The 2009
Hospitality Law Conference

February 9-11, 2009

Privacy Please:
Data Security in the Hospitality Industry

Presented By:

Scott Brown
Skadden, Arps, Slate, Meagher & Flom LLP
Boston, Massachusetts
scott.brown@skadden.com

Scott Brown has been practicing exclusively in the intellectual property area for nearly a decade. His principal areas of concentration include transactions, licensing, litigation, and counseling involving trademarks, copyrights, the rights of publicity and privacy, software, data security and domain names. Mr. Brown is also well-versed in the legal issues involved in creating, substantiating and disseminating advertising and marketing materials, and he often reviews and pre-clears advertising copy.

Mr. Brown's transactional and licensing experience includes structuring and negotiating the development, apportionment and transfer of intellectual property rights in the context of mergers and acquisitions, divestitures, joint ventures, strategic alliances and other commercialization opportunities. He also has handled the intellectual property aspects of numerous securities offerings and corporate finance matters.

On the litigation front, Mr. Brown has successfully prosecuted and defended copyright, trademark, trade dress, unfair competition, publicity and privacy, trade secret, breach of contract and false advertising matters in state and federal trial and appellate courts. Many of the cases he has worked on are matters where one or both parties sought preliminary and permanent injunctive relief, in addition to substantial monetary damages. Mr. Brown has also successfully represented several claimants in domain name administrative proceedings brought under the Uniform Domain Name Dispute Resolution Policy (referred to as the "UDRP").

Mr. Brown also has substantial experience counseling clients on the clearance and protection of their intellectual property rights both in the United States and abroad. He has handled trademark and copyright clearance and prosecution matters, including conducting and reviewing searches and investigations; preparing opinion letters; filing and prosecuting trademark and copyright applications; and handling the prosecution and defense of trademark and copyright administrative proceedings. Mr. Brown also manages the domestic and international trademark portfolios of a number of clients.

Over the years, Mr. Brown has worked with a broad spectrum of clients, from growth-stage companies to some of the largest U.S. and foreign corporations, as well as private equity firms and investment banks. Among the clients Mr. Brown has represented are Carnegie Hall, Textron, Esselte, EMC, Citigroup, Sage Software, Wenner Media, SG Cowen & Co., Sycamore Networks, Estee Lauder, Daum Communications, American Biltrite, Trimaran Capital Partners, Knight Capital Group, Keurig, Thomas Wiesel Partners, Chicago Mercantile Exchange, Global Insight, Register.com, Grosvenor Capital Management, Blackrock, Praecis Pharmaceuticals, Virgin Mobile USA, Weil Lifestyle, Activision, Revlon, Upromise, Getronics and Fortunoff.

A frequent speaker and author, Mr. Brown lectures regularly on topics related to intellectual property. Mr. Brown's recent speaking engagements include moderating a panel discussion on legal issues impacting the video game industry at the New York State Bar Association's 2006 Annual Meeting, serving as a guest lecturer at Fordham Law School, and making a presentation on early-stage techniques for protecting intellectual property and trade secrets at Insight Information's Third Annual Negotiating and Drafting Business Agreements seminar. Mr. Brown was also selected for inclusion in the 2005-2006 *Strathmore's Who's Who*.

PRIVACY PLEASE: DATA SECURITY IN THE HOSPITALITY INDUSTRY

By Scott Brown and Kelly Stevens*

TABLE OF CONTENTS

* Mr. Brown is a Counsel and Ms. Stevens an Associate at Skadden, Arps, Slate, Meagher & Flom LLP in Boston. They can be reached at scott.brown@skadden.com and kelly.stevens@skadden.com, respectively. The opinions expressed in this Article are those of the authors and not necessarily those of Skadden, Arps or its clients.

SCOPE OF THIS ARTICLE

This article highlights several critical data security issues facing professionals in the hospitality industry and is intended to offer an informative, albeit high-level, overview of recent developments in state, federal, and international regulation and private sector "best practices" related to information security. Nevertheless, in this constantly-changing area there is no substitute for careful examination of each company's unique facts and circumstances with the participation of management, information technology personnel and knowledgeable counsel.

The hospitality industry invests considerable resources on creating a positive guest experience. While traditional notions of "security" may engender thoughts of physical safety and the protection of tangible valuables, recent history has witnessed a sharp increase in the incidence and severity of data theft crimes -- and significant financial consequences for the individual victims and the business whose information system was compromised. The first part of this article reviews the current regulatory landscape and relevant state, federal, and international legislation, as well as class action trends. The second part of this article outlines specific, actionable measures that will help you assess your business's data security plan and implement industry best practices.

INTRODUCTION

Nearly every business sector has been affected by the significant rise in the number of consumer data security breaches in recent years. Just as the use of electronic communication and filing systems have streamlined business operations, the shift to a predominantly digital environment has made sensitive commercial and consumer information more vulnerable. Information that once would have been stored on paper is now routinely stored on computer files, which are often accessible via networks or the Internet and are increasingly vulnerable to attack.[1] The functions of booking airline, hotel and rental car reservations via the Internet, storing customers' preferences, ordering stock, hiring employees, and maintaining finances all depend on complex computer networks and storage devices that, if compromised, are susceptible to being hacked.

Legislation, regulations, and "best practices" addressing this growing problem are continuously evolving. Additionally, there has been a recent flood of litigation and enforcement action affecting a wide variety of industries -- sometimes against the perpetrators (if they can be identified), but also against the companies whose data was compromised.[2] Even when the

---

[1] Use of the Internet is increasing exponentially, and the rise of opportunistic criminal behavior seeking to capitalize on such use is keeping pace. According to a study sponsored by the Internet Systems Consortium, the number of Internet host computers has increased from 213 host computers in 1981 to 570,937,778 as of July 2008. See Internet Software Consortium, *Internet Domain Survey*, https://www.isc.org/solutions/survey (last visited January 7, 2009).

[2] For example, despite eleven arrests made in connection with the attacks on the TJX Companies' computer systems in 2005 and 2006, TJX paid out millions of dollars to the Federal Trade Commission (its federal regulator), banking institutions, credit card companies, and

(cont'd)

wrongdoer can be identified (which is not always possible), hackers often have insufficient resources to compensate for the widespread harm they cause. Thus, victims are likely to seek relief from the business or institution whose system was exposed, often alleging that harm was preventable or caused as a result of insufficient security that allowed hackers to infiltrate the system.

Information security breaches can occur in a number of ways. A breach can occur as the result of the physical loss of electronic hardware, such as a stolen laptop computer,[3] a Blackberry inadvertently left in a taxicab or a misplaced USB flash drive.[4] Data breaches can also result from intentional actions, such as Internet hacking, theft, an employee's purposeful divulging of security information,[5] and deception, where an identity thief pretends to be his victim for the purpose of garnering more information. Breaches also can occur simply as a result of human error, such as an employee unsuspectingly disclosing customer information, or the accidental revealing of information on the Internet.[6] A company's employees, consultants, and

---

(cont'd from previous page)

consumers that experienced losses as a result of a breach into the TJX system. See Brad Stone, *11 Charged In Theft Of 41 Million Card Numbers*, N.Y. TIMES, Aug. 5, 2008, at C1, available at http://www.nytimes.com/2008/08/06/business/06 theft.html.

[3] In May 2006, a data analyst in the United States Department of Veterans Affairs ("VA") took home electronic data that was stored on a laptop computer and external hard drive in contravention of the VA's policies. The employee's home was subsequently burglarized, the laptop stolen, and the personal information of 26.5 million individuals was compromised. See Department of Veterans Affairs News Release, *Secretary Nicholson Provides Update On Stolen Data Incident*, June 6, 2006, available at http://www1.va.gov/opa/pressrel/pressrelease.cfm?id=1134.

[4] In November 2006, an employee of the California State University, Los Angeles had a USB drive stolen out of her car. The USB drive contained sensitive personal information of 2,534 individuals, including names, Social Security numbers, campus identification numbers, phone numbers, and e-mail addresses of applicants, students, and faculty members. See Cal State L.A. Website, *Frequently Asked Questions About Information Security Incident: Stolen USB Drive*, July 5, 2007, available at http://www.calstatela.edu/security/061019/faq.htm.

