CARLTON FIELDS

SEC Cyber Update: Official Outlines Active Role for SEC on Cybersecurity as Enforcement Questions Persist

CYBERSECURITY AND PRIVACY | SECURITIES TRANSACTIONS AND COMPLIANCE | JUNE 29, 2016

John E. Clabby

SEC Chicago Regional Director David Glockner spoke at a PLI Conference in New York on June 6 regarding the SEC's data security regulations and enforcement efforts. Mr. Glockner acknowledged frustration with the Division of Corporation Finance's 2011 guidance as to cyber disclosures, but explained that the Commission must balance generality and specificity in an admittedly complex area of the law.

The SEC's Three Main Areas of Concern

Mr. Glockner identified three areas where the SEC is active as to cybersecurity. The first concerns a public company's or issuer's disclosure of cyber risk factors and disclosures following a breach incident, both of which are overseen by the SEC's Division of Corporation Finance. Mr. Glockner explained that the Division of Corporation Finance has typically handled perceived issues with such disclosures through staff comments and letters, noting that the Division of Enforcement has yet to bring an enforcement action. Notwithstanding Mr. Glockner's explanation, it is unclear how long this SEC preference will last. There is no guarantee that a shift from staff comments to enforcement will come with additional warnings.

The second area of concern is ensuring market integrity from manipulative cyberattacks seeking material nonpublic information. The SEC continues to work with domestic and international regulatory and law enforcement agencies in response to this threat. From this practitioner's perspective, while the Justice Department's public statements and prosecutions in recent years have established its view that companies that experience hacks will be treated primarily as victims, the SEC's public statements and recent actions in this regard have not been as clear.

The third area of concern, according to Mr. Glockner, is an ongoing effort to protect investors by requiring SEC-registered entities' compliance with certain cybersecurity standards. The SEC has promulgated several regulations aiming to improve industry-wide security, including the privacy requirements of Regulation S-P (the "Safeguards Rule") and the identity-theft provisions of Regulation S-ID. Note that the controls-related standards are specific to SEC-registered entities, such as broker dealers and investment advisers, rather than to public companies generally. And in contrast to disclosure-based violations, enforcement efforts in this area are well underway.

Letters and Penalties

As noted, the SEC has yet to bring an enforcement action against a company for inadequate cybersecurity disclosures, but

the agency has been active with comment letters.

For example, in August 2015 the SEC sought to clarify whether Santander UK Group Holdings plc, in its filing on Form 20-F, had been the victim of any cyberattacks in the past and asked the bank to revise its disclosure if those attacks were material. Santander's initial disclosure had stated only that it had faced risks from a "host of cyber threats" but did not discuss whether the bank had suffered any such attack. In response to the SEC letter, Santander noted that it had not suffered any "material" cyber incidents in the past five years, and it otherwise amended its disclosure to add additional detail.

The SEC has not been as hesitant to bring actions against registered entities for failing to protect consumer data, even when the company was the victim of a crime.

Two days after Mr. Glockner gave his remarks, the SEC announced that Morgan Stanley Smith Barney LLC had agreed to pay $1 million to settle charges under Regulation S-P's Safeguards Rule for failure to adequately protect customer personal information. The findings, which Morgan Stanley neither admitted nor denied, stated that an employee impermissibly accessed and transferred the data of more than 700,000 customer accounts to his personal server over a period of three years due to inadequate security measures. The employee was only caught when a third party hacked his computer and posted the data online.

The employee was convicted last year for his offense and was sentenced to 3 years' probation and $600,000 restitution. Although Morgan Stanley was the victim of a crime – the employee's theft of its customer data – the bank still had to pay $1 million to settle the action because of its alleged failure to restrict access in certain customer portals based on each employee's legitimate business needs.

It remains to be seen what impact, if any, the SEC's enforcement actions under Regulation S-P will have on registered entities' willingness to cooperate with the SEC when they have been the victim of a data theft in the cyber context.

Guidance Proves Elusive

Mr. Glockner referenced the frustration that many companies have expressed that the SEC has not provided direction beyond the Division of Corporation Finance's 2011 guidance as to cyber risk disclosures. Guidance generally is difficult in this area owing to the complex and nuanced nature of cybersecurity enforcement and compliance, but Mr. Glockner noted that materiality as to cybersecurity is no different than in other areas of financial reporting.

Mr. Glockner's remarks offer some comfort for companies making reasoned decisions over cybersecurity disclosures. Furthermore, the Commission has been consistent in the view that a breach is not per se evidence of inadequate cybersecurity measures or disclosures.

There remain substantial questions over what does constitute an inadequate disclosure of cyber risk or a violation of the Safeguards Rule and other privacy-related regulations. For so long as the SEC responds to disclosure-based deficiencies with only letters and comments, the brunt of this enforcement uncertainty will be borne by registered entities attempting to protect customer data under somewhat better-understood regulations.