Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Morgan Stanley Fine Backs Up SEC's Tough Cybersecurity Talk

By **Carmen Germaine**

Law360, New York (June 9, 2016, 10:44 PM ET) -- The U.S. Securities and Exchange Commission backed up a lot of big talk and showed it has little patience for poor cybersecurity with a sizable fine against Morgan Stanley on Wednesday for failing to secure its internal client information systems and prevent a breach, proving the agency is ready to take its place with the big boy privacy regulators, experts said.

Wednesday's $1 million fine against Morgan Stanley Smith Barney LLC is the largest the SEC has imposed yet for violations of the so-called safeguards rule, which requires firms to adopt policies and procedures to safeguard customer information, and experts said that the seven-figure penalty against a major financial institution shows the SEC is making good on its promises to make cybersecurity a priority.

"I think this is the most significant SEC cybersecurity-related action to date," said John Reed Stark, the president of cybersecurity firm John Reed Stark Consulting LLC and founder and former chief of the SEC's Office of Internet Enforcement.

The fine also shows that the SEC is ready and willing to use its power under the safeguards rule to police companies that fall behind on cybersecurity, even if the firm is a victim of a data breach.

Data from 730,000 Morgan Stanley customer accounts was compromised when a former employee of the bank, Galen Marsh, downloaded the data to a personal account and was hacked by a third party, and the bank was on the hook after the SEC found the breach was possible because the bank failed to implement proper controls on two internal client data portals and failed to monitor employee access to the information over the course of 13 years.

A spokesman for Morgan Stanley, James Wiggins, told Law360 that the bank had promptly alerted law enforcement and affected clients after discovering the breach and has since strengthened its mechanisms for safeguarding client data. The SEC order accepting the settlement, which Morgan Stanley agreed to without admitting or denying the charges, said the agency had taken the bank's remedial efforts into account when deciding the fine.

"The takeaway point here is that certainly, when it comes to the so-called safeguards rule, the enforcement staff is going to interpret it rigorously and enforce it aggressively," said Jonathan A. Shapiro, a partner with Baker Botts LLP.

The SEC has been urging companies to pay close attention to cybersecurity for years. Cybersecurity made the Office of Compliance and Examination's annual list of exam priorities for both 2015 and 2016,

and the office has implemented several sweeps testing broker-dealers and investment advisers' cybersecurity compliance and controls.

Agency officials have also been making the rounds touting the benefits of strict cybersecurity controls and threatening enforcement actions. SEC Chair Mary Jo White, for one, has said that cybersecurity is the biggest risk facing the financial system.

In April, broker-dealer Craig Scott Capital LLC paid $100,000 over allegations that it violated the safeguards rule by using nonfirm email addresses to receive faxes. Meanwhile, investment adviser R.T. Jones Capital Equities Management Inc. paid $75,000 in September to settle claims that it failed to implement proper cyber policies before its system was hacked in 2013.

But the agency has brought few cases concerning cybersecurity controls in the past and none against major firms.

"This case demonstrates that even the largest and most significant firms can experience dramatic failures," Stark said.

Experts said that the scope of the case puts the SEC's cybersecurity regime on the map, allowing the agency to stake out territory traditionally dominated by the Federal Trade Commission and the Federal Communications Commission.

Christopher Hart, an attorney with Foley Hoag LLP, said the fine is "another data point" showing the SEC is going to take a more active role in cybersecurity enforcement in the future.

"This is yet further evidence that the FTC is not going to be the only federal agency flexing its muscles in the cybersecurity realm," Hart said.

The fine also offers a preview of how the SEC might continue to flex its muscles in the cybersecurity space using the safeguards rule, experts said.

Stark compared the agency's use of the rule to how it investigates and prosecutes internal controls violations, saying the Morgan Stanley case illustrates how the rule can be a "catch-all" to prosecute cybersecurity weaknesses because it can apply if any customer data is ever at risk, whether or not the firm was actually reckless with the data.

Indeed, experts noted that the SEC order doesn't allege Morgan Stanley committed any kind of fraud against a client account.

Rather, the SEC alleged the bank failed to properly implement or monitor the controls it had in place to prevent a breach, including software restrictions allowing employees to view only data for clients of the financial advisers the employee worked with. Although the bank had effectively blocked employees from using removable storage devices such as thumb drives, it did not keep them from using websites to upload company data to private servers.

"Once you get beyond the truly distressing number of client accounts that were compromised, this is absolutely not a case where Morgan Stanley did anything venal or that frankly feels very reckless," Shapiro said.

Adam Aderton, an assistant director in the asset management unit of the SEC's Division of Enforcement, addressed how the agency enforces cybersecurity in April, saying the SEC had fielded questions from firms concerned that its action against R.T. Jones was doubling down on a firm already victimized by a cyberattack.

But Aderton said at the time that the agency's enforcement actions in the R.T. Jones matter and other cases are "pretty black and white." In the R.T. Jones case, he explained, "there were no policies or procedures, basically a victim with the wallet open, [saying,] 'Come take the money.'"

Similarly, Stark said that while Morgan Stanley had evidently taken swift action to mitigate the breach once it detected the breach, the alleged breakdown in the firm's cyber controls was what enabled the attack in the first place.

"In this instance, Morgan Stanley wasn't the victim of any kind of attack — they were the enabler of an attacker to exfiltrate client data because of their systemic and procedural failures," Stark said.

Agencies like the SEC recognize that data breaches are, to a certain extent, inevitable and are more concerned with what steps companies took to prevent a breach or minimize the harm, according to Hart.

"The agencies want to see companies take cybersecurity seriously because the kind of data that's at stake is so important," he said.

Going forward, experts said that the case shows firms have a lot of work still to do on cybersecurity to keep regulators from knocking on their doors. Stark noted that the case particularly illustrates how customer data is at risk as soon as it leaves the protections of the firm.

In April, Steven Levine, the associate regional director of the SEC's National Exam Program in the agency's Chicago office, said the cybersecurity exams had found weaknesses in how firms monitor their employees' access to and use of sensitive data and urged firms to test to make sure their procedures are working.

"Sometimes the cybersecurity rules are a real pain and your employees will want to take a shortcut," he said.

Notably, while Marsh was criminally convicted for downloading the data and sentenced to three years of probation, forensic analysis later found that it was likely a third party that hacked into Marsh's server and posted the data online.

"Morgan Stanley started the narrative that Galen Marsh sold these records to foreign entities, and that's how they ended up on the internet, and that, on the basis of the evidence, turned out to be flatly false," said Marsh's attorney, Darrelle Janey, a partner at Gottlieb & Gordon LLP.

Shapiro suggested that firms take a close look at their audit programs and thoroughly test their technology in an effort to detect the programming flaws that enabled the breach in the Morgan Stanley case.

"It will help ensure that you're getting it right, but even if you don't get it right, it at least will buttress a good-faith defense when inevitable mistakes happen," he said.

The SEC is represented by William Martin, Simona Suh and Joseph G. Sansone.

Morgan Stanley is represented by Robert Juman of Quinn Emanuel Urquhart & Sullivan LLP.

Marsh is represented by Derrelle Janey of Gottlieb & Gordon LLP.

The administrative proceedings are In the Matter of Morgan Stanley Smith Barney LLC, file number 3-17280, and In the Matter of Galen J. Marsh, file number 3-17279, before the U.S. Securities and Exchange Commission.

--Additional reporting by Jody Godoy and Max Stendahl. Editing by Christine Chun and Philip Shea.