[5] In August 2008, the FBI arrested a Countrywide Financial Corporation employee in an alleged scheme to steal and sell sensitive personal information, including Social Security numbers. The breach occurred over a two-year period, with the data thief downloading approximately 20,000 customer profiles each week and selling the lists for as little as $500. Approximately two million records are believed to be compromised. See The Privacy Rights Clearinghouse, *A Chronology of Data Breaches*, Apr. 20, 2005 (updated Jan. 10, 2009), http://www.privacyrights.org/ar/ChronData Breaches.htm#Total.

[6] In August 2008, the *New York Times* reported that the Princeton Review test-preparatory service accidentally published the personal data and standardized test scores of tens of thousands of Florida students on its Website, where they were available for public viewing for seven weeks. In an interview regarding the incident, an analyst at an Internet security firm commented that we

(cont'd)

vendors[7] may also improperly misplace, access, use or disclose customer information.[8] Even where a company seeks to protect itself, security breaches can arise from the implementation of software or security systems, which themselves contain vulnerabilities.

Consumer confidence (or lack of confidence) following a data security breach can have serious (and often severe) effects on the economy and individual businesses.[9] Indeed, a recent study by the Federal Bureau of Investigation extrapolating results from a survey of 2,066 organizations suggests that computer-related crimes costs U.S. businesses $67.2 billion each year.[10] Recent studies related to data security breaches of individuals' personal information suggests an average resolution time of 40 hours per victim in 2006 and 25 hours per victim in 2007.[11] In addition to the financial and productivity costs associated with data breaches, consumer security breaches can inflict significant damage to a company's reputation and

---

(cont'd from previous page)
are finding that companies today don't change until they have experienced the pain of a data breach that is exposed to the public." See Brad Stone, *Students' Files Are Exposed On Web Site*, N.Y. TIMES, Aug. 18, 2008, at C1, available at http://www.nytimes.com/2008/08/19/technology/19review. html.

[7] On January 20, 2009, the *Wall Street Journal* reported that cyber criminals compromised the computer network of Heartland Payment Systems, Inc., a credit-card processor which processes transactions for more than 250,000 businesses nationwide, including restaurants and smaller retailers. Some analysts say this breach "may rank among the biggest ever reported," though it may be too soon to determine. See Ben Worthen, *Card Data Breached, Firm Says*, WALL STREET JOURNAL, WSJ.com, http://online.wsj.com/article/SB123249174099899837.html.

[8] A recent study by the Center for Hospitality Research at Cornell University, "Hotel Network Security: A Study of Computer Networks in U.S. Hotels" examined the security of 147 hotels by performing on-site data security testing at 46 hotels. Of the networks tested, the study concluded that the majority were vulnerable to attack, and in some cases hotel employees inadvertently assisted in the breach by disclosing passwords and access instructions. See Josh Ogle, et al., *Hotel Network Security: A Study Of Computer Networks In U.S. Hotels*, CORNELL HOSPITALITY REPORT, Sept. 2008, available at http://www.hotelschool.cornell.edu/research/chr/pubs/reports/abstract-14928.html.

[9] Identity Thief Task Force, *The President's Identity Theft Task Force Report*, Sept. 2008, available at http://www.idtheft.gov.

[10] Joris Evers, *Computer crime costs $67 billion, FBI says*, ZDNET NEWS, Jan. 19, 2006, available at http://news.zdnet.com/2100-1009_22-146423.html.

[11] Javelin Strategy and Research 2006 and 2007 Identity Fraud Survey Reports, as interpreted and reported by the Privacy Rights Clearinghouse. See The Privacy Rights Clearinghouse, *How Many Identity Theft Victims Are There? What Is the Impact on Victims?*, Sept. 2003 (updated June 2007), available at http://www.privacyrights.org/ar/idtheftsurveys.htm.

goodwill, affecting relationships with customers, potential customers, and business partners.[12] In short, data security touches every business sector in today's global economy.

I. ELECTRONIC INFORMATION LAWS, REGULATIONS AND STANDARDS RELEVANT TO THE HOSPITALITY INDUSTRY

Today there are no uniform national or international information security standards or data breach notification requirements. With many varying (and often inconsistent) data security and privacy laws, standards, and regulations, the patchwork of requirements and recommendations can leave businesses without a clear understanding of their obligations and responsibilities. What is clear, however, is that data security is no longer solely the province of IT professionals – it is a company's legal obligation to protect the information it keeps.[13] Maintaining best business practices with respect to information security requires that companies, with the assistance of counsel, monitor the evolving regulatory landscape (some of which is sector-specific),[14] expanding Federal Trade Commission ("FTC") regulations, state laws (many of which are seemingly conflicting, and some of which apply to businesses that don't operate within the regulating state),[15] and the Payment Card Industry Data Security Standards (which

---

[12] According to an April 2007 Information Week article, *Companies Say Security Breach Could Destroy Their Business*, reporting on a recent McAfee study, "one-third of companies said in a recent poll that a major security breach could put their company out of business." See Sharon Gaudin, *Companies Say Security Breach Could Destroy Their Business*, INFORMATION WEEK, Apr. 24, 2007, available at http://www.informationweek.com/news/security/showArticle.jhtml. Furthermore, as one hospitality, hotel, and travel news magazine warned, "[d]eveloping a brand takes time and resources. The brand equity you've spent so much time building could be at risk with a single data loss incident." See Romkey Property Management System, *How Safe is Your Hotel Data?*, 4Hoteliers, Dec. 26, 2007, http://www.4hoteliers.com/4hots_fshw.php.

[13] The FTC is taking an active role in reminding businesses of their duty to protect information, as well as supporting them in their efforts. In a recent article directed at businesses, Lesley Fair, an attorney in the FTC's Bureau of Consumer Protection, warns that every company "has an obligation to its customers, affiliates, and employees to safeguard sensitive data." See Lesley Fair, *Take Stock: Conducting a Data Security Audit in Your Office*, Federal Trade Commission, July 2007, http://www.ftc.gov/bcp/ edu/pubs/articles/art02.shtm.

[14] See e.g., The Privacy Act of 1974, 5 U.S.C. § 552(a) (governing federal government privacy and security practices relating to individuals' personal information); the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (imposing privacy and security requirements on the health care sector); the Gramm-Leach-Bliley Financial Modernization Act of 1999, 15 U.S.C. §§ 6801-6809 (requiring financial institutions to implement certain privacy and data security safeguards); the Sarbanes-Oxley Act of 2002 (requiring the implementation of internal safeguards and information security controls over financial information technology systems).

[15] For example, new Massachusetts regulations, The Standards for the Protection of Personal Information of Residents of the Commonwealth, 201 Mass. Code. Regs. 17.00,

(cont'd)

bring the possibility of hefty fines and the potential of losing the right to process payment card payments). This part of the article provides an overview of several statutes, regulations, and standards currently in place, as well as recent class action trends.[16]

A. Federal Trade Commission Act (Section 5)

Section 5 of the Federal Trade Commission Act ("FTC Act")[17] charges the FTC with preventing "persons, partnerships, or corporations" from using "unfair or deceptive acts or practices in or affecting commerce."[18] The FTC has recently named data security as one of its top enforcement priorities.[19] In a March 2007 press release, the FTC Chairman announced that "the message should be clear: companies that collect sensitive consumer information have a responsibility to keep it secure."[20]

Under the FTC Act, the Agency has pursued companies that violate their own security policies[21] and those that have mediocre or substandard practices.[22] Consequently, it is

---

(cont'd from previous page)

promulgated pursuant to Massachusetts's security breach notification law are widely applicable to all persons (including corporations, partnerships, and other legal entities) that own, license, store, or maintain personal information about any Massachusetts resident. See MASS. GEN. LAWS. ch. 93H, § 1 et seq. (effective January 1, 2009). Suffice it to say, these regulations, and others like them, are far-reaching.

16 Certain federal privacy statutes with very sector-specific implications have been purposefully left out of the scope of this paper. Such laws include, for example, the Health Insurance Portability and Accountability Act (health services sector), the Privacy Act of 1974 (agencies of the United States Government), and a number of rules passed pursuant to the Gramm-Leach-Bliley Act (financial services and creditors).

17 15 U.S.C. § 45.

18 Id. § 45(a).

19 The President's Identity Theft Task Force Report, supra note 8. The FTC Division of Privacy and Identity Protection, the newest of the Bureau's divisions, oversees issues related to consumer privacy, credit reporting, identity theft, and information security, and this Division specifically governs unfair practices involving the use or protection of consumers' personal information.

