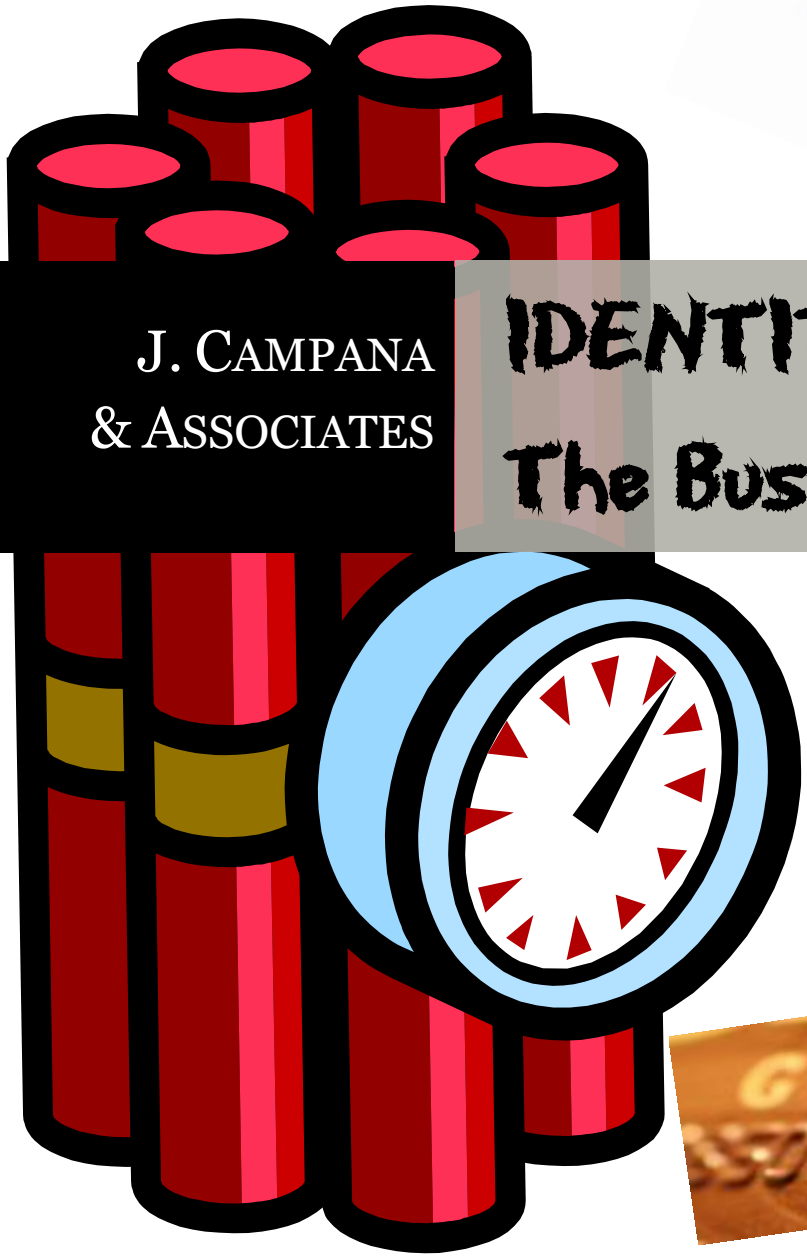
September 2006

J. CAMPANA
& ASSOCIATES

# IDENTITY THEFT:
# The Business Time Bomb





Identity Theft: The Business Time Bomb | Joseph Campana, Ph.D., CITRMS

## Table of Contents

**Forward**

During the last several years, I have met with hundreds of executives in various industries representing for-profit, not-for-profit, local and state governments, and the self-employed to discuss proven methods to manage and minimize a broad range of legal and business risks.

Three years ago we added a new expertise to our services: identity theft risk management. We have been building our experience in providing employers an affirmative defense against workplace identity theft through employee training and risk mitigation services for employees and customers. We have given hundreds of educational presentations as a public service to businesses, professional groups, service clubs, and numerous others on the risks of identity theft.

The trends we have observed during these interactions with hundreds of people include:

1. Few individuals and entities understand identity theft. Most people, including financial services professionals view identity theft as a form of simple financial fraud. Most people lack a basic understanding of how broad and insidious identity theft can be.
2. Although entertained and sometimes scared by our presentations, most people did not view identity theft as an immediate risk to them.
3. The majority of entities were either not aware or not concerned that they are subject to federal and state laws requiring them to safeguard non-public personal information. We conducted a study where we contacted businesses by telephone to explain identity theft laws. The majority of the businesses contacted expressed "no interest" or literally "hung up." Those to whom we spoke, generally took a defensive position.
4. The few who expressed a concern of being victimized did not respond by taking preventive action. Some expressed a sentiment that the government, not them, should solve the identity theft crisis. They called for more and tougher laws. Ironically, some of those who represented businesses were apparently in violation of federal laws that apply to businesses regarding the protection of non-public personal information.
5. Few individuals or entities understood that they have a major role in significantly reducing identity theft by following rather simple steps to insure privacy and security of non-public personal and business information.

