The SEC brings its first enforcement action under the identity theft red flags rule

Vincente L. Martinez, Julia B. Jacobson and Nancy C. Iheanacho

Abstract

Purpose – *To explain the significance of the first enforcement action under the Identity Theft Red Flags Rule by the US Securities and Exchange Commission (SEC), which was announced on September 26, 2018.*

Design/methodology/approach – *Explains how the SEC's order not only cites violations of the Safeguards Rule under Regulation S-P (a staple of SEC cybersecurity enforcement actions against broker-dealers and investment advisers) but also is the SEC's first enforcement action for a violation of the Identity Theft Red Flags Rule under Regulation S-ID, which requires certain SEC registrants to create and implement policies to detect, prevent and mitigate identity theft.*

Findings – *Cybersecurity policies and procedures must match business risks and change as business risks change.*

Originality/value – *Practical guidance from experienced cybersecurity and privacy lawyers.*

Keywords *Privacy, US Securities and Exchange Commission, Cybersecurity, Identity theft red flags rule, Safeguards rule*

Paper type *Technical paper*

Vincente L. Martinez (Vince.Martinez@klgates.com) is a partner at K&L Gates LLP, Washington, District of Columbia, USA. Julia B. Jacobson (Julia.Jacobson@klgates.com) is a partner at K&L Gates LLP, Boston, Massachusetts, USA. Nancy C. Iheanacho (Nancy.Iheanacho@klgates.com) is an associate at K&L Gates LLP, Washington, District of Columbia, USA.

On September 26, 2018, the US Securities and Exchange Commission (SEC) settled claims that Voya Financial Advisors, Inc. (VFA) failed to adequately protect customer information following a six-day cyberattack in 2016[1]. The SEC's order not only cites violations of the Safeguards Rule under Regulation S-P[2] (a staple of SEC cybersecurity enforcement actions against broker-dealers and investment advisers) but also is the SEC's first enforcement action for a violation of the Identity Theft Red Flags Rule under Regulation S-ID[3], which requires certain SEC registrants to create and implement programs to detect, prevent and mitigate identity theft.

The cyber attack

The SEC's order states that, from 2013 to 2017, VFA provided its independent contractor representatives with access to a web portal that enabled them to access brokerage and advisory customer account information. In April 2016, fraudsters impersonating five contractors called VFA 's technical support line to request password resets. VFA's technical support staff reset the passwords, provided temporary passwords over the phone and, on at least two occasions, usernames. The fraudsters then used the credentials to access information for at least 5,600 customers and to manipulate information for certain customers, including by changing customer profiles to reroute account statements to fake email addresses. Notably, the SEC did not find any unauthorized transfers or distributions; i.e. there was no known financial harm to VFA customers[4].

SEC violations

The safeguards rule

Rule 30(a) of Regulation S-P [17 C.F.R. § 248.30(a)], known as the "Safeguards Rule," requires certain SEC registrants (including broker-dealers and investment advisers) to adopt written policies and procedures that are "reasonably designed to:

- Insure the security and confidentiality of customer records and information;
- Protect against any anticipated threats or hazards to the security or integrity of customer records and information; and
- 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 SEC's order, VFA's policies and procedures were not reasonably designed to meet the Safeguards Rule's requirements because (among other issues) they allowed technical support staff to provide users with temporary passwords over the phone, allowed multiple concurrent web portal sessions for a single contractor, failed to identify higher-risk representatives and customer accounts for additional security measures, and failed to notify a customer when his or her contact information and document delivery preferences were changed.

The SEC's order also notes that certain policies and procedures were not adequately applied to remote contractors, such as a 15-minute inactivity timeout setting and a multi-factor authentication requirement that was enforced when password resets were requested by phone. The order also cites the lack of a procedure for terminating individual remote sessions and inadequate procedures for testing that remote contractors performed software updates, and maintained antivirus and encryption software.

