



Identity Theft Security and Compliance
Issues for Business

An Identity Theft Loss Prevention, LLC Whitepaper



IDENTITY THEFT SECURITY AND COMPLIANCE: *ISSUES FOR BUSINESS*

Written by:

Frank R. Mitchell, CITRMS

Thomas Glanville, CITRMS

INTRODUCTION

In the past few years identity theft has grown from a little known concept into a household buzzword. What has been traditionally recognized as a consumer issue is now a critical concern for every business. Why business, you might ask? Isn't identity theft the unauthorized or illegal use of another *person's* information?

The truth is thieves are getting consumer information from businesses. As of June 19, 2008, the Privacy Rights Clearinghouse has documented that 229,441,775 records have been compromised from United States government agencies, businesses, schools, and other organizations since January 2005!¹ According to a Javelin Strategy & Research Survey published in 2008, the total one year amount of identity fraud in 2007 cost \$45 billion.

Every business manages personal, financial, medical, or business information in one form or another. Confidential and Sensitive Information is necessary for most business operations. However, there can be serious consequences for the company owners, executives, employees, contractors, and consumers if that information is lost or stolen. The results of a breach are often imposed fines and penalties, loss of customers, and potential class action lawsuits involving those who become victims of identity theft.

FEDERAL AND STATE LEGISLATION

The growing awareness of vulnerability to these security incidents, and the damages that have ruined the lives of the innocent victims, have federal and state regulators taking action. There are several laws that may impact businesses in the event of a loss or breach of information.

State Notification Laws. Currently 43 states have enacted laws regarding requirements for the notification of victims in the event of a loss or breach of information from a business. As a general rule, if your business has a loss or breach of information, then you have to notify the potential victims in writing within a "reasonable" period of time. According to the Ponemon Institute, in the event of a breach . . . 31% percent of your affected customers will terminate their relationship, 57% percent will lose trust and confidence in the company, 8% will file formal complaints (lawyers), 72% said there is a great chance they will become victims of Identity Theft.²

Common Law of Torts. "As a fundamental principle, even before reaching theories applicable to information security, parties are generally responsible under the common law of torts to use due care in handling the information regarding others."³ Businesses that do not take reasonable steps to protect information could be held civilly liable for criminal acts committed by others with the stolen information. This was the outcome of *Bell v. Michigan Council 25 of the AFSCME*, 2005 Mich. App. LEXUS 353(Mich. Ct. App. Feb. 15, 5005).

In addition to state laws, there are several federal statutes that expose businesses to civil and criminal liability for not taking appropriate measures to safeguard information. They include, but are not limited to:

The Identity Theft Assumption and Deterrence Act. In 1998, the Identity Theft Assumption and Deterrence Act defined identity theft as a crime. The Act criminalized the knowing transfer or use, without lawful authority, of "a means of identification of another person" with the intent to commit, or to aid or abet, any violation of federal law. 18 U.S.C. §1028(a)(7).

A "means of identification" is defined as: any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any –

- a) name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number; government passport number, employer or taxpayer identification number;
- b) unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
- c) unique electronic identification number, address or routing code;
- d) telecommunication identifying information or access device (as defined in section 1029(c))

If convicted under this statute, a defendant faces up to 15 years in prison if he obtained anything in value aggregating \$1000 or more during a 1-year period. 18 U.S.C. §1028(b)(1)(D).

The Federal Trade Commission Act. Under this Act, the Commission is empowered, among other things, to

- a) prevent unfair methods of competition, and unfair or deceptive acts or practices in or affecting commerce;
- b) seek monetary redress and other relief for conduct injurious to consumers;
- c) prescribe trade regulation rules defining with specificity acts or practices that are unfair or deceptive, and establishing requirements designed to prevent such acts or practices;
- d) conduct investigations relating to the organization, business, practices, and management of entities engaged in commerce; and
- e) make reports and legislative recommendations to Congress.