20 FTC Press Release, *Agency Announces Settlement of Separate Actions Against Retailer TJX, and Data Brokers Reed Elsevier and Seisint for Failing to Provide Adequate Security for Consumers' Data*, Mar. 27, 2008, available at, http://www.ftc.gov/opa/2008/03/datasec.shtm.

21 See also In the Matter of Life is Good, Inc., FTC Docket No. C-4218 (Apr. 16, 2008) (Final Consent Order) (alleged failure to protect credit card numbers from electronic attacks, contrary to company's representations about its information security practices); see FTC Press Release, *Online Apparel Retailer Settles FTC Charges That It Failed to Safeguard Consumers' Sensitive Information, in Violation of Federal Law*, Jan. 17. 2008, available at

(cont'd)

imperative to (1) have a plan in place because the FTC has shown little patience for inadequate security measures and (2) follow the plan in place because the FTC demands that corporate practices conform to the plan in place.

B. The Fair Credit Reporting Act And Related Credit Regulations

The Fair Credit Reporting Act ("FCRA"),[23] which is enforced by the Federal Trade Commission,[24] regulates the collection, dissemination, and use of consumer credit information. This Act is the underlying basis for many other consumer credit laws and rights in the United States, such as the Fair And Accurate Credit Transactions Act Of 2003, The Red Flags Rule, and the FTC Disposal Rule.

(cont'd from previous page)
http://www.ftc.gov/opa/2008/01/lig.shtm; United States v. ValueClick, Inc., No. CV08-01711 (C.D. Cal. 2008) (Stipulated Final Judgment and Order entered on Mar. 17, 2008) (imposing $2.9 million in civil penalties charging that defendants failed to encrypt and secure sensitive customer information against electronic attacks, contrary to representations); *see* FTC Press Release, *ValueClick to Pay $2.9 Million to Settle FTC Charges*, Mar. 17, 2008, available at http://www.ftc.gov/opa/2008/03/vc.shtm.

[22] In the Matter of Goal Financial, LLC, FTC Docket No. C-4216 (Apr. 9, 2008) (Final Consent Order) (charging that defendant failed to provide reasonable and appropriate security for consumers' sensitive personal information in violation of federal law and alleging security failures that resulted in inadvertent transfer of 7,000 student loan application files to third parties), available at http://www.ftc.gov/os/caselist/0723013/ index.shtm; In the Matter of BJ's Wholesale Club, Inc., FTC Docket No. C-4148 (Sept. 20, 2005) (Final Consent Order) (charging that defendant's failure to take appropriate security measures to protect the sensitive information of thousands of its customers was an unfair practice that violated federal law, resulting in the information being used by unauthorized persons to make millions of dollars of fraudulent purchases).

[23] 15 U.S.C. § 1681 et seq.

[24] While much of the regulation in this area is enforced solely by the government, the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, as amended in 2001 by the U.S. PATRIOT Act, Pub. L. No. 107-56 (2001), provides a private right of action and civil damages, as well as imposes criminal penalties, ranging from fines to imprisonment. This Act has broad application to the unauthorized interception of information or access to a protected computer, which includes any computer that is involved in interstate or foreign commerce or communication. In effect, this protects every computer connected to the Internet. Any person or entity who has suffered harm as a result of a violation of this Act may bring a civil action for compensatory damages or equitable relief.

1. The Fair And Accurate Credit Transactions Act Of 2003

The Fair And Accurate Credit Transactions Act Of 2003 ("FACTA")[25] was designed to help consumers combat the growing crime of identity theft. At the time of its enactment, an FTC report estimated that approximately 10 million people were victims of identity theft in 2002 alone.[26] In addition to providing certain rights to consumers and victims of identity theft (the most widely-reported being the right to obtain a free copy of your credit report every year), the FACTA also imposes duties on businesses to protect consumers' personal information. For example, the FACTA establishes a national standard requiring businesses to truncate credit card information.[27] Under this provision, credit and debit card receipts may not include more than the last five digits of the card number, and such receipts may not include the card's expiration date.[28]

2. The Red Flags Rule

Several federal agencies[29] issued joint regulations on November 9, 2007, commonly known as The Red Flags Rule, that address the detection and prevention of identity theft. The Red Flags Rule applies to financial institutions[30] and creditors[31] with covered

---

25 Pub. L. No. 108-159.

26 See The Privacy Clearing House, *FACTA, The Fair and Accurate Credit Transactions Act: Consumers Win Some, Lose Some*, Aug. 2004 (updated Dec. 2008) available at http://www.privacyrights.org/fs/fs6a-facta.htm.

27 15 U.S.C. § 1681c(g)(1).

28 Id.

29 Those agencies include the Office of the Comptroller of the Currency, Treasury; Board of Governors of the Federal Reserve System; Federal Deposit Insurance Corporation; Office of Thrift Supervision, Treasury; National Credit Union Administration; and the Federal Trade Commission.

30 Financial institutions include entities that offer accounts that enable consumers to write checks or to make payments to third parties through other means, such as other negotiable instruments or telephone transfers.

31 A creditor is defined as any entity that regularly extends, renews, or continues credit (or any entity that regularly arranges such extension, renewal, or continuation); or any assignee of an original creditor who is involved in the decision to extend, renew, or continue credit. According to a Federal Trade Commission ("FTC") press release, dated October 22, 2008, examples of creditors are "finance companies, automobile dealers, mortgage brokers, utility companies, telecommunications companies, and non-profit and government entities that defer payment for goods or services." FTC Press Release, *FTC Will Grant Six-Month Delay of Enforcement of 'Red Flags' Rule Requiring Creditors and Financial Institutions to Have Identity Theft Prevention Programs*, Oct. 22, 2008, available at http://www.ftc.gov/opa/2008/10/ redflags.shtm.

accounts,[32] and requires that those entities implement identity theft prevention programs to identify, detect, and respond to patterns, practices, or specific activities that could indicate identity theft. Though these joint regulations were to have become effective on January 1, 2008, the FTC has suspended enforcement of the Red Flags Rule until May 1, 2009 to allow additional time to develop and implement written identity theft prevention programs. [33]

While the Red Flags Rule likely does not directly apply to most businesses in the hospitality industry, the Red Flags Rule and its requirements remain instructive. First, while the Red Flags Rule technically applies only to financial institutions and certain creditors, recent consent decrees entered into by the FTC with retailers and other non-financial institutions have mirrored the requirements the Red Flags Rule establishes.[34] Second, a financial institution or creditor subject to the Red Flags Rule "is ultimately responsible for complying with the final rules and guidelines even if it outsources an activity to a third-party service provider."[35] Thus, financial institutions are likely to contractually demand that merchants comply with these guidelines regardless of their direct legal application.

---

[32] According to the guidelines issued with the Red Flags Rule, "a covered account is (1) an account primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, or (2) any other account for which there is a reasonably foreseeable risk to customers or the safety and soundness of the financial institution or creditor from identity theft."

[33] FTC Press Release, *FTC Will Grant Six-Month Delay of Enforcement of 'Red Flags' Rule Requiring Creditors and Financial Institutions to Have Identity Theft Prevention Programs*, Oct. 22, 2008, available at http://www.ftc.gov/opa/2008/10/ redflags.shtm.

[34] For example, in accordance with an FTC Consent Order, BJ's Warehouse Club must for twenty years: (1) designate an employee or employees to coordinate an information security program; (2) identify risks to the security, confidentiality, and integrity of personal information the company stores; (3) assess the sufficiency of any safeguards in place to control these risks; and (4) take various other steps, as enumerated in the Consent Order, to protect consumers' personal information. In the Matter of BJ's Wholesale Club, Inc., supra note 21; see also In the Matter of Life is Good, Inc., supra note 21 (Final Consent Order) (ordering retail company which failed to adequately safeguard consumers' financial information to designate an employee to coordinate an information security program; identify risks and safeguards already in place, design safeguards to control risks identified, develop steps to oversea service providers, and evaluate and adjust its program as necessary to reflect changing needs).

[35] For the text of the federal register notice, see *Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003; Final Rule*, Federal Register Part IV, Vol. 27. No. 217, Nov. 9, 2007, available at http://ftc.gov/os/fedreg/2007/november/071109redflags.pdf.

