Bond Case Briefs

Municipal Finance Law Since 1971

SEC Charges Broker-Dealer/Investment Adviser with Deficient Cybersecurity Procedures.

The Securities and Exchange Commission ("SEC") recently charged a firm registered with the SEC as both a broker-dealer and an investment adviser in connection with a cyber-intrusion that compromised the personal information of thousands of customers. This case is significant both because cyber security is an area of heightened concern for the SEC and because this is one of the first cases to bring charges against a registered broker-dealer or investment adviser in connection with a cyber-intrusion.

The current chairman of the SEC has identified cybersecurity as a significant concern and stated that the "Commission is focused on identifying and managing cybersecurity risks and ensuring that market participants—including issuers, intermediaries, investors and government authorities—are actively and effectively engaged in this effort and are appropriately informing investors and other market participants of these risks." See Statement on Cybersecurity, Chairman Jay Clayton (Sept. 20, 2017) available here. Moreover, the Commission's Office of Compliance Inspections and Examinations ("OCIE") has identified cybersecurity as a priority and has stated that "[e]ach of OCIE's examination programs will prioritize cybersecurity with an emphasis on, among other things, governance and risk assessment, access rights and controls, data loss prevention, vendor management, training, and incident response." See SEC Office of Compliance Inspections and Examinations Announces 2018 Examination Priorities (SEC Press Release 2018-12) (Feb. 7, 2018) available here.

The SEC charged the firm with violating Rule 30(a) of Regulation S-P (17 C.F.R. §248.30(a); the "Safeguards Rule") and Rule 201 of Regulation S-ID (17 C.F.R. §248.201; the "Identity Theft Red Flags Rule").These rules, respectively, require broker-dealers and investment advisers registered with the SEC to adopt written policies and procedures that are reasonably designed to safeguard customer records and information and require broker-dealers and investment advisers that offer or maintain covered accounts to develop and implement a written Identify Theft Prevention Program that is designed to detect, prevent, and mitigate identify theft in connection with the opening of a covered account or any existing covered account.

This case is the first SEC enforcement action charging violation of the Identity Theft Red Flags Rule and appears to be just the second case, and the first since 2015, charging a registered broker-dealer or investment adviser in connection with a cyber-intrusion. For the earlier case, see SEC Charges Investment Adviser with Failing to Adopt Proper Cybersecurity Policies and Procedures Prior to Breach (SEC Press Release 2015-202)(Sept. 22, 2015) available here.

In its press release announcing this action, available here, the SEC referenced both weaknesses in the firm's cybersecurity procedures and the firm's failure to apply its procedures to systems used by the greater part of its workforce. The firm agreed to pay a $1 million fine. The firm also agreed to retain a compliance consultant to conduct a comprehensive review of the firm's policies and procedures and to implement the recommendations resulting from such review. A copy of the underlying order is available here.

The firm offered investment and brokerage services to its customers through a national network of registered representatives. A significant majority of these representatives worked out of their own offices with a majority of these representatives consisting of independent contractors. These independent-contractor representatives typically used their own IT equipment and their own networks to access customer information, including personally identifiable information ("PII") through a web portal that was proprietary to the firm. This is in contrast to employee representatives who used IT equipment and IT systems provided by the firm.

The firm's procedures allowed independent-contractor representatives who could not remember their passwords to reset their passwords by calling firm support centers, which were authorized to provide temporary passwords by phone after the requesting representative provided at least two pieces of his or her own PII. Significantly, these procedures were left unchanged after the firm was aware of prior fraudulent attempts to impersonate contractor representatives using their PII. While the firm did keep a "monitoring list" of phone numbers that were previously used in connection with fraudulent activity, there was no written policy or procedure that required the support centers to consult the monitoring list when responding to password-reset calls.

The firm's procedures also provided for the personal computers of the independent-contractor representatives to be scanned for antivirus software, encryption, and certain software updates, but as stated in the SEC's order, these scans were scheduled to occur "only" three times a year. Often the scan, which required action by the contractor representative before it could occur, did not occur at all, and even though approximately 30% of the scans that did occur revealed critical failures such as a lack of encryption and antivirus software, the firm conducted no review or follow up of such scans to ensure these failures were remedied. The order also stated that the firm's policies and procedures with respect to customers' profiles were not reasonably designed as no notice was provided to a customer when an initial profile was created or when contact information and document-delivery preferences were changed.

The order also highlighted weaknesses in the firm's incident-response policies and procedures. While these procedures generally required that potentially compromised user accounts be disabled and relevant applications shut down to prevent additional compromises, the incident-response team did not receive adequate training regarding the system used by the independent-contractor representatives and mistakenly believed that resetting a password for a user would terminate the user's existing session. As a result, cyber-intruders were able to continue to access firm systems even after the incident-response team had taken steps to deny such access. Moreover, the firm's procedures did not require informing the support centers about an ongoing intrusion. In addition, the firm's procedures for designating compromised representatives' and customers' accounts as requiring additional security measures, which were meant to alert the support centers to the need to take additional measures, were ineffective, as the flags placed to identify such representatives and accounts were erased periodically in connection with unrelated automated system activities. The order also states that the firm had not updated its Identity Theft Prevention Program after 2009, notwithstanding significant changes in external cybersecurity risks since then.

This case should serve as a warning that the SEC is prepared to use its enforcement powers where it believes broker-dealers or advisers have put their customers at an unreasonable risk of cyber-intrusion. Accordingly, broker-dealers, investment advisers, and municipal advisors should take steps to protect themselves from possible enforcement actions by ensuring that they have reasonable and comprehensive cybersecurity policies and procedures in place. Firms that allow multiple-access systems must ensure that their policies and procedures are appropriate for each system used by the firm. Firms must also keep their policies and procedures up to date by responding not only to changes in their own systems and technologies but also by keeping current

with respect to best practices in the rapidly advancing world of cybersecurity. At a minimum, firms should review their cybersecurity programs on an annual basis as well as whenever changes to the firm's systems or technology warrant. Firms should also ensure, and document, that cybersecurity-related red flags and other concerns receive prompt attention and, as necessary, that policies and procedures are revised to respond to such concerns. Firms should also ensure that persons charged with critical aspects of cybersecurity, including those who respond to cyber intrusions, receive the training they need to successfully perform their functions and that such training covers all relevant systems.

by Glen P. Barrentine

USA October 3 2018

Winston & Strawn LLP