PERSONAL DATA SECURITY IN THE WAKE OF CHOICEPOINT

A recent wave of high-profile data security breaches involving unauthorized access to personal data highlights the increasing problem of identity theft and other information-related crimes. These personal data security breaches and proposed state and federal legislation triggered by such security failures mean that companies' data security practices will be subject to increased scrutiny. Failing to take appropriate measures to prevent a data security breach might result in potential enforcement action from federal and state governmental authorities (and possibly also from foreign authorities), private lawsuits, and negative publicity.

Companies, particularly those entities that have become complacent about adhering to data security requirements, should reevaluate their data security practices for any inadequacies in light of applicable data protection laws and the representations made in their privacy policies. For example, do the statements in your company's privacy policy relating to securing personal data accurately reflect your company's actual practice of securing such data? The Federal Trade Commission ("FTC") has brought actions against companies for deceptive security claims.

This memo discusses recent cases involving the breach of data security; it also informs companies of certain governmental enforcement actions, relevant legislation and federal agency guidance involving data security issues, and describes certain actions that companies should take when reevaluating their data security practices. Finally, this memo discusses briefly data security issues in the context of global outsourcing.

I. Recent Breach of Data Security Cases

The most notable case in the recent string of breach of data security cases involves ChoicePoint, one of the largest consumer data warehousers in the U.S. ChoicePoint allowed criminals posing as legitimate businesses access to the personal data of approximately 145,000 individuals. ChoicePoint notified consumers whose personal data was stolen that such data might have been compromised as a result of the security breach. The notification was prompted in large part by a California law requiring such disclosure (discussed in more detail below). Other recent cases include Lexis Nexis (a compiler of legal and other information), which initially admitted that hackers had gained access to the personal data of 32,000 individuals, but then revised that number to approximately 310,000 affected individuals, and DSW (a nationwide shoe retailer), which informed the public that credit card information had been stolen from more than 100 of its stores. Furthermore, data security breaches have occurred abroad. Japan's Mizuho Bank, for example, recently acknowledged losing the personal data of 270,000 customers.

In addition to companies, universities have had significant data security problems due to "hacker" incidents or lost laptops. Boston College, for example, recently warned over 100,000 alumni that their identities could be compromised as a result of a data security

breach. At the University of California, Berkeley, a thief stole a computer laptop that reportedly contained the personal data of approximately 100,000 students, former students and applicants. Hackers also gained access to a computer system of the University of California, San Diego, compromising the personal data of 380,000 individuals.

II. State and Federal Reaction

A. Enforcement Actions and Authority

In a recent 8-K filing with the Securities and Exchange Commission ("SEC"), ChoicePoint states that "the SEC is conducting an informal inquiry into the circumstances surrounding any possible recent identity theft, recent trading in ChoicePoint stock by [certain ChoicePoint officers] and related matters." In the same filing, ChoicePoint further states that the FTC "is conducting an inquiry into [ChoicePoint's] compliance with federal laws governing consumer information security and related issues." In addition, it has been reported that the ChoicePoint incident is being investigated by a number of states, including North Carolina, Louisiana, Pennsylvania, California, Massachusetts, Connecticut and Texas.

Generally, federal agencies may bring enforcement actions under several federal laws that address the protection of personal data, including without limitation the Gramm-Leach-Bliley Act (protects personal data collected by financial institutions and nonaffiliated third parties); the Health Insurance Portability and Accountability Act (protects personal data collected by *covered entities*, such as health plans, healthcare clearinghouses and healthcare providers); the Children's Online Privacy Protection Act (protects personal data collected from children under the age of 13); and the Fair Credit Reporting Act (protects consumer privacy, enhances the accuracy of credit report information, and helps prevent identity theft).

Additionally, the basic consumer protection law enforced by the FTC under its general enforcement authority is Section 5(a) of the Federal Trade Commission Act, which prohibits unfair and deceptive practices affecting commerce, including misrepresentations in a privacy policy regarding the use and disclosure of personal data. Under its general enforcement authority, the FTC may investigate and, if necessary, file civil law enforcement actions against businesses that have allegedly engaged in fraudulent or misleading privacy practices. As stated above, the FTC has brought several enforcement actions against companies for misrepresenting the security provided to consumers' personal data. In addition, the FTC brought an enforcement action against two companies in November 2004 for violating the FTC's "safeguards rule" under the Gramm-Leach-Bliley Act.

From an international perspective, U.S. companies could also face enforcement action from foreign governmental authorities in the event there is a data security breach that involves the personal data of foreign customers.

B. Proposed Laws, Congressional Hearings and Federal Guidance

What prompted ChoicePoint and perhaps others to disclose the fact that there was a breach in data security is a California law (S.B. 1386) that requires companies to provide notification to consumers when there is a data security breach involving their personal data. Other states, including Georgia, Florida, North Dakota, Texas, Washington, Minnesota, Illinois, Rhode Island, Colorado, North Carolina and Connecticut, have introduced or are expected to introduce legislation similar to the California law.

Senator Dianne Feinstein has called for additional federal protection against identity theft, and has introduced legislation setting federal standards for consumer notification of data security breaches (S. 115). In addition, there are bills pending in the House and Senate, H.R. 1080 and S. 500, respectively, that would give the FTC additional authority to oversee entities that collect and sell personal data.