The purpose of this publication is to address these misconceptions and issues through education. Our target audience is all employers and small businesses including the self-employed, local governmental entities, local not-for-profits, and certain individuals who may be covered by one or more laws. With this business focus, this article will not provide in-depth discussion on victimization, prevention, and resolution for individuals, which are topics that have been discussed elsewhere including in the literature cited throughout this publication.

Joseph E. Campana, Ph.D., CITRMS
Madison, WI
September 2006

## Introduction

Most everyone has heard of identity theft; yet unless you have been a victim, few people and businesses believe they are at risk.

The false sense of immunity to identity theft is indicative of a general misunderstanding of what identity theft is. It points to the need for education among businesses and consumers alike. The clever and amusing advertising by financial institutions, designed to maintain consumer confidence in banking and credit transactions, as well as the frequent coverage in the media of credit card and bank account fraud, together create a dangerous misconception about what identity theft is. Advertising and media most frequently portray identity theft as "existing account fraud," especially related to credit card fraud. Some experts eschew categorizing "existing account fraud" as identity theft because it diminishes the severity of true identity theft. "Existing account fraud" composed approximately one fourth of all the reported types of identity fraud and identity theft last year. It is the other 75% of identity theft crimes that devastates consumers, employees, business owners, their families, as well as the business entity itself.

For example, a recent news story reported a university employee who stole debit cards from dormitory mailboxes and made unauthorized charges to the cards. The thief was apprehended and charged with identity theft and other criminal offenses. The incident was widely publicized as identity theft. Technically, the crime involved mail theft, punishable under federal law, and credit card fraud. The effect of publicizing incidences like this one as identity theft leads to the common misconception that identity theft is synonymous with unauthorized use of a credit card. People who do not use credit cards, or who use extreme care and caution, feel immune and unknowingly remain vulnerable to much more complicated and dangerous forms of identity theft that do not involve finances or credit.

Even businesses think they are immune, despite the frequent and unfavorable publicity of security and privacy breaches by some of the "most trusted" names in business, government, and non-profits where profiles of customers, constituents, employees, vendors, donors, etc. have been reported to have been lost or compromised[1]. Federal and state laws require all entities, including your own, and certain individuals, to comply with privacy and security measures.

These laws require the implementation of policies and procedures through employee training on privacy and security of non-public personal information (NPI). Violations of these laws carry substantial penalties including imprisonment, and violations open entities to other legal risks and consequences. The wave of prosecutions and laws suits for violations was recently reported (1).

[1] ADP, Aetna, AFLAC, AIG, AllState, American Family Insurance, American Institute of CPAs, America Online, Red Cross, Ameritrade, AT&T, Bank of America, Beaverton School District, Blue Cross & Blue Shield, CitiFinancial, Department of Veterans Affairs, Diebold, Dollar Tree, Earnst & Young, Fedex, Fidelity Investments, Ford Motor Co., GMAC, H&R Block, Humana, ING, Marriott International, MCI, Moraine Park Technical College (Beaver Dam, Fond du Lac, & West Bend), OfficeMax, Progressive, Sam's Club/Wal-Mart, Sentry Insurance, University of Minnesota, Verizon, Wachovia, Wells Fargo, YMCA to name a few of the nearly 350 reported (3).

What's the purpose? To bring identity theft under control. Business identity theft is a growing problem and a substantial portion of identity theft can be traced to origins in the workplace (2).

**Statistics**

The statistics are disconcerting. Nearly 100 million consumers have had their identity profiles compromised since 2005 in approximately 350 "reported incidences" of privacy and security breaches by major financial, medical, educational institutions, governmental entities, and retailers (3). Some of the less publicized breaches are listed in the previous footnote. Think you are immune? How many of these entities have you done business with? It is reasonable to assume that many more unreported security breaches affect additional people and businesses each year.

Based on annual consumer complaints and surveys, the Federal Trade Commission (FTC) estimates there are about 10 million new victims of identity theft every year (4). Various independent sources estimate that each victim will devote on average 30 – 600 hours to restoring their identity, and they will spend on average $500 to $1,500 out of pocket, not including attorney fees, to resolve their crisis[2]. USA Today reported that victims of financial identity theft must resolve over $90,000 on average of unauthorized loans and credit resulting from the misuse of their identity (5). The Aberdeen Group estimated losses to the financial services industry to reach 2 trillion dollars worldwide in 2005 (6), while the FTC says the annual cost to businesses and consumers in the U.S. is nearly $60 billion.

An alarming figure to businesses is that as much as 70% of all identity fraud and identity theft originate from a place of business, an employer, or other entity (not-for profit; local, state, or federal government) (7).

Employers and businesses of all sizes, public and private, not only contribute significantly to the proliferation of identity theft, but these "entities" are required under federal and state legislation to implement measures, policies, procedures, and training programs to bring identity theft originating in the workplace under control. Violations of these laws carry hefty statutory fines as high as a $1,000,000 per occurrence; the prospect of class action lawsuits, which magnify the penalties by the number of class members; potential civil liability for victim losses; and in some instances the legislation provides for imprisonment of culpable business executives. These are serious penalties for any covered entity to face.