3. The FTC Disposal Rule

Under the FTC Disposal Rule,[36] any business that uses a consumer report for a business purpose must take appropriate precautions when disposing of sensitive information derived from consumer reports to protect against "unauthorized access to or use of the information."[37] Although the FTC Disposal Rule applies only to consumer reports and the information contained therein, the FTC has encouraged broader adoption of those principles and has stated that "those who dispose of any records containing a consumer's personal or financial information should take similar protective measures."[38]

The Disposal Rule requires "reasonable" disposal practices. According to an FTC "Business Alert" designed to guide businesses in compliance with the Disposal Rule, reasonable measures for disposing of protected information could include (1) burning, pulverizing, or shredding papers such that sensitive information cannot be read or reconstructed; (2) destroying or erasing electronic files or other media; (3) hiring a document destruction contractor with sound information security policies to dispose of material specifically identified as consumer report information.[39]

C. The Financial Privacy Rule And The Safeguards Rule Under The Gramm-Leach-Bliley Act

The Financial Privacy Rule and the Safeguards Rule, both passed pursuant to the Gramm-Leach-Bliley Act,[40] apply only to financial institutions and companies providing financial services and products. While not directly aimed at the hospitality industry, the requirements of these rules present a prudent standard that would be beneficial to any business that collects and maintains personally identifying information with financial information (e.g., credit or debit card numbers, or bank account information in connection with names, addresses, or social security numbers).

---

36 16 C.F.R. § 682.

37 The FTC brought its first case under the Disposal Rule against American United Mortgage Company. The FTC charged the company with improperly disposing of loan documents containing consumers' sensitive personal and financial information in and around an unsecured dumpster. The Company was ordered to pay a civil penalty in the amount of $50,000. United States v. Am. United Mortgage Co., Civil Action No. 07C 7064 (N.D. Ill. Dec. 18, 2007) (last visited January 16, 2009).

38 FTC Press Release, *FACTA Disposal Rule Goes into Effect June 1*, June 1, 2005, available at http://www.ftc.gov/opa/2005/06/disposal.shtm.

39 FTC Business Alert, *Disposing of Consumer Report Information? New Rule Tells How*, June 2005, available at http://www2.ftc.gov/bcp/edu/pubs/business/alerts/alt152.shtm.

40 15 U.S.C. §§ 6801-09.

The Financial Privacy Rule requires that institutions present customers with a "clear and conspicuous disclosure" of the institution's privacy policy as it relates to the collection, protection, and disclosure of customers' nonpublic information. That statement should accurately disclose which nonpublic personal information the company will share, how such information will be disclosed, and how long the information will be protected.

The Safeguards Rule requires all financial institutions (as well as other fringe institutions, such as credit reporting agencies that receive customer information in connection with a financial institution) to develop and implement certain safeguards to protect the private information of its customers. The Safeguards Rule requires the development and implementation of "administrative, technical, and physical safeguards" to insure the security and confidentiality of customer records and information to prevent against unauthorized access or use of these records, resulting in harm or inconvenience to the customer.

D. Individual State Laws

In the absence of a uniform federal data security law, individual states have enacted a panoply of state-specific statutes. Nearly every state has enacted such a statute and requires notification to consumers when certain types of data breaches occur. Some states have gone further, such as Minnesota, which has adopted a cost-sharing law that requires a business to reimburse financial institutions' losses if the business does not comply with data-protection laws and failed to appropriately secure customer data. The financial exposure under such a rubric is potentially immeasurable. Other states have debated enacting such provisions. As such, failing to satisfy these state statutes can have a significant financial cost to hospitality companies, particularly those that operate in many (if not all) states.

Some states have passed general data protection statutes aimed at keeping consumers' personally identifiable information safe. As but one example, Massachusetts recently enacted the Standards for the Protection of Personal Information of Residents of the Commonwealth.[41] The standards are broad in scope, technically specific, and demand the implementation of administrative, electronic, and physical safeguards. The law provides a data security "minimum standard" to which businesses must adhere. Other states have passed equally complex and exacting data security statutes.

---

[41] 201 MASS. CODE REGS. 17.00 et seq. The Massachusettes Office of Consumer Affairs and Business Regulation has extended the original Januray 1, 2009 comliance deadline for most provisions of 201 CMR 17.00 to May 1, 2009. Certain requirements, e.g., obtaining a certification from third party service providers and encrypting portable devices, have been extended until January 1, 2010. For more information see Consumer Affairs and Business Regulation Press Release, *Business Community Given Additional Time to Comply with Identity Theft Prevention Regulations*, November 14, 2008, http://www.mass.gov/?pageID=ocapressrelease&L=1&L0=Home&sid=Eoca&b=pressrelease&f=081114_IDTheftupdate&csid=Eoca.

1. Breach Notification Laws

Forty-four states, Washington D.C., the Virgin Islands, and Puerto Rico have enacted legislation mandating organizations which experience a breach in the security of personal information to institute formal notification procedures.[42] Data breach notification laws typically require covered entities (often broadly defined) to implement an internal breach notification policy and include various requirements for incident reporting; e.g., protocols that outline the timing and method of such notification to consumers and, in some instances, credit reporting agencies, and state governmental bodies.

When a company becomes aware of and discloses a breach, the company should be prepared to set in motion a range of programs that address the security of its data going forward, the concerns of those individuals whose information was breached, and the public's response to the occurrence of such an intrusion. Some examples of this include organizing a call center for potential victims of the breach to receive information, designating a point person to coordinate the efforts of the company, and assembling a team of persons who can ascertain the degree of the breach.

2. Laws That Force Businesses To Share The Loss Incurred By A Breach

When a data breach results in the theft of financial account information, the loss incurred can be enormous. If a company's system is breached, the company incurs costs in investigating and containing the infiltration, enhancing computer security and systems, and communicating with customers. In addition, companies face the potential cost of lawsuits going forward. At the same time, there is a loss suffered by payment card companies and financial institutions.

Minnesota has enacted a cost-sharing law, and several other states have proposed laws pending, that address the effect that the breach of one business's system has on other businesses. Under this law, if a business fails to implement a sufficient degree of security (as

---

[42] The states which presently have a breach notification provision (and the year such provision became effective): Alaska (2009); Arizona (2006); Arkansas (2005); California (2003); Colorado (2006); Connecticut (2006); Delaware (2005); Florida (2005); Georgia (2005); Hawaii (2007); Idaho (2006); Illinois (2006); Indiana (2006); Iowa (2008); Kansas (2006); Louisiana (2006); Maine (2006); Maryland (2008); Massachusetts (2008); Michigan (2007); Minnesota (2006); Montana (2006); Nebraska (2006); Nevada (2006; additional requirements 2008); New Hampshire (2007); New Jersey (2006); New York City and New York State (2005); North Carolina (2005); North Dakota (2005); Ohio (2006); Oklahoma (2006); Oregon (2007); Pennsylvania (2005); Rhode Island (2006); South Carolina (2008); Tennessee (2005); Texas (2005); Utah (2006); Vermont; Virginia (2008); Washington (2005); West Virginia (2008); Wisconsin (2006); Wyoming (2007); District of Columbia (2007); Puerto Rico (2006); the Virgin Islands (2005). For a more comprehensive analysis of each state's statute, see KEVIN P. CRONIN & RONALD W. WEIKERS, DATA SECURITY AND PRIVACY LAW: COMBATING CYBERTHREATS (2008).

required under Minnesota law),[43] it may have to share the costs incurred by other businesses as a result of such breach. The statute authorizes financial institutions to recover reasonable costs incurred in responding to the theft of cardholder data when there is a breach in a business's security system that is out of compliance with data security law.[44] A business in Minnesota that has not properly secured the data in its systems may be liable to reimburse affected financial institutions for any costs incurred and reasonable actions undertaken by the institutions in responding to a data breach, including but not limited to: the cancellation, closure, reopening or reissuance of any affected account; any action to stop payments or block transactions with respect to the account; any refund or credit made to a cardholder to cover the cost of any unauthorized transaction relating to the breach; and any costs relating to the notification of cardholders affected by the breach.[45]

A recently enacted Connecticut law[46] requires any person or business in possession of personally identifying information of another person to "safeguard the data, computer files and documents containing the information from misuse by third parties," and requires the proper destruction and disposal of such information. The law provides for a civil penalty up to $500,000 for a single event to be imposed on persons or businesses that intentionally violate the statute's data security requirement.

