BROOKS PIERCE

SEC Enforcement Lays out Approach to Cybersecurity

Digital Media and Data Privacy Law Blog

on 02.23.2016

Posted in Data Security, Digital Media and Data Privacy Law, Privacy

If you've ever attended the SEC Speaks conference, you know that the official program is an intensely uninteresting collection of short speeches by SEC officials who don't have a lot of incentives to say groundbreaking things. But occasionally there are exceptions. I think Deputy Director Stephanie Avakian's discussion of cybersecurity cases on Friday was one of those.

Avakian broke those cases down into three categories.

1. Failures of registered entities to safeguard information. She cited the *R.T. Jones Capital Equities Management* case from September of last year as an example of those.
2. Electronic thefts of material nonpublic information, and illicit securities trading following the thefts. Avakian cited the *Dubovoy* case filed in the District of New Jersey last August and updated on Thursday as an example of these.
3. Cyber-related disclosure failures by public companies. The SEC hasn't brought any cases in this category yet, and much of Avakian's discussion focused on why that is the case and how the SEC might get to the point of bringing one.

Assuringly for companies that are investing resources in cybersecurity and trying to do the right things for its customers and shareholders, Avakian said, "A company that has been a victim of an intrusion is just that: a victim." She also said in several different ways that the Division understands that when attacks happen, critical facts can change and develop very quickly. These developing facts can make any necessary disclosures a moving target. Along these lines, the Enforcement Division will appreciate the difficulty of the circumstances, Avakian says. She added that the SEC is not looking to second guess well thought decisions in this area.

With all of that said, the Enforcement Division very much wants companies that are victims of cyber attacks to involve appropriate law enforcement authorities as quickly as they reasonably can. It will also examine (1) whether companies have policies and procedures that are reasonably designed to protect customer information; and (2) whether companies with potential liability have self-reported issues to the Division. Regarding the second factor, the SEC's Seaboard Report from 2001 continues to include the guideposts the Division will consider.

While no cases have yet been brought against public companies in this third category, *Avakian can imagine circumstances* in which the Commission does file a case to penalize inadequate cybersecurity disclosures. I can, too. Be careful out there.