[2] The statistics vary widely depending on the agency or trade group that commissioned the study and on how the data is interpreted. Industry trade groups provide some of the lowest estimates, while FTC statistics tend to be higher. Some of the lower estimates appear to relate to "existing account fraud" rather than to the other more frequent and complex types of financial and non-financial identity theft. Regardless, even the lowest estimates of time and money spent restoring an identity would prove burdensome to the average person. With today's complex and busy lifestyles most people do not have 30 hours, and certainly not 600 hours, of discretionary time to handle an identity theft crisis on top of the stress and emotions of feeling personally violated by the crime.

Businesses and other entities as well as consumers must realize these strict penalties exist because (a) identity theft is a serious crime affecting tens of millions of people and (b) employers and businesses are often the source of the NPI information obtained by the thieves.

**What is identity theft?**

Simply and broadly stated, identity theft is the misuse of personal or business identifiers by an imposter for their advantage, which may be financial, non-financial, or both.

Unauthorized uses include obtaining credit; goods; services; money; property; employment; government, medical and other benefits; or to commit crimes.

Personal identifiers include name, date of birth, Social Security number, and many others including account and biometric information.

Business identifiers include the business name and federal tax ID, business indicia, and other business information including account information and the personal identifiers of management and employees, which could be used to falsely authenticate a business identity.

In general, these personal and business identifiers are broadly defined by law and protected in the legislation, which will be discussed in a subsequent section of this report.

A name and federal identifier can be misused to commit a wide variety of identity theft crimes that even the savviest business or consumer would not detect for months or years until something radical occurs to them personally, such as an arrest, denial of insurance or benefits, an IRS audit, denial of credit, etc. The same applies to businesses; however, business identity theft may be more difficult to detect.

The most devastating identity theft crimes include (a) establishing "new" (non-existing) credit, bank, phone and utility accounts in a victim's name, which account for approximately 25% of all reports (as stated previously, "existing account fraud" also accounts for about 25%) and (b) non-financial uses. Non-financial identity theft, the most insidious, comprises the remaining 50%.

Non-financial identity theft includes using the personal identity of another to: obtain health, auto, and other insurance; obtain personal or commercial driver's license(s) and other government identification such as a passport; obtain government benefits such as social security; disability; and Medicare benefits; obtain employment; commit crimes including terrorism and capital crimes; obtain medical treatment and benefits; and commit any other type of identity fraud or crime that the criminal mind can conceive. Business identities can be used in many similar ways.

Using the identity of another to obtain employment creates erroneous Social Security records and taxable income in the victim's name. Employment fraud is common in Wisconsin and throughout the U.S., and an employer who does not take reasonable care to verify identification documents is also at risk for accepting false identification. Unlawful employment could be perhaps the most common type of identity theft, although it is one that few consumers hear of.

Most people do not understand the full consequences of having their identification used by one or even hundreds of other people for employment purposes. The imposters using that identification for employment, will very likely use it for banking, credit, loans, insurance, medical treatment, to obtain a driver's license, and if they are apprehended or identified in committing a crime. Multiple imposters working under your Social Security number can rack up hundreds of thousands of dollars in reported taxable income in your name.

Following the compromises of large database security breaches, a common public relations response (e.g. the Department of Veterans Affairs security breaches) is that there have been no reports of financial fraud in the name of any of the individuals whose profiles were compromised. It is more probable though, that compromised identities (names, Social Security numbers, and birthdates) will be sold multiple times to desperate people in need of an identity for employment, a driver's license, insurance, and to obtain other benefits. The consequences of those kinds of misuses of an identity could take years to become apparent to a victim. Credit monitoring services, which are an excellent means for early detection of financial fraud and financial identity theft, will not detect unlawful employment or other non-financial uses of one's identity. The victims may not detect the use of their identity for employment and other non-financial purposes for years, if at all (8)

Some of these identity theft crimes, which are not well known to the general public, are significantly more challenging for a victim to detect and correct in their lifetime. Recently, a women shared with me that her sister was a victim of identity theft in the 1970's, and that her sister made efforts for over thirty years, right up until the time of her recent death, to get back her good name. It is still likely that today her identity continues to be misused!

One of the most frightening and the second most frequently reported types of identity theft is when a victim's identity is linked to a crime (9). Crimes may include drug trafficking, pornography, DUI/DWI, capital crimes such as murder, and terrorist activities. Imagine the consequences of being mistaken for a criminal and trying to prove your innocence. "But officer, it isn't me!" isn't going to prove your innocence or gain your release. When you are finally released after spending days if not months in jail, expunging the crime from your court records will prove formidable, if not impossible, even with specialized legal counsel (10). This is a serious misuse of identity.

I have had recent contact with a local victim who was the subject of a local newspaper feature (11). His life has been all but destroyed as a result of criminal or character identity theft, as it is also called. This victim relocated and received a new identity, and yet he is still struggling with employment, legal, family, financial, emotional, and health issues that reasonably appear to be related to his identity theft victimization.

