CHICAGOLAWBULLETIN.COM

Serving Chicago's legal community for 160 years

THURSDAY, JULY 23, 2015

Chicago Daily Law Bulletin®

Volume 161, No. 143

Data security: How to answer when the FTC comes calling

The Federal Trade Commission wants companies to know that being the subject of a data security investigation isn't a reason to panic — usually.

That's one of the messages of a May 20 blog post by Mark Eichorn, the agency's assistant director for privacy and identity protection. Titled "If the FTC Comes to Call," the post outlines what companies should expect when the FTC initiates an investigation into their data security practices, the type of information the agency reviews and the parameters it uses during an investigation.

The FTC has increasingly focused its enforcement efforts on these types of data security investigations in the past several years. In the past 10 years, the FTC has opened more than 50 new data security investigations.

Last year alone, the FTC reported that it took administrative action against several well-known companies, including Snapchat, Fandango and Credit Karma.

The agency accused Snapchat of deceiving customers. Snapchat, the developer of a mobile messaging app, told consumers that photos taken with the app would disappear forever after a short time, when, in reality, the photos could be retrieved and saved by the recipient. In addition, the app collected location and address book data without properly disclosing its collection practices to users.

In the Fandango and Credit Karma cases, the FTC alleged that both Fandango and Credit Karma failed to take reasonable steps to secure their mobile apps by disabling a critical default process for security certificate validation thereby leaving information sent or received through their mobile apps vulnerable to attack.

All three companies settled with the FTC with consent orders that required them to dedicate time, money and personnel to creating, maintaining and monitoring a data security program.

Of course, not all investigations result in enforcement actions. According to the blog post, most begin informally, with the FTC initiating the investigation on its own or based on outside tips such as news reports, consumer complaints or complaints from other companies. The agency may also launch an investigation at the request of Congress or other agencies.

If the FTC decides a full investigation is necessary, a company usually can expect to be first notified by a letter requesting more information. The purpose of the information gathering is to determine whether what a company says about its data security practices matches what it does. The FTC also wants to assess whether the practices "are reasonable in light of the sensitivity and volume of consumer information the company holds, the size and complexity of its business and the cost of available tools to improve security and reduce vulnerabilities," the FTC said.

Records the FTC may expect the company to hand over include documents related to the organization's policies and practices, such as audits or risk assessments that the company or its service providers have performed; the company's information security plan, privacy policies and any other promises the company has made to consumers about its security; and the employee handbooks and training materials. The FTC says it also may want to interview employees and people outside the company, such as data security experts, consumers and vendors' employees, who have knowledge about the company's data security practices.

Some companies are subject to statutes such as the Gramm-Leach-Bliley Act, which require financial institutions to explain their information-sharing practices to their customers and to safeguard sensitive data, or the Fair Credit Reporting Act, which governs the collection, dissemination and use of consumer credit information. If so, the FTC will evaluate the company's compliance with those regulations.

If a data breach triggers the investigation, the agency will zero in on the likely or actual harm the breach may have caused to consumers.

"As a consumer protection agency," the FTC noted, "we're focused on the security of consumer information entrusted to the company — not its IP portfolio, trade secrets or the loss of other company information that doesn't concern consumers."

The FTC said it looks favorably on companies that take steps to mitigate damage by reporting a breach, assisting affected consumers and cooperating with law enforcement agencies.

If the FTC decides the company under investigation has broken the law, it will take administrative action, which may be resolved through settlement and a consent order. The agency also can file a complaint in federal court.

A company under formal investigation can expect to divert significant resources in terms of the time employees must spend responding to the FTC's requests for documents and other materials as well as testifying before the agency. A company defending itself in federal court may need to hire outside counsel and other experts and may be tied up in litigation for years. In addition, negative news coverage can damage the organization's business and reputation — regardless of the outcome.

While these investigations are expensive and burdensome for affected companies, they present amazing learning opportunities for other companies. In fact, the FTC has launched a Start Off With Security education initiative and has issued guidance gleaned from previous investigations. (Look for more on this initiative in next month's column.)

In the meantime, companies can take steps to ensure that internal and consumer-facing practices reflect the company's written policies, which should be appropriate to its size and industry.

Companies also must train employees and vendors to comply with those policies. Companies that regularly review their data security policies, employee and vendor practices and compliance with any industry regulations may be able to limit the time, costs and bad publicity of an FTC investigation.

PRIVACY, TECHNOLOGY AND LAW

Nerissa Coyle McGinn

Nerissa Coyle McGinn is a Chicago-based partner at Loeb & Loeb LLP. Her practice focuses on matters involving the convergence of advertising and promotions, emerging media, technology and privacy law as well as intellectual property law, focusing on trademark clearance and counseling.

A company defending itself in federal court may need to hire outside counsel and other experts and may be tied up in litigation for years.