In March 2005, the Office of Thrift Supervision, the Comptroller of the Currency, the Federal Reserve System and the Federal Deposit Insurance Corporation jointly issued "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice."[1] This final guidance interprets these agencies' customer information security standards under the Gramm-Leach-Bliley Act and states that financial institutions should implement a response program addressing data security breaches involving customer information. The guidance document describes the appropriate elements of a response program, including customer notification procedures. Additionally, under the final guidance, an institution should notify its primary federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of certain "sensitive customer information."

In addition, the FTC similarly has published a guidance document on how to comply with the "safeguards rule" of the Gramm-Leach-Bliley Act, which includes a discussion on managing system failures for financial institutions subject to FTC jurisdiction.[2] For example, this document suggests that customers should be notified promptly if their personal data is subject to loss, damage or unauthorized access. The FTC also offers a separate guidance document on information compromise and the risk of identity theft.[3] This second document provides guidance on when it would be appropriate to notify law enforcement, affected businesses and consumers in the event of a security breach.

---

1 *See* http://www.federalreserve.gov/BoardDocs/Press/bcreg/2005/20050323/attachment.pdf.

2 *See* http://www.ftc.gov/bcp/conline/pubs/buspubs/safeguards.htm.

3 *See* http://www.ftc.gov/bcp/conline/pubs/buspubs/idtrespond.htm.

III. Data Security Practices

A company that collects personal data should reevaluate its data security practices and ensure that:

(1) one or more employees have been designated to coordinate such practices;

(2) procedures are in place to regularly monitor and test such practices;

(3) firewall, encryption and other data security software is in place and up to date;

(4) customers are properly verified before they are allowed access to their personal data;

(5) third parties receiving personal data are verified as legitimate businesses;

(6) the company's privacy policy is up to date and accurately reflects its data security practices (e.g., personal data is in fact safeguarded in accordance with the representations made in the privacy policy);

(7) for employees who have access to personal data, there are employee background checks, employees sign nondisclosure agreements and employees are properly and adequately trained regarding data security measures;

(8) unusual employee access (and timing) to personal data is monitored;

(9) clear and effective security management procedures are in place to address issues raised by an actual breach in data security;

(10) paper shredders or similar devices are used to properly dispose of offline data;

(11) hard drives and backup devices are properly wiped or destroyed before being discarded;

(12) access to data servers and other storage devices is restricted, and physical measures are used to protect such devices;

(13) large-scale downloads and transfers of personal data are monitored and restricted; and

(14) reasonable steps are taken to select and retain service providers that are capable of maintaining appropriate safeguards for personal data, and such service providers should be required by contract to implement and maintain such safeguards, among other measures (e.g., requiring such service providers to notify the company in the event there is a breach of data security).[4]

---

[4] Existing contracts with service providers should also be amended to provide for the security of personal data.

The security measures discussed herein should be adopted and implemented in harmony with data protection laws applicable to a company's business practices. Data security procedures should be flexible enough to keep pace with evolving data protection laws, as well as sophisticated cyber threats, and companies should continue to monitor such laws in light of their business practices. It is important to note that, although computer hackers cause data security breaches by circumventing firewalls and stealing personal data, there are other situations that involve stolen laptops or similar portable devices that store personal data. Thus, companies should simply avoid storing personal data on such devices if it is not necessary to do so. In addition, companies should reduce the amount of personal data on their systems by removing, and no longer collecting, data that they do not actually need (in accordance with applicable laws).

IV. Global Outsourcing and Data Security

In the FTC's view, a company subject to privacy obligations under U.S. laws may not avoid such obligations by outsourcing its data processing activities to offshore service providers. Specifically, the FTC stated that "[a] company that is subject to U.S. laws is responsible for the use and maintenance of consumer information in accordance with those laws. Simply because a company chooses to outsource some of its data processing to a domestic or offshore service provider does not allow that company to escape liability for any failure to safeguard the information adequately." In those cases, the FTC "would look to whether the company that outsourced the data processing employed sufficient measures reasonable and appropriate under the circumstances to maintain and protect the privacy and confidentiality of personal information."

Thus, it is imperative that companies engaging in global outsourcing arrangements understand the significant legal implications that arise when personal data is involved in such arrangements. Of particular concern is that many countries to which personal data is outsourced do not have data protection laws. Before entering into an outsourcing relationship with a foreign service provider, a company should take appropriate due diligence measures with respect to the service provider (*e.g.*, ensure that the provider has procedures in place to accommodate certain standards imposed by the company). The foreign service provider should be obligated by contract to take appropriate measures to safeguard the personal data that is collected, used or disclosed on behalf of the company, in accordance with the company's data protection standards. Companies should be particularly wary of "confidential" contract form language in these arrangements.

* * * * * * * * * * * * * * *

If you have any questions concerning this memorandum, please contact Timothy McTaggart at 202-303-1121 or Demetrios Eleftheriou at 202-303-1134, both in our Washington, DC office, or the attorney with whom you regularly work.

Willkie Farr & Gallagher LLP is headquartered at 787 Seventh Avenue, New York, NY 10019-6099. Our telephone number is 212-728-8000, and our facsimile number is 212-728-8111. Our website is located at www.willkie.com.

April 13, 2005