INFOSEC: What Is The Legal Standard Of Care?

Claire R. La Roche, (E-mail: claroche@longwood.edu), Longwood University
Mary A. Flanigan, (E-mail:mflaniga@longwood.edu), Longwood University
Glenn S. Dardick, (E-mail: gdardick@longwood.edu), Longwood University

ABSTRACT

The convenience of conducting personal business in the comfort of one's home attracts millions of individuals to shop, pay bills, and bank online. In the process, sensitive personal and financial information is disclosed and the exchange of this information creates a risk of identity theft. Providing effective cyber security is an issue with significant implications for companies. Failure to provide adequate security for consumer information may subject a company to legal action by the Federal Trade Commission (FTC). Information vulnerability, recent security failures and the standard of care are discussed.

INTRODUCTION

In today's business environment, transactions frequently involve the exchange of sensitive personal information and this information is most likely collected, processed, stored and disseminated through electronic means. For the most part, consumers are willing to provide this information based on assurances of security. However, while electronic information processing is convenient, efficient, and cost-effective, it has a down side: the information process may be subject to compromise through inadequate electronic safeguards, computer hackers, unauthorized requests for information, and by the negligence of employees.

This paper will first describe some of the common methods of information theft and provide examples of recent incidences involving the compromise of large data-bases. Second, the federal statutes covering organizations' responsibility for information security will be reviewed and recent Federal Trade Commission actions concerning violations of these laws will be summarized. Finally, the implications of these actions will be examined in an attempt to establish what may be the standard of care required of organizations maintaining the personal information of others.

METHODS OF BREACHING CYBER SECURITY

Information vulnerabilities do not reside only at the entity entrusted with the personal information. Vulnerabilities may also reside with the individuals to whom the information applies. Personal information may be compromised physically or electronically through social engineering and technical subterfuge. It may involve the active participation of the victim, the passive or unknowing participation of the victim or be totally out of the victim's control.

Social-engineering schemes called "phishing" use 'spoofed' e-mails to lead consumers to counterfeit websites. These website are designed to trick the victims into providing financial data such as credit card numbers, account usernames, passwords and social security numbers. The phishers generally hijack brand names and corporate logos of banks, e-retailers and credit card companies to convince recipients that the information requests are legitimate. Those who cooperate provide their own information to the criminals. Individuals can protect themselves from this type of violation by always checking with the organization about the legitimacy of information requests.

A second, more insidious method of data theft is referred to as technical subterfuge. In these cases information is retrieved from the victim's computer or result from his electronic activities without his knowledge.

These schemes may plant crimeware onto PCs to steal information directly. Personal information may be backed up on media that is vulnerable to theft; it may reside on computers and be vulnerable through unauthorized access (hacking, viruses and spyware); it may be transferred between computers and be vulnerable through unauthorized electronic snooping or sniffing (programs that capture and analyze packets of data as it passes across a network) and hijacking (DNS exploits) or "pharming" (crimeware that misdirects users to fraudulent sites or proxy servers, typically through DNS hijacking or poisoning). It is more difficult to prevent these types of information theft. There are computer programs that will install firewalls on PCs and detect spyware. However, these programs are not foolproof.

Finally, information may be obtained from others who have stored personal information about their customers, clients, etc. In these cases the victim is completely innocent of any compliance in the problem and is powerless to prevent the theft. This paper will focus on these cases and examine the responsibility of the organizations to protect information.

RECENT SECURITY BREACHES

Consumers are often shocked when they fall victim to misappropriation of their personal information, commonly referred to as identity theft. They are particularly dismayed when the security of that information had been guaranteed by the company. Many consumers assume that when a company represents that it has a certain level of security, that sensitive personal information is absolutely protected from misappropriation. As seen recently, this assumption could not be further from the truth.

