FOR METRO AREA IN-HOUSE COUNSEL

An incisivemedia publication

GC New York

New York Law Journal

Thursday, September 18, 2008

Surviving an FTC Investigation After a Data Breach

BY LISA J. SOTTO
AND AARON P. SIMPSON

Most large companies have likely experienced numerous information security incidents in the recent past. Given the high number of state security breach notification laws, incidents requiring notification have become relatively commonplace. These incidents range from the most innocuous to the most malicious—from a simple theft of an employee's laptop or a vendor's loss of backup tapes to a rogue employee stealing customer credit card data, a phishing attempt or a large-scale system intrusion.

Companies that have experienced information security breaches are required to notify not only the individuals whose personal information was impacted but also numerous state regulators. Rather than end the process there, however, in an increasing number of cases, breach notification triggers a new process: an investigation of the company's privacy and information security practices by the U.S. Federal Trade Commission (FTC).

When a company notifies affected individuals of a security breach, the information quickly becomes public. Security breaches garner not only the attention of the media, but also the attention of the consumer advocacy community. Since 2005, the Privacy Rights Clearinghouse, a nonprofit consumer advocacy organization, has maintained a publicly available Web site containing a chronology of reported security breaches. See http://www.privacyrights.org/ar/ChronDataBreaches.htm (last visited Aug. 19, 2008).

The chronology currently provides details on more than 1,000 breaches impacting more than 236 million records containing sensitive personal information. Given the publicity, it should come as no surprise that a byproduct of the notification requirement is increased awareness by regulators at both the state and federal levels. Most prominently, this has resulted in increased investigatory activity by the FTC.

FTC Authority

Since 1999, the FTC has asserted its jurisdiction in the privacy and information security arena pursuant to §5 of the FTC Act. See 15 USC §45 (2007). Section 5 states that the FTC is empowered to "prevent persons, partnerships, or corporations…from using…unfair or deceptive acts or practices in or affecting commerce." Id. at §45(a)(2). The FTC investigates and enforces data privacy and security incidents under both the "deceptiveness" prong and the "unfairness" prong of §5.

The 'Deceptiveness' Prong. Between 1999 and 2005, FTC enforcement in the privacy and information security arena focused primarily on the "deceptiveness" prong of §5. A "deceptive" trade practice in the privacy context typically involves inaccurate or untrue representations to the public regarding a company's information practices. In practice, these representations are made in Web site privacy notices, which California law requires many companies to post. See Calif. Bus. & Prof. Code §§22575-22579 (2005). The FTC has brought a number of enforcement actions against companies for failing to honor representations made in their Web site privacy notices, including enforcement actions against GeoCities, ToySmart.com, Eli Lilly, Microsoft and Gateway Learning Corporation ("Gateway").

The FTC's enforcement action against Gateway typifies this line of cases. In Gateway, the company's Web site privacy notice originally indicated that the company did not sell, rent or loan personal information about its customers to any third party without explicit consent. After collecting personal information from customers under this privacy notice, Gateway changed its policy to indicate that it would share the information with third parties without notifying customers or obtaining their consent. The new policy offered customers the opportunity to opt out of Gateway's disclosure of personal information to third parties.

The FTC charged Gateway with violating §5 of the FTC Act by making false claims in its privacy statement and deceptively changing its policy without notifying consumers. The FTC required, among other things, that Gateway obtain opt-in consent from customers prior to disclosing personal information to third parties and to disgorge the money it had earned from renting consumer information without explicit consent under the revised policy. See Gateway Learning Corp., FTC Decision and Order, Docket No. C-4120, at http://www.ftc.gov/os/caselist/0423047/040917do0423047.pdf (last visited Aug. 18, 2008).

The 'Unfairness' Prong. Starting in 2005, the FTC began to expand its jurisdiction in the privacy and information security context

Lisa J. Sotto *is a partner and head of the privacy and information management practice at Hunton & Williams in the New York office. She is also vice chair of the Department of Homeland Security's Data Privacy and Integrity Advisory Committee.* **Aaron P. Simpson** *is an associate with the firm in the New York office in the privacy and information management practice.*

by focusing on information security breaches using the "unfairness" prong of §5. The timing of the FTC's enhanced scrutiny was perhaps not coincidental; it commenced soon after the vast majority of states passed breach notification laws in 2005. Rather than using companies' Web site privacy statements as its sole enforcement hook, the FTC's use of the "unfairness" principle provided the agency with a way to significantly expand its consumer protection powers, resulting in its highest-profile data security cases to date, including those against BJ's, ChoicePoint, CardSystems, DSW, TJX and Reed Elsevier. These cases undoubtedly were prompted by the publicity generated as a result of the state breach notification laws.

FTC Enforcement Actions

From beginning to end, an FTC investigation and enforcement action against a company as a result of a data security incident can take over two years and cost the target company millions of dollars in legal and consulting fees. Once the initial process is complete, the FTC often imposes obligations on target companies that last decades into the future.

