THE
NATIONAL LAW REVIEW

SEC Charges Broker-Dealer/Adviser With Inadequate Cybersecurity Procedures

Thursday, October 11, 2018

On September 26, the Securities and Exchange Commission (SEC) charged a dually registered broker-dealer and investment adviser (the "Registrant") with deficient cybersecurity procedures. This is the first SEC action alleging violations of the Identity Theft Red Flags Rule and provides important guidance on the SEC's expectations relating to cybersecurity procedures.

Article By David Y. Dickstein
Janet M. Angstadt Mark D. Goldstein
Christian B. Hennion Richard D. Marshall
Katten Muchin Rosenman LLP Advisories

Communications, Media & Internet
Financial Institutions & Banking
Securities & SEC
All Federal

The Relevant Rules That Were Allegedly Violated

Two SEC rules applicable to broker-dealers and investment advisers were allegedly violated, the Safeguards Rule (Rule 30(a) of Regulation S-P (17 C.F.R. § 248.30(a)) and the Identity Theft Red Flags Rule (Rule 201 of Regulation S-ID (17 C.F.R. § 248.201)).

The Safeguards Rule requires every registered broker-dealer and every registered investment adviser to adopt written policies and procedures that address administrative, technical and physical safeguards for the protection of customer records and information. Those policies and procedures must be 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 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.

The Identity Theft Red Flags Rule requires certain financial institutions and creditors, including broker-dealers and investment advisers registered or required to be registered, to develop and implement a written Identity Theft Prevention Program that is designed to detect, prevent and mitigate identity theft[1] in connection with the opening of a covered account[2] or any existing covered account. An Identity Theft Prevention Program must include reasonable policies and procedures that are intended to: (1) identify relevant red flags for the covered accounts and incorporate them into the Identity Theft Prevention Program; (2) detect the red flags that have been incorporated into the Identity Theft Prevention Program; (3) respond appropriately to any red flags that are detected pursuant to the Identity Theft Prevention Program; and (4) ensure that the Identity Theft Prevention Program is updated periodically to reflect changes in risks to customers from identity theft.

The Alleged Facts

The Registrant outsourced its cybersecurity functions to its parent company, which in turn relied heavily upon independent contractors to support those efforts. These independent contractors had access to a portal through which they could obtain personally identifiable information about the Registrant's customers.

Over six days in April 2016, persons impersonating personnel of those independent contractors called the Registrant's technical support line requesting that three of their passwords be reset. In two cases, the calls were placed from numbers identified with prior fraudulent activity, including efforts to impersonate independent contractors. In spite of these red flags, the callers allegedly were provided with new passwords over the phone, and in two cases also were provided with the representative's user name.

Three hours after these calls, an independent contractor notified the Registrant that an email had been sent confirming a request for a password change when no such request had been made. Over the next several days, although the Registrant took some steps to respond to the red flags, the Registrant did not promptly block access from the user names and passwords involved. Improper access allegedly was given to the account information for more than 5,600 customers; one customer's documents were accessed. There were no known unauthorized transfers of any customer funds or securities from the impacted customer accounts.

After the intrusion, the Registrant blocked the malicious email addresses, revised its policies and procedures relating to changing passwords over the telephone, notified the impacted customers, offered them free one-year credit monitoring, and named a new chief information security officer.

Alleged Defects in the Registrant's Policies and Procedures

The SEC alleged the following defects in the Registrant's policies and procedures relating to the Safeguards Rule:

[The Registrant's] policies and procedures with respect to resetting [the Registrant's] contractor representatives' passwords, terminating web sessions in its proprietary gateway system for [the Registrant] contractor representatives, identifying higher-risk representatives and customer accounts for additional security measures, and creation and alteration of [the Registrant's] customer profiles, were not reasonably designed. In addition, a number of [the Registrant's] cybersecurity policies and procedures were not reasonably designed to be applied to its contractor representatives.

The SEC also alleged the following defects in the Registrant's policies and procedures relating to the Identity Theft Red Flags Rule:

[The Registrant] did not review and update the Identity Theft Prevention Program in response to changes in risks to its customers or provide adequate training to its employees. In addition, the Identity Theft Prevention Program did not include reasonable policies and procedures to respond to identity theft red flags, such as those that were detected by [the Registrant] during the April 2016 intrusion.

Remedies Imposed

The Registrant was required to retain an independent compliance consultant to review its relevant procedures and to adopt the consultant's recommendations. The Registrant also was fined $1 million.

Key Lessons

Three key lessons can be learned from this enforcement action:

First, although it may already have been obvious from prior SEC pronouncements, this action re-emphasizes how seriously the SEC treats firms' obligations relating to cybersecurity procedures. This is highlighted by the fact that the dual registrant was fined $1 million even though there was no apparent investor harm resulting from the cyberattack.

Second, this action highlights the special risks posed by reliance on independent contractors. While such reliance is entirely legal, these non-employees pose particular risks that should be addressed both contractually and operationally.

Third, the failure to identify and respond promptly to red flags may potentially create significant regulatory risks for a registrant, in addition to the reputational and liability risks from the firm's customers. The SEC appears to have been concerned that calls from numbers identified with fraudulent conduct should not have been responded to and that when warnings that a hack may have occurred began to surface, access from the suspicious addresses should have been blocked in a timely manner. The SEC expects recognition of, and appropriate and prompt responses to, red flags. Also of note, the Commodity Futures Trading Commission (CFTC) requires futures commission merchants, introducing brokers, commodity trading advisers, commodity pool operators, and certain other registrants to comply with its version of the Theft Red Flags Rule.

---

1 The rule defines "identity theft" as a fraud committed or attempted using the identifying information of another person without authority.

2 The rule defines a "covered account" to include an account that a broker-dealer or investment adviser 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.