Medical identity theft is the most recent and growing threat. It was widely publicized in May 2006 by the World Privacy Forum, although other experts had predicted medical identity theft to

be a real threat nearly two years prior (12). Stolen identities are being used to obtain medical benefits and treatment, which may result in financial liability, erroneous medical records, and termination of health benefits in the name of the victim. The worst-case scenario is when a victim dies as a result of medical mistreatment based on erroneous medical records created during the treatment of the imposter (13).

**Other Human Consequences of Identity Theft**

As you can see, the benefit to an imposter can be other than financial, although it should not be forgotten that most all identity theft has a financial element. It is the sale and trading of stolen identities that links identity theft to drug trafficking, money laundering, organized crime, and terrorism.

Victims are often left helpless to navigate through the quagmire of government bureaucracy to resolve their identity theft crisis. The FTC's 46 page publication "Take Charge: Fighting Back against Identity Theft (10)" is a sobering read that reveals how complicated identity theft resolution can be. An attorney and noted identity theft expert commented that he would need a staff of six people to complete the resolution steps in the FTC publication (12). What about the average person?

The side effects of victimization include emotional stress and a sense of helplessness. Some victims describe it as being "personally violated," "worse than rape," and "a living hell." Couple the emotional consequences with the excessive time and finances required to reconstruct a previously good name (14). The news is littered with hundreds of reports each week of identity theft and the stories of families of victims that have been torn apart by identity theft.

No person, business or employer is immune from identity theft and its financial, social and emotional consequences. While identity theft cannot be completely prevented, even by the most vigilant consumer who follows all of the obvious preventative measures, it can be significantly reduced by following good privacy and security practices.

**Enforcement, Community, and Business Involvement**

Some experts feel that the public is becoming immune to its risks, roles and responsibilities in controlling identity theft. Activists and legislators call for more and stricter laws, while the reality is that criminals are nearly impossible to apprehend and only about 1 in 700 crimes are solved. Current laws cannot be enforced because of, for example, multijurisdictional issues and limitations in enforcement personnel. The majority of businesses and employers, especially small businesses and smaller public entities (e.g. towns and school districts), do not seem to be aware of the existing laws and their legal and ethical responsibilities in protecting non-public personal information of consumers, clients, constituents, and employees.

Financial institutions generally adhere to privacy and security compliance under the Gramm-Leach-Bliley Act (GLBA). Health industry organizations tend to align their privacy and security compliance under the Health Insurance Portability and Accountability Act (HIPAA). These acts address privacy and security issues of non-public personal financial and health-related information respectively. These industry groups and others are also responsible for taking broader responsibility regarding privacy and security. All industry groups, including financial and health, are also covered by the Fair and Accurate Credit Transactions Act (FACTA) Disposal Rule, a broader and more encompassing law in certain respects.

It is time that consumers, employers, businesses, law enforcement, and government act in concert by taking appropriate responsibility to bring identity theft under control, rather than expecting that the government is going to solve the problem entirely by enacting and enforcing more laws. The solution to this crime is not unlike how Americans have addressed other social-criminal issues, for example, theft and vandalism in neighborhoods and business districts through neighborhood and business watches; drunk driving through Mothers against Drunk Driving; and others; where citizens and businesses become involved in preventing crimes and addressing social issues by taking action and responsibility. Education, vigilance, and proactive risk management by all entities, as well as consumers, can control and reduce identity theft. Public and business involvement is also essential for America's war on terror since identity theft is related to crimes that fund terrorism and the terrorists who operate under stolen identities (2).

**Business Vulnerability**

Identity theft impacts business entities[3]. Identity theft is a global economic crisis affecting every country. Recently, a leading commercial insurer called corporate identity theft one of the fastest growing risks to businesses today, and they projected 1300% future growth in losses (15).

The major risks to entities include:

- Business Owner/Management Victimization
- Employee Victimization
- Customer, Client and Vendor Victimization
- Business Identity Theft or Business Victimization
- Security and Privacy Breaches – Public Relations, Financial and Legal Consequences
- Regulatory Breaches - Public Relations, Financial and Legal Consequences

The nearly 70% (7) of the 10 million (4) victims each year are people whose identity crisis can be traced back to the workplace. They are people like you and me: the owners, managers,

[3] In this context, a business entity is synonymous with any for-profit business; not-for-profit organization; local, state or federal governmental unit; or an individual (sole proprietor, landlord, home business operator, etc).

administrators, executive staff, other employees, customers, and others who have a relationship to the business where their personal identifiers were compromised.

When any person with a relationship to a business becomes a victim of identity theft, the business is potentially at risk. We already enumerated the financial, non-financial, and secondary consequences people face as victims. Identity theft can have a significant impact on the management, operations, financial credit, public credibility, and income of a business. For example, a key executive's and especially a small business owner's loss of creditworthiness, mistaken arrest, or adverse action by the IRS because of identity theft can disrupt and even destroy a business.