The identity theft red flags rule

Rule 201 of Regulation S-ID [17 C.F.R. § 248.201], known as the "Identity Theft Red Flags Rule," requires certain institutions (including SEC-registered broker-dealers and investment advisers) that offer or maintain "covered accounts"[5] to develop and implement a written "identity theft prevention program" with "reasonable policies and procedures to:

- Identify relevant Red Flags for the covered accounts that the financial institution or creditor offers or maintains, and incorporate those Red Flags into its Program;
- Detect Red Flags that have been incorporated into the Program of the financial institution or creditor;
- Respond appropriately to any Red Flags that are detected pursuant to [subsection ii immediately above]; and
- Ensure the Program (including the Red Flags determined to be relevant) is updated periodically, to reflect changes in risks to customers and to the safety and soundness of the financial institution or creditor from identity theft."

Although VFA adopted a written identity theft prevention program in 2009, the SEC found that VFA did not review and update its program to address changes in risks to its customers or to provide adequate training to its employees. The order also found that VFA failed to detect and respond to indications of fraudulent activity. Specifically, the order found that two of the fraudsters' calls originated from phone numbers that VFA previously identified as associated with fraudulent activity. The order also noted that VFA's procedure required next-business day review for reset requests, which was not consistently followed. The SEC also took issue with the manner in which VFA responded to known or suspected intrusions, finding (among other things) that a technical support team member provided a password

reset over the phone after VFA suspended the practice, and that VFA failed to block IP addresses identified as likely involved in fraudulent activity.

Takeaways

The SEC's action is an important development in its cybersecurity enforcement activities. The expansion of the SEC's cybersecurity enforcement activities into Regulation S-ID underscores the focus on the protection of retail investors emphasized by the SEC's Chairman, Office of Compliance Inspections and Examinations, and Division of Enforcement during the current administration because the types of accounts covered under the Identity Theft Red Flags Rule are primarily held by retail investors.

Both the Safeguards Rule and the Identity Theft Red Flags Rule are principles-based regulations that require firms to establish, implement and maintain "reasonable" policies and procedures to protect customer information. Reasonableness, however, is not defined in either regulation; rather, whether cybersecurity policies and procedures are reasonable is generally based on fact-specific analyses in enforcement actions. This order is helpful, however, because the SEC describes what the SEC finds unreasonable for firms working on updating their cybersecurity practices in light of an increasingly challenging threat environment.

Policies and procedures must change as risks change

In the press release accompanying the settlement order[6], Robert Cohen, Chief of the SEC Enforcement Division's recently-formed Cyber Unit, stated that "[broker-dealers and investment advisers] also must review and update the procedures regularly to respond to changes in the risks they face." Although the SEC provided no specifics, it noted that the firm's Identity Theft Prevention Program had not changed since its inception in 2009 to match advancements in technology and increasing threats.

The need for continual monitoring of the cybersecurity threat landscape through periodic risk assessments and adapting policies and procedures to changes is a consistent theme for securities regulators that can be found in staff guidance from the SEC's Office of Compliance Inspections and Examinations and Division of Investment Management, as well as the Financial Industry Regulatory Authority (FINRA)[7]. Ongoing monitoring and threat assessment also is a key factor in cybersecurity best practice standards generally, such as ISO 27001[8] and the NIST Cybersecurity Framework[9]. Accordingly, we suggest that firms review and consider revising their policies, procedures and technological safeguards periodically and, when possible, benchmark them against a generally-accepted industry standard.

Policies and procedures must match business risks

Mr Cohen also emphasized in the accompanying press release another theme of the SEC's cybersecurity efforts when he stated that "[t]his case is a reminder to brokers and investment advisers that cybersecurity procedures must be reasonably designed to fit their specific business models." In its order, the SEC found that VFA's policies and procedures were not tailored to address the risks posed by remote login activity of contractors, who were the largest part of its workforce.