The Gramm-Leach-Bliley Act. The Gramm-Leach-Bliley Safeguard Rule requires financial institutions, and non-financial institutions significantly engaged in financial activities, to take steps to protect customer data. Violations of the subsections I and II under Title V are punishable by civil and criminal penalties. 15 U.S.C. §6823.

The Health Insurance Portability and Accountability Act (HIPAA). The Health Insurance Portability and Accountability Act obligate health care providers to safeguard personal and medical information. If health information is wrongfully disclosed the penalties may be

maximum fines up to \$250,000 and imprisonment with a maximum sentence up to 10 years. 18 U.S.C. §1177.

“The HIPAA rules also impose privacy and security obligations on virtually any employer that provides health care benefits to its employees, to insure that the medical information is protected appropriately and is not misused by the employer to make employment decisions about individuals.”⁴

The Fair and Accurate Credit Transactions Act (FACTA) The Fair and Accurate Credit Transactions Act states that consumer reporting agencies must maintain procedures to avoid improper disclosure of information. Anyone seeking information from a consumer report must identify themselves, certify their purpose for the information, and certify that they will not use the information for any other purpose. 15 U.S.C. §1681e. Furthermore, Red Flag revisions to sections 114 and 315 require financial institutions, creditors, and any business with “covered accounts” to implement an Identity Theft Prevention Program by November 1, 2008.

“Now there is a law with a provision going into effect this summer that says if you employ even one person- a nanny, a yardman- and you have their personal information because you are doing the right thing and paying social security taxes, you have to ‘destroy’ the information before you throw it away.”⁵

The Family Educational Rights and Privacy Act (FERPA). The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

WORKPLACE REQUIREMENTS

In regulated industries, there are specific codes within the laws mentioned above that require compliance. For every business, a common factor in the legislation is the requirement to make a “reasonable effort” to protect confidential and sensitive information. Where code may not specify what a “reasonable effort” is, recent court cases involving identity theft have defined it as the following:

1. The designation of an Information Security Officer.
2. A risk assessment of material internal and external risks to the security of confidential and sensitive information.
3. The design and implementation of a written Information Security Policy.
4. The implementation of a vendor management program.
5. Employees must be trained on security policies.
6. The evaluation and adjustment of the program in light of the results of testing and ongoing monitoring of the program.
7. A plan for security incidents.^{6,7}

INFORMATION SECURITY PROGRAM

While most business leaders feel pressure to comply with the law to avoid fines and penalties, information security itself is the more serious underlying issue. “Obviously, the best way to maintain consumers’ trust is to avoid a data breach in the first place with safeguards that will secure customer and employee data from loss or theft.”⁷ *“Ponemon Institute Research Report, 2008.*

Every business must have an Information Security Officer. If you currently do not have one, then designate someone to fulfill that roll. Any responsible member of senior management within an organization may be appointed as the Information Security Officer. In a sole proprietorship it automatically becomes the responsibility of the sole proprietor. Smaller businesses often designate an assistant, or an office manager. As businesses become larger in size, with several departments or facilities, the Information Security Officer often becomes part of a security team which may include executives or department heads from Human Resources, Technology, and Public Safety/Security.

Common Causes of Information Loss or Breach. To create an effective Information Security Program it is important to understand the internal and external threats to your business. Internal threats include poorly trained personnel, inadequate security measures, insufficient support from management, unsupervised third party providers, dishonest insiders, and inadequate IT systems. External Threats include hackers, organized crime, social engineers, and competitors.