Consider the impact on a business when a few key employees are victimized or consider the scenario where the majority of employees become victimized because the employer failed to provide adequate safeguards to protect NPI. The victimized employees have the onerous, frustrating, and sometimes expensive restoration process to contend with on a day-to-day basis for months without end. The net effect on the business is employee lost work time, reduced productivity, lower morale, poor attitude, decreased quality of work, distractions, mistakes, and proneness to accidents due to inattentiveness. Employees (customers and others) may report the breach to authorities, and the employer would be subject to fines, penalties, and civil lawsuits to compensate employees for their losses.

When customers, clients, vendors or strategic partners become victims of identity theft through the negligence of the business, the business suffers financial losses and expends significant additional time and money in administration to address the multitude of considerations in dealing with the affected customers, creditors, lawyers, regulatory agencies, and the press.

So you don't have employees and you don't collect, maintain, or dispose of any NPI. You are still at risk, because your identity and that of your business or both can be misused.

The business entity itself can become a victim of financial, as well as non-financial, identity theft when your business identifiers are compromised and misused by dishonest people or employees. Business tax ID, tax exempt, and business license numbers are easy to obtain. Business indicia such as stationary and business cards are easy to replicate through color copiers and desktop publishing software. Business credit card numbers and other account numbers are not held as strictly confidential as our individual personal information, and the business identifiers are generally accessible to many employees and others. Because businesses are generally eager to do business-to-businesses transactions, they may be less rigorous in verifying information. Businesses should take the same steps in verifying information of businesses as when dealing with consumers to insure they are dealing with the authentic business and not an imposter.

Businesses and employers who collect or maintain protected consumer information face a plethora of legal requirements and responsibilities, as well as potential liabilities including regulatory and civil penalties and lawsuits for harm suffered to consumers (including employees

and vendors) in the event of a security breach (16). The first and foremost issue they will be addressing is a public relations crisis when they notify the people affected as required under state and proposed federal laws. Consider the negative publicity from some of the recent national and local stories involving small businesses, local government, schools, health care facilities, insurance companies, financial institutions, non-profits, and other entities.

In a recent "Chief Information Officer (CIO) magazine editorial (17), "The Coming Pandemic," the necessity for entities to take responsibility to protect their customers, employees, and others on whom they maintain NPI is discussed. They cite the cost of cleaning up the mess created by identity theft as 1,600 work hours per incident at a cost of $40,000 - $92,000 per victim.

Another consequence for negligence is the cost in customer relations. Legal experts are quoted as saying (17) that in the event of a security breach a business will lose 20 percent of the affected customer base, 40% will consider ending the relationship, and 5% will be hiring lawyers!

Privacy or security breaches will leave a business reeling to address the ensuing employee and client public relations crisis. The impact to the business will be multifaceted in terms of lost business, lost work time, regulatory issues, fines, legal expenses, and civil law suits.

**Laws requiring businesses to protect non-public personal information (NPI).**

In this survey article, a brief synopsis is given of the most relevant state and federal laws. Businesses should consult with risk management specialists and with legal counsel to ensure compliance with these and other applicable laws. To minimize risk all businesses and employers are advised to interpret the applicability of the laws broadly. By taking a broader responsibility than required by current laws, future risks and identity theft can be reduced (18).

***Fair and Accurate Credit Transactions* Act *Disposal Rule***

This provision of FACTA (aka FACT Act) became effective on June 1, 2005 to assure the secure disposal and destruction of NPI (19). This rule reduces the risk of identity theft created by improper disposal of NPI (e.g. through "Dumpster Diving") by taking steps to prevent sensitive financial and personal information from falling into the hands of identity thieves, dishonest employees, or others who might misuse the discarded information to victimize consumers.

This rule applies to any person who maintains for business purposes or otherwise possesses consumer information or any compilation of consumer information. The rule applies to individuals (e.g. landlords), businesses (large and small), and employers (including government entities and non-profits) that store, receive, maintain or otherwise possess consumer information.

Some examples are: banks, lenders and creditors, insurers, auto dealers, realtors, landlords, mortgage brokers, accountants, attorneys, debt collection companies, financial advisors, insurers, consultants, government agencies, retailers, utility companies, and employers or individuals that obtain consumer reports for employment or contractual purposes (e.g., tenant, nanny, contractor

screening), etc. Numerous small entities across almost every industry could potentially be subject to the rule.

A common misunderstanding is that entities defined as financial institutions under and compliant with the GLBA Safeguards Rule (see below) are exempt from the FACTA Disposal Rule. FACTA uniquely demands the protection of NPI for all consumers; whereas GLBA applies only to customers. For example, employees and applicants for employment or financing/credit who have been rejected are not customers under GLBA; however, they are defined as consumers under the FACTA Disposal Rule. All employers should note that "consumer information" also applies to employees under the FACTA Disposal Rule, and it would even apply to a non-business individual who obtained a consumer report on an illegal nanny who was being illegally compensated in the home!

The rule requires reasonable measures to protect against unauthorized access to, or use of, consumer information in connection with its disposal. To comply with the rule, businesses are expected to have written policies and procedures for burning, pulverizing or shredding of paper records and destruction or erasure of electronic media that contain consumer information as well as having appropriate policies, procedures, and employee training.

