Asia-Pacific
Economic Cooperation

2006/SOM1/ECSG/SYM/012
Agenda Item: 9

A Business Guide: Meeting Your Legal and Business Obligations to Safeguard Personal Information

Purpose: Information
Submitted by: Hunton & Williams LLP

APEC Symposium on Information Privacy Protection in E-Government and E-Commerce
Ha Noi, Viet Nam
20-22 February 2006

THE CENTER
FOR INFORMATION
POLICY LEADERSHIP
HUNTON & WILLIAMS LLP

A Business Guide:
Meeting Your Legal and Business Obligations to Safeguard Personal Information

by
Ellen Finn

February 2006

The Center for Information Policy Leadership develops initiatives that encourage responsible information governance in today's digital society. The Center is a member-driven organization that operates within the Privacy and Information Management practice at Hunton & Williams LLP. Through collaboration with industry leaders, consumer organizations and government representatives, the Center provides leadership in developing policy to help ensure privacy and information security while balancing economic and societal interests. Visit us at www.informationpolicycenter.com.

Introduction

Identity fraud and financial account fraud are not new and many of the tried and true methods for committing these crimes are decidedly low-tech; dumpster-diving and stealing mail have long been the primary methods by which criminals gain access to individual's sensitive personal information. But the methods used by criminals to gain access to the personal information that makes these crimes possible are changing with our times. Increasingly, criminals are turning to more technologically sophisticated methods of gathering and exploiting personal information along with their traditional tricks of the trade.

Willie Sutton is frequently quoted as saying that he robbed banks, "because that's where the money is."[1] Today, criminals are discovering that personal data can be as good as money and they are increasingly targeting businesses to get it. Why? Because that's where the data is collected. Criminals are also increasingly using technology to gather and use personal information. For example, law enforcement officials have begun to see local drug dealers, who used to rely on street addicts to supply them with credit cards, checks, or account statements stolen from mailboxes and dumpsters, now engaging in complex joint ventures with organized crime rings around the world by using the Internet to communicate, buy and sell personal data, and transfer money.[2] In addition, "phishing" schemes that use deceptive email messages to trick individuals into disclosing credit card numbers, Social Security numbers, passwords, and other information, are an increasingly common way of obtaining information for fraudulent purposes.[3]

Businesses that collect, use, and store individuals' personal information need to be aware of these threats — both old and new — and take steps to protect the security of individuals' information. First and foremost, it is the right thing to do as a matter of human decency and respect, as well as being a good business practice. But, in addition, and, perhaps surprisingly given the variety of laws have been proposed recently to address information security

---

1 Ironically, it appears that Sutton did not utter this famous line, although he later appropriated it for the title of his autobiography, "Where the Money Was: The Memoirs of a Bank Robber." See reporter Steve Cocheo's March 1997 article, "The bank robber, THE QUOTE, and the final irony," in the ABA's Banking Journal, available at http://www.banking.com/aba/profile_0397.htm.

2 See, for example, USA Today articles, "Meth addicts use Internet to cash in on identity theft" and "Meth addicts' other habit: Online theft" both by Byron Acohido and Jon Swartz, published on December 24, 2005; and the Seattle Post-Intelligencer article "Many meth users turn to identity theft" by Greg Risling, published on December 28, 2005.

3 "Phishing" messages typically purport to be from legitimate businesses with which large numbers of consumers may have accounts. They generally tell the consumer that there is some kind of problem with their account and provide a link to a website where the consumer is requested to sign in and provide various personal details. These websites look legitimate, but they are set up by criminals to gather user names, passwords, and other information that is then used to defraud consumers. Statistics on the increasing number of unique phishing attacks are available from the Anti-Phishing Working Group at http://www.antiphishing.org/index.html.

and identity theft,[4] the safeguarding of personal information is already required by law of companies doing business in the United States.

Legal Requirements to Protect Personal Information

Legal requirements to protect individuals' personal information have existed for some years now for companies in particular industries. Financial institutions[5] have been subject to the Gramm-Leach-Bliley Act[6] and its implementing regulations, which require them to protect the privacy and security of their customers' nonpublic personal information.[7] In particular, financial institutions must implement a comprehensive information security program that includes administrative, technical, and physical safeguards designed to:

- ensure the security and confidentiality of customer information;
- protect against any anticipated threats or hazards to the security or integrity of the information; and
- protect against unauthorized access to or use of the information that could result in substantial harm or inconvenience to the customer.