George Mason University in Virginia admitted that personal information on up to 30,000 students had been compromised by hackers (McCullagh, 2005). Unfortunately, they are not the only educational institution that has been hit by online intruders. Georgia Institute of Technology's arts and theatre program had the credit card numbers of 57,000 patrons stolen (Lemos, 2003, at press b), 55,000 social security numbers were taken from the University of Texas at Austin (Lemos, 2003, at press a), and the personal information of over 1 million California residents was compromised though two incidents – one at UCLA and the other at the University of California at Berkeley (Becker, 2004). The theft at Berkeley was accomplished by simply stealing a laptop that contained the information. San Jose Medical Group had to inform 185,000 current and former patients that both their financial and medical records may be at risk following the theft in an office break-in of two Dell computers (Kawamoto, 2005).

Citibank Financial, a unit of Citigroup put the financial records of 3.9 million customers in a box and shipped it via UPS. The box never arrived at its destination and now the company admits that the customers' identities are at risk. Bank of America is still looking for backup tapes with information on 1.2 million government employees that they simply lost in a shipment to a backup center. (Levy & Stone, 2005, p. 43)

Choice Point is an information broker that keeps or can electronically access 19 billion records on American consumers. Last year Choice Point inadvertently sold the secret information (including some social security numbers) of at least 145,000 consumers to a fake company run by criminals.

However, the "mother of all security breaches" happened at a company called CardSystems. A privately owned company, each year it processes an estimated $15 Billion in credit card transactions between the merchant and the bank. In direct violation of their agreement with MasterCard and Visa, they kept on file 40 million credit card numbers. Digital invaders sucked these out of the system (Levy & Stone, 2005, p.45).

When organizations collect and store information they have a corresponding duty of care to safeguard that information from unauthorized access or dissemination. Companies should face significant legal liability if they are found responsible for failing to protect personal information. What are the federal laws governing the protection of information and what, if any, is the standard of care required of organizations that store personal information?

FEDERAL INFORMATION SECURITY LAWS

Two Federal statutes govern the organization's duty for protection of information about customers. The first is the Federal Trade Commission Act (FTC Act) and the second is the Graham-Leach-Bliley Act (GLBA).

The Graham-Leach-Bliley Act was signed into law in 1999 and applies exclusively to financial institutions. The GBLA contains provisions that address both the privacy and safeguarding of consumer information. The Act clearly states "It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information." (GLBA) The Act requires that each agency covered under the law establish standards for financial institutions that pertain to administrative, technical and physical safeguards to:

- Insure the security and confidentiality of customer records and information;
- Protect against any anticipated threats or hazards to the security or integrity of such records; and
- Protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer." (GLBA)

The Safeguards Rule section of the GLBA, enumerates specific steps that all financial institutions must take to protect customers' personal information. To comply with the Safeguards Rule, a financial institution must do the following:

- Designate one or more employees to coordinate the safeguards;
- Identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling these risks;
- Design and implement a safeguards program and regularly monitor and test it;
- Select appropriate service providers and contract with them to implement safeguards; and
- Evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business arrangements or operations, or the results of testing and monitoring safeguards. (Financial Institutions and Customer Data, 2002)

Recent breaches in security and the misappropriation of consumer data have prompted Congress to consider additional security initiatives. Congress is now considering FTC recommendations that would extend the Safeguards Rule to all businesses, not just financial institutions. On June 16, 2005, Deboroah P. Majoras, Chairman of the FTC, encouraged Congress to require that businesses notify customers when the security of consumer information has been breached. Additionally, Majoras testified that:

The Commission recommends that Congress consider whether companies that hold sensitive consumer data, for whatever purpose, should be required to take reasonable measures to ensure its safety. Such a requirement would extend the FTC's existing GLBA Safeguards Rule to companies that are not financial institutions (Prepared Statement, 2005).

"Privacy is a central element of the FTC's consumer protection mission….Under the FTC Act, the Commission guards against unfairness and deception by enforcing companies' privacy promises about how they collect, use and secure consumers' personal information." (Privacy Initiatives) Under Section 5 of the Federal Trade Commission Act, the FTC has the power to enjoin and prohibit "unfair or deceptive acts or practices in or affecting commerce." (FTC Act, 15 U.S.C. Section 45(a)). The Commission has interpreted the failure of a company to provide information security as promised as an "unfair or deceptive act" and thus has employed this section of the Act to control information security in non-financial institutions. The FTC enforces compliance mainly through the use of consent orders. The major cases where the FTC has issued consent orders in this are discussed in the next section.