Bills similar to Minnesota's cost-sharing law have been proposed in Connecticut, Illinois, and Texas. The Connecticut bill, if passed, would render businesses liable for costs incurred by banks or financial institutions in connection with the breach, plus costs for "any assistance provided to customers to help mitigate loss or inconvenience or to prevent loss or further inconvenience."[47] Likewise, the Illinois bill, SB 1675, which is scheduled for a reading in the Senate on January 13, 2009, provides that whenever a payment card is used to obtain money, goods, services, or anything else of value without the consent of its rightful owner as a result of a breach of a security system of an entity, such entity will be liable to any financial institution that incurs costs or damages relating to such breach. The damages the financial institution will be able to recover mirror those reflected in the Minnesota law.

---

43 MINN. STAT. § 325E.64.

44 Id. § 324E.64(2) (effective August 1, 2008). Minnesota's data security law takes guidance from the PCI Data Security Standards. For example, businesses are prohibited from retaining data from the magnetic strips on payment cards, as well as security codes from such cards, for more than 48 hours after a card transaction is approved.

45 Id. § 324E.64(3) (effective August 1, 2008).

46 An Act Concerning The Confidentiality Of Social Security Numbers. Conn. Pub. L. No. 08-167, § 1.

47 An Act Encouraging The Safekeeping Of Consumer Information In Retail Establishments, Connecticut Raised Bill No. 1089, January 2007.

Similarly, a Texas bill, which was passed unanimously by the House of Representatives, charges businesses to "implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect and safeguard from unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business." The bill provides for destruction of sensitive material in a way that makes the information unreadable by any means, and requires businesses that accept payment cards to comply with all PCI Data Security Standards.[48] Further the bill provides a means for financial institutions to bring actions against businesses if, at the time of breach, the business was out of compliance with the PCI Standards.

This Texas bill highlights a legislative trend, and the need for businesses, both located in and out of Texas, to conduct internal or third party audits to ensure compliance with laws and standards related to data security. Under this Texas bill, before a financial institution can bring an action to recover damages from a business whose information security system was breached, the institution must request that the business produce certification of compliance with the PCI DSS. The action will be dismissed with prejudice if the business provides this certification of compliance issued by a payment-card industry-approved auditor.

E. European Union And United States Of America: Safe Harbor Rule

The European Union's comprehensive privacy legislation, the Directive on Data Protection[49] (the "Directive"), which became effective in 1998,[50] prohibits the transfer of personally identifiable data to countries that do not provide an "adequate" level of privacy protection under the Directive's standard.[51] In order to bridge the different privacy approaches taken by the United States and the European Union's Directive, a Safe Harbor Policy was developed and approved jointly by the European Commission and the U.S. Department of Commerce so that U.S. companies doing business in Europe could do so efficiently, without experiencing delays in their European business transactions and without concern of prosecution by European authorities under European privacy laws.[52] This Safe Harbor exempts U.S.

---

48 H.B. 3222, 80th Leg. Reg. Sss. (Tex. 2007). The text of the bill, as passed by the Texas House of Representatives is available at http://www.legis.state.tx.us/tlodocs/80R/billtext/html/HB03222E.htm (last visited January 10, 2009). The last action on this bill was a referral to the Texas Senate Committee on Business and Commerce.

49 European Union Directive 95/46/EC On The Protection Of Individuals With Regard To The Processing Of Personal Data And On The Free Movement Of Such Data, 1995 O.J. (L 281) 31.

50 Although the Directive on Data Protection was published in the Official Journal of the European Community on November 23, 1995, it did not become effective until three years from the date of its adoption.

51 European Union Directive 95/46/EC, supra note 48.

52 For more information on the Safe Harbor policy, see http://www.export.gov/ safeHarbor/ (last visited January 14, 2009).

companies doing business in the European Union and instead applies the law of the United States rather than the more strict scrutiny of the European Union's Directive on Data Protection.

While U.S. organizations are not required the participate in the Safe Harbor (membership is entirely voluntary), the framework offers a simpler and less expensive means of complying with the standards of the E.U. Directive. Businesses that wish to participate in the Safe Harbor must comply with a set of seven "Safe Harbor Principles"[53] and self-certify in writing on an annual basis to the Department of Commerce that such organization agrees to adhere to the Safe Harbor's requirements.

All businesses participating in the Safe Harbor must adhere to the following seven principles:

- *Notice*: An organization must provide notice to individuals about the purposes for which it collects and uses information, the third parties with which it shares information, and the choices such organization offers regarding limitations on its use and disclosure of such information. Additionally, an organization must provide contact information for inquiries or complaints.

- *Choice*: An organization must allow individuals the option to decline to have their information disclosed or used for a purpose other than that for which it was collected. For sensitive information, individuals must be provided with a specific choice to "opt-in" to any secondary use of the data.

- *Transfer to Third Parties*: An organization must apply the notice and choice provisions, infra, and where the organization wishes to share information with a third-party agent, it must ensure such agent's privacy protection policies are adequate under the Directive or the Safe Harbor principles.

- *Access*: Generally, individuals must have access to the information held about them, and the ability to amend or delete that information where it is inaccurate.

- *Security*: Reasonable precautions must be taken to protect data from loss, misuse, and unauthorized access.

- *Data Integrity*: Reasonable steps must be taken to ensure data is accurate, complete, and current, so that it is relevant for the purposes for which it is being used.

- *Enforcement*: An organization must ensure compliance with the Safe Harbor principles. Additionally, independent mechanisms must be available to investigate and resolve disputes.

---

[53] For an overview of the Safe Harbor policy, and a description of the seven principles with which organization must comply, see http://www.export.gov/safeharbor/SH_Overview.asp (last visited January 20, 2009).

Further, organizations must publish a privacy policy, disclosing that they adhere to the Safe Harbor. The Department of Commerce maintains a list of all organizations that file self-certification letters; both the list and these letters are publicly available.[54]

F. Class Action Trends Regarding Data Breaches

In addition to the potential for fines, government enforcement actions, and increased regulatory scrutiny following a data security breach, companies are also likely to face a consumer class action lawsuit. Among the claims that consumers whose data has been breached are likely to raise are: negligence,[55] violation of various states' security breach notification laws,[56] breach of contract,[57] various claims under state law unfair trade practices statutes, breach of fiduciary duty,[58] and violations of the FACTA.[59] To date, these consumer class actions have

---

[54] This list is available at http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list.

[55] See e.g., Pinero v. Jackson Hewitt Tax Service Inc., 2009 WL 43098, *3 (E.D. La. Jan. 7, 2009) (dismissing plaintiff's negligence claims for a failure to allege "any concrete financial losses resulting from the alleged negligence" where defendant tax service discarded sensitive information in a trash dumpster without making such information unreadable); Melancon v. Louisiana Office of Student Financial Assistance, 567 F.Supp. 2d 873, 877 (E.D. La. Jun 05, 2008) (granting summary judgment in favor of defendants where defendant truck operator lost electronic media containing certain students' personal information because "the mere possibility that personal information may be at increased risk does not constitute actual injury sufficient to maintain a claim for negligence" under Louisiana law).

[56] See e.g., Ponder v. Pfizer, Inc., 522 F.Supp. 2d 793, 797 (M.D. La. 2007) (dismissing plaintiffs' claim that defendant employer violated Louisiana's Database Security Breach Notification law where defendant did in fact notify plaintiffs of security breach, and where plaintiffs failed to allege that the information was used to their detriment, thus failing to allege actual damages).

[57] See e.g., Forbes v. Wells Fargo Bank, N.A., 420 F.Supp. 2d 1018, 1021 (D. Minn. 2006) (granting summary judgment in favor of defendants where bank customers' personal information was lost when the computers on which such information was stored were stolen, finding that "plaintiffs' injuries [were] solely the result of a perceived risk of future harm" and that plaintiffs showed no actual injury to support a claim for damages); see also, Caudle v. Towers, Perrin, Forster & Crosby, Inc., 580 F.Supp. 2d 273, 282-283 (S.D.N.Y. Aug. 28, 2008) (dismissing plaintiffs' negligence and breach of fiduciary duty claims where plaintiffs' personal information was stored on defendant employer's laptop computers, which were stolen, but where plaintiffs showed no evidence that their personal data was accessed or misused as a result of the theft, and where plaintiffs had not yet suffered any economic damage caused by the breach).