The security program must contain safeguards that are appropriate to the institution's size and complexity, the nature and scope of the institution's activities, and the sensitivity of the customer information at issue.[8]

Similarly, companies in the health care industry have had to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA")[9] and its implementing Security

---

4 Proposed identity theft legislation includes the Identity Theft Protection Act, S. 1408 (Smith); Comprehensive Identity Theft Prevention Act, S. 768 (Schumer); and the Personal Data Privacy and Security Act of 2005, S. 1789 (Specter). Proposals to limit the use and display of Social Security numbers include the Social Security Number Protection Act, HR. 1078 (Markey); and the Social Security Number Privacy and Identity Theft Prevention Act, HR. 1745 (Shaw). Proposals targeted at the regulation of data brokers include the Consumer Data Security and Notification Act, HR. 3140 (Bean); and the Information Protection and Security Act, S. 500 (Nelson).

5 The term "financial institution" is extremely broadly defined, and includes companies that are "significantly engaged" in any of a variety of specified "financial activities" such as transferring money, extending credit, or providing certain financial data processing and transmission services. 16 C.F.R. § 313.3(k)(1) (2005).

6 15 U.S.C. §§ 6801-6827 (2004).

7 "Nonpublic personal information" is defined as personally identifiable information (i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise obtained by the financial institution in connection with its provision of a financial product or service. It does not include most publicly available information. 15 U.S.C. § 6809 (2005).

8 16 C.F.R. § 314.3(a) (2005).

9 Pub. L. No. 104-191, 110 Stat. 1936 (1996).

Rule.[10] Covered entities[11] are required to ensure the confidentiality, integrity, and availability of all electronic protected health information that they create, receive, maintain, or transmit. Pursuant to the Security Rule, each covered entity must:

- conduct a risk assessment of potential threats to the confidentiality of protected health information and implement a risk management program to reduce the identified risks to a reasonable and appropriate level;
- have in place specified administrative, physical, and technical safeguards to protect information and adopt written policies and procedures regarding how these safeguards will be implemented; and
- enter into "business associate agreements" with unrelated persons or entities that contractually obligate them to abide by the legal standards in the Security Rule.

In addition, companies with privacy policies — which have generally been online companies or the online operations of offline companies — have faced liability for deceptive trade practices under Section 5 of the Federal Trade Commission Act[12] when statements in their privacy policies, including statements about the confidentiality and security of consumers' personal information, were false or misleading. Since 2002, the Federal Trade Commission has brought five cases against companies for deceptive security claims.[13] State Attorneys General have also enforced their mini-FTC acts in privacy and security cases where companies did not live up to their promises.[14]

But, until this past year, the vast majority of companies — those outside the financial services and health care industries and without published privacy policies — believed that they were not subject to a legal requirement that they safeguard individuals' personal information. Then, in June 2005, the FTC announced a settlement agreement with BJ's Wholesale Club resolving charges that BJ's failure to implement appropriate security measures to protect

---

10 45 C.F.R. §§ 160, 162, 164 (2004).

11 The Health Insurance Portability and Accountability Act applies to health plans, health care clearinghouses or health care providers that transmit health information in electronic form in connection with certain specified transactions.

12 15 U.S.C. § 45(a) (2005).

13 The five FTC cases are: Petco Animal Supplies, Inc. (Docket No. C-4133); MTS Inc., doing business as Tower Records, Tower Books, or Tower Video (Docket No. C-4110; Guess?, Inc. (Docket No. C-4091); Microsoft Corp. (Docket No. C-4069); and Eli Lilly (Docket No. C-4047). Complaints, consent agreements, and additional related information are available at http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html.

14 Companies signing settlement agreements with individual states regarding information compromises have included the ACLU (http://www.oag.state.ny.us/press/2003/jan/ jan14a_03.html); Barnes and Noble (http://www.oag.state.ny.us/press/2004/apr/ apr29a_04.html); Eli Lilly (http://caag.state.ca.us/newsalerts/2002/02-084.htm and http://www.epic.org/privacy/medical/lillyagreement.pdf); Victoria's Secret (http://www.oag. state.ny.us/press/2003/oct/oct21b_03.html); and Ziff Davis Media (http://www.oag. state.ny.us/press/2002/aug/aug28a_02.html).

the sensitive information of thousands of its customers was an unfair practice that violated federal law.[15]

Specifically, the FTC charged that BJ's failed to encrypt consumer information when it was transmitted or stored on computers in BJ's stores; created unnecessary risks to the information by storing it for up to thirty 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 or to conduct security investigations. Millions of dollars worth of fraudulent purchases were made using counterfeit copies of credit and debit cards used at BJ's stores, causing banks to cancel and re-issue thousands of credit and debit cards and causing consumers inconvenience, worry, and time loss dealing with the affected cards. The FTC alleged that BJ's failure to secure customers' sensitive information was an unfair practice because it caused substantial injury that was not reasonably avoidable by consumers and not outweighed by offsetting benefits to consumers or competition. The settlement required BJ's to establish and maintain a comprehensive information security program that includes administrative, technical, and physical safeguards and requires BJ's to obtain audits from a qualified, independent, third-party professional every two years for the next twenty years, certifying that BJ's security program meets the standards of the order.

