

ON THE VERY IDEA OF COMPELLING BUSINESS SECRECY THROUGH THE LAW:
OBLIGATIONS AND IMPERATIVES REGARDING PRIVACY, BUSINESS DATA INTEGRITY
PRESERVATION, AND IDENTITY THEFT PREVENTION
KEVIN GOVERN*¹

ABSTRACT

Today, more than ever before in the history of modern commerce, businesses find themselves acquiring, using, and protecting personal and corporate identity information. At the same time, identity theft and identity-fraud crimes have “grown to epidemic proportions, [especially] theft of sensitive, non-public protected information.”² Consumers needing access to diverse goods and essential services increasingly turn over more and more identity data. Forbes Magazine has noted the existence of an increasingly acute market tension as “companies and the public sector grow more aggressive in gathering and using information,” while increasing the risk of identity theft and fraud.³ The biggest driver of information sharing – and current and future potential risk of breach - is cloud computing, “where the software is based somewhere else and retrieved over the Internet. With cloud computing, upfront costs are usually much less and new versions of software appear as easily as an update on a smartphone, so the product is never out of date.”⁴

Given the current risk environment, businesses are obligated to do their utmost to protect systems and ensure consumer confidentiality, partially by legal requirements for maintaining certain data as private, in effect creating legal obligation for, and protection of, “private secrecy.” A classic example of this used to be banking secrecy, especially but not exclusively in Switzerland.⁵ Unfortunately, even the prudent and vigilant business entities may still be susceptible to data-theft or other outside system intrusion. In this respect, sound corporate

*Associate Professor of Law, Ave Maria School of Law, and Law and Public Policy Instructor, California University of Pennsylvania. LL.M., 2004, University of Notre Dame School of Law; LL.M., 1995, The Judge Advocate General’s School, U.S. Army; J.D., 1987, Marquette University Law School; B.A., 1984, Marquette University (khgovern@avemarialaw.edu).

¹ Substantial portions of this paper have been adapted, and reprinted with permission, from the Chapter 12, Data Integrity Preservation and Identity Theft Prevention: Operational and Strategic Imperatives to Enhance Shareholder and Consumer Value by Kevin Govern and John Winn in Risk Management and Corporate Governance, Abol Jalilvand and A.G. Malliaris, eds., (2012) at 300 and an article by John Winn and Kevin Govern, *Identity Theft: Risks and Challenges to Business of Data Compromise*, 28 TEMP. J. SCI. TECH. & ENVTL. L. 49 (2009).

² Institute of Fraud Risk Management, *Critical Need for Certified Identity Theft Risk Management Specialists*, available at <http://www.tifrm.net/content.aspx?id=91>.

³ Kevin Allison & Michael Peel, *Devil in the Details: Why Personal Data are ever more open to Loss and Abuse*, FORBES at 45, Dec. 11, 2007.

⁴ Quentin Hardy, *Cutting Through The Cloud*, New York Times, September 22, 2013, http://www.nytimes.com/2013/09/23/technology/companies-that-spend-big-on-tech-face-a-glut-of-choices.html?_r=0

⁵ Aaron Kirchfeld & Elena Logutenkova, *Private Banks Leave Switzerland as End of Secrecy Hurts*, Bloomberg.com, June 30, 2013, <http://www.bloomberg.com/news/2013-06-30/private-banks-leave-switzerland-as-end-of-secrecy-hurts-profits.html>. The article further cites the erosion of legal protections of banking secrecy, inasmuch as “[a]greements with the U.K. and Austria to collect taxes on behalf of those countries on accounts held in Switzerland have been in force since January, and Switzerland is in talks with other European countries on taxing secret accounts. The country will join the international push against tax dodgers and help develop global standards allowing banks to share customers’ details to combat tax evasion.” *Id*

governance should include some degree of planning and preparation for worst-case scenarios. There are several fundamental questions that every business should consider in order to effectively prepare for a breach of cyber security and ensure the integrity of stored data, including legal obligation and liability, but going well beyond those obligations to practical business imperatives. For instance, in the event of a major system compromise, who bears the cost of system restoration or reimbursement? What about negative publicity, loss of goodwill, and lawsuits? What constitutes due diligence before and after a data-compromise? What steps should management consider post-breach? Considering the legal consequences to our business, customers, and other stakeholders, should we purchase cyber-insurance?

This paper seeks to provide answers to those questions, as well as to offer valuable suggestions for both individual private consumers and business entities on how to best protect electronic information. Part I of the paper addresses current infrastructure risks and the challenges associated with cyber-insurance underwriting. Further, Part II will attempt to summarize the increasingly complex legal and regulatory landscape inherent in preserving data integrity and preventing identity theft. Finally, Part III of this paper will address the concept of “due diligence” and emphasize the importance of post-breach best practices which seek to protect revenue streams and customer goodwill while minimizing business disruptions and legal liability.

PART I: THE CYBER-RISK CLIMATE AND CYBER INSURANCE

The Internet has been the greatest boon in history for interpersonal communications, international commerce, and, unfortunately, the perpetuation of criminal theft and fraud. In 2007, market-leader Microsoft Inc. announced in a “Data Privacy Imperative” that “as advances in technology simplify and accelerate the flow of information, concerns about the collection and use of personal data, widely publicized security and data breaches, and growing alarm about online fraud and identity theft threaten to erode public confidence in the computing ecosystem and digital commerce.”⁶

As businesses assess their operational as well as legal responsibilities, a culture of risk management should transcend mere risk mitigation and shareholder value. Jeffrey Liesendahl, CEO of Accertify, advises e-security is more than “cutting fraud losses and fraud-related complaints. It’s about increasing accuracy, efficiency, and productivity of fraud-fighting efforts so the issue doesn’t damage profitability, expansion plans, or brand reputation.”⁷ In assessing cyber threats confronting the U.S., the FBI notes threats to commerce as emanating from two distinct areas: “(1) [T]raditional criminal activity that has migrated to the Internet, such as fraud, identity theft, child pornography, and trade secret theft; and (2) Internet-facilitated activity, such as terrorist attacks, foreign intelligence threats, and criminal intrusions into public and private networks for disruption of theft.”⁸

⁶ Data Privacy Imperative: *Microsoft’s Approach to Helping Protect Personal Information in the Digital Ecosystem*, February 2007 at 1, available at <http://download.microsoft.com/download/c/0/d/c0ddb7d5-287d-4b65-88d4-c0ee1b94adbb/Microsoft%20Data%20Privacy%20Imperative.doc>.

⁷ Jeffrey Liesendahl, Washington Post, Media Planet: 2 Information Security Supplement, *Ask the Information Security Experts*, 8 (2009).

⁸ Federal Bureau of Investigation (“FBI”) Strategic Plan 2004–2009, at 16, available at <http://www.fbi.gov/filelink.html?file=/publications/strategicplan/strategicplanfull.pdf>.