[58] See e.g., Shafran v. Harley-Davidson, Inc., 2008 WL 763177, *2 (S.D.N.Y. Mar. 20, 2008) (dismissing plaintiffs' claims for breach of fiduciary duty, negligence, unjust enrichment, breach of warranty, deceptive acts or practices, false advertising, fraud and negligent misrepresentation, prima facie tort, and breach of contract where a laptop computer containing the personal information of 60,000 customers was lost, finding that actual injury is a required element of each of plaintiffs' claims, and that no actual injury was shown).

[59] See e.g., Aliano v. Texas Roadhouse Holdings, LLC, 2008 WL 4671716 (N.D. Ill. Oct. 22, 2008) (granting plaintiff's motion to extend the date by which the motion for class certification is due where

(cont'd)

been largely unsuccessful. Many courts are dismissing the class actions, finding that the plaintiffs have failed to state a claim upon which relief can be granted because such plaintiffs had not yet suffered an economic harm or loss as a result of the alleged breach. In these cases, plaintiffs brought suits merely upon a security breach or invasion, and courts dismissed because "without more than allegations of increased risk of future identity theft, the plaintiffs have not suffered a harm that the law is prepared to remedy."[60] Though the current trend in these consumer class action suits is for courts to dismiss where plaintiffs cannot show actual harm or economic damages, it would be imprudent to rely too heavily on this trend going forward. With legislation and regulation increasing at a rapid clip, the definition of what constitutes harm may become more flexible, allowing courts to find "harm" where data has been made insecure because of a company's failure to comply with various regulations.

II. GOING FORWARD: SAFEGUARDING YOUR CUSTOMERS' PRIVATE INFORMATION AND PROTECTING YOUR BUSINESS

Companies in every business sector, including the hospitality industry, must assess their current data security strategies and formulate a comprehensive plan to safeguard sensitive customer information. Businesses are faced with customer demands for data security, competitive pressures to maintain an integrated and streamlined security system, contractual obligations related to the protection of private information, and the ever-changing and often-cumbersome legal and regulatory requirements being imposed on both the state and federal levels. Although the majority of existing regulation focuses on the financial services sector, the FTC has brought enforcement actions against other businesses due to substandard security measures. The result of these aforementioned actions has been the entry of consent decrees requiring companies to implement and maintain policies that result in the same functional ends as those reported by the regulations governing the financial services sector. Consequently, the FTC's use of its more generic jurisdiction over unfair or deceptive trade practices under the FTC Act has had (and will continue having) the effect of bringing retailers and other service industries within the ambit of these requirements.

This section presents a non-exhaustive list of key questions companies should be asking as they develop and refine a comprehensive security plan.

A. Does Your Company Comply With The Payment Card Industry Data Security Standards?

Any company that accepts credit or debit payment cards is subject to the Payment Card Industry Data Security Standards ("PCI DSS"). The Payment Card Industry ("PCI") is a consortium of credit card processing associations and institutions, acting as an "open global

---

(cont'd from previous page)
defendant allegedly violated the FACTA by printing plaintiff's credit card expiration date on a cash register receipt).

[60] See e.g., Pisciotta v. Old Nat. Bancorp, 499 F.3d 629, 639 (7th Cir. 2007) (affirming dismissal of plaintiffs' claims and finding no cognizable injury to exist where defendant bank was storing plaintiffs' personal information and suffered a security breach, but where no actual economic loss ensued).

forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards" related to protecting account data.[61] The PCI DSS is a "multifaceted security standard" that includes requirements for security management policies and procedures, in addition to generally dictating the manner in which organizations that use payment cards and must handle sensitive payment card data.

The PCI DSS are a set of technical and operational standards that apply to any business which processes card payments. These standards were developed to assist such entities in preventing credit card fraud, hacking, and other security vulnerabilities. The PCI DSS are enforced by the founding members of the PCI Security Standards Counsel: American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc.[62] While the PCI is a private organization and does not technically have the force of law, it can motivate merchants to act by imposing fines as well as sanctions up to and including the termination of a merchant's right to accept credit cards.

For companies with legitimate business reasons to store the personal information of cardholders, it is important to understand what data elements the PCI DSS allows them to store and what measures they must take to protect such personal information. Companies that fall under these standards must annually validate their compliance. The fines imposed for noncompliance can be significant.[63]

The most recent version of these standards was released on October 1, 2008 and does not reflect substantial revisions to the existing twelve requirements. Rather, the goal of the latest revision was to ease implementation, reduce compliance cost, and clarify the standards for the benefit of those merchants controlled by them. The twelve PCI DSS requirements address such concerns as security management, network architecture, software design, and other critical policies, procedures, and protective measures related to security.

The PCI DSS present an effective market standard that can be used in contract negotiations with third parties. Businesses that contract with third parties for the collection, maintenance, or storing of personal information may be well-served to require proof of compliance with PCI DSS, in addition to contractually requiring such compliance going forward.

---

61 See generally https://www.pcisecuritystandards.org.

62 PCI Security Standards Counsel, *PCI Quick Reference Guide – Understanding the Payment Card Industry Data Security Standard, version 1.2*, 2008, available at https://www.pcisecuritystandards.org/pdfs/pci_ssc_quick_guide.pdf (last visited January 12, 2009).

63 In January 2008, Visa announced that it began to levy monthly fines of $25,000 against non-PCI-compliant large merchants and $5,000 non-compliant middle-sized merchants. Visa Press Release, *PCI Compliance Continued to Grow in 2007*, Jan. 22, 2008, http://www.corporate.visa.com/md/nr/press753.jsp.

B. Does Your Company Know What It Has, Why It Has It, and Where It Is?

It is essential to take an inventory of the personal information your business collects and maintains. By knowing what information you have, how it is stored, where it is saved, how and when it is deleted, and which persons have access to it, your business can better control how it protects this critical information.

In addition to simply keeping an inventory, companies should revisit their data retention policies, seeking to reduce the amount of information that is maintained. By keeping only information that is essential -- and only for as long as it is needed -- companies can balance the need to maintain sufficient information to efficiently operate their business while simultaneously minimizing the potential exposure should a data security breach occur.

Further, companies can increase information security and further mitigate the potential exposure by storing information in a fragmented manner. By viewing customer information in small parts, businesses can do a thorough review of exactly what pieces of information they need. For example, if a business marketing department tracks user information online to determine the click-through rate on its website, it is possible that personal profiles do not need to be connected to that information. In this example, if the two databases were not linked, the personal user information could be stored with greater security separate from the marketing information.

Consider, also, the opposite: often data is saved in many different places, both intentionally and unintentionally. There are many reasons for this; perhaps the same information is useful to different departments or perhaps the business has changed computer hardware or software systems, or replaced back-up programs. Sometimes data is stored in email, on paper, and on hard drives simply by happenstance. Data unintentionally stored in a variety of places conflicts with a business's goal of maintaining control over its data inventory. A company cannot protect information unless it knows where it is, and when information is stored (or duplicated) in widely dispersed locations, companies increase the risk that data thieves will access valuable information undetected.

An institution may assess vulnerabilities in the ways it gathers and stores information by identifying past instances of security breaches and the methods used to accomplish such unauthorized intrusion. By compiling this historical "breach inventory," institutions can develop an educated view of their security vulnerabilities unique to their own operations.

C. Does Your Company Have The Right Tools For The Job?

Is your business protected against computer worms or viruses[64] while your corporate offices are being burglarized? Are uniform security guards posted in your building

---

[64] A computer worm is a self-replicating computer program, which uses a network to send copies of itself to other networked computers, requiring no user intervention. Unlike a virus, it does not need to attach itself to an existing program. Worms cause harm to the network, whereas viruses corrupt or modify files on a targeted computer. See MERRIAM-WEBSTER'S ONLINE

(cont'd)

lobby while your reservation system is being hacked remotely via the Internet? Once you establish a "breach inventory" unique to your business operations, you can tailor a program specifically targeted at your vulnerabilities.

There are innumerable ways for those with malicious intentions to steal valuable information. To counter, there are countless methods, products, services, and strategies a company could implement to protect its data, such as firewalls, intrusion detection software, employee training, and traditional "offline" brick and mortar security systems. Conducting a thorough assessment of existing technical architecture is critical to developing a data security program that uniquely targets your business needs. Such an assessment should identify present internal and external risks and vulnerabilities, as well as catalog all prior breaches to security resulting from accidental and intentional behavior. Once this list is compiled, assess the likelihood of each risk factor you have identified, and the total estimated cost of such a breach materializing.