FTC CONSENT ORDERS

Significant steps have been taken by the FTC to enforce cyber security standards. In the past three years, companies have faced FTC charges for both misrepresenting the level of security and for failing to provide adequate security for personal and credit information. Consent orders have been reached settling several cases and establishing standards of care for website security and include the following *caveat:* "When the Commission issues a consent order on a final basis, it carries the force of law with respect to future actions. Each violation of such an order may result in a civil penalty of $11,000." (*Eli Lilly* Consent Order, 2002) Although there is a dearth of case law, the FTC has issued five final consent orders in connection with cyber security and protecting the integrity of personal information.

In *Eli Lilly*, the FTC was made aware of a breach of confidentiality by Eli Lilly, the manufacturer of Prozac. Eli Lilly inadvertently disclosed sensitive personal information collected about patients on their Prozac.com website. As a service to patients taking Prozac, Eli Lilly's website, Prozac.com, offered a *Medi-messenger* service. As a part of this service, consumers could sign up for e-mail reminders to take their medicine and/or refill their prescription. On June 27, 2001, a *Medi-message* e-mail revealing the e-mail addresses of all 669 recipients was inadvertently sent to recipients of this service The FTC was prompted to file a complaint against Eli Lilly based on the disclosure of the personal and confidential nature of the information revealed in this e-mail. Specifically, the FTC charged Eli Lilly with failure to adequately train and supervise "its employees regarding consumer privacy and information security…" (*Eli Lilly*, 2002) In addition, the FTC alleged that Lilly had breached its own security policies. In the settlement reached by the FTC and Lilly, a four-stage security policy was established that consisted of establishing an information security program and:

- Designating an appropriate person or persons to oversee their information security program.
- Identifying reasonably foreseeable risks to security and confidentiality of personal information.
- Conducting an annual review by qualified persons and adjusting the program in light of any findings and recommendations from reviews or ongoing monitoring, and in light of any material changes that affect the program.
- Revising the program in light of recommendations or material changes. (*Eli Lilly*, 2002)

In 2001, complaints were filed with the FTC against Microsoft alleging that Microsoft had made false and misleading statements about the information practices and the security of its *Passport*, *Passport Wallet* and *Kid's Passport* services. All three of these related services collected consumer information and allowed sign-in at participating websites with a single user name and password. Specifically, the *Passport* service collected information and allowed a single user name and password that was universally recognized at participating websites. In addition to simplified sign-in, the *Passport Wallet* collected credit card, billing, and shipping information. The purpose of Kid's Passport is to allow parents to regulate the collection of information on their children at sites recognizing this service. In the FTC Complaint, some of the false and misleading "Security and Privacy" statements made by Microsoft included the following:

".NET Passport achieves a high level of Web Security by using technologies and systems designed to prevent unauthorized access to your personal information."

"Use .NET Passport from any computer on the Internet. Your .NET Passport is protected by powerful online security technology and a strict privacy policy."

*"Your .NET Passport information is stored on secure .NET Passport servers that are protected in controlled facilities." (*Microsoft *Complaint, 2002, p.1-2)*

In a unanimous decision, the FTC concluded that Microsoft had made false statements about the safety and security of consumer information as well as false statements about the information collected through its Passport services. The Commission entered into a Consent Order that prohibited Microsoft from making false allegations about the security and privacy of consumer information. Part II of the Consent Order required Microsoft "to establish and maintain a comprehensive information security program in writing that is reasonably designed to protect the security,

confidentiality, and integrity of personal information collected from or about consumers." (*Microsoft*, 2002, p. 4) Specifically, Microsoft was ordered to:

- Designate an employee or employees to be accountable for their information security program.
- Identify and assess security and privacy risks.
- Design and implement safeguards and monitor the effectiveness of these programs.
- Periodically evaluate their security program and monitor changes that may materially affect their information security. (*Microsoft*, 2002)

The Microsoft Consent Order added an additional requirement that a report be filed biannually with the FTC assessing their privacy and security programs. This report is required to be created by a Certified Information System Security Profession (CISSP) or by an independent professional approved by the Associate Director for Enforcement, Bureau of Consumer Protection, at the FTC (*Microsoft*, 2002).