The loss of private customer data to unauthorized third parties — such as Social Security numbers, credit card numbers, birth-dates, and other confidential information — presents a daunting set of challenges as well as legal obligations for affected businesses. Identity theft has been America’s “fastest growing crime” since at least 1989, and, although actual cost data is difficult to gauge, various studies estimate direct domestic losses to the U.S. business community at between 56 and 100 billion dollars per year.⁹ These rather staggering figures do not include significant additional tangential costs such as the criminal prosecution and incarceration of offenders.¹⁰

According to the Association of Certified Fraud Examiner’s (“ACFE”) 2006 Report to the Nation on Occupational Fraud, U.S. organizations lose an estimated five percent of their annual revenues due to fraud.¹¹ When applied to the estimated 2006 GDP, those losses added up to approximately \$653 billion.¹² Organizations with anti-fraud programs — such as fraud hotlines, internal audit departments, and anti-fraud training — lost approximately half as much as those without such programs.¹³

Identity theft, and the resulting aftermath of a stolen identity, costs private consumers over two billion dollars and one-hundred million hours of time each year. The Privacy Rights Clearinghouse, a nonprofit consumer organization, reported over eight million individual victims of identity theft in 2007 alone.¹⁴ Also reported that year were 900 business-related data breaches in the United States alone, involving the compromise of over 245 million records containing personal information.¹⁵ In just the past two years, hackers, disaffected employees, and other cyber criminals have compromised data networks at TJ Maxx/Marshalls, Barnes & Noble, Bank of America, Wells Fargo, Stanford University, Princeton University, The Veterans Administration, Fannie Mae, and the City of San Francisco.¹⁶ According to the Department of Justice, reports of data breaches increased even more dramatically in 2008, with 656 reported breaches, an increase of 47% over the preceding year’s total of 446.¹⁷ This includes a total of 35,691,255 stolen or otherwise compromised identities. According to that same study, only 2.4 percent of all breaches occurred while encryption or other strong protection methods were in use, and 8.5 percent of reported breaches had password protection.¹⁸ Considering the enormity of

⁹ See *Identity Theft: Is There Another You?* Joint Hearing before the House Subcommittees on Telecommunications, Trade, and Consumer Protection, and on Finance and Hazardous Materials, 106th Cong. 16 (1999), Serial No. 106–16, December 7, 2009. See also GAO-02-363 *Identity Theft: Prevalence and Cost Appear to be Growing*, March 2002, available at <http://www.gao.gov/new.items/d02363.pdf>.

¹⁰ *Id.*

¹¹ Association of Certified Fraud Examiners, *2006 ACFE Report to the Nation on Occupational Fraud and Abuse*, 8–9, available at <http://www.acfe.com/documents/2006-rttn.pdf> (2009).

¹² *Id.*

¹³ See e.g., *Managing the Business Risk of Fraud: A Practical Guide*, cited with authority on Corporate Governance Website, July 2008, <http://corpgov.net/news/archives2008/july.html>.

¹⁴ Privacy Rights Clearing House, *Reducing the Risk of Identity Theft*, <http://www.privacyrights.org/fs/fs17-it.htm>.

¹⁵ Privacy Rights Clearing House, *A Chronology of Data Breaches*, <http://www.privacyrights.org/ar/ChronDataBreaches.htm>.

¹⁶ *Id.*

¹⁷ The Identity Theft Resource Center (“ITRC”), Report Database 1/2/2009, at 1, 201, http://www.idtheftcenter.org/BreachPDF/ITRC_Breach_Report_2008_final.pdf.

¹⁸ *Id.*

these incidents, there is no way to be certain “how many other retailers, who might not be quite as careful, are already being breached.”¹⁹ As dependence upon data access — especially wireless applications — continues to grow, new vulnerabilities will be further exploited.

Cyber-crooks perpetrate criminal theft and fraud over the Internet to obtain goods, services, and cash impersonally while exploiting time lags in discovery and investigation. Cyber-crooks also seek out valuable non-ID specific business data including executive emails, engineering and marketing data, bid sheets, and trade secrets. In the financial services sector, the vast majority of credit card, debit card, and ATM transactions — even mortgage transactions — occur online in virtual anonymity without the risks normally associated with in-store, face-to-face transactions. Cyber-theft is usually non-violent, has high profit margins, and incurs little or no risk of detection or prosecution. In ideal circumstances, identity theft can go undetected for months — or may never be detected at all. The 2003–2004 breach at TJ Maxx/Marshalls, which compromised over 94,000,000 Visa and MasterCard accounts, remained undiscovered for nearly two years.²⁰

Journalist Sandra Block recently wrote about the insidious and persistent nature of such cybercrimes, noting their ability to haunt victims for months.²¹ At particular risk are young adults, or whom about 5.3 percent age eighteen to twenty-four self-identify as victims of identity theft within the past 12 months in 2007 (up from 4.5 percent in 2006) according to Javelin Strategy and Research.²² The same study also found that 3.7 percent of all adults were victimized, down from four percent a year earlier.²³ Yet, when only a single individual is victimized, the loss of private information is usually attributable to theft by another family member, friends, or “data-mining” via home waste (i.e. “dumpster-diving”), or scams such as data “phishing.” Out-of-pocket consumer costs in these instances rarely exceed one hundred dollars because the business community absorbs most individual account losses associated with consumer data-theft.²⁴ Federal consumer protection laws under Title 15 of the U.S. Code limit liability for most losses — such as unauthorized electronic fund and credit card charges — to a maximum of fifty dollars per account.²⁵ The Electronic Funds Transfer Act also limits consumer liability for unauthorized ATM or debit card transactions.²⁶ Of course, this does not take into account the difficulties, aggravations, and expenses entailed in canceling compromised accounts and activating new ones.

Despite the significant burdens placed on individual victims of cyber-theft, it is rare for the perpetrators to find themselves faced with sanctions. Although convictions for cyber-related

¹⁹ Evan Shuman, *Data Theft Began in 2005; Data Taken from 2003*, E-WEEK.COM, <http://www.eweek.com/c/a/Security/TJX-Data-Theft-Began-in-2005-Data-Taken-from-2003>.

²⁰ See Shuman, *supra* note 17. See also, e.g., Allison McGevna & Mike Levine, *Three Indicted in Largest Corporate Identity Theft Case in History*, (August 17, 2009), <http://www.foxnews.com/story/0,2933,540060,00.html>

²¹ Sandra Block, *Identity Thefts a Big Pain, But Protecting Yourself Needn't Be*, USA TODAY, February 6, 2007 at C1.

²² Javelin Strategy and Research Study, *U.S. Identity Theft Losses Fall*, Feb. 1, 2007, <http://www.privacyrights.org/ar/idthefts-surveys.htm#Jav2007>.

²³ *Id.*

²⁴ GAO, *supra* note 9, at 9.

²⁵ 15 U.S.C. §1643.