The BJ's case was not a fluke. On December 1, 2005, the FTC announced that DSW Inc., an Ohio-based footwear retailer, had agreed to a nearly identical settlement of similar FTC allegations that it engaged in "unfair" business practices by failing to properly secure customer data.[16] The FTC's requirements in these cases, as well as the earlier deception cases based on security promises to consumers, closely resemble the requirements imposed on financial institutions by the Commission's Safeguards Rule. The result is, in essence, a de facto requirement that any business that collects, uses, or maintains consumers' sensitive personal information implement a safeguards program.

The practical significance of the FTC's enforcement actions would not be nearly as great, however, in the absence of the security breach notification laws enacted first by California and now by 22 other states.[17] In the absence of these breach notification laws, companies that suffered an information compromise could generally keep the incident quiet and, as a result, were unlikely to face an investigation from the FTC or State Attorneys General. Consumers were generally not notified of breaches and therefore companies were unlikely to face class action lawsuits. In the absence of consumer notice, security incidents rarely hit

[15] Case materials for BJ's Wholesale Club, Inc. (FTC Docket No. C-4148) are available at http://www.ftc.gov/os/caselist/0423160/0423160.htm.

[16] See http://www.ftc.gov/os/caselist/0523096/0523096.htm.

[17] The states and related laws include: Arkansas (SB 1167); California (SB 1386); Connecticut (SB 650); Delaware (HB 116); Florida (HB 481); Georgia (SB 230); Illinois (HB 1633); Indiana (SB 503); Louisiana (SB 205); Maine (LD 1671); Minnesota (HF 2121); Montana (HB 732); Nevada (SB 347); New Jersey (AB 4001); New York (AB 4254); North Carolina (SB 1048); North Dakota (SB 2251); Ohio (HB 104); Pennsylvania (SB 712); Rhode Island (HB 6191); Tennessee (HB 2170); Texas (SB 122); and Washington (SB 6043).

the press, so there was little damage inflicted to a company's reputation or stock price.[18] By contrast, consumer notification laws now all but guarantee private class action lawsuits, bad publicity that damages company brands and reputation, FTC and State Attorney General investigations, and a drop in stock price. In severe cases, the breach may raise questions under Sarbanes-Oxley with respect to a company's internal controls. Because notification laws create such significant costs for companies that suffer a data breach, they provide a powerful incentive to safeguard data in the first instance.

So what exactly is it that you are required to do?

Safeguards

Every business should develop a written information security plan that describes its program to protect individuals' personal information. The plan should be appropriate to the size and complexity of the organization, the nature and scope of its activities, and the sensitivity of the information it handles. While there are a handful of basic elements listed below that every safeguards plan should address, businesses have the flexibility to implement policies, procedures, and technologies that are appropriate to their unique circumstances.

1. Designate one or more employees to coordinate your safeguards program.

Whether you decide to task a single employee with coordinating safeguards or you spread the responsibility among a team of employees, someone in your organization needs to be accountable for information security. In deciding who it should be, you should recognize that information security is fundamentally a management issue, not a technology issue. While information technology can play a significant role in protecting data, effective information security requires a broader focus and should include physical security, employee training and management, and business processes. Even with respect to information technology, the focus should be on managing your technology, not the technology itself. Buying a firewall, for example, does little to improve your security unless you configure and monitor it properly.

In addition, your safeguards program will almost certainly require the coordination of legal, human resources, information technology, audit, and business functions. The person or team that you choose to coordinate your program should have the ability to communicate and work effectively with all of these different groups.

2. Identify and assess the risks to individuals' personal information in each relevant area of your company's operations, and evaluate the effectiveness of your current safeguards for controlling these risks.

To conduct a risk assessment, you will need to understand what you are protecting and what you are protecting it from. In particular, in this context, you should focus on protecting individuals' personal information in addition to your company's business information and operations. To begin, therefore, you should identify what personal information you are actu-

[18] The exceptions generally are cases where a "security researcher" publicized an incident claiming that going to the press was an attempt to fix the problem after efforts to contact the company directly had failed.

ally collecting, how your company uses it, where it is stored, to whom it is disclosed, who has access to it for what purposes, and how it will ultimately be disposed. You should map these data flows and classify data by sensitivity so you can prioritize your security measures.

Next, you need to think about all the ways that this personal information could be compromised. While you obviously need to consider intrusions by computer hackers, you should also think about ways that employees, service providers, business partners, or vendors could compromise the security of your personal information either intentionally or through carelessness. You should think about risks beyond those associated with information technology and consider business processes as well. It is a good idea to have the risk assessment process conducted by a team that includes both technical and business personnel because their perspectives on the likelihood and impact of threats may differ.