Perhaps the greatest liability to any business is people. “From an organization’s perspective, people include employees, customers, third parties, and business partners. All of these people are vital to the organization’s survival and are privy to the organization’s information in varying degrees through different means. As a result, all of these people represent risk. Well aware that infrastructures and perimeters have been fortified, today’s sophisticated crooks no longer batter the fortress directly – they take a subtler approach through its people.”⁸ *Deloitte 2007 Global Security Survey: The Shifting Security Paradigm*

Behavioral, Operational, and Technological Information Systems. A common misconception is that identity theft is a technology issue. Companies spent a great deal of time and resources securing their networks but overlook other behavioral and operational concerns. “Criminals first gather personal information through low-tech methods such as stealing mail or workplace records, or ‘dumpster diving,’ or through complex and high tech frauds such as hacking and the use of malicious computer code.”⁹ *The President’s Identity Theft Task Force Report, April 2007.*

Information security programs and training must address the “human element” to get to the root of identity theft in the workplace. Employees, vendors, and consumers are vulnerable to pretexting, pharming, social engineering, and mistakes made due to laziness or complacency.

Third Party Consultants. Most businesses prefer to spend time and money on efforts that add to their bottom line. Compliance and information security are necessary evils that rate low on the agenda. However, the right third party consultant can bring a business up to speed quickly and efficiently.

When looking for a risk management consultant Tom Glanville, founder and CEO of Identity Theft Loss Prevention, LLC suggests that you consider the following:

- Often newly designated Information Security Officers have little or no background with information security issues. Many experienced Information Security Officers only address technology issues. Will the consultant train them to develop an Information Security Program that gets to the root of identity theft?
- Do they address behavioral, operational, and technological concerns in relation to identity fraud and theft?
- Do they complete processes with the Information Security Officer during training or do they just educate and leave the work for a later date?
- Is the Information Security Program customized for the scope of your business?
- Does the consultant offer a solution that addresses compliance *and* information security issues unique to your business?
- Can the Information Security Program be designed and implemented in a reasonable period of time?
- Is the solution cost effective? Does it allow for flexibility in daily business operations?

CONCLUSION

This white paper summarized some of the current state and federal legislation, compliance standards, information security issues and their impact on business. As public attention to information security breaches increase with media coverage of identity theft cases, the number of regulatory actions and litigation is likely to rise. It is critical that you prepare your business to reduce probability and mitigate loss in the event of an information breach.

ABOUT IDENTITY THEFT LOSS PREVENTION, LLC

Identity Theft Loss Prevention, LLC works with sole proprietors, small and mid-sized businesses to understand, create, and implement Information Security Programs addressing identity fraud and theft. Their *information* Compliance and Awareness Process is an entire system designed to address identity theft compliance requirements, and to assist business leaders in making a reasonable effort to safeguard information systems.

It is a behavioral, operational, and technological approach to assess and reduce the risk of fraud, theft, or loss during the collection, handling, storage, communication, transmission, transfer, and destruction of confidential and sensitive information in the workplace.



Identity Theft LOSS Prevention, LLC
7330 Turk Road
Ottawa Lake, Michigan 49267
Phone: (888) LOST MY ID
www.idtlp.com

REFERENCES

1. See A Chronology of Data Breaches available at <http://www.privacyrights.org>
2. *Ponemon Institute Research Report*, 2008.
3. *Not on My Watch – When are Companies Liable for Security Breaches of Their Information Systems*, By Thomas P. Vartanian, Mark Fajfar, and Robert H. Ledig, June 2005 | *Electronic Banking Law and Commerce Report*
4. See *Your Growing Exposure for Identity Theft Risks*, By Kirk J. Nahra, available at <http://www.bbb.org/securityandprivacy/download.asp>
5. *Identity Theft, New Law About to Send Shredding on a Tear*, By Mindy Fetterman. 2005 | *USA Today*
6. *Effective Security Practices Now a National Requirement*, By Kirk J. Nahra June 2005 | *Privacy In Focus*
7. *What Are a Company's Obligation's Regarding ID Theft?* By Howard W. Goldstien September 5, 2006 | *Business Crimes Bulletin*
8. *Deloitte 2007 Global Security Survey: The Shifting Security Paradigm*, Deloitte 2007
9. *The President's Identity Theft Task Force Report*, April 2007, p10.