²⁶ 15 U.S.C. §1693g.

theft and fraud may carry substantial criminal penalties under existing statutes such as the False Identification Crime Control Act and the Internet False Identification Act, few law enforcement agencies have the time, expertise, or even inclination to pursue on-line criminals.²⁷ Because identity theft crimes take place in “cyber-space,” police must often coordinate with other state, federal, or even international agencies in what can easily become a cross-jurisdictional and diplomatic three-ring-circus. Even when jurisdictional issues are capable of resolution, normally only high-profile or careless offenders face actual criminal prosecution by federal, state, or local authorities.

Private consumers are not the only ones burdened by cyber-theft, as many businesses also have private and valuable information to protect. In many respects, businesses have become even easier targets for identity theft than private consumers. Almost anyone can obtain a business’ tax identification number (i.e. the business’ social security number). A merchant’s basic financial information, including back account numbers, may be known to hundreds of wholesale customers and suppliers. Data access can be exploited by numerous employees and such insider theft and fraud is often difficult to detect, especially when carried out by trusted individuals. Businesses virtually never review their own credit information for fraud and may not be as careful as they should be in shredding or disposing of documents. Few businesses ensure the bona-fides of their commercial waste shredding contractor and even fewer conduct background checks of in-house or contract cleaning staff.²⁸ Businesses are also slow to upgrade data security. One commentator noted that, in his experience, most retail data systems are “put together with baling wire and packing tape . . . as retailers move from dial-up or proprietary networks to open networks and wireless connectivity, the risks go up exponentially.”²⁹

In the business sector, however, data-compromises usually involve an in-house or organic information network.³⁰ Such business-specific data-breach operational risks may include:

Hundreds, if not thousands, of separate consumers, business partners, as well as other stakeholders. In addition to costs for indemnifying individual consumer accounts, business must also absorb indirect remediation expenses such as making contact with affected customers, coordination with credit report agencies, and assisting law enforcement. There may also be business disruption expenditures to upgrade compromised information systems and litigation expenses. Indirect remediation costs may easily exceed the costs attributable to consumer reimbursement alone.³¹

²⁷ False Identification Crime Control Act, Pub. L. No. 97-396, 96 Stat. 2009 (December 31, 1982); Internet False Identification Act, Pub. L. No. 106-578, 114 Stat. 3075.

²⁸ See Shuman, *supra* note 19.

²⁹ Shuman, *supra* note 19.

³⁰ U.S. Secret Service, *Identity Fraud Trends and Patterns: Building a Data-Based Foundation for Proactive Enforcement*, Center for Identity Management and Information Protection, 67 (October 2007), http://www.utica.edu/academic/institutes/ecii/publications/media/cimip_id_theft_study_oct_22_noon.pdf.

³¹ *National Security: Cyber Infrastructure Risk, Operational Risk Management*, November 22, 2009, <http://operationalrisk.blogspot.com>.

A Fall 2013 Wall Street Journal study found strong demand for cyberinsurance: 31% of companies already have policies, and another 39% are planning to buy in the near future.³² To deal with traditional risks such as fire, flood, and thefts, businesses purchase blanket or umbrella insurance policies. Unlike individual consumers who may purchase relatively low cost (and usually unnecessary) “identity theft” insurance, commercial identity theft and data intrusion coverage is quite expensive, and, in some instances, remains unavailable. In fact, insuring business losses associated with cyber-crime has been a singular challenge to the entire insurance industry worldwide, where less than a third of U.S. companies have cyber-indemnification for data-theft, hacking, business disruption, or customer reimbursement.³³

Because threats to IT systems change almost daily, predicting loss scenarios, the frequency of cyber-attacks, or victim financial outcomes on an actuarial basis are extremely difficult. It is generally conceded by IT professionals that one-hundred percent security is impossible to achieve and IT security is almost entirely reactive. In fact, “penetrate and patch” is the term most widely used in the cyber-security field.³⁴ Not surprisingly, even when available, cyber-insurance may incorporate a myriad of confusing definitions, pre-conditions, limitations, and exclusions. Premiums for even small and mid-size businesses often begin at ten thousand dollars, and rapidly escalate to a point at which they rival the cost of predicated losses. Deductibles are also high, sometimes only beginning coverage after the first twenty-five thousand dollars in documented losses.³⁵

Some policies mandate expensive third-party IT system audits, which, by necessity, allow unfettered access by strangers to proprietary data such as budgets, security, or trade secrets. Not surprisingly, most businesses have determined that preventative measures are a more efficient allocation of resources than cyber-insurance. When purchased, however, some cyber-insurance policies do cover legal and public relations expenses. In one instance, a cyber-risk insurer indemnified a policyholder for payments made to settle threats from a web-based extortionist.³⁶ Even the best cyber insurance policies, however, do not indemnify for lost customer trust and good will.

Certain industries which are particularly susceptible to cyber-theft have responded by developing their own specific defenses and procedures. A specific partial response to network vulnerabilities in the credit card industry is the Payment Card Industry Data Security Standard (“PCI-DSS”) initiated by Visa and MasterCard and even more recently by several other major credit card companies.³⁷ PCI-DSS requirements are part of a global network that requires participating merchants (or service providers) to establish and maintain rigorous standards

³² Gregory J. Millman, *Cyberinsurance: A Buyer’s Guide*, Wall Street Journal, September 12, 2013, <http://blogs.wsj.com/riskandcompliance/2013/09/12/cyberinsurance-a-buyers-guide/>

³³ Russ Wiles, *Cybercrime Insurance Growing*, ARIZONA REPUBLIC, September 15, 2004, <http://www.azcentral.com/arizonarepublic/business/articles/0915insure15.html>.

³⁴ David Maynor, *Why the “Penetrate and Patch” Idea is not only Great, but also Essential*, Errata Security (Apr. 21, 2008), <http://erratasec.blogspot.com/2008/04/why-penetrate-and-patch-idea-is-not-only.html>.

³⁵ Dan Briody, *Full Coverage: How to Hedge your Cyber Risk*, INC. COM, (April 1, 2007), <http://www.inc.com/magazine/20070401/technology-insurance.html>.

³⁶ 2006 CSI/FBI Computer Crime and Security Survey, http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf.

