wiley

ARTICLE

The Importance of Watching Your Employee Data

Intellectual Property & Technology Law Journal
September 2011

Two recent Federal Trade Commission (FTC) cases serve as an important reminder to everyone in corporate America-while much of the attention on privacy and security (deservedly) goes to customer data, it is critical also to pay close attention to protecting your employee information. The FTC enforcement actions provide some specific points of guidance:

- Most companies maintain very sensitive information about their employees;
- Most companies also give this sensitive information to service providers, often to many service providers;
- Security breaches-including risky breaches involving Social Security numbers-are quite likely with employee data; and
- Many companies do not do a good job of identifying reasonable business needs for maintaining sensitive employee information.

Accordingly, any company with employees needs to take specific steps to ensure that sensitive employee information is protected, and that these protections extend to the wide range of service providers used by the company. Companies also should have a security breach plan for situations involving employee data.

Background to the FTC's Actions

The two most recent FTC settlements-announced the same day-follow a path similar to that blazed by the FTC in its first groundbreaking security case, related to the BJ's Wholesale company. In the *BJ's*

Practice Areas

Privacy, Cyber & Data Governance

Wholesale case (announced June 16, 2005), the FTC took enforcement action despite the fact that BJ's Wholesale apparently made no representations whatsoever to its customers concerning security protections. Instead, the FTC alleged that BJ's Wholesale's information security practices, taken together, did not provide "reasonable security for sensitive customer information." Specifically, the FTC alleged that BJ's Wholesale violated the FTC Act because it:

- Failed to encrypt consumer information when it was transmitted or stored on computers in BJ's Wholesale stores;
- Created unnecessary risks to the information by storing it for up to 30 days, in violation of bank security rules, even when it no longer needed the information;
- Stored the information in files that could be accessed using commonly known default user IDs and passwords;
- Failed to use readily available security measures to prevent unauthorized wireless connections to its networks; and
- Failed to use measures sufficient to detect unauthorized access to the networks and to conduct security investigations.

While the *BJ's Wholesale* case did not involve employee data, it created the broadest security mandate possible-any company that maintains information about either customers or employees needs to have reasonable and appropriate protections for that information, regardless of industry, specific regulations or specific commitments made by the company.

New FTC Enforcement

The FTC's recent actions serve as a reminder about the need for effective and appropriate overall security practices, whether for employers that own and control employee data, or for the wide range of service providers across the country and the globe. According to the FTC's May 3 press release on the cases, both actions "are part of the FTC's ongoing efforts to ensure that companies secure the sensitive consumer information they maintain." The cases were brought against companies that "claimed they would take reasonable measures to secure the consumer data they maintained, including Social Security numbers, but failed to do so. These flaws were exposed when security breaches at both companies put the personal information of thousands of consumers at risk." The FTC's enforcement actions "challenged the companies' security practices as unfair and deceptive."

While these two cases, therefore, were driven by the idea of "unfair and deceptive" statements about security practices, the FTC has also made clear (starting with the *BJ's Wholesale* case) that such misstatements are not a requirement for FTC activity-there is a general need, independent of any regulation or any specific company representations, to maintain reasonable and appropriate security practices.

The *Ceridian* Case

While the two cases are similar, one stands out because of the prominence of the company involved, Ceridian, a payroll servicing company based in Minneapolis. According to the FTC's complaint and the related press release, Ceridian had claimed "that it maintained 'Worry-free Safety and Reliability . . . Our comprehensive security program is designed in accordance with ISO 27000 series standards, industry best practices and federal, state and local regulatory requirements.'" In fact, according to the FTC complaint, the FTC viewed Ceridian's security practices as "inadequate." Specifically, the company:

- Did not adequately protect its network from reasonably foreseeable attacks;
- Stored personal information in clear, readable text indefinitely on its network without a business need;
- Did not adequately assess the vulnerability of its web applications and network to commonly known or reasonably foreseeable attacks, such as "Structured Query Language" (SQL) injection attacks;
- Did not implement readily available, free or low-cost defenses to such attacks; and
- Failed to employ reasonable measures to detect and prevent unauthorized access to personal information.

As a result of these security weaknesses (according to the FTC allegations), an intruder was able to access the payroll processing application and compromise certain personal information-including Social Security numbers-for more than 28,000 employees of Ceridian's small-business customers.