Consumer information means any record about an individual in paper, electronic or other form that is a consumer report or derived from a consumer report. Although credit header information, which includes name, address, and Social Security number, is not itself a consumer report, it is generally derived from a consumer report. Similarly, public record information is often part of consumer reports and falls within the scope of the rule. The FTC suggests that persons subject to the rule should always consider the sensitivity of the consumer information in determining what protection measures are reasonable.

If the entity's disposal practices are not compliant with the rule, or if disposal results in the theft of an identity or identities, the business can face a lawsuit by the victim or victims in a class action lawsuit. There are state fines of up to $1,000 per violation and federal fines of up to $2,500 per violation. One thousand profiles compromised or improperly disposed of equates to a million dollars in state penalties plus $2.5 million in federal penalties plus liability for victim losses. It is one stiff penalty that could put any entity out of business.

***The Gramm-Leach-Bliley Act Safeguards Rule***

The GLBA Safeguards Rule (20) requires any company defined under the law as a "financial institution" to implement policies and procedures to maintain the security and confidentiality of NPI. Under GLBA, the term financial institution is defined as a business significantly engaged in providing financial services or products for personal, family, or household use. This definition encompasses check-cashing and payday loan services companies, mortgage brokers, non-bank lenders, personal property and real estate appraisers, professional tax preparers, credit

reporting agencies, ATM operators, debt collectors, financial advisors, insurance agents, agencies and brokers, and a variety of other businesses that fit the definition.

As noted in the preceding sections, the GLBA Safeguards Rule provides for protecting NPI of "customers" whereas the FACTA Disposal Rule applies to protecting all "consumer" information. "Consumer" includes customers as well as employees, job and credit/loan applicants, and other third parties such as contractors, affiliates, strategic partners, etc. Those businesses defined as financial institutions are subject to both laws.

NPI compromised under the wrong set of circumstances can lead to fines of $1,000,000 per occurrence, up to 10 years imprisonment, removal of management, and civil and criminal penalties against executives.

***Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules***

These HIPAA rules (21) apply to any individual or organization that collects or retains protected health information in paper or electronic form. The more recent HIPAA security rule became effective on April 20, 2005. It applies to any individual or organization that retains or collects electronic protected health information (EPHI). Beginning April 20, 2006, it required all businesses with small self-insured or fully-insured health plans to maintain the confidentiality, integrity and security of employee health information. (Note that the earlier HIPAA Privacy Rule (2003) applies to all forms of protected health information (PHI) paper or electronic).

Generally, HIPAA applies to entities, who are health care providers, a health care clearing house, and health plans. To determine if your business is a covered entity, use the available web tools provided by the Department of Health and Human Services (22).

Medical information compromised under negligent circumstances may result in fines of up to $250,000 per occurrence and up to 10 years of jail time for executives.

***Wisconsin Senate Bill 164 (2005 Wisconsin Act 138)***

Beginning April 1, 2006, Wisconsin SB-164 requires any entity, including state and local governments, that conducts business in Wisconsin and maintains personal information to notify the individuals whose NPI is compromised in a security breach. NPI is defined broadly under Wisconsin law to include a person's first and last name in combination with any of the following: Social Security number; driver's license or state identification number; a financial account number of any kind including access codes; DNA profile; and biometric data. Entities have a maximum of 45 days from the time they learn of the breach of NPI to notify the affected persons. Failure to comply with this law may be used as evidence of negligence or breach of duty in civil and class action lawsuits against the entity.

***California Senate Bill 1386 (Security Breach Notification Act of 2003)***

What does California Law have to do with a business domiciled in Wisconsin? California's SB 1386 was the first law of its kind, and similar to Wisconsin's SB 164. It requires public disclosure of security breaches. It applies to any company in any state that does business in California, even with a single California customer. Failure to comply with this law subjects the company to civil and class action lawsuits by any consumer injured by violation of the law.

Many states have enacted similar laws to those of California and Wisconsin, and federal legislation to require disclosure of security breaches is pending. In the event of a security breach, an entity may be subject to security breach laws of numerous states.

***Other Considerations***

There are a number of legal, regulatory, human resource, and insurance issues that employers must consider.

Businesses and other entities need to be aware that like most laws, these and others are constantly enacted and amended. For these reasons, it is necessary to consult with an attorney skilled in privacy and information security compliance on a regular basis.

Employee dishonesty can play a major role in security and privacy through theft or misuse of confidential consumer and employee information. It is widely known that some criminals circulate among employers posing as employees for the sole purpose of stealing consumer information. Some of these fraudsters may obtain employment under false identities. All employers should conduct criminal background checks and obtain investigative consumer reports as part of the employment process. Employers should also be cognizant of employee financial wellness. A financially troubled employee may create a risk to your business. Today, there are several voluntary employee benefits that can have a positive effective on financial wellness; a few examples include supplemental insurance, disability insurance, financial and social counseling and family legal plans.