The third FTC Consent Order addressing the misrepresentation of information security involved Guess?, a company that had been selling clothes and accessories at its website www.guess.com. In the Complaint, The FTC maintained that Guess had made the following assurance regarding privacy and security: "This site has security measures in place to protect the loss, misuse and alteration of information under our control… All of your personal information, including your credit card information and sign-in password, are stored in an unreadable, encrypted format at all times." (*Guess?* Complaint, 2003, p.2) Unfortunately, consumer information was not always stored in a secure encrypted form and in 2002 the Guess website was subjected to a Structured Query Language (SQL) injection attack and the names and credit card numbers were misappropriated. In the settlement agreement the FTC required Guess to implement a comprehensive information security program much like the one required in the Microsoft case. Guess was also prohibited from misrepresenting its information security policy.

The fourth FTC Consent Order involved Tower Records, a company doing business online since 1996. In this case, Tower made representations to consumers that its website was secure and that it protected the confidentiality of consumer information. Their privacy policy claimed that "We use state-of-the-art technology to safeguard your personal information." and "You and only you have access to this information." (*MTS, Inc.* Complaint, 2004) In 2002 the software code for the Order Status application was re-written and Tower failed to include the "authentication code", a critical element that ensured that only the consumer was authorized to view the order. This security flaw resulted in customers with a valid order number viewing the personal information of other Tower customers. "In December 2002, personal information relating to approximately 5,220 customers was accessed by unauthorized users, and at least two Internet chat rooms contained postings about the vulnerability as well as comments about the vulnerability…" (*Tower* Complaint, 2004, p. 3) In the FTC Decision and Order, Tower was ordered to establish a comprehensive information security program similar to the ones established in the prior three cases. However, the FTC further ordered that Tower obtain an information security risk assessment report within six months and biannually thereafter. "Each Assessment shall be prepared by a person qualified as a Certified Information System Security Professional (CISSP) or holding Global Information Assurance Certification from the SysAdmin, Audit, Network, Security Institute, or by a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission." (*MTS, Inc.*, Order, 2004, p.4).

The fifth and most recent FTC Final Consent Order involved misleading privacy and security claims on the part of Petco, a national retailer of pet supplies. The Petco Complaint alleged that PETCO.com made the following misleading claims: "At PETCO.com our customers' data is strictly protected against any unauthorized access…entering your credit card number via our secure server is completely safe. The server encrypts all of your information; no one except you can access it." (*Petco* Complaint, 2005, p. 4) Petco's Web site was subjected to SQL injection attacks, a vulnerability that was well-known to information security experts and easily remedied by applying a patch. As a result of this security breach, customers' credit information was accessed. The situation was exacerbated by the fact that personal information on Petco's server was not stored in an encrypted form, a clear violation of its security guarantee. In the Final Consent Order, Petco was ordered to implement and monitor the same security program and bi-annual assessment required in the *MTS, Inc.* case.

CONCLUSION

When individuals make a purchase or transact business, personal information is most likely transferred and stored electronically. Consumers have the right to expect that personal information provided to others is maintained in a secure environment and businesses have a legal obligation to do so. Realistically, no computer or information system is infallible. For every system defense, someone will attempt, and possibly succeed, in developing an attack. It is the responsibility of the system's owner to continually update and maintain the highest standards of security available. The legal standard of care for information security for financial institutions was established by the GLBA. The standard of care for non-financial organizations has not been codified. However, the FTC has issued basic information security guidelines for any business collecting personal information:

