wiley

ALERT

Morgan Stanley Pays $1 Million in Settlement with SEC Over Failure to Protect Customer Data from Insider

June 9, 2016

On June 8, 2016, the U.S. Securities and Exchange Commission (SEC) announced that it reached a $1 million settlement with Morgan Stanley over its failure to protect sensitive information about Morgan Stanley's customers.

Under SEC's Regulation S-P broker-dealers and investment advisers registered with the SEC are obligated to adopt written policies and procedures to protect against unauthorized access to customer records and secure the confidentiality of consumer information. 17 C.F.R. § 248.30(a) (the Safeguards Rule). According to the SEC order, Morgan Stanley failed to follow these rules when its system permitted an employee, Galen Marsh, to take information about 730,000 customer accounts, associated with approximately 330,000 different households, off of its software portals and download it to a personal server through his personal website. The misappropriated data included information such as customers' full names, phone numbers, street addresses, account numbers, account balances and securities holdings. Some of this data was later posted for sale on the internet, likely as a result of a hack by a third party.

On September 21, 2015, Marsh 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 in violation of 18 U.S.C. § 1030(a)(2)(A). The SEC said that the misappropriation also constituted a violation of the Safeguards Rule on the part of Morgan Stanley because it had failed to provide reasonable security by not maintaining: "reasonably designed and operating authorization modules for the Portals that restricted

Authors

Kevin B. Muhlendorf
Partner
202.719.7052
kmuhlendorf@wiley.law

Practice Areas

Privacy, Cyber & Data Governance

White Collar Defense & Government Investigations employee access to only the confidential customer data as to which such employees had a legitimate business need; auditing and/or testing of the effectiveness of such authorization modules; and monitoring and analysis of employee access to and use of the Portals."

The SEC made this finding despite the fact that Morgan Stanley had written policies, like its Code of Conduct, that prohibited employees from accessing customer data that was beyond the scope of their employment. In addition to written policies, Morgan Stanley had installed technology controls, including authorization modules that only allowed an employee to access the data for that employee's customers. However, their system was not perfect. As Marsh discovered, he could defeat Morgan Stanley's authorization modules by correctly guessing branch IDs and employee group numbers until he hit upon a combination that gave him access to customer data that was beyond what he was permitted to access. After exploiting these gaps to obtain customer reports, Mr. Marsh was able to transfer the data he obtained to his personal server through his personal website, galenmarsh.com, which he could access while at work because it was "uncategorized" and therefore not blocked by Morgan Stanley.

The most salient part of the case is that even though Morgan Stanley had taken steps to create and implement policies and procedures designed to prevent exactly what occurred here, the SEC deemed the policies insufficient because they did not prevent an insider, later convicted of criminal hacking, from accessing PII. The SEC's standard of care for "reasonable" policies and procedures in this context seems to require that employers tailor an employee's access to PII so that it only extends as far as is necessary to complete the employee's job function. In any large organization this is an enormous undertaking, and it places a heavy burden on employers to discover and prevent any unauthorized access to PII with flawless accuracy.

The SEC's enforcement action is yet another data point showing that after a cyber incident federal regulators are increasingly taking a hard look at companies' cybersecurity practices. There is no such thing as perfect cybersecurity, and unfortunately, it is easy to cast even mature cyber practices in a bad light after an incident. This action again underscores the need for companies to take every step possible to keep current and document the positive aspects of their cybersecurity before—not after—a cyber incident in order to create a positive record to present to regulators.