Business liability insurers are issuing clarifications to policies that specifically exempt lawsuits that result from information compromise and security breaches of consumer information. The burden of best practices and security is squarely on the shoulders of employers and businesses.

Employers can take an affirmative defense against penalties, lawsuits, and other business risks by making some form of identity theft detection and risk mitigation services available to employees (23) and, if appropriate to their customers (e.g. businesses defined as financial institutions), even at the cost of the employee and customer. The types of risk mitigation services available are varied; some will do little to contribute to risk reduction (e.g. insurance) while others provide comprehensive restoration and legal services including on-site employee training and compliance documentation. The aim of an affirmative defense system is to

minimize lost work time, penalties, lawsuits, and compensatory damages that may result from workplace identity theft by educating employees and officially documenting the training; providing a benefit that mitigates the risks to employees (and indirectly to the employer); and by documenting that risk mitigation services have been made available to employees on a voluntary basis.

Recently, Business and Legal Reports said, "A rise in identity theft is presenting employers with a major headache: They are being held liable for identity theft that occurs in the workplace (24)." An affirmative defense approach can reduce risks associated with workplace identity theft (23).

**Policies, Procedures, Education, and Training**

The adoption, implementation and enforcement of appropriate policies and procedures is the foundation for reducing the risk of having your business, customer, employee, client, and vendor identifiers compromised and ultimately used for fraudulent purposes.

Businesses should take the same type of preventive actions that experts prescribe for individuals to protect the privacy and identifiers of the business (10). Taking such steps goes beyond what the law requires; however, it is for the protection of your business identity, which is a growing area of risk (15). For example, do not share non-public business information (NBI) over the telephone or through the Internet without authenticating the communication; shred all sensitive information including pre-approved business credit card offers and scrap paper that may include your business indicia; deposit outgoing mail in a secure mailbox, do not leave incoming or outgoing mail openly accessible in the reception area; scrutinize your business banking, business credit card and other invoices for unauthorized charges, etc. These and many other preventive steps, which are provided in numerous other publications (for example, Ref. (10)), apply to you personally and to your business. Put your policy in writing; educate and train your employees. Repeat training regularly, and train new employees as part of the orientation process.

I have heard some financial institutions boast about policies and procedures; yet I heard that consumer information is routinely disposed of in the daily trash. Thieves can pick that consumer information from dumpsters. Policies and procedures are worthless without training and audits.

The education and training of your people is a key element to protecting your business. Make training mandatory. Over many years, we have learned that training conducted by a third party is more effective than in-house training. There is something almost magical about an employee listening to a credible third party compared to listening to a familiar co-worker providing the same information. Documented training by a certified trainer will add credibility to your affirmative defense.

According to the FTCs Division of Privacy and Identity Protection, entities need to have a plan in writing describing how NPI is to be secured and disposed of and an officer on staff for implementing the plan. Large entities will have a chief technical or a chief privacy officer. Small

businesses would not be expected to hire a full-time privacy specialist; nevertheless, they must be able to show they have a security plan in place with appropriate training of employees (1).

Betsy Broder, Assistant Director of the FTC Division of Privacy and Identity Protection says, "We're not looking for the perfect system, but we need to see that you've taken reasonable steps to protect your customer's information (1)." Today you need to go beyond protecting customer information; you must also protect your employee, vendor, applicant, and your own business information.

**What you can do**

All entities and affected individuals, for example, landlords and solo entrepreneurs, should review what NPI they have been collecting, storing, and disposing of and take responsibility for protecting NPI by complying with applicable laws as well as going beyond the requirements of the law by adhering to a stronger ethical standard of sound privacy and security practices. Also include policies, procedures, and training to protect your non-public business identifiers.

1. Understand what legislation may apply to your business; intentional ignorance of the law is no excuse for violations.
2. Assess your customer, employee, business and facility risks with a risk assessment professional.
3. If you are covered by HIPAA or GLBA, appoint an information security officer.
4. Develop a policy and procedure for the handling, securing, and disposal of all NPI, whether currently covered by law or not.
5. Conduct and document employee training on the policy and procedures, identity theft, confidentiality, and other relevant security issues. A certified third party, who your employees will view as your independent unbiased expert, is desirable because it generally results in more effective training. A certified trainer also adds credibility to your affirmative defense.
6. Take an affirmative defense against potential penalties and litigation by making identity theft risk mitigation services available to employees, and if appropriate, to your customers.
7. Because of constantly changing privacy and security laws, and because each entity is different, establish a relationship with qualified legal counsel in privacy and information security compliance.
8. Revise your policies and procedures as necessary and train your employees at least semi-annually for the first two years.
9. Develop an orientation procedure to train new employees on your privacy and security policies, procedures, and affirmative defenses.
10. Develop a crisis management plan. No matter what risk prevention measures you take, there is always risk. All you can do is manage the risk responsibly. Identify a public

relations firm or attorney or both who will be able to handle the crisis that could ensue from a privacy or security breach.

Defuse the identity theft time bomb and minimize your risks by taking broader responsibility to protect the NPI of employees, customers, others, and your business. It's all good for business.