The *Lookout Services* Case

The *Lookout Services* complaint relied on similar (although less egregious) statements about security practices, followed by an FTC conclusion (in the wake of a specific breach incident) that Lookout's practices were inadequate. The relevant Lookout Services product (the I-9 Solution) focused on offering employers a means to meet certain federal immigration law requirements. The product allowed employers to store information such as names, addresses, dates of birth and Social Security numbers in an "I-9 database." Lookout's representations about its security were less dramatic than Ceridian's-Lookout claimed that its security practices "kept data reasonably secure from unauthorized access," but, according to the FTC, this system "did not in fact provide adequate security." Specifically, Lookout Services:

- Failed to implement reasonable policies and procedures for the security of sensitive consumer information it collected and maintained;
- Failed to establish or enforce rules sufficient to make user credentials (*i.e.*, user ID and password) hard to guess;
- Failed to require periodic changes of user credentials, such as every 90 days, for customers and employees with access to sensitive personal information;
- Failed to suspend user credentials after a certain number of unsuccessful login attempts;

- Did not adequately assess and address the vulnerability of its web application to widely known security flaws, such as "predictable resource location";
- Allowed users to bypass the authentication procedures on Lookout's website when they typed in a specific URL;
- Failed to employ sufficient measures to detect and prevent unauthorized access to computer networks, such as by employing an intrusion detection system and monitoring system logs;
- Created an unnecessary risk to personal information by storing passwords used to access the I-9 database in clear text; and
- Failed to provide adequate employee training.

As a result of these overall security weaknesses, an employee of one of Lookout's customers (it is unclear if this was an inappropriate user of the system or just an individual who demonstrated the security weaknesses) was able to access sensitive information, including Social Security numbers, for approximately 37,000 Lookout consumers.

The Consequences

The FTC settlement agreements revolving around these matters embody now-familiar terms. While the FTC typically does not have authority in security cases to issue specific fines, it does implement remedial programs with detailed and long-term behavioral consequences. First, in both cases, the FTC resolution prohibits misrepresentations about privacy or security practices. Then, it imposes specific security program obligations. Most of these practices track a "typical" security program that is mandated (explicitly) for those subject to the Gramm-Leach-Bliley Act and implicitly for all companies through the FTC's enforcement policies reflected in prior settlements. These programs (imposed on both Ceridian and Lookout) require the companies to establish and maintain a comprehensive information security program that is reasonably designed to protect the security, confidentiality and integrity of such information (whether in paper or electronic format) about consumers, employees and those seeking to become employees. The security program must contain administrative, technical and physical safeguards appropriate to the company's size and complexity, the nature and scope of its activities, and the sensitivity of the information collected from or about consumers and employees.

The programs also require the companies to:

- Designate an employee or employees to coordinate and be accountable for the information security program;
- Identify material internal and external risks to the security, confidentiality and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks;
- Design and implement reasonable safeguards to control the risks identified through risk assessment and regularly test or monitor the effectiveness of the safeguards' key controls, systems and procedures;

- Develop and use reasonable steps to select and retain service providers capable of appropriately safeguarding personal information they receive from the company, and require service providers by contract to implement and maintain appropriate safeguards; and
- Evaluate and adjust their information security programs in light of the results of testing and monitoring, any material changes to operations or business arrangements, or any other circumstances that they know or have reason to know may have a material impact on their information security program.

The most burdensome component of these settlements (again, one that is typical of FTC settlements) requires each company to obtain an assessment and report from a qualified, objective, independent third-party professional, certifying, among other things, that: (1) it has in place a security program that provides protections that meet or exceed the protections required by the agreement; and (2) its security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality and integrity of sensitive consumer, employee and job applicant information has been protected. **This assessment must be obtained within 180 days of the final resolution of the investigation and then "on a biennial basis thereafter for a period of twenty (20) years"** (emphasis added).

The agreement also includes specific additional reporting, document retention, communication and compliance provisions.

Specific Hints from These Agreements

These two FTC cases are nothing unique; in fact, they represent part of a continuing and growing trend in FTC enforcement actions related to failures to provide overall effective security. In addition, the sanctions imposed by the FTC represent what is now "typical" in resolutions of these situations. Nonetheless, there are particular points that companies should pay specific attention to as a result of these cases:

- Make sure you have evaluated each of the security weaknesses identified in these FTC cases (and all other FTC enforcement actions). This is a list of specific weaknesses that the FTC is aware of and watching.
- While both cases addressed representations made about security practices (and companies should evaluate such statements carefully), the particular misrepresentations are not crucial to the FTC's enforcement activities-they simply give the FTC a more direct approach for its enforcement actions.
- Make sure you know everywhere in your company where you collect, store and disclose Social Security numbers (and other highly sensitive employee information). Most companies-when they review these practices-find many situations where there is no ongoing business need for the Social Security numbers.
- Make sure you have evaluated whether there is a need to keep all of this information, whether it can be protected in additional ways if it must be kept, and whether particularly sensitive information (such as Social Security numbers) can be redacted or otherwise separated from the remainder of the information.
- Make sure that you evaluate carefully whether specific service providers need this sensitive information-you should never send a Social Security number to a vendor unless you have a specific demonstrable

need to do so.

- Make sure you have developed an approach to how you will evaluate the security practices of your vendors. This approach is a requirement of an effective information security program and must involve not only contractual protections but also appropriate oversight of such vendors.
- Make sure you have a security breach plan that addresses employee information. Many of the considerations in employee data cases are different from customer cases. It is critical to review these differences and generate an overall approach to dealing with breaches involving employee data.