D. Does Your Company Have An Appropriate Instruction Manual To Operate The Required Tools?

For the sake of maintaining a clear and complete data security program, a business should develop and maintain a written program and distribute it to all relevant persons in the organization. "Relevant persons" includes not only the IT department or those employees charged with administering the program, but every employee with access to stored data who will thus be bound by the terms of the program. Further, there is a value to appointing a designated authority in the continued oversight, development, implementation, and administration of the program.[65]

Once developed and documented in written form, a company should regularly review its security policy and compare its policy to its security practices. To pass FTC muster, a business's policy and practices must be strong enough to be fair and reasonable to consumers. For example, the FTC pursued Life is good™ based not on allegations that the company violated any privacy law or regulation, but rather under the agency's generic unfair-trade-practices authority. The FTC brought a complaint against Life is good™ on the theory that the company made certain representations to the public in the course of soliciting and entering commercial

---

(cont'd from previous page)
DICTIONARY, http://www.merriam-webster.com/dictionary/worm & http://www.merriam-webster.com/dictionary/virus, (last visited January 16, 2009).

[65] Under the Red Flags Rule, every institution must obtain approval of its written program from its board of directors, an appropriate committee of the board, or a senior level manager, and is encouraged to appoint a designated authority to maintain the program.

transactions, and then failed to "provide reasonable and appropriate security for the sensitive consumer information stored on its computer network."[66]

E. Has Your Company Covered All Three Bases – Physical, Technical, and Administrative Security Measures?

The growing trend is for legislation to require companies to generally address physical, technical, and administrative security measures. To date, those laws allow companies significant flexibility to assess their security needs and craft an appropriate means of protection. Whether or not your company is specifically bound by a data security law, it is a good business practice to consider your approach to each of the following categories of protective measures. Some examples of security measures falling within each category are:

- *Physical*: Take reasonable measures to dispose of information;[67] restrict and monitor access to data; lock up any paper files containing sensitive information; restrict employees' access to certain websites which could potentially disrupt the integrity of your system; carefully screen employees and third-party vendors who will have access to sensitive information.

- *Technical*: Install identity and access management software; utilize firewalls; encrypt, scramble, or remotely disable data files; use "data wipe" software when disposing of any computer which contains or has contained sensitive information; implement multi-factor remote access controls (such as requiring pin numbers and randomly generated information from security tokens, or other such devices).[68]

---

66 See FTC Press Release, *Online Apparel Retailer Settles FTC Charges That It Failed to Safeguard Consumers' Sensitive Information, in Violation of Federal Law*, Jan. 17. 2008, http://www.ftc.gov/opa/2008/01/lig.shtm.

67 On September 7, 2006, Chase Bank released a statement informing 2.6 million current and former Circuit City credit card account holders that computer tapes containing their personal information were mistakenly identified as trash and thrown out. See JP Morgan Press Release, *Chase Notifying Individuals About Improperly Discarded Tapes*, Sept. 7, 2006, available at http://investor.shareholder.com/jpmorganchase/press/releasedetail.cfm?ReleaseID=210276&ReleaseType=Currentv.

68 Practicing Law Institute, Patents, Copyrights, Trademarks and Literary Property Course Handbook Series. June – July, 2007. Eighth Annual Institute on Privacy and Security Law: Pathways to Compliance in a Global Regulatory Maze. Dreifach, K., *Data Privacy, Web Security, and Attorney General and FTC Enforcement*. In a discussion of remote access controls, Mr. Dreifach refers to three layers of security: "Who you are, what you know, and what you have." This multi-layer system is prudent; requiring access information that could never be saved or stored in one place (e.g., because a security access system which randomly generates a pin-number can never, by definition, be saved) decreases the chances that a data thief will be able to amass the necessary information to access the protected data.

- *Administrative*: Document your information security and privacy policies and protocol; provide periodic training and regular reminders of the information security protocol for employees; consistently enforce sanctions when employees breach data security protocol;[69] remain up-to-date on the most current security risks and system vulnerabilities; install available patches frequently; regularly (and safely) dispose of data that is no longer needed; contractually require third-party vendors with whom you share sensitive information to maintain acceptable data security standards and practices.

F. Does Your Company Know If Its Plan Is Working?

In order to maintain effectiveness over time, a program must be updated periodically to reflect changes in risk, trends, and security vulnerability. Businesses should consider changes and developments in methods of data theft as well as in methods to detect, prevent, and mitigate such theft. The United States government is working with the private sector to provide training, outreach, and support in the area of data security.[70] The outreach effort has included business alerts, articles, tip sheets, speeches, and public interviews, alerting businesses to trends in security compromises, as well as guiding companies in developing and maintaining sound and effective data security programs.

It is important for businesses to take advantage of this information and to remain up-to-date about the current trends of data theft and data security. Additionally, businesses must remain up-to-date regarding their own unique ever-changing security vulnerabilities. To do so, companies should note any changes in the types of data it collects and stores due to modifications of its organizational structure that result from any mergers, alliances, joint

---

69 A Boeing employee was terminated when his laptop contained identifying information on 382,000 then-current and former employees was stolen. A spokesperson for the company reported that the company terminated the employee because he violated company policy by downloading the information onto the laptop and not encrypting it. See Sharon Gaudin, *Boeing Employee Fired After Laptop With Employee Info Is Stolen*, INFORMATIONWEEK, Dec. 15, 2006, available at http://www.informationweek.com/ news/security/cybercrime/showArticle.jhtml?articleID=196700288.

70 On April 15, 2008, the Federal Trade Commission, International Association of Privacy Professionals, and Northwestern University School of Law co-hosted a one-day public workshop on how businesses can secure the personal information of consumers and employees. See FTC Press Release, *FTC, IAPP, Northwestern University Law School to Co-Host April 15 Workshop for Businesses on Best Practices for Protecting Personal Information and Securing Data*, Feb. 1, 2008, http://www.ftc.gov/opa/2008/02/data.shtm. A second data security workshop was help on August 13, 2008 in Los Angeles and was co-hosted by the Federal Trade Commission and the California Office of Privacy Protection. See FTC Press Release, *FTC, California Office of Privacy Protection to Co-Host Workshop for Businesses on Best Practices for Protecting Personal Information and Securing Data*, July 22, 2008, http://www.ftc.gov/opa/2008/07/datasec.shtm.

ventures, or service provider arrangements. Maintaining detailed records of an institution's own experiences with identity theft will guide the process of keeping it updated as well.

G. Does Your Whole Team Operate From The Same Playbook?

1. Employees

No matter how sophisticated or elaborate your security system and data protection technology, you need humans (employees) to implement it. There are four ways your employees are essential pieces to your information security plan: (1) Employees make mistakes. Even the most sophisticated data protection system is useless if someone with authorized access inadvertently makes the information publicly available.[71] (2) Employees can be unaware. Data thieves can be sophisticated and dubious, making even an intelligent employee, if not on guard, capable of sharing valuable information. (3) Employees can be the thieves. Employees with authorized access to sensitive information can be motivated to use that information in unauthorized and harmful ways.[72] (4) Employees are people with sensitive personal information, which businesses keep in order to function efficiently. Businesses keep Social Security numbers, payroll information, birthdates, and addresses, often in the same place.[73] Furthermore, even

---

[71] A file containing the personal information of approximately 18,000 Ohio State University students was posted to the Internet by the employee of a third party vendor. Security precautions were written into the contracts with their insurance company and their vendors, but those security provisions were not followed. The Ohio State University – Office of Student Life Press Release, *Data Exposure – Security Alert*, 2009, http://www.studentlife.osu.edu/ dataexposure/ (last visited January 10, 2009). In October 2008, the Florida State Agency for Workforce Innovation accidentally posted the personal information of about 250,000 job-seekers in the state on a test server that could be accessed online. The information was available online for 19 days before "the state Department of Revenue came across it during 'routine work,' officials said." See Aaron Deslatte, *State agency put Social Security numbers of 250,000 job seekers online*, ORLANDOSENTINEL.COM, Dec. 3, 2008, http://blogs.orlandosentinel.com/ news_ politics/2008/12/state-agency-pu.html.

