SEC Fine Against Morgan Stanley Underscores Focus on Cybersecurity

Morgan Stanley Smith Barney LLC recently agreed to pay a $1 million penalty to the U.S. Securities and Exchange Commission after a Morgan Stanley employee downloaded and exposed sensitive investor information. This penalty reflects the SEC's insistence on greater cybersecurity controls among its registrants. As the Director of Enforcement, Andrew Ceresney stated, "Given the dangers and impact of cyber breaches, data security is a critically important aspect of investor protection, we expect SEC registrants of all sizes to have policies and procedures that are reasonably designed to protect customer information."

Over a three year period, a Morgan Stanley employee downloaded personal information from nearly 730,000 investor accounts to a personal server in his home so that he could conduct "cold calls." Although Morgan Stanley's policies and safeguards prohibited downloading information to thumb drives, they did not prohibit employees from downloading information to third-party servers through web portals. Ultimately, the employee's private server was hacked, resulting in the investor information being posted to YouTube and other websites. (See SEC Press Release, SEC: Morgan Stanley Failed to Safeguard Customer Data (June 8, 2016), available at https://www.sec.gov/news/pressrelease/2016-112.html.)

Rule 30(a) of Regulation S-P (codified at 17 C.F.R. §§ 248.30), commonly known as the "safeguards rule," requires brokers, dealers, investment companies, and investment advisers to adopt policies and procedures to protect customer records and information from unauthorized access. In September 2015, the SEC issued a risk alert providing guidance to registrants on securing sensitive information. (See OCIE's 2015 Cybersecurity Examination Initiative (Sept. 15, 2015), available at https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf.)

This is only the second SEC enforcement action related to cybersecurity. A few months ago, the SEC fined R.T. Jones Capital Equities Management, a St. Louis-based investment adviser, $75,000 under the safeguards rule after Chinese hackers stole information relating to more than 100,000 clients from an unsecured third-party server. (See SEC Press Release, SEC Charges Investment Adviser With Failing to Adopt Proper Cybersecurity Policies and Procedures Prior To Breach (Sept. 22, 2015), available at https://www.sec.gov/news/pressrelease/2015-202.html.)

SEC registrants should take note. Data breaches are far too common and can have a devastating impact, particularly in the financial sector. It is highly likely that the SEC will continue to use enforcement actions to push the investment industry to develop strong cybersecurity measures to protect their clients and the economy as a whole.

For more information, please contact:

Dennis Klein, *Partner*
+1 (305) 379-5574
dennis.klein@hugheshubbard.com

Seth Rothman, *Partner*
+1 (212) 837-6872
seth.rothman@hugheshubbard.com

Jeffrey Goldberg, *Associate*
+1 (305) 379-5573
jeffrey.goldberg@hugheshubbard.com

Tyler Grove, *Associate*
+1 (202) 721-4625
tyler.grove@hugheshubbard.com

June 2016

Hughes Hubbard & Reed