STRATEGIC PERSPECTIVES: FTC increasingly looks to public companies’ SEC disclosures for privacy and cybersecurity enforcement opportunities, (Mar. 24, 2020)

Cooley experts offer practical considerations for companies preparing privacy and cybersecurity-related disclosure to help them address the growing risk of FTC investigations based on that disclosure.

While the FTC does not make its initial privacy and cybersecurity investigations public, there have been reports that the FTC has initiated an increasing number of privacy and cybersecurity-related enforcement actions following disclosures of privacy or cybersecurity incidents by public companies in their SEC filings.

The FTC has the authority to take enforcement actions under Section 5 of the FTC Act. Section 5 makes any "unfair" or "deceptive" business practices—including those relating to privacy and cybersecurity—unlawful and subject to investigation and enforcement by the FTC.

In applying Section 5, the FTC has taken the position that inadequately disclosing privacy and cybersecurity incidents in SEC filings may be a deceptive business practice that violates Section 5. The FTC then appears to rely on its review of SEC filings as a launching pad to investigate privacy and cybersecurity incidents, even where the filings themselves are adequate.

Typically, the FTC launches such an investigation through a Civil Investigative Demand (CID) that asks a company to produce information and documents about a privacy or cybersecurity incident disclosed in an SEC filing. A CID is a type of subpoena that the FTC uses to obtain documents and other information related to an FTC investigation. Receipt of a CID following disclosure of a privacy or cybersecurity incident may indicate that the FTC is investigating whether the company’s disclosures or the underlying incident constitute unfair or deceptive practices prohibited by Section 5.

To address the increasing risk of FTC privacy and cybersecurity investigations, public (or soon-to-be public) companies should consider the following:

- If the company is preparing for an IPO, consider whether the company, or key vendors that handle information or provide systems on the company’s behalf, have experienced privacy or cybersecurity incidents that may have been material, but which the company may not have timely disclosed in compliance with applicable contractual and statutory notification obligations. Companies should disclose such incidents when preparing for an IPO.
- When reviewing SEC filings (whether registration statements or periodic reports), confirm the accuracy of disclosures regarding privacy or cybersecurity incidents that the company or its key vendors experienced, and disclose the risk that such incidents may occur in the future. Consider confirming that the company handled any material privacy or cybersecurity incidents appropriately (i.e., in compliance with applicable contractual and statutory notification obligations).
- Work with counsel skilled in public company governance and cyber/data/privacy issues to draft SEC disclosures in a way that mitigates the risk of piquing the FTC’s interest. Drafting these disclosures is a careful balancing act between providing reserved transparency and avoiding well-meaning disclosures that are—in the FTC’s view—an indictment of the company's data or cybersecurity practices.
- If the company received a CID from the FTC, reach out to counsel with experience handling FTC privacy and cybersecurity enforcement actions. The FTC has a dedicated team handling these investigations, and understanding the FTC’s methods, pain points and limitations is key to an effective representation.
Attorneys: Boris Segalis and Tonia Soris (Cooley LLP).

MainStory: CyberPrivacyFeed GCNNews PublicCompanyReportingDisclosure Enforcement RiskManagement IPOs