³⁷ PCI Security Standards Council, *The Prioritized Approach to Pursue PCI-DSS Compliance*, (March 31, 2009) https://www.pcisecuritystandards.org/education/docs/Prioritized_Approach_PCI_DSS_1_2.pdf.

related to network security, encryption, and access controls. PCI-DSS also requires continuous monitoring and testing of system vulnerabilities, including wireless networks. Merchant compliance may be validated by third-party industry-certified auditing terms, self-assessment for small merchants, or network scanning.³⁸

PART II: IDENTITY THEFT AND THE CYBER-LAW LANDSCAPE

In light of substantial media coverage of identity theft, especially upon individual consumers, the cyber-law regulatory climate has changed substantially. Virtually all states have new “information privacy” laws on their books. And while most other new state legislation focuses upon criminal actors, penalties, and restitution (following California’s lead), at least 44 states have also enacted customer notification laws.³⁹

In the federal sector, the focus has shifted somewhat from criminal enforcement to regulation. The Federal Trade Commission (“FTC”) in particular has imposed heavy fines for rule violations and requires affected businesses to self-report data breaches. In November of 2004, the FTC filed a civil enforcement action against Nationwide Mortgage for its failure to protect private mortgage data under the Gramm-Leach-Bliley (“GLB”) Act Safeguards Rule.⁴⁰ Sunbelt Lending Services was cited the next year for similar violations.⁴¹ In 2005, the FTC held that BJ’s Wholesale Club created unnecessary risks by: (1) storing information longer than 30 days; (2) allowing anonymous employee access to consumer accounts; (3) failing to encrypt data; (4) failing to secure wireless access portals and; (5) failing to detect intrusions or conduct follow-up security investigations.⁴² As part of the settlement in this case, BJ’s agreed to allow FTC supervision for 20 years and third-party verification of security procedures. BJ’s was also forced to write-off sixteen million dollars in claims for reimbursement from related fraudulent credit card purchases.⁴³ Both of these cases indicate the level of precaution a business entity must take in order to protect electronic data, at the risk of paying the expenses of potential fraudulent misuse of that information.

Another important challenge for businesses to consider is the risk of class action lawsuits by disaffected and angry customers. Even in light of recent limiting legislation, including the Class Action Reform Act of 2005 (a.k.a. Class Action Fairness Act)⁴⁴, identity theft victims are probably much more likely than other litigants to share a jurisdictional “commonality of issues” requirement.⁴⁵ For large businesses especially, consumer losses from data-theft could easily exceed the five million dollar threshold, triggering exclusive federal jurisdiction for class

³⁸ *Id.*

³⁹ State Security Breach Notification Laws, National Conference of State Legislatures (“NCSL”), <http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm>.

⁴⁰ FTC Website, <http://www.ftc.gov/os/caselist/0423153/0423153.htm>

⁴¹ In re: Sunbelt Lending Services, FTC File No.:042 3153, January 7, 2005.

⁴² Thomas Claburn, *BJ’s Wholesale Club Settles FTC Data – Protection Complaint*, INFORMATION WEEK, June 26, 2005.

⁴³ Federal Trade Commission: In the Matter of BJ’s Wholesale Club, Inc. File No. 042 3160, *Analysis of Proposed Consent Order to Aid Public Comment*, <http://www.ftc.gov/os/caselist/0423160/050616anal0423160.pdf>.

⁴⁴ Class Action Fairness Act, Public Law 109–2, 119 Stat. 4 (2005).

⁴⁵ Federal Rule of Civil Procedure 23(a)(2) lists “questions of law or fact common to the class” as a prerequisite to bringing a class action.

actions.⁴⁶ In addition to extensive litigation costs, class actions also expose businesses to intrusive and disruptive pre-trial discovery processes, including the possibility of punitive or even trebled damages.

In this complex and dangerous environment it is therefore of critical importance to be aware of the most important federal laws affecting business and industry interests. A lack of understanding about current regulation could result in a heavy fine, in addition to the loss of customer trust and the creation unnecessary risks for the business' financial future. The following is a brief overview of relevant and evolving identity theft and cyber laws.

Identity Theft and Assumption Deterrence Act (“ITADA”)

Primary among cyber-related federal criminal statutes is the Identity Theft and Assumption Deterrence Act of 1998 (“ITADA”).⁴⁷ The ITADA distinguishes identity theft from other crimes such as wire fraud by encompassing theft of data and mandating significant fines and imprisonment, even for certain first offenders. The ITADA encompasses businesses or persons that seek access to personal records via banks, state and federal agencies, or insurance companies. Federal criminal jurisdiction, however, requires an underlying felony (such as fraud or conspiracy) and must involve an “identification document” that either: (a) is purportedly issued by the United States, (b) is used or intended to defraud the United States, (c) is sent through the mail, or (d) is used in a manner that affect interstate or foreign commerce.⁴⁸

Fair and Accurate Credit Transactions Act of 2003 (“FACTA”)

The Fair and Accurate Transactions Act of 2003 (“FACTA”)⁴⁹ established a national fraud detection system to preempt fraud and theft as early as possible with or without subsequent law enforcement investigation. The final rules were effective January 1, 2008. They require financial institutions and creditors to develop and implement an Identity Theft Prevention Program (“ITPP”) to mitigate the risk of identity theft from customer accounts.⁵⁰ The compliance deadline was May 1, 2009. Approximately two million financial institutions, credit unions, and creditors had until May 1 to adopt security updates to their ITPPs.⁵¹

Due to FACTA, a consumer may alert all three major credit reporting agencies of purported criminal misuse of financial data or accounts via phone or email. FACTA also led to the creation of the well-known “free” annual credit report regime, additionally requiring mortgage lenders to provide actual FICO credit scores (not just credit account data) if that score could be used to determine interest rates for home loans.⁵² For additional consumer protection, FACTA also mandates that merchants leave off all but the last five digits of credit card numbers on store receipts. It also established a nationwide fraud alert system to “red flag” suspicious

⁴⁶ Office of the Clerk, U.S. House of Representatives, 105th Congress, Second Session, March 5, 1998. http://commdocs.house.gov/committees/judiciary/hju59921.000/hju59921_cf.htm.

⁴⁷ 18 U.S.C. §1028(a)(7).

⁴⁸ *Id.*

⁴⁹ Fair and Accurate Credit Transactions Act of 2003 (FACT Act or FACTA, Pub. L. 108-159).

⁵⁰ *Id.*

⁵¹ *Id.*

⁵² *Id.*

requests for consumer data and allow military personnel to “freeze” credit files while they are deployed overseas.⁵³ While individual consumers may not have the sophistication or wherewithal to perform a detailed red flag approach, one suggested corporate strategy from the Jefferson Wells Corporation recommends the following:

KEY ACTIVITIES

Phase 1: Perform an IT risk assessment: Analyze the current environment for risks, including redundancies, inefficiencies, and insufficient and nonexistent controls. Identify current process and procedures related to identity theft and incident response.

Phase 2: Develop the appropriate identity theft program: Set up a framework and integration plan with the participation of senior leadership. Create a mitigation plan for identity theft risks, develop or update security policy and procedures, and create a security awareness program.

Phase 3: Implement the policy and procedures: Execute mitigation plan for identity theft risks and train organization on identity theft and security awareness program.

Phase 4: Perform regular review and analysis of identity theft program: Update risk assessment related to identity theft and re-evaluate legislation and modify policy and procedures to reflect requirements.

