Cybersecurity and the SEC

By Alan S. Wernick, Esq.

The U.S. Securities and Exchange Commission ("SEC") has been active in promulgating regulations, guidance, and enforcement concerning cybersecurity as part of the growing concern of government regulators about cybersecurity risks. The SEC has published an online portal to address Cybersecurity and the SEC.

In 2011 the SEC Division of Corporation Finance issued "CF Disclosure Guidance: Topic No. 2 Cybersecurity." In that Disclosure Guidance the SEC states several observations including:

- "For a number of years, registrants have migrated toward increasing dependence on digital technologies to conduct their operations. As this dependence has increased, the risks to registrants associated with cybersecurity have also increased, resulting in more frequent and severe cyber incidents."
- "…material information regarding cybersecurity risks and cyber incidents is required to be disclosed when necessary in order to make other required disclosures, in light of the circumstances under which they are made, not misleading. Therefore, as with other operational and financial risks, registrants should review, on an ongoing basis, the adequacy of their disclosure relating to cybersecurity risks and cyber incidents."
- "Registrants should disclose the risk of cyber incidents if these issues are among the most significant factors that make an investment in the company speculative or risky. In determining whether risk factor disclosure is required, we expect registrants to evaluate their cybersecurity risks and take into account all available relevant information, including prior cyber incidents and the severity and frequency of those incidents. As part of this evaluation, registrants should consider the probability of cyber incidents occurring and the quantitative and qualitative magnitude of those risks, including the potential costs and other consequences resulting from misappropriation of assets or sensitive information, corruption of data or operational disruption. In evaluating whether risk factor disclosure should be provided, registrants should also consider the adequacy of preventative actions taken to reduce cybersecurity risks in the context of the industry in which they operate and risks to that security, including threatened attacks of which they are aware."

In September 2015 the SEC announced that it settled an enforcement action against an investment advisor stemming from allegations by the SEC that the investment advisor failed to establish the required cybersecurity policies and procedures in advance of a breach that compromised the PII of approximately 100,000 individuals, including thousands of the firm's clients. The investment advisor, R.T. Jones,

agreed (1) to cease and desist from committing or causing any future violations of Rule 30(a) of Regulation S-P; (2) to be censured; and (3) to pay a $75,000 penalty. About the time of the announcement of the settlement the SEC issued an "Investor Alert: Identity Theft, Data Breaches and Your Investment Accounts."

In the SEC's "Examination Priorities for 2016" the SEC states "In September 2015, we launched our second initiative to examine broker-dealers' and investment advisers' cybersecurity compliance and controls. In 2016, we will advance these efforts, which include testing and assessments of firms' implementation of procedures and controls."

On June 8, 2016, the SEC announced an agreed settlement order with Morgan Stanley Smith Barney (the "Registrant") which included the payment of a $1 million penalty to settle charges related to the Registrant's failures to protect customer information. The SEC's order found that the Registrant had violated the "Safeguards Rule" (Rule 30(a) of Regulation S-P). Among other things, the SEC order alleged that registrant (a) did not have effective authorization modules for more than 10 years to restrict employees' access to customer data based on each employee's legitimate business need; (b) did not audit or test the relevant authorization modules, nor did it monitor or analyze employees' access to and use of the portals; and (c) had policies and procedures which were not reasonable for two internal web applications or "portals" that allowed its employees to access customers' confidential account information. In addition, Registrant's employee, Galen J. Marsh, was found to have downloaded and transferred confidential data to his personal server at home between 2011 and 2014, and that a likely third-party hack of Marsh's personal server resulted in portions of the confidential data being posted on the Internet with offers to sell larger quantities of the confidential data. Morgan Stanley agreed to settle the charges without admitting or denying the findings. Marsh agreed to an industry and penny stock bar with the right to apply for re-entry after five years, was criminally convicted for his actions, and received 36 months of probation and a $600,000 restitution order.

While the SEC Disclosure Guidance is directed at publicly held companies, privately owned companies may want to take heed – the bad actors behind the cybersecurity threats do not necessarily care if you are a publicly held company. If you have clients who are in the financial services industry, then you will want to consider the evolving attention to the SEC's cybersecurity risks guidance, regulations, and enforcement actions involving cybersecurity risks.

For comments about this article or to be added to the *ITIP Alert™* subscriber's list, please contact ALAN WERNICK (E-MAIL: ALAN@WERNICK.COM; PHONE: 847.786.1005 OR 614.463.1400).