Kit Addleman, Tim Newman and Carrington Giammittorio on American Bar Association Website: 'A Look at SEC's Last Decade of Cybersecurity Enforcement Efforts, Part 1: Focus on Public Companies'

February 17, 2022 Kit Addleman, Tim Newman, Carrington Giammittorio

PRACTICES Litigation, Corporate Governance, Crisis Management

A decade ago, the Securities and Exchange Commission (SEC) increased its focus on cybersecurity and the impact cybersecurity incidents and risks have on the market and on investors. For public companies, the commission began to focus on what those companies were saying (or not saying) about cybersecurity incidents they suffered or the cybersecurity risks that affect their businesses. For regulated entities, the commission's attention was heightened on cybersecurity controls—i.e., what policies and procedures did registered entities have in place to protect customer data and to prevent, detect, and respond to cybersecurity attacks?

Over the past 10 years, the commission has discussed cybersecurity obligations under federal securities laws through staff-level and commission-level guidance, comment letters, division priorities, and alerts; a section 21(a) report of investigation; and, more recently, enforcement actions. This two-part series looks back at what the SEC has said about cybersecurity, starting with the focus on public company disclosure obligations (in Part I) and following with the focus on registered entities' cybersecurity controls (in Part II).

The Initial Salvo Was Staff-Level Guidance from the SEC's Division of Corporation Finance

On October 13, 2011, the SEC's Division of Corporation Finance released guidance, CF Disclosure Guidance: Topic No. 2—Cybersecurity (Oct. 13, 2011) (the 2011 guidance), outlining its views on public company disclosure obligations related to cybersecurity. This was the first time the commission or any of its divisions spoke explicitly about cybersecurity disclosure obligations. The 2011 guidance did not establish any new disclosure requirements. Instead, it reviewed the existing framework of disclosure obligations, highlighting the following disclosure areas, which might be implicated by cybersecurity incidents or risks:

- Risk Factors;
- Management's Discussion and Analysis of Financial Condition and Results of
- Operations (MD&A);
- Description of Business;
- Legal Proceedings;

- Financial Statement Disclosures; and
- Disclosure Controls and Procedures

Excerpted from *The American Bar Association*. To read the full article, click here.