- Identifying internal and external risks to the security, confidentiality and integrity of your customers' personal information;
- Designing and implementing safeguards to control the risks;
- Periodically monitoring and testing the safeguards to be sure they are working effectively;
- Adjusting your security plan according to the results of testing, changes in operations or other circumstances that might impact information security; and
- Overseeing the information handling practices of service providers and business partners who have access to your personal information. If you give another organization access to your records or computer network, you should make sure they have good security programs too. (Security Check, 2003)

In the cases where the FTC has issued consent orders, they appear to have modeled the remedial actions on the provisions of the GLBA. These FTC consent orders should be considered instructive and "could prove significant in any case challenging a company's failure to provide adequate information security protection." (Westermeier, 2004, p. II, 3) The consent orders issued by the FTC imply that the acceptable standard of care for all organizations, financial and non-financial, will be one similar if not identical to the standards established in the GBLA. Corporations could have a defensible position if they could prove they were in compliance with the provisions of the GLBA. Consequently, the FTC may have established a *de facto* standard of care even though it has not yet been codified.

REFERENCES

1. Becker, David (2004, June 10) UCLA laptop exposes ID info. CNET News.com, http://news.com.com/2102-1029_3-5230662 (accessed 4/14/2005)
2. Eli Lilly & Co., (FTC Docket No. C-4047) (May 8, 2002). Documents relating to this action are available at http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html
3. Federal Trade Commission Act, 15 U.S.C. §§41-58, as amended.
4. Financial Institutions and Customer Data: Complying with the Safeguards Rule, (September 2002) http://www.ftc.gov/bcp/conline/pubs/buspubs/safeguards.htm (accessed 9/7/05).
5. Graham-Leach Bliley Act, 15 U.S.C. §§6801-09, http://www.ftc.gov/privacy/glbact/glbsub1.htm#6801(accessed 9/6/2005).
6. *Guess?, Inc.*, (FTC Docket No. C-4091) (July 30, 2003). Documents relating to this action are available at http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html
7. Kawamoto, Dawn (2004) Medical group: Data on 185,000 people was stolen. ZDNet.com, http://news.zdnet.com/2102-1009_22-5660514.html (accessed 4/14/2005)
8. Lemos, Robert (2003, March 6) Data thieves nab 55,000 student records. CNET News.com, http://news.com.com/2102-1002_3-991413.html (accessed 4/14/2005)
9. Lemos, Robert (2003, March 31) Data thieves strike Georgia Tech. CNET News.com, http://news.com.com/2101-1002_3-994821.html (accessed 4/14/2005)
10. Levy, S. and Stone, B., (2005, July 4) Grand theft identity, *Newsweek*, 39-47.
11. McCullagh, Declan (2005, January 10) Hackers steal ID info from Virginia University. CNET News.com, http://news.com.com/2102-7349_3-5519592.html (accessed 4/14/2005)
12. *Microsoft Corp.* (FTC Docket No. C-4069) (December 20, 2002). Documents relating to this action are available at http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html

13. MTS Inc., d/b/a Tower Records/Books/Video (FTC Docket No. C-4110) (May 28, 2004). Documents relating to this action are available at http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html
14. Petco Animal Supplies, Inc. (FTC Docket No. C-4133) (March 4, 2005). Documents relating to this action are available at http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html
15. Prepared Statement of the Federal Trade Commission before the Committee on Commerce, Science, and Transportation U.S. Senate on Data Breaches and Identity Theft, June 16, 2005, http://www.ftc.gov.
16. Privacy Initiatives, www.ftc.gov/privacy
17. Safeguards Rule of the GLBA, 16 C.F.R. pt. 314, http://www.ftc.gov/bcp/conline/pubs/buspubs/safeguards.htm
18. Security Check: Reducing Risks to Your Computer Systems (June 2003). http://www.ftc.gov/bcp/online/pubs/buspubs/security.htm (accessed 9/15/2005)
19. Westermeier, J.T., Key New Developments and Lessons Learned, (September 29, 2004) Virginia Information Technology Legal Institute, Virginia CLE

NOTES

NOTES