the firm experiences a cyberattack that differs from the types of attacks (if any) the firm experiences in the ordinary course of its business.[8]
- *Remedial Measures Following a Breach.* Managers should carefully consider the advice of forensic and other advisers they hire to investigate incidents; failure to follow that advice could be viewed by the SEC as a contributing factor in determining that the manager's cybersecurity policies are deficient.
- *Scrutiny of Notices to Investors.* Managers should consider including details on the handling of breach notices in their policies and procedures to ensure drafts of such notices (including notices prepared by outside counsel) are carefully reviewed by personnel with knowledge of the incident to identify any inaccuracies or misleading information. Personnel reviewing notices should be particularly careful to confirm any template language used to facilitate the preparation of large numbers of notices has been adjusted to accurately describe the incident as it relates to the specific client (or group of clients) to which the notice is addressed.
- *Absence of Harm.* The SEC does not require there to have been actual harm to investors for there to be a violation of Regulation S-P and the Advisers Act. In all three cases, the SEC's order notes that the breaches do not appear to have resulted in any unauthorized trades or fund transfers. Therefore, managers should carefully document their response to all cyber incidents.

Notes

[1] Cybersecurity-Related FAQs, https://bit.ly/3Di4hpq.

[2] https://bit.ly/3lnl83d

[3] https://bit.ly/3DqDJCr

[4] The SEC's Office of Compliance Inspections and Examinations ("OCIE") has previously issued guidance on cybersecurity-related compliance issues under the Safeguards Rule, in particular, in a Risk Alert dated April 16, 2019, https://bit.ly/3lmGmz2, in which OCIE identified numerous compliance issues under the Safeguards Rule arising from insufficient cybersecurity policies (or failures to properly implement such policies), and a Risk Alert dated May 23, 2019, https://bit.ly/2Yxdye9, in which OCIE discussed compliance issues, including under the Safeguards Rule, associated with the use of cloud-based solutions. *See* SRZ's August 2019, https://bit.ly/2Yztptf, update discussing these risk alerts.

[5] Phishing is a type of attack perpetrated by using a fraudulent or "spoofed" email address to trick a victim into downloading malicious software, or entering login credentials, and employing such software or credentials to gain unauthorized access to accounts and systems.

[6] Credential stuffing is a type of attack perpetrated by collecting compromised client login credentials from the dark web and, through the use of automated scripts, employing such credentials to gain unauthorized access to accounts and systems. *See* SRZ's October 2020, https://bit.ly/3uTJplo, update on credential stuffing.

[7] These requirements included maintaining strong passwords, securing wireless networks, using anti-virus and malware protection, securing backup and stored data, and encrypting hard drives.

[8] OCIE issued a cybersecurity Risk Alert, https://bit.ly/3Di4CbG, on Sept. 15, 2020 discussing the risks associated with credential stuffing. SRZ's October 2020 update, https://bit.ly/3oJoPDx, provides further recommendations on steps managers should take to safeguard against credential stuffing.

About the authors



Marc E. Elovitz (L) is co-managing partner of **Schulte Roth & Zabel**. He serves as chair of the investment management regulatory and compliance group and as a member of the firm's executive committee. He can be reached at marc.elovitz@srz.com. **Kelly Koscuiszka** (C) is a partner in the firm's investment management group. She can be reached at kelly.koscuiszka@srz.com. **Edward H. Sadtler** (R) is head of the firm's intellectual property, sourcing and technology group. He can be reached at edward.sadtler@srz.com. All of the authors are based in the firm's New York office. This article was originally published Sept. 2, 2021, on the firm's website. Republished with permission.

This article was published on Westlaw Today on October 14, 2021.