Akin®

Morgan Stanley Fined $1 Million by SEC for Cybersecurity Violations

Jun 16, 2016

Reading Time : **3 min**

By: Natasha G. Kohne

In December 2014, MSSB, an indirect, wholly owned subsidiary of Morgan Stanley, discovered through routine Internet sweeps that certain of its confidential customer information had been posted to at least three Internet sites, purportedly for sale to a third party. MSSB identified Galen Marsh, an employee at the time, as the likely source of the data breach. Specifically, from approximately June 2011 through 2014, Marsh accessed confidential customer information—including information for customers outside his group—and conducted nearly 6,000 unauthorized searches of customer data on two firm portals that stored sensitive personally identifiable information (PII).[1] He then downloaded the data and transferred it from his MSSB computer to a personal server located at his home. A forensic analysis of Marsh's personal server revealed that a third party likely hacked into the server and copied the confidential customer data that Marsh had downloaded. MSSB promptly took steps to remove this data from the Internet and notified law enforcement and other authorities, as well as customers who were impacted by the breach.

In its order, the SEC found that MSSB had written policies and procedures, including a Code of Conduct, that prohibited employees from accessing confidential information other than what employees had been authorized to access in order to perform their responsibilities. MSSB also had designed and installed authorization modules that, "if properly implemented," should have permitted each employee to run reports only with respect to the data for customers whom that employee supported.

However, MSSB's authorization modules were ineffective and/or absent in limiting access with respect to two types of reports available through the two firm portals, allowing Marsh to

access the customer information. MSSB also "failed to conduct any auditing or testing of the authorization modules" since they were created and "did not monitor user activity in the Portals to identify any unusual or suspicious patterns."

MSSB was ordered to cease and desist, and pay a $1 million civil money penalty.

The order emphasizes that the Safeguards Rule requires every broker-dealer and investment advisor registered with the SEC to adopt written policies and procedures that "address administrative, technical and physical safeguards reasonably designed to (1) [e]nsure 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."

This enforcement action comes on the heels of statements by the SEC indicating tougher enforcement of cybersecurity controls. Less than a month prior to the SEC's Order against MSSB, SEC Chair Mary Jo White had warned that the biggest risk the financial system faces is cybersecurity. Speaking at the Financial Regulation Summit in Washington D.C. in May, White had said that the SEC has found "a lot of preparedness" in the industry, but that companies' policies and procedures are not "tailored to their particular risks."

Andrew Ceresney, director of the SEC's Division of Enforcement, also recently stated in an SEC webcast that "cyber is obviously a focus of [the SEC Enforcement Division], as I know it is for the other divisions, and we've brought a number of cases there relating to Reg S-P and failure to have policies and procedures relating to safeguarding information. . .There'll be others coming down the pike."

The SEC recently announced similar cease-and-desist proceedings under Regulation S-P against broker-dealer Craig Scott Capital, LLC and two of its principals.

These recent actions should serve as a further warning and example for registered firms to ensure that:

- Cybersecurity policies and procedures are thoroughly and carefully constructed.
- Employee access to confidential customer data is restricted appropriately to those who have a legitimate business need for the information.
- Audits and/or testing of authorization modules are conducted regularly.

- Employee access to, and use of, customer information is regularly monitored and analyzed, including to identify any unusual or suspicious patterns.
- Internet filtering programs should be complete and tailored to the companies' specific business and practices.

Akin Gump can assist with tailoring comprehensive cybersecurity policies and procedures appropriately.

---

[1] On September 21, 2015, Marsh pled guilty to a criminal information in United States v. Galen Marsh, No. 15 Cr. 641 (KTD) (S.D.N.Y.) that charged him with one count of exceeding his authorized access to a computer and thereby obtaining information contained in a financial record of a financial institution, in violation of 18 U.S.C. § 1030(a)(2)(A). On December 22, 2015, a judgment in the criminal case was entered against Marsh. The court sentenced Marsh to 36 months' probation and ordered him to pay restitution in the amount of $600,000.

Categories

Cybersecurity, Privacy & Data Protection | Compliance