KEY RESULTS

Phase 1: Risk assessment

Phase 2: Identity theft policy and procedures, mitigation plan, implementation plan, and documented security awareness program

Phase 3: High-performing identity theft process

Phase 4: Update risk assessment policy and procedure.⁵⁴

Consumer “red flags” include actual fraud alerts from a reporting business that has identified either a data-breach, unusual patterns in credit usage, suspicious documentation, credit usage after long periods of inactivity, known mail drop addresses, or other anomalies.⁵⁵ FACTA enables consumers to place either an “initial” alert or “extended” alert to prevent credit grantors from opening new accounts. An “initial alert” is for individuals who suspect they are victim of an ID theft, while an “extended alert” are for those individuals who are confident they have been victimized and have filed a police report. The extended alert remains in place for up to seven years. As part of the extended alert package, credit agencies must also exclude the consumer’s name from pre-screened credit or insurance offers for five years. A third option is available to members of the U.S. military, who may also place an “active duty alert” during active duty or assigned when they are assigned to service away from the usual duty station.⁵⁶

⁵³ FTC, *Agencies Issue Final Rules on Identity Theft Red Flags and Notices of Address Discrepancy*, (October 31, 2007), <http://www.ftc.gov/opa/2007/10/redflag.shtm>.

⁵⁴ Identity Theft “Red Flag” Rules - Compliance may save money and your reputation, Jefferson Wells, 2009, 1 <http://files.shareholder.com/downloads/MAN/0x0x319886/87c56829-0434-458d-9826-75ea0c76a4cc/IdentityTh2.pdf>

⁵⁵ FACTA §§114, 335

⁵⁶ 15 U.S.C. §1681c

According to FACTA, not only must businesses shred documents containing employee data, but those which supply or facilitate consumer credit must also secure or destroy consumer information. The so-called “disposal rule” requires reasonable and appropriate destruction of all information derived from a consumer credit report before disposal. Failure to comply with destruction requirements (i.e. shredding) may be charged penalties of up to \$2,500 per violation.⁵⁷ Proper destruction prior to disposal may consist of burning, pulverizing, or shredding papers as well as electronic files. There is an implied obligation within the FACTA disposal rule to conduct due diligence in hiring or contracting out data disposal including audits, reference checking, and physical inspection of licenses or certificates.

Notable FACTA developments include the October 30, 2009 decision in the related case of order by U.S. District Court Judge Reggie B. Walton regarding the American Bar Association’s seeking to enjoin the FTC from applying its “Red Flags Rule” to practicing attorneys. Judge Walton granted the ABA’s motion in a partial summary judgment, holding that the FTC had exceeded its authority by interpreting the term “creditor” to include attorneys engaged in the practice of law. That same day, the FTC issued a press release announcing that it was delaying enforcement of the rule until June 1, 2010, a decision welcomed by the American Institute of Certified Public Accountants (“AICPA”).⁵⁸

The AICPA has filed a lawsuit against the Federal Trade Commission challenging the applicability of the “Red Flags Rule” to Certified Public Accountants. The lawsuit follows on the heels of FTC’s recent decisions to delay the enforcement of the rule for the fourth time.⁵⁹ The rule, promulgated by the FTC in November 2007 to comply with the Fair and Accurate Credit Transactions Act of 2003, requires financial institutions and creditors to develop and implement written identity theft programs to help identify, detect and respond to patterns, practices or specific activities — known as “red flags” — that could indicate identity theft. It was originally set to take effect on November 1, 2008, but after the latest extension, it became effective June 1, 2010.

Fair Credit Reporting Act (“FCRA”)

Victims of identity theft may also bring legal action against businesses under the Fair Credit Reporting Act (“FCRA”).⁶⁰ FCRA requires reporting businesses and agencies to adopt reasonable procedures to maintain and report consumer data with confidentiality, accuracy, relevancy, and reasonable security. Credit reporting businesses must ensure “reasonable procedures to assure maximum possible accuracy of the information concerning the individual about whom the report relates.”⁶¹

Consumer victims may sue for willful or negligent failure to verify the accuracy of disputed information or correct inaccurate information resulting from a stolen identity.

⁵⁷ FACTA §216

⁵⁸ American Bar Association v. FTC C.A. No. 09 1636 (RBW) October 20, 2009.

⁵⁹ *FTC Extends Deadline for “Red Flags” ID Theft Rule*, WEBCPA, November 2, 2009, <http://www.webcpa.com/news/FTC-Extends-Deadline-Red-Flags-ID-Theft-Rule-52277-1.html>.

⁶⁰ Fair Credit Reporting Act (FCRA), 15 U.S.C. §1681.

⁶¹ *Id.* at §1681e(b).

Consumers who report errors or fraudulent transactions are entitled to a “reasonable investigation” by the reporting business and an expectation that discovered errors will be corrected and reported back promptly. The statute provides for attorney’s fees and punitive damages for willful violations under the act. Under FCRA, victims of identity theft may authorize law enforcement agencies to obtain their credit reports and other records without the necessity of obtaining a subpoena at no additional cost. FCRA, however, imposes a two-year statute of limitations that begins when an inaccurate disclosure or report is filed, not when the consumer actually becomes aware of the inaccuracies.⁶²

Similar to FACTA, the FCRA also includes a “disposal rule” requiring any business that has access to or which utilizes consumer reporting information (usually credit reports) to dispose of this sensitive information properly. The FCRA disposal rule is broader than the FACTA disposal rule however and encompasses any company that compiles, sells or purchases any reports containing private personal or medical information. This includes employment agencies, banks, private investigators, landlords, auto dealers, insurance agents, claims adjusters, and others. This particular disposal rule applies to the disposal of information in any format, requiring it to be done using a method which renders the documents or information unreadable or incapable of reconstruction.

Gramm-Leach-Bliley Act (“GLBA”)

Additional consumer credit information safeguards for financial institutions are found in the Gramm-Leach-Bliley Act (“GLBA”) of 1999. GLBA instructs eight federal regulatory agencies and the states to administer and enforce the Financial Privacy Rule and the Safeguards Rule, to ensure the financial institutions prevent unauthorized disclosure of consumer financial information. Within the category of unauthorized disclosure is fraudulent access, a crime which financial institutions are instructed to prevent by implementing appropriate policies, procedures, and controls. Also known as the Financial Services Modernization Act of 1999, GLBA defines financial institutions as a “business significantly engaged in providing financial services or products for personal, family, or household use.”⁶³ This encompasses both traditional banks and credit unions, but also includes check-cashing and payday loan services, non-bank lenders, real estate appraisers, tax preparers, debt collectors, financial advisors, and insurance agents and brokers. GLBA prohibits “pretexting” by identity thieves or others seeking consumer data via financial institution or other listed quasi-financial institutions.⁶⁴

Right to Financial Privacy Act (“RFPA”)

The Right to Financial Privacy Act of 1978 (“RFPA”) falls under the auspices of the Federal Deposit Insurance Corporation (“FDIC”) and targets industrial loan companies, trust companies, saving associations, building and loan companies, credit unions and consumer finance institutions.⁶⁵ RFPA creates statutory Fourth Amendment protection for personal bank records by stating that:

⁶² TRW Inc. v. Andrews 122 S. Ct. 441 (2001).

