SEC Enforcement Action under Regulation S-P for Data Intrusion

The Securities and Exchange Commission (SEC) recently took enforcement action against a broker-dealer/registered investment adviser (the Firm) for violations of Rule 30(a) of Regulation S-P (the Safeguards Rule), due to the Firm's failure to protect customer data from an intruder. The Safeguards Rule requires that every broker, dealer, and investment company, and every registered investment adviser (Covered Institutions), adopt written policies and procedures reasonably designed to protect customer information. After an intruder used a malware virus placed on a registered representative's computer to access customer account information, the SEC found that the Firm's information security policies and procedures were inadequate. A copy of the enforcement action may be accessed through the SEC's website and highlights the importance of renewed attention to information security for all Covered Institutions.

Summary of Enforcement Action

The Firm is a registered broker-dealer and investment adviser that offers a variety of general securities, mutual funds, and variable insurance products to its retail customer base. The Firm employs approximately 55 people but has approximately 1,600 independent contractor registered representatives operating from approximately 1,069 branch offices. Registered representatives access the Firm's intranet and its online trading platform from any computer with an Internet connection and are required to supply their own computer hardware and software. The customer account information is available on both the firm's intranet and the trading platform.

In or around November 2008, an unauthorized party obtained the login credentials of one of the Firm's registered representatives through the use of a malware/keystroke logger virus. The virus was placed on the registered representative's computer, which at the time did not have antivirus software properly employed. The Firm, which recommended but did not require antivirus software, was aware that the registered representative's computer did not have antivirus software installed because during the two months prior to the November 2008 intrusions, the Firm's information technology (IT) help desk received several calls from the registered representative indicating that the computer had been compromised by a software virus. Although the IT help desk identified the computer as lacking the recommended antivirus software and logged the deficiency in its files, no further action was taken by the IT help desk to prevent the registered representative from using the computer. Ultimately, the intruder was able to access the account name, account number, account registration type, account net worth, cash balance, and the last four digits of the account owner's Social Security number for 368 of the registered representative's customer accounts. The intruder also attempted to execute security transactions through the accounts.

The SEC found that the Firm's written policies and procedures failed to adhere to the standards of reasonable design imposed by the Safeguards Rule by failing to implement basic security measures, such as requiring antivirus software on all registered representatives' computers conducting business over the Internet, and failing to follow up, or have written procedures addressing follow up, on security issues either uncovered in branch audits or reported to the IT help desk. As a result, the SEC found that the Firm willfully violated the Safeguards Rule and ordered that the Firm: (1) cease and desist from committing or causing any violations and any future violations of the Safeguards Rule; (2) be censured; and (3) pay a civil money penalty in the amount of $100,000 to the U.S. Treasury.

Lessons for Covered Institutions

This enforcement action highlights the risks to Covered Institutions for failing to craft policies and procedures under the Safeguards Rule to address current information security threats to computer networks and information storage systems. It also underscores that the SEC will pay particular attention to the implementation of policies and procedures, including whether the Covered Institution uses basic security protections for computer systems such as anti-virus, anti-"phishing," and password protection software, and institutes mechanisms to identify and follow-up on threats and deficiencies. It is also noteworthy that this enforcement action follows the March 2008 proposed amendments to the Safeguards Rule, which set forth more specific requirements for safeguarding information and responding to information security breaches.[1] In proposing more stringent requirements under the Safeguards Rule, the SEC indicated that it was concerned that many Covered Institutions were not regularly re-evaluating and updating their written policies and procedures to address more regular and advanced threats against consumer records and information. The enforcement action and proposed amendments to Regulation S-P, which have not been finalized, strongly suggest that information security will continue to be an enforcement focus of the SEC in the future.

The Firm's decentralized operations, with dispersed branch offices and registered representatives operating remotely, may not be typical of most Covered Institutions. The same issues may arise, however, for firms with more centralized operations, given the increasing adoption of business continuity programs and telecommuting options that rely on employees to access company databases and intranet sites from remote locations and personal computers. Given the ever-increasing focus on information security issues by regulators around the world, as well as the potentially costly measures required to remediate once there has been an information security breach, we encourage all clients to review their written policies and procedures under the Safeguards Rule, as well as their implementation, to ensure they are reasonably designed to address technological advances and new threats to information security systems.

Please note that this Alert should not be viewed as a comprehensive discussion of all Regulation S-P and Safeguards Rule issues and exposure to potential liability under Regulation S-P. It also does not address other laws or regulations related to information security that may apply to Covered Institutions. If you would like to learn more about the issues raised by this Alert, please contact your usual Ropes & Gray attorney. Ropes & Gray has extensive experience in handling the array of legal challenges arising from breaches of information security, including representing companies experiencing data breaches in class action and other litigation, in federal and state governmental investigations and enforcement proceedings, and in developing information security programs to protect data from future breaches.

To learn more about Ropes & Gray's experience and capabilities in this area, please view our Privacy and Data Security Practice Group webpage.

[1] For additional information regarding the proposed amendments to Regulation S-P and the Safeguards Rule, please see a copy of the proposing release on the SEC's website. Proposed changes would require Covered Institutions to: (1) develop an information security program appropriate to the size and complexity of the firm, to the nature and scope of its securities activities, and to the sensitivity of any personal information in the possession of the firm; (2) designate an employee (or employees) responsible for the oversight and coordination of the program; (3) require the coordinator to be responsible for identifying foreseeable security risks, designing policies and measures to prevent those risks, regularly testing and monitoring the effectiveness of the safeguards, training staff on the key elements of the security program and how to implement the program, and overseeing service providers to the firm and assessing their safeguards regarding privacy of customer information and monitoring; and (4) implement procedures for responding to unauthorized access and use of customer information, including prompt notice to any affected customers, as well as notice to the appropriate designated examining authority (on newly proposed Form SP-30).