June 14, 2016

SEC Imposes Sanctions for Failure to Protect Customer Information from Insider Data Breach

Through a cease-and-desist order and $1 million penalty leveled against a prominent investment adviser last week, the Securities and Exchange Commission flexed newfound muscle in the cybersecurity arena. In the wake of an insider breach by a rogue employee that affected 730,000 customer accounts, the SEC determined that policies and procedures employed by Morgan Stanley Smith Barney LLC (MSSB) failed to sufficiently safeguard customer data from unauthorized access. Following two years of cybersecurity examination sweeps, this enforcement action demonstrates the SEC's resolve to heighten industry focus on cybersecurity.

In December 2014, MSSB's own monitoring discovered customer account data being offered for sale on the Internet. MSSB promptly notified law enforcement authorities and affected customers and took steps to remove the data from the Internet. The ensuing internal investigation revealed that a financial advisor employed by MSSB had, without authorization and in violation of company policy, downloaded customer data, including personally identifiable information (PII) and investment information from 730,000 customer accounts associated with 330,000 households, by circumventing MSSB's database application restrictions. The advisor had transferred the misappropriated data to his personal server, which in turn had been hacked by a third party. The advisor pleaded guilty to federal charges and was sentenced to serve a three-year term of probation and pay restitution of $600,000 to MSSB, the direct victim of the crime.

Rather than treating MSSB as a victim, the SEC accused the company of violating the "Safeguards Rule," which requires broker-dealers and investment advisers to adopt written policies and procedures reasonably designed to safeguard customer records and information from threats that include unauthorized access. The SEC acknowledged that MSSB had adopted controls designed to prevent unauthorized access, including applications restricting employee access to relevant data, but found that the policies and procedures suffered from technical deficiencies, lacked an auditing function, and failed to include systems for monitoring employee access and use. According to the SEC, proper auditing and testing would "likely" have revealed the deficiencies. In resolving the action, MSSB neither admitted nor denied the allegations, but agreed to pay a $1 million penalty and to cease and desist from violating the Safeguards Rule.

While the SEC had previously disciplined smaller investment firms that had failed to take the most basic cybersecurity precautions, the MSSB action targeted an industry leader that had implemented significant cybersecurity procedures. With SEC Chair Mary Jo White recently naming a new Senior Advisor for Cybersecurity Policy and describing cybersecurity as "the biggest risk facing the financial system," we can only expect that SEC activity in this area will continue to expand. While the Safeguards Rule applies only to SEC-regulated financial services firms, the case is a reminder to all companies of the need to invest not only in state-of-the-art data protection systems, but also in robust auditing to detect hidden system flaws and monitoring for internal and external breaches alike.

John F. Savarese
Wayne M. Carlin
Sabastian V. Niles
Marshall L. Miller