Another Cybersecurity Enforcement Action Emphasizes Monitoring and Testing of Data Protection Systems

June 17, 2016 Kit Addleman, Ronald Breaux, Tim Newman

PRACTICES Privacy and Cybersecurity, Securities and Shareholder Litigation

The Securities Exchange Commission (the "**Commission**") recently announced a $1 million settlement with Morgan Stanley Smith Barney LLC ("**Morgan Stanley**") for charges related to a data breach that the Commission alleged resulted from inadequate policies and procedures protecting customer data. Through examination priorities letters in 2015 and 2016, the data security enforcement action against an investment adviser in September 2015, and multiple speeches by Commission officials, the Commission has widely publicized its increased focus on cybersecurity. The settlement with Morgan Stanley, including the imposition of a sizeable fine, demonstrates that the Commission is applying increased scrutiny to the cybersecurity practices of registered entities and intends to bring actions where firms have failed to adopt, as well as adequately implement and test, policies and procedures to protect customer data.

Background

The Commission's action arises from the misconduct of one Morgan Stanley employee who compromised the financial data and personal information of Morgan Stanley clients. According to the Commission, Morgan Stanley stores customer data on hundreds of internal information management applications as part of its wealth management business. Morgan Stanley employees use these applications to run reports and analyze customer information for business purposes. To ensure that these programs are used only for legitimate business needs, Morgan Stanley installed authorization modules that only allow access to the specific customer data each employee required to do their jobs. In addition to these authorization modules, Morgan Stanley's Code of Conduct, among other written policies, prohibits employees from accessing customer data unrelated to their job responsibilities.

In 2011, a Morgan Stanley employee discovered a glitch in the authorization module for one of the information management applications that allowed the employee to run reports and obtain client data to which he should not have had access. In 2014, the employee found a separate glitch in another Morgan Stanley application that allowed him to run additional reports to gather further client data beyond his authorized access. The employee conducted approximately 5,900 unauthorized searches, downloaded the resulting customer data, and transferred the data to a personal server he maintained in his home. In transferring the client data to his personal server, the employee bypassed security controls Morgan Stanley implemented to prevent employees from copying data to external storage.

In December 2014, Morgan Stanley discovered through a routine internet sweep that portions of the client data downloaded by the employee were purportedly for sale on the internet. Morgan Stanley quickly identified the employee as the source of the data breach[1], and further forensic analysis indicated that a third-party hacker had accessed the employee's home server and copied the stored customer data. Morgan Stanley notified impacted customers shortly thereafter.

The Enforcement Action

The Commission brought its enforcement action against Morgan Stanley under Rule 30(a) of Regulation S-P (the "**Safeguards Rule**"). The Safeguards Rule requires that registered broker-dealers, investment companies, and investment advisers adopt policies and procedures "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."

According to the Commission, Morgan Stanley violated the Safeguards Rule by failing to adopt policies and procedures designed to do the following:

- Create operating authorization modules that restricted access to confidential customer data to employees with a legitimate business need;
- Audit and test the effectiveness of those authorization modules; and
- Monitor and analyze employee access to customer data on internal information management applications.

The Commission alleged that as a result of Morgan Stanley's failure to adopt appropriate procedures restricting employee access to customer data, an employee was able to access, misappropriate, and transfer to a personal server large amounts of confidential customer data that ended up in the hands of a third-party hacker.

The Commission acknowledged that, in fact, Morgan Stanley did have written policies and procedures restricting employees' access to confidential customer data available on information management applications and authorization features embedded within the applications intended to prevent unauthorized access. However, the Commission ultimately faulted Morgan Stanley with failing to ensure that those policies and procedures were effective through testing and monitoring. The Commission alleged that had Morgan Stanley tested its procedures and authorization features and monitored employee access to customer data, Morgan Stanley would have uncovered the flaws in the system that allowed the employee to misappropriate the customer data involved in the data breach.

Takeaways

In September 2015, the Commission brought an action against R.T. Jones Capital Equities Management, a St. Louis-based investment adviser, for charges that it violated the Safeguards Rule by failing to establish cybersecurity policies and procedures in advance of a data breach (see our coverage here). The action against Morgan Stanley emphasizes that the adoption of procedures must be followed by rigorous surveillance and testing thereafter.

Throughout 2015 and 2016, a number of senior SEC officials, including Chair Mary Jo White, have publicly indicated that cybersecurity is an important area of focus of examination and enforcement within the Commission. The action against Morgan Stanley illustrates the seriousness with which the Commission approaches the protection of customer data and the enforcement of Regulation S-P. Entities registered with the Commission, including broker-dealers, investment advisers, and investment companies, should carefully examine their data security practices to ensure that they are adequately designed, implemented and regularly tested.

For more information, contact any of the lawyers listed below.

---

[1]The Morgan Stanley employee was criminally charged with and pled guilty to one count of exceeding his authorized access to a computer and thereby obtaining information contained in a financial record of a financial institution.