**Disclaimer**

The author is not an attorney and the information provided herein should not be taken as legal advice.

**Acknowledgement**

The author thanks identity theft expert Michael Koll for his careful review and comments.

***About the Author***


*Joseph Campana, Ph.D. is a certified identity theft risk management specialist (CITRMS) accredited by The Institute of Fraud Risk Management and The Institute of Consumer Financial Education. He is also a member of the International Association of Privacy Professionals.*

*J. Campana & Associates provides consultation, training, and risk management solutions to businesses, employers, and employees. Dr. Campana is a frequent seminar speaker on identity theft and has appeared on radio and TV. He founded the LegalEase Group, Madison, Wisconsin in 1998, which provides insurance continuing education on legal expense insurance and identity theft topics. He has also been affiliated as an executive and trainer with a publicly–traded international services firm. Dr. Campana may be contacted by telephone: 608-241-3500 or by email: campana@JCampana.com. The J. Campana & Associates website is: www.JCampana.com.*

## *Literature Cited*


1. **Krause, Jason. .** Stolen Lives. *ABA Journal.* , March 2006

2. **Collins, Judith M. .** Business Identity Theft : The Latest Twist. *Journal of Forensic Accounting.* , 2003, Vol. IV, 303-306

3. **Privacy Rights Clearinghouse. .** A Chronology of Data Breaches. *www.privacyrights.org/.* [Online] , www.privacyrights.org/ar/ChronDataBreaches.htm

4. **Synovate. .** *Federal Trade Commission - Identity Theft Survey Report.* Washington, D.C. : Federal Trade Commission, 2003

5. **Fetterman, Mindy. .** Identity Theft, New Law about to Send Shredding on a Tear. *USA Today.* , 24 January 2005

6. **Aberdeen Group. .** Identity Theft: A $2 Trillion Dollar Criminal Enterprise in 2005. , 23 May 2003

7. **Collins, J.M. and Hoffman, S.K. .** *Identity Theft: Perpetrator Profiles and Practices.* School of Criminal Justice, Michigan State University. East Lansing, MI : s.n., 2002, Case Study to the National Institute of Justice, U.S. Department of Justice, Office of Justice Programs. Conducted in preparation for grant funding, submitted January 2003.

8. **Sullivan, Bob. .** The Secret List of ID Theft Victims. [Online] MSNBC, 29 January 2005. , http://www.msnbc.msn.com/id/6814673/

9. **Davis, Kristin. .** But, Officer that isn't Me. *Kiplinger's.* , October 2005, 86-90

10. Take Charge: Fighting Back Against Identity Theft. *www.ftc.gov.* [Online] Federal Trade Commission, June 2005. , http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.pdf

11. **Schuetz, Lisa. .** For Victim of ID Theft, Woes came in Bunches. *Wisconsin State Journal.* , 23 May 2004

12. **Attorney John Gardner, Jr. [interv.] .** Darlington, S.C. : s.n.. Private communication..

13. **Mary Harris, Lara Setrakian, Teri Whitcraft, and ABC News' Law and Justice Unit. .** Stealing Your Health: Medical ID Theft. [Online] ABC World News, 3 May 2006. , http://abcnews.go.com/WNT/Health/story?id=1918228&page=1&CMP=OTC-RSSFeeds0312

14. **Rivlin, Gary. .** Purloined Lives. *nytimes.com.* [Online] The New York Times, 17 March 2005.

15. **Royal & SunAlliance. .** *Risk Uncovered Index.* The Center for Economics and Business Reearch. London : s.n., September 18, 2006

16. **Myers, Randy. .** Who Will Class-Action Lawyers Go After Next? *Corporate Board Member/Special Issue: Lawyers.* , July/August 2006

17. **Friedenberg, Michael. .** The Coming Pandemic. *CIO Magazine.* , 15 May 2006

18. **Nahra, Kirk J. .** *Your Growing Exposure for Identity Theft Risks.* Wiley Rein & Fielding LLP. Washington, D.C. : s.n., 2006, Legal Opinion

19. FACTA Disposal Rule. [Online] Federal Trade Commission, 2004. , http://www.ftc.gov/os/2004/11/041118disposalfrn.pdf

20. Gramm-Leach-Bliley Safeguards Rule. [Online] Federal Trade Commission, 22 May 2002. , http://www.ftc.gov/os/2002/05/67fr36585.pdf#search=%22%22Gramm-Leach-Bliley%20Safeguards%20Rule%22%22

21. Health Insurance Portability and Accountability Act. [Online] United State Department of Health and Human Services. , http://www.hhs.gov/ocr/hipaa/

22. Covered Entity Decison Tools. [Online] U.S. Department of Health and Human Services. , http://www.cms.hhs.gov/apps/hipaa2decisionsupport/default.asp

23. **Marshall, Peter. .** Identity Theft: Limiting Your Employees' Risk -- and Your Liability. *Business and Legal Reports.* , 19 January 2006

24. **Hottle, D. .** Workplace Identity Theft: How to Curb an HR Headache. *Business and Legal Reports.* , 19 September 2006