⁶³ Gramm-Leach-Bliley Act, Pub. L. 106-102, 113 Stat. 1338 (1999).

⁶⁴ 15 U.S.C. §§6821, 6823

⁶⁵ Right to Financial Privacy Act (“RFPA”), 12 U.S.C. §3401 (1978).

No government authority [state or federal] may have access to or obtain copies of, or the information contained in the financial records of any customer from a financial institution unless the financial records are reasonably described and:

- 1.) the customer authorizes access;
- 2.) there is an appropriate administrative subpoena or summons;
- 3.) there is a qualified search warrant
- 4.) there is an appropriate judicial subpoena; or
- 5.) there is an appropriate written request from an authorized government authority.⁶⁶
- 6.)

In addition, RFPA prohibits banks and other covered entities from requiring customers to release financial records as a condition of doing business and mandates banks provide customers with access to records of all disclosures made to third parties.⁶⁷

Health Insurance Portability and Accountability Act (“HIPAA”)

Health care systems are extremely dependent upon computer-based or electronic medical records. Medical staff and other users are also heavy users of hand-held data units, laptops, home-computer links, smartphones, electronic table devices, smart cards, USB “flash drives,” and as well as other emergent technology. Medical data is transmitted and stored among a myriad of computerized patient record networks. Doctors and others are moving very rapidly to paperless “E-Prescribe” systems linking them directly to pharmacies via laptops and hand-held wireless devices such as smartphones and tablets.

Healthcare networks implement varying security systems, practices, and policies but within the context, all “covered entities” that collect or retain private health information in paper or electronic form must comply with privacy provisions of HIPAA of 1996.⁶⁸ HIPAA, which is administered by the U.S. Department of Health and Human Services (“HHS”), establishes nation-wide security standards for electronic health care information. This so-called HIPAA “security rule,”⁶⁹ requires all covered entities to be compliant with specific administrative, technical, and physical security standards and procedures for electronic data. HIPAA rules apply not only to doctors, clinics, hospitals, pharmacies, and laboratories, but may also apply to certain collection agencies, health insurers, and lawyers. HIPAA rules also apply to any businesses that maintain self-insure employee health care plans.

Under HIPAA, cyber-data is labeled as “electronic protected health information” or “EPHI.”⁷⁰ EPHI is of particular value to identity thieves because health-care data is

⁶⁶ *Id.*

⁶⁷ *Id.*

⁶⁸ Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), Pub. L. 104-191, 110 Stat. 1936 (1996) (as amended).

⁶⁹ U.S. Dep’t of Health and Human Services, 45 Code of Federal Regulations (CFR) Part 160 — General Administrative Requirements, and 45 CFR Part 164 — security and Privacy (2009).

⁷⁰ *See* HIPAA, *supra* note 68.

truly the “mother-lode” of private information. Included in the category of EPHI are names, addresses, birthdates, Social Security numbers, insurance information, bank and credit card data, and records of past and present medical treatment. HIPAA also requires covered entities to only do business with secondary organizations that also adequately and appropriately safeguard EPHI. A more detailed discussion of HIPAA’s complex requirements is outside the ambit of this analysis — but like any data loss — the consequences of medical identity theft, besides direct financial costs, include negative publicity, loss of customers, and potential civil liability.

Health Information Technology for Economic and Clinical Health Act (“HITECH”)

The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, was signed into law on February 17, 2009, “to promote the adoption and meaningful use of health information technology.”⁷¹ Subtitle D of the HITECH Act addresses the privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules. It mandated that all “business associates” of caregivers must also come into compliance with the same administrative, technical and physical security standards protecting electronic protected health information within covered healthcare entities. Also, for the first time, third-party business associates risk the same civil and criminal penalties for privacy violations as faced previously by covered entities alone.⁷²

Section 13410(d) of the HITECH Act, which became effective on February 18, 2009, revised section 1176(a) of the Social Security Act (the Act) by establishing:

- Four categories of violations that reflect increasing levels of culpability;
- Four corresponding tiers of penalty amounts that significantly increase the minimum penalty amount for each violation; and
- A maximum penalty amount of \$1.5 million for all violations of an identical provision.⁷³
-

It also amended section 1176(b) of the Act by:

- Striking the previous bar on the imposition of penalties if the covered entity did not know and with the exercise of reasonable diligence would not have known of the violation (such violations are now punishable under the lowest tier of penalties); and
- Providing a prohibition on the imposition of penalties for any violation that is corrected within a 30-day time period, as long as the violation was not due to willful neglect.⁷⁴

⁷¹ Health Information Technology for Economic and Clinical Health Act (HITECH Act). Title XIII of the American Recovery and Reinvestment Act of 2009 (Pub.L. 111–5), <http://www.gpo.gov/fdsys/pkg/BILLS-111hr1enr/pdf/BILLS-111hr1enr.pdf>.

⁷² Kevin Govern and John Winn, *HITECH Ratchets Up HIPAA Accountability* (January 11, 2010). Modern Medicine, January 2010. <http://www.modernmedicine.com/modern-medicine/news/modernmedicine/modern-medicine-feature-articles/hitech-ratchets-hipaa-accountab>

⁷³ HITECH Act Enforcement Interim Final Rule, HHS Health Information Privacy Website, 2009, <http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html>.

⁷⁴ *Id.*

On November 30, 2009, the regulations associated with the new enhancements to HIPAA enforcement took effect, such that the HITECH Act requires “HIPAA covered entities to report data breaches affecting 500 or more individuals to HHS and the media, in addition to notifying the affected individuals.”⁷⁵ This subtitle extends the complete Privacy and Security Provisions of HIPAA to” business associates of covered entities, to include the extension of newly updated civil and criminal penalties to business associates [and t]hese changes are also required to be included in any business associate agreements with covered entities.”⁷⁶

Foreign Legal Requirements – The European Example

While largely beyond the scope of this paper, modern business will likely involve overseas transactions, investments, clients, and patients. The words “cloud computing” never appeared in a 119-page digital privacy regulation introduced in Europe in 2012, but now does in 2013.⁷⁷ Journalist Danny Hakim has quoted Viviane Reding, the European Commission’s justice minister, having said that she wanted to see “the development of European clouds” certified to strict new European standards, promoted “by making sure that data processed by them are only stored in clouds to which E.U. data protection laws and European jurisdiction applies.”⁷⁸

What are the ramifications of EU or other national or regional governmental entities creating such new obligations? Cameron F. Kerry, the general counsel of the United States Commerce Department, recently reflected that: “It would be a sad outcome of the surveillance disclosures if they led to an approach to Internet policy-making and governance in which countries became a series of walled gardens with governments holding the keys to locked gates.”⁷⁹ Kerry went on to also opine “that is where we will end up if all data has to stay on servers located in the nation in which a citizen lives or where a device is.”⁸⁰ In his view, the regulation might restrict the flow of information among citizens, as is the case in China with

⁷⁵ *HIPAA/HITECH Enforcement Action Alert*, The National Law Review, Morgan, Lewis & Bockius LLP, March 22, 2012, <http://www.natlawreview.com/article/hipaahitech-enforcement-action-alert>.