An FTC enforcement action generally begins with an investigation. Following a data breach, the agency typically sends an access letter to the target company, inquiring into the company's information security practices. The access letter consists of numerous questions and requests, including inquiries concerning:

- the personal information the company processes on behalf of consumers;
- the steps the company has taken to secure personal information it processes; and
- information related to the incident that led to the investigation, including the production of all documents relating to the incident.

Based on the information it receives in response to the access letter and any follow-up inquiries, the FTC will decide whether to bring a formal enforcement action. If the FTC chooses to bring an action, it provides to the target company after a series of discussions a Draft Complaint and Proposed Consent Order. These documents do not become part of the public record unless and until they are accepted by a vote of the five FTC commissioners. This vote typically takes place 30 days after the Draft Complaint and Proposed Consent Order are provided to the target company. Assuming the FTC commissioners accept the Proposed Consent Order, it is subject to public comment for 30 more days, after which the FTC commissioners decide whether to make the Proposed Consent Order final. If they decide to make it final, the FTC formally issues its Complaint and enters its Decision and Order, which typically occurs approximately two months after the end of the public comment period.

Complying With an FTC Order

When the Order becomes final about four to six months after the Draft Complaint and Proposed Consent Order are provided to the target company, the company's substantive obligations officially begin. The FTC typically requires target companies to establish and implement, no later than the date the Order is issued, a comprehensive information security program to protect consumer personal information. "Personal information" typically is defined broadly to include data such as name and address. The FTC requires that this information security program, which must be fully documented in writing, contain specific administrative, technical and physical safeguards.

Administrative safeguards include (i) privacy and information security policies and procedures, (ii) information security and awareness training, and (iii) the implementation of reasonable steps to select and retain service providers that will have access to personal information. Technical safeguards are security measures that dictate how technology within the company should be used to protect personal information, including implementing (i) mechanisms to control internal and external risks to the security, confidentiality and integrity of personal information and (ii) security measures to prevent unauthorized access to personal information transmitted over electronic communications networks. Physical safeguards are security measures designed to protect information systems from unauthorized intrusions, including limiting physical access to information systems and the facilities where they are housed.

Given how ubiquitous this requirement to implement administrative, technical and physical safeguards has become in FTC orders, it is imperative that companies subject to an FTC investigation get a head start on this process as it can take far longer than the four to six months allotted by the FTC to develop such a program. Establishing or enhancing an information security program presents unique challenges. The development of a solid program requires an in-depth understanding of the flow of personal information throughout the organization, from its collection or creation to its ultimate disposition. This information about data flow forms the foundation of any successful information security program.

Developing and implementing an information security program are only the beginning of the target company's substantive obligations under an FTC Order. Within six months after service of the Order, the FTC requires the target company to file a formal written report setting forth the manner and form in which it has complied with the Order. For most companies that have experienced an FTC enforcement action, this means months of drafting and consultation with the many relevant stakeholders within the organization.

In addition to requiring the target company to submit its own written report on compliance, the FTC also requires the company to obtain a third-party assessment within two months after filing the company's report. This assessment must be conducted by a qualified, objective, independent third-party professional and it must (i) set forth the administrative, technical and physical safeguards implemented and maintained by the target company during the first six months after service of the Order; (ii) explain how such safeguards are appropriate to the target company's size and complexity, the nature and scope of the company's activities, and the sensitivity of the personal information collected from or about consumers; (iii) explain how the safeguards that have been implemented meet or exceed the protections required by the FTC Order; and (iv) certify that the target company's security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality and integrity of personal information is protected.

The target company must provide this assessment, as well as all plans, reports, studies, reviews, audits, audit trails, policies, training manuals and assessments, whether prepared by or on behalf of the target company, to the FTC within 10 days after the independent assessment has been prepared.

Continuing Obligations

While the independent assessment marks the end of the immediate obligations imposed on the target company, the FTC typically imposes continuing obligations on companies subject to an Order. These obligations include:

- Conducting third-party assessments biennially for 20 years and retaining the written assessments and all materials relating to the assessments until the Order is terminated.
- Maintaining, and making available to the FTC for five years, a copy of each document relating to compliance with the terms and provisions of the Order.
- Delivering for 10 or more years a copy of the Order to all future principals, officers, directors and managers of the company, and to all future employees and other representatives having supervisory responsibilities with respect to the subject matter of the Order.

In most cases, the FTC Order terminates 20 years from the date of its issuance, or 20 years from the most recent date the FTC files a complaint in federal court alleging any violation of the Order, whichever comes later. The continuing obligations required by an FTC Consent Order mean that the target company is beholden to the FTC in nearly all aspects of its operations for decades after the Order is issued. The toll on employees responsible for compliance with the Order and the financial burden associated with compliance cannot be underestimated.

Conclusion

The sharp uptick in FTC enforcement activity (along with a concurrent increase in state enforcement activity) sends a strong message: in today's digital economy, the privacy and security of personal information must be assured. This new focus on personal data as a company asset to be carefully safeguarded requires focus at the highest levels of management. Given the ubiquity of customer and employee personal information, and the FTC's broad jurisdiction to enforce against companies that fail to take serious steps to protect the data entrusted to them, the message to secure data is one every U.S. company should heed.