The SEC has repeatedly emphasized the importance of tailoring of policies and procedures to a firm's specific environment[10]. The SEC also brought enforcement actions under the Safeguards Rule when template policies and procedures were not properly customized[11]. The SEC takes the position that what is reasonable for one firm may not be reasonable for another and that the policies and procedures a firm deploys must fit its business practices. Thus, firms should evaluate whether their policies and procedures are

grounded in an appropriate risk assessment that considers closely the firm's business model and unique vulnerabilities.

A firm is more likely to face an enforcement action if it ignores red flags

The SEC appears more likely to undertake an enforcement action when a firm has not only had shortcomings with its policies and procedures but also has ignored signs of trouble. Examples from previous SEC cybersecurity enforcement actions include a failure to act on internal audit recommendations or in light of known breaches[12], a lack of procedures for responding to potential security issues discovered during branch audits or help desk calls[13], and a failure to strengthen policies and procedures after a laptop and credentials were stolen[14]. Accordingly, we recommend that firms include in their policies and procedures mechanisms to quickly identify and respond to security incidents and concerns as they arise. As made clear in the order, the ability to quickly identify and respond to security incidents requires employee training to ensure that employees know cybersecurity warning signs and what to do when they observe them.

Conclusion

No firm is immune from the risk of a cyber intrusion. Fraudsters are constantly finding new ways to find and exploit vulnerabilities. Firms must plan for cybersecurity resilience by training employees and periodically revisiting policies and procedures to consider new threats, lessons learned, and changes in law and regulation, all of which are critical elements of cyber-resilience.

Notes

1. SEC, Advisers Act Rel. No. 5048 (Sept. 26, 2018). VFA is an indirect wholly-owned subsidiary of Voya Financial, Inc. that provides retail wealth management services.
2. 17 C.F.R. § 248.30(a).
3. 17 C.F.R. § 248.201.
4. The z enforcement actions where no financial harm was found. *See*, *e.g.*, Advisers Act Rel. No. 4204 (Sept. 22, 2015) (noting that "the firm has not learned of any information indicating that a client has suffered any financial harm as a result of the cyber attack.").
5. Under Rule 201(b)(3), a "covered account" is defined as "(i) An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a brokerage account with a broker-dealer or an account maintained by a mutual fund (or its agent) that permits wire transfers or other payments to third parties; and (ii) Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks."
6. SEC, Press Release No. 2018-213 (Sept. 26, 2018).
7. *See* SEC, IM Guidance Update 2015-02 (Apr. 2015) at 1; SEC, National Exam Program Risk Alert, Volume IV, Issue 2 (Apr. 15, 2014) (referring to risk assessments in the attached Appendix of examination topics and questions, which was derived from the National Institute of Standards and Technology (NIST), "Framework for Improving Critical Infrastructure Cybersecurity" (Feb. 12, 2014)); and FINRA, Report on Cybersecurity Practices (Feb. 2015) at 12-15; see also K&L Gates Client Alert, "OCIE Observations from the Second Round of Cybersecurity Examinations," available at: www.klgates.com/ocie-observations-from-the-second-round-of-cybersecurity-examinations-08-16-2017/
8. *See* www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en (requires purchase).
9. *See* Tier 4 of the most recent NIST Framework, available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

10. For instance, following two SEC cybersecurity examination sweeps, SEC Chair Mary Jo White stated in prepared remarks in May 2016 that "[w]hat we found, as a general matter so far, is a lot of preparedness, a lot of awareness but also their policies and procedures are not tailored to their particular risks." Reuters, "SEC says cyber security biggest risk to financial system" (May 18, 2016).
11. *See*, *e.g.*, SEC, Exchange Act Rel. No. 4204 (Sept. 22, 2015).
12. *See* SEC, Advisers Act Rel. No. 2775 (Sept. 11, 2008).
13. *See* SEC, Advisers Act Rel. No. 2929 (Sept. 29, 2009).
14. *See* SEC, Exchange Act Rel. No. 64220 (Apr. 7, 2011).

Corresponding author

Vincente L. Martinez can be contacted at: Vince.Martinez@klgates.com