⁷⁶ Press Release, *HHS Strengthens HIPAA Enforcement*, HHS Website, last updated May 7, 2011, <http://www.hhs.gov/news/press/2009pres/10/20091030a.html>

⁷⁷ Danny Hakim, *Europe Aims To Regulate The Cloud*, New York Times, October 7, 2013, <http://www.nytimes.com/2013/10/07/business/international/europe-aims-to-regulate-the-cloud.html>, citing with authority Proposal for A Regulation Of The European Parliament And Of The Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), European Commission (EC), January 25, 2012, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

⁷⁸ *Id.*

⁷⁹ U.S. Commerce Department General Counsel Cameron F. Kerry Keynote Address at the German Marshall Fund of the United States, US Commerce Department Website, August 28, 2013, <http://www.commerce.gov/news/speech/2013/08/28/us-commerce-department-general-counsel-cameron-f-kerry-keynote-address-german>, cited with authority in Hakim, *supra* note 74. In Kerry’s speech, he referred to the security disclosures in question regarding the National Security Agency (NSA), a direct allusion to the Edward Snowden disclosures. Relating to EU reaction to these disclosures, subsequent to Kerry’s speech *see, e.g.*, Jerin Mathew, Edward Snowden NSA Scandal: EU to Suspend US Data Sharing After Swift’s Interbank Messaging System Breach, International Business Times, September 25, 2013 <http://www.ibtimes.co.uk/articles/508882/20130925/edward-snowden-nsa-scandal-swift-tftp-eu.htm>

⁸⁰ *Id.*

barriers that are called the Great Firewall. “The digital world does not need another Great Firewall — in Europe or anywhere else.”⁸¹

PART III: OPTIONAL AND REQUIRED SAFEGUARDS FOR BUSINESSES

As recently highlighted in an editorial of the New York Times:

Most Internet users know that Web sites and advertisers monitor what they do online and use that information to pitch products and services. What’s not as well known is that these companies can track individuals as they move between devices like personal computers, cellphones and tablets. This type of “cross-device” tracking raises significant privacy concerns because most users are simply unaware that it is taking place.⁸²

Good business data protection equates to good preservation and promotion of customer and shareholder value, consumer confidence, and operational efficiency, not just compliance with domestic and international laws and regulations. Any effort to ensure the integrity of on-line data requires an effective combination of administrative, physical, and technical safeguards. Access to data should always be limited to the absolute minimum number of persons with a valid need for access. Employees with access to data must be properly screened, trained, supervised, and disciplined as necessary. In the event of resignation, suspension, or termination of employees, Human Resources departments must be diligent to ensure that systems and infrastructure are firewalled from further access. Risks assessment must be uncompromising and include the possibility of audits of system administrator functions by trusted outside agents.

Working partnerships and similar business arrangements with third parties must be based upon a shared commitment to data privacy, safeguards, and systems oversight. Security policies must be created in accordance to the highest reasonably assessed risk. In this respect, pinching pennies is a poor business strategy if any significant system compromise yields a “zero” return on cyber-security. There is a wealth of best practices information available to business managers and leaders via the Internet Security Alliance (“ISA”).⁸³ ISA provides a 12-step security program for small businesses at no cost.⁸⁴ Similar secure networking information is available from the National Cyber Security Alliance (“NCSA”), the Chamber of Commerce, and the United States Federal Trade Commission.⁸⁵

Proper protection does not end at preventative measures. A business which believes it is facing a criminal compromise of IT data or systems should call their local police department immediately. The sooner law enforcement officials become involved,

⁸¹ *Id.*

⁸² Editorial Board, *Monitoring Your Every Move*, New York Times, October 10, 2013, A30, <http://www.nytimes.com/2013/10/10/opinion/monitoring-your-every-move.html>.

⁸³ Internet Security Alliance, *Articulating the Value of Cyber Security*, (2010), available at www.isalliance.org.

⁸⁴ *Id.*

⁸⁵ Chapter 12, *supra* note 1.

the more effective their efforts at assistance can be. In many instances, local police agencies may additionally seek the assistance of the FBI or U.S. Secret Service. Financial institution fraud (“FIF”) continues to be a significant “white collar crime” problem throughout the country.⁸⁶ Since 9/11, the FBI has refocused its FIF program and is now investigating higher-priority cases to a much greater degree. Large-scale mortgage fraud and identity theft operations, many perpetrated by organized criminal enterprises, also continue to plague the United States.⁸⁷

The Secret Service has concurrent jurisdiction with the Justice Department for financial crimes and primary jurisdiction for crimes involving financial infrastructure and bank payment systems. This includes both domestic and international access device fraud, theft of debit and credit information, identity theft, false identification, and computer fraud. As part of the USA PATRIOT Act of 2001, the Secret Service was mandated to establish a nationwide Electronic Crimes Task Force (“ECTF”).⁸⁸ The ECTF network coordinates with federal, state and local law enforcement agencies to prevent, detect, and mitigate threats to financial infrastructures.⁸⁹ The benefit of agencies at different levels sharing information can be seen in certain instances such as mail-related fraud, or the theft of information from the mail, where local authorities will coordinate their investigative efforts with the Office of the Postal Inspector at the federal level.

Proper communication procedure requires not only the notification of law enforcement agencies, but also the notification of those affected by the crime. Section 609(e) of the Fair Credit Reporting Act (“FCRA”) requires businesses to provide copies of transactions records to victims of identity theft (and law enforcement) upon request.⁹⁰ Victims of identity theft may in turn authorize law enforcement agencies to obtain records free of charge within 30 days of receiving the request in writing. There is no requirement for a subpoena under these circumstances as long as the agency in question has a victim’s written permission.⁹¹ Required records may include invoices, credit applications, or account statements. Businesses should be careful to avoid making matters worse by requesting victims or law enforcement agencies to provide affidavits or police reports before complying with such requests.

Further, a proper response to identity theft also requires communication with other businesses which may be impacted. Identity theft from one business frequently impacts other businesses, especially banks, credit card issuers, and credit reporting agencies. For this reason, it is critical that every business that may need to monitor a customer’s accounts (for subsequent fraudulent activity) be notified as soon as possible.

⁸⁶ Internal Revenue Service, *Financial Institution Fraud- Criminal Investigation (CI): Overview*, (Nov. 03, 2009), available at <http://www.irs.gov/compliance/enforcement/article/0,,id=117522,00.html> (describing their program designed to combat Financial Institution Fraud as addressing “criminal violations involving fraud against banks, savings and loan associations, credit unions, check cashers, and stockbrokers.”)

⁸⁷ FBI Strategic Plan 204-2009 *supra* note 8, at 4.