Once you have identified the risks you face, you will need to conduct a gap analysis to see where your current safeguards are inadequate. Where current safeguards are inadequate to address the risks you have identified, you will need to analyze your options. You should consider the likelihood a given risk will occur and the severity of the consequences if it does. You should also consider the effectiveness of the various available security measures and their cost relative to the harm caused by a compromise.

When thinking about the costs of a compromise you should consider the full range of potential costs you could face: the cost of investigating a security breach; mitigating and remediating damage to your systems and securing the systems after the breach; lost sales or productivity caused by the unavailability of systems or data; notifying affected individuals and government agencies, as appropriate; responding to regulator inquiries and enforcement actions; legal fees and costs for the defense of private lawsuits; lost customers; reputational damage; and a possible drop in stock price. The harm caused by a compromise, however, should be defined more broadly than just the resulting financial costs. Traditional risk assessment has systematically undervalued the protection of individuals' personal information because it has focused on the costs of compromise to the company rather than including costs to individuals. Moreover, it has focused only on financial costs rather than including less quantifiable harms such as anxiety, intrusion, individual reputation, and privacy. Despite the difficulty in quantifying these broader harms, they should be included in your analysis of the cost of available security measures relative to the harm caused by a compromise. Your calculation of the cost of a particular security measure should include not only the cost of any technology, but also the human resources and training needed to configure and monitor the technology properly.

3. Design and implement a safeguards program, and regularly monitor and test it.

In designing your safeguards program, you should consider all areas of your operations. In particular, you should be sure to address employee management and training; information systems; and managing system failures, which includes prevention, detection and response to attacks, intrusions, or other system failures. Believe it or not, despite the scope of issues that your program should address, designing a safeguards program may actually be the easier part of this process; implementing the program is often the harder part.

Your goal is to be sure that your security policies and procedures are more than mere paper and that they are actually followed in the day-to-day operation of your business. You also

want to be sure that any technology you deploy is properly configured and maintained and that any reports or alerts it provides are regularly reviewed and investigated. How can you tell whether these things are happening? By monitoring and testing each of the elements of your program. Your testing should reveal whether your safeguards program is being followed consistently and whether it is operating effectively to manage the risks to personal information that it was designed to address.

4. Select appropriate service providers and contract with them to implement safeguards.

When service providers or other third parties have access to your data or information systems, you should take steps to determine whether they can be trusted not to compromise your information security and to ensure that they are contractually required to meet your safeguards standards. Although the FTC's Safeguards Rule explicitly addresses only service providers, you should consider whether contractual provisions regarding safeguards are warranted in other relationships, for example, with vendors, business partners, or customers whose activities may affect your information security.

Your due diligence on service providers and other third parties should include some or all of the following measures: reviewing an independent audit of the third party's operations; obtaining information about the third party from several references or other reliable sources; requiring that the third party be certified by a recognized trade association or similar authority; reviewing and evaluating the service provider's information security policies or procedures; or taking other appropriate measures to determine the competency and integrity of the party.

Your contracts with third parties should specifically address safeguards obligations; a general confidentiality provision is really not sufficient. You should also require third parties to notify you of significant security incidents (so you can determine whether you have any legal obligations to provide notice to individuals of a possible data compromise) and to cooperate in responding to security incidents and investigating data breaches. In addition, you may want to ask for the right to audit a third party's safeguards program for compliance with legal and contractual requirements.

5. Evaluate and adjust your safeguards program in light of relevant circumstances, including changes in your business arrangements or operations, or the results of testing and monitoring.

Security is an ongoing process, not a static condition. You will need to evaluate and adjust your safeguards program at regular intervals and make appropriate changes in light of the results of your testing and monitoring. In addition, you need to consider whether changes to your safeguards program are needed in connection with changes in technology, business practice, and personnel. You should also keep up to date on new or emerging threats to information security and changes in the legal and regulatory environment. If you have an institutionalized change management process, it should include a security and risk management component.

* * *

We live in a world of unprecedented dependence on information and technology. The networked nature of our information systems means that we also live in a world of unprecedented dependence on the actions of others to ensure our own security. Safeguarding individuals' personal information is an important part of our collective responsibility to secure and sustain the viability of our information economy and our technological infrastructure. Compliance with legal requirements regarding the safeguarding of individuals' personal data should be understood within this broader context.

 Contact: Martin E. Abrams, Executive Director, The Center for Information Policy Leadership, 1900 K Street, NW, Washington, DC 20006-1109, (202) 955-1627, mabrams@hunton.com.