[72] On March 27, 2002, a disgruntled former employee of Global Crossing was charged with posting on the Internet the personal information (e.g., payroll information, Social Security numbers, birth dates, and residential addresses) of nearly 2,000 employees. This intentional breach was thought to be an act of vengeance following the employee's termination. See Simon Romero, *Ex-Global Crossing Worker Arrested by F.B.I.*, N.Y. TIMES, Mar. 28, 2002, available at http://query.nytimes.com/gst/fullpage.html?res=9E06E4D9113BF93BA15750C0A9649 C8B63&sec=&spon=&pagewanted=1.

[73] On December 11, 2008, a virus was detected on a computer at the University of North Carolina at Greensboro which allowed access to information used to process the institution's payroll, including included names, Social Security numbers, and routing and bank account information. See Steven Gilliam, *UNCG Discovers Security Breach; Employees Being Notified*, UNC-GREENSBORO NEWS, Dec. 15, 2008, available at http://www.uncg.edu/ure/news/stories/ 2008/dec/Security121508.htm.

those businesses which do not keep personal information about outsiders are keeping valuable personal information about employees. If the security of such information is breached, even unwittingly by an employee, the employer/business can be held liable.[74]

Employees need to be apprised of the security plan in place and understand the importance of its functioning. Employees may not be intuitively aware of how to keep information safe. Employees need to be trained, fully and frequently, on the mechanics of the data security system and the policies for a breach of such system need to be regularly enforced. A well-designed plan does very little to keep your company's valuable data secure if its implementation is in the hands of an untrained workforce.

2. Third Parties, Venders And Outsourcing

It is essential that businesses carefully select and continually manage third party vendors that are entrusted with sensitive business data. Every company in the United States is charged with the responsibility of following a standard of due care to protect its customer and business data. Moreover, the FTC has made it clear that businesses are responsible for protecting the security of the data they collect and keep, whether such data is in their custody or has been given to a third party vendor.

A recent consent decree issued on December 10, 2008 by the FTC regarding Premier Capital Lending, Inc. ("PCL") demonstrated the FTC's unwillingness to give a pass to a company whose information was breached while in the custody of a third party.[75] In this case, a

---

[74] In a recent case, the Michigan Court of Appeals affirmed a jury verdict for $275,000 in damages against a union where the union's treasurer brought home documents containing the name and Social Security number of members and the treasurer's daughter stole this information and used it to commit identity theft against union members. Bell v. Michigan Council 25, 2005 WL 356306 (Mich. App. Feb. 15, 2005). The court found that the union had a "special relationship" with its members and thus was negligent in failing to adequately safeguard their personal information. Notably, the court found the thieving of the information to be foreseeable, in part because the "crime of identity theft has been gaining momentum in recent years due to the accessibility of personal information," and that "the severity of the risk of harm in allowing personal identifying information to be…unsecured…is high." Id. at *14. Importantly, the court found that "it is the *potential* severity of the risk, *not* the *actual* risk encountered" that is considered in determining liability. Id.

[75] In the Matter of Premier Capital Lending, Inc., FTC Docket No. C-4241 (Dec. 10, 2008) (Final Decision and Order) (requiring the company to "implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of consumers' personal information. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondent [the company's] size and complexity, the nature and scope of its activities, and the sensitivity of the personal information collected from or about consumers."), available at http://www.ftc.gov/os/caselist/0723004/081216 pcldo.pdf.

hacker came in through the third party's system. The FTC asserted that PCL never visited the third party's facility or audited its computer networks on which the sensitive data would be stored. In just over a week, the hacker obtained consumer reports including the names, addresses, and Social Security numbers of about 400 consumers. The FTC charged PCL with violating the Commission's Standards for Safeguarding Customer Information Rule,[76] the Commission's Privacy of Consumer Financial Information Rule,[77] and Section 5 of the FTC Act.[78] The FTC found that "PCL failed to take reasonable steps to assess the [third-party's] procedures to handle, store, or dispose of personal information," and "never conducted, or directed the [third party] to conduct, an inventory…to determine what personal information related to PCL's customers" the third-party was storing.[79] As a result of PCL's failure to supervise and adequately audit its third party vendor, the FTC concluded that PCL, "failed to provide reasonable and appropriate security for [its] consumers' personal information."[80]

H. Is Your Company Prepared For Its Fail-Safe Plan To Fail?

Any comprehensive information security program must include policies for responding to a data breach. The way a company responds to a breach of its security system may determine the depth and breadth of the intrusion, the total loss incurred as a result of the breach, and the public response to the infiltration. The President's Identity Theft Task Force described having a plan in place before a breach occurs to be "critical in ensuring a proper response."[81]

Policies for responding to a breach must take into account the variety of ways a breach can occur. Responses should be commensurate with the degree of risk posed by the particular invasion. In formulating an appropriate response, institutions should consider aggravating factors that may heighten the risk of identity theft (e.g., unauthorized access to records that contain more than one kind of personally identifying information, such as names, addresses, and Social Security numbers listed together).[82] When developing a response protocol, a company should consider including procedures to address the following:

---

[76] The "Safeguards Rule," 16 C.F.R. Part 314, issued pursuant to the Gramm-Leach-Bliley Act, see supra note 13, applies to financial institutions and institutions which extend credit.

[77] The "Privacy Rule," 16 C.F.R. Part 313.

[78] 15 U.S.C. § 45(a).

[79] In the Matter of Premier Capital Lending, Inc., FTC Docket No. C-4241 (Dec. 10, 2008) (Federal Trade Commission Complaint), available at http://www.ftc.gov/os/caselist/0723004/081206pclcmpt.pdf.

[80] Id.

[81] See The President's Identity Theft Task Force Report, supra note 8.

[82] For example, an industry blog noted that personalized guest service has always entailed knowing the preferences of customers and then exceeding their expectations. This information is no longer a matter of managerial memory – hotels "now use complex relational database systems *(cont'd)*

- Assessing the nature and scope of the incident and pinpointing the exact information that has been accessed or misused (including, if possible, specifically which customers or groups may be affected and exactly what pieces of information were compromised);

- Notifying the appropriate division of federal, state or local law enforcement officials, and additionally the institution that maintains the accounts so that it can monitor the accounts for fraudulent activity (e.g., if debit card information was stolen, notify the banking institution);

- Launching the appropriate physical, technical, or administrative systems to quarantine the intrusion and preventing further access and loss (e.g., by closing accounts, taking certain systems "offline," or offering access to free credit monitoring for those individuals whose information was breached);

- Preserving all appropriate records, logs or other evidence, to aid in the recapture of information or prosecution of the infiltrator; and

- Notifying customers in accordance with the proper state breach security law(s), and setting up a call center or website (if the size of the breach warrants it) to instruct customers and to respond to questions and concerns.

CONCLUSION

In sum, companies must be devoted to protecting their information. Take an inventory of the personal information your business keeps in its files and computers. Reduce the amount of information that is kept, and keep only what you need. Lock up the information, both physically and electronically, to protect the information you keep. When disposing of any information you no longer need, do it in a safe manner. Create a policy to manage the security of your data and a plan to respond effectively and efficiently to data breaches. Be sure any third party vendors with whom you deal with have commensurate data protection standards and are bound contractually to keep your information safe. But most importantly, make sure you staff is trained on this plan.

(cont'd from previous page)

to store knowledge about their guests, such as the blend of their favorite whiskey, and the names and birthdays of their children. Hotel employees use this information every day in every department of the hotel, and they access the information using multiple applications that store the data in different databases each with different levels of security." See Marcus Bruninghaus, *Protecting Guest Data: Why Hotel Information Security Awareness Training is So Important*, THE ENTERPRISE INNOVATOR, Aug. 21, 2006, available at http://enterpriseinnovator.com/index.php. This level of personal information can potentially allow identity thieves to guess at passwords or successfully navigate password-reminder security questions. Even without financial information explicitly present, personal information stored in an unsecured way can be used by thieves.

Companies that develop comprehensive information security strategies -- and implement and routinely reevaluate them -- can significantly mitigate the risk of a data security breach (and the financial and goodwill costs associated therewith). If, despite those best efforts, a data breach still occurs, companies that understand the varying state, federal, and international legal obligations will be best equipped to respond rapidly and in a manner that restores the integrity of the information system and customer confidence.