⁸⁸ Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 84 Stat. 1116.

⁸⁹ *Id.*

⁹⁰ Fair Credit Reporting Act (“FCRA”), 15 U.S.C. §1681 et seq. (1978).

⁹¹ *Id.*

This is especially important if names or Social Security numbers are compromised, in which case all three major credit bureaus should be advised of the situation as soon as possible. A quick response and direct communication better prepares these agencies to facilitate customer requests for fraud alerts and account freezes.

Throughout the process of responding to an identity theft, businesses must be sure to protect any information which may be helpful for criminal prosecution. Safeguarding the evidentiary digital “chain of custody” for future prosecution of wrongdoers is often difficult. This process may require the assistance of a computer forensics specialist, or someone who is capable of preserving computer data in the proper format. Thus, when cases finally get to court, records will be properly admitted under the “business records” exception to the hearsay rules.⁹² One case from 2003 demonstrates what happens if this information is not properly protected. In that case, a cyber-extortionist threatened to expose customer data from 350,000 credit cards obtained from CD Universe Inc. In the subsequent investigation, law enforcement officials (including the FBI) admitted that failure to properly preserve the electronic evidence “virtually eliminated the possibility of prosecution.”⁹³

Despite past difficulties in criminal enforcement, advances in the process and law enforcement capabilities are still being made. For example, an important change in the prosecution of cybercrime and identity theft came about in October 2008 via the Identity Theft Enforcement and Restitution Act (“ITERA”).⁹⁴ This Act allowed for the prosecution of even more cybercrimes than previously allowed, eliminating the past requirement that prosecutors show the illegal activity caused at least five thousand dollars in damages before they can bring charges for unauthorized access to a computer. As this Act amends Title 18’s Crimes and Criminal Procedure,⁹⁵ it is now a felony, during any one-year period, to damage ten or more protected computers used by or for the federal government or a financial institution. The Act also directs the U.S. Sentencing Commission to review its guidelines and consider increasing the penalties for those convicted of identity theft, computer fraud, illegal wiretapping or breaking into computer systems.⁹⁶

Avoidance and Prevention

Due diligence measures address the problem of cyber-theft or identity theft before it happens, and may include some or all of the following practices:⁹⁷

- Compile a list of state, federal, and foreign laws and regulations affecting or applicable to your business.

⁹² FRE §803(6).

⁹³ Mike Brunker, *CD Universe Evidence Compromised*, ZDNET, June 8, 2000, http://news.zdnet.com/2100-9595_22-96132.html.

⁹⁴ The Identity Theft Enforcement and Restitution Act of 2008, amending Title 18, Part II, Chapter 232, § 3663 (2008).

⁹⁵ *Id.*

⁹⁶ *Id.*

⁹⁷ *See, e.g.*, Chapter 12, *supra* note 1.

- Develop policies, procedures, and training to ensure compliance with applicable rules and regulations.
- Review confidentiality agreements with business partners, IT vendors, and archive services (if applicable).
- Appoint a qualified and trusted employee as an information security officer.
- Set and enforce strict access and encryption policies including rules describing what data can be printed, emailed, or copied.
- Limit, monitor, or block employees from disclosing confidential information (or inadvertently downloading malware) via social networking and blogging sites.
- Strengthen password and authentication regimes via one-time password generation, smart-cards, or a combination of these technologies plus electronic access badges.
- Test systems to ensure they are able to detect and prevent intrusions and inappropriate usages.
- Consistent with legal requirements, contractual obligations, and corporate values, prepare contact lists of persons and entities (including credit reporting agencies) that should be notified in the event of a data breach.
- Ensure your corporate governance, including board members, are cognizant of your IT security planning. (Note: Sarbanes-Oxley standards require that accurate reporting systems and sufficient internal controls are in place).⁹⁸
- Ensure HR departments document all employee security training.
- Promulgate a policy requiring employees to report lost or stolen laptops, smart-phones, and other PDA's immediately.
- Monitor reports of data-theft and other incidents via organizations such as the non-profit Identity Theft Resource Center.
- Audit janitorial, waste disposal, and shredding services to ensure compliance with applicable disposal rules.
- Develop a continuity plan to protect critical business processes in emergency or disaster scenarios (including plans for data-base failure or physical loss).
- Designate and train a post-incident/post-detection "Computer Incident Response Team" ("CIRT") composed of IT professionals and appropriate managers.
- Consider adding information security and privacy to your business or corporate code of conduct.

Post-Compromise Measures:

- Review state and federal disclosure and notification regulations.
- Ensure adequate information is provided to customers, law-enforcement, and other stakeholders regarding how the breach may affect them and what steps your organization is taking.
- Designate one member of the Computer Incident Response Team (CIRT) as primary point of contact (person and office) within your organization for information dissemination to customers, police, and press inquiries.

⁹⁸ Public Company Accounting Reform and Investor Protection Act of 2002, Pub. L. 107-204, 116 Stat. 745 (2002).

- Prepare an informative press release to reassure the public that appropriate measures are in place to minimize any disruptions to customers or service. Be sure to provide the same information via your home web-page.
- Notify customers promptly via mail that their private customer data may be compromised and advise them of the appropriate steps they should take to protect their accounts from further misuse, obtain refunds, etc.
- Keep affected customers and others updated as information develops or mitigation strategies are put in place.
- Consider engaging the services of a qualified IT consulting company to provide customers with professional ID monitoring and restoration services such as “TheftSmart” or “Lifelock” at no personal cost.⁹⁹
- File a complaint with the FTC using the online complaint form, the Identity Theft Hotline, or non-governmental Privacy Rights Clearinghouse to provide information that can help law enforcement officials across the nation track down identity thieves and stop them, and for referrals to other government agencies and companies for further action.¹⁰⁰

CONCLUSION

This survey of issues highlights some of the most pervasive threats to individuals and business entities in the 21st Century. In reviewing this assessment, managers and leaders should consider the need to integrate both preventative security and post-breach survivability into IT planning, and communicate their proactive strategies to their shareholders and consumers alike to build their confidence — as well as market confidence — in the soundness of their efforts. In other words, implement data-security prospectively, but don’t neglect strategic planning for worst-case scenarios, and keep a simultaneous focus on the security of day-to-day operations. As present and future opportunities for IT-based commerce grows, both private and governmental entities must also heighten their appreciation and anticipation of future infrastructure risks and the cyber-risk climate, and adapt corporate and public policies and laws not just to resist but to more effectively prevent and combat cybercrime and identity theft.

⁹⁹ Chapter 12, *supra* note 1.

¹⁰⁰ DEFEND: *Recover from Identity Theft*, Federal Trade Commission (FTC) Website, available at <http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/defend.html>. The FTC Website provides a link to the online complaint form at <https://www.ftccomplaintassistant.gov/>; it provides the FTC’s Identity Theft Hotline toll-free number as: 1-877-THEFT (438-4338); TTY: 1-866-653-4261; and provides the address to write to the Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.