Advisory

JUNE 2016

If you have any questions about this Advisory, please contact:

DAVID HALL
215.988.8325
dhall@wiggin.com

JOHN KENNEDY
203.363.7640
jkennedy@wiggin.com

CONOR MULLAN
215.988.8319
cmullan@wiggin.com

Morgan Stanley Hit with $1 Million Fine in SEC Cybersecurity Enforcement Action

On June 8, 2016, the SEC announced that Morgan Stanley Smith Barney LLC ("MSSB") has agreed to pay a $1 million penalty to settle an enforcement action. The enforcement action is based on the charge that MSSB failed to adopt written policies and procedures reasonably designed to protect customer data in violation of Rule 30(a) of Regulation S-P (the "Safeguard Rule"). The **SEC Order** alleged that, from 2011 to 2014, then-current MSSB financial advisor Galen Marsh was able to access and download personal identifiable information ("PII") of over 700,000 MSSB advisory and brokerage clients to his personal server. Portions of the stolen PII were later posted online with an offer to sell additional information, and MSSB discovered the breach during one of its routine internet searches shortly thereafter. The misappropriated PII included such information as names, phone numbers, addresses, account numbers, account balances, and holdings.

According to the SEC's Order, Marsh was only authorized by MSSB policy to access client data for the hundreds of MSSB clients that he advised or that were advised by his group within MSSB. Nonetheless, Marsh was able to access data for all MSSB clients through a programming flaw in MSSB portals where the data was stored. He accessed this data thousands of times over a three-year period. Marsh was also able to transfer the data to a personal server, despite MSSB's controls that were intended to prevent employees from copying data onto removable storage devices and access certain categories of websites. He did this by transferring the data to a personal website. MSSB's controls at the time did not restrict access to this type of "uncategorized" site. Thereafter, starting in December 2014, the MSSB data began appearing on various websites for sale.[1] MSSB discovered this breach shortly thereafter during a routine internet sweep, identified Marsh as the source of the leak, alerted authorities, and notified affected customers.

Based on these data security flaws, the SEC alleged that MSSB violated the Safeguard Rule by failing to adopt written policies and procedures reasonably designed to protect customer records and information[2] But, based on the limited amount of information set forth in the SEC Order, it appears that MSSB actually had adopted fairly comprehensive cybersecurity/privacy policies and procedures. The policies and procedures were designed to keep client data restricted by investment teams or business lines. Further, MSSB had disabled or otherwise prohibited employee use of removable storage devices and web-based storage sites, and had conducted internet sweeps and internal sweeps for prohibited software and website access. The SEC's focus in the Order appears to be on MSSB's apparent failure to audit and test its security policies and procedures. In fact, the most significant, concrete allegations against

CONTINUED ON NEXT PAGE

Morgan Stanley Hit with $1 Million Fine in SEC Cybersecurity Enforcement Action

MSSB were that it failed to: (1) audit and/or test the effectiveness of the authorization modules for the portals; and (2) monitor employee access to and use of the portals. In this regard, perhaps the most damning allegation was that MSSB had not conducted any auditing or testing of the authorization modules for the portals that contained the client data that Marsh misappropriated over the 10 years that they were in use.

This settlement should serve as a reminder to investment advisers, broker-dealers, and other financial services firms that adopting comprehensive written policies and procedures is not enough to avoid a cybersecurity enforcement action. The SEC has made it clear that there is an expectation that firms under its jurisdiction fully address industry and firm-specific cybersecurity risks. To address these risks, firms need to conduct periodic risk assessments, assess vulnerabilities, and, to the extent that a firm's cybersecurity risks warrant it, engage third parties to conduct vulnerability scans and penetration testing.

If you have any questions about the MSSB's settlement or cybersecurity issues, please do not hesitate to contact us.

[1] According to the SEC Order, forensic analysis of Marsh's personal server revealed that a third-party likely hacked into Marsh's server, copied the information, and that the third-party was likely responsible for posting the information online (not Marsh).
[2] In a separate SEC Order, Marsh agreed to an industry bar with the right to reapply after five years. Marsh was also criminally convicted in the Southern District of New York last year for his misconduct and received 36 months' probation and was ordered to pay $600,000 restitution.