Identity theft and its affect on business

Identity Theft and its Affect on BusinessMillions of Americans fall victim to identity theft each year. The increase of illegal immigrants and millions of foreigners entering the United States has created a state of emergency for various government and financial agencies. Being the victim of identity theft is one of the most personal and painful crimes to experience. This type of theft affects a person??™s ability to make major purchases: such as cars, homes, and even personal loans. The effects of this crime are as devastating to businesses as it is to the individual victim. There could be a significant impact on the management, operations, financial credit, public credibility, and income of a business, according to Joe Campana, a certified identity theft risk management specialist. He defines identity theft as, ??? The misuse of personal or business identifiers by an imposter for their advantage, which may be financial, non-financial, or both???. Consequences of this type of theft are the same for both the individual and business.

To minimize the risk of a stolen identity follow these three recommend steps: Deter, Detect, and Defend. Criminals that steal identities are often looking for people with good or above average credit. The purpose for targeting these people is the privileges they are able to access with good credit information. Identification thieves can drain your bank account, ruin your credit, and run up thousands of dollars of debt in your name. The sad thing about this type of crime is that many people are unaware they have become a victim of identity theft.

Although sentencing is becoming more severe for those convicted of identity theft crimes, the best way to avoid becoming a victim is to minimize the risk by deterring thieves from ever getting to your personal information. The

stealing of personal identity has cost Americans more than $50 billion a year and hundreds of hours in trying to restore their credit. Protect your social security number.

The only time you should have your social security card with you is when required by law to present it for verification. Never give your social security number out over the phone. Keep social security cards in a safe place and never put them in a wallet where someone might have access to your number.

Thieves are notorious for sneaking into personal trash and looking around the outside of homes for any bits of personal information to use to their benefit, thus destroying your credit reputation. Shred important documents that have personal information on them when ready to discard them such as: bank statements, charge card bills, physician statements, and credit offers received in the mail. If near a post office, use the collection box to drop mail to be sent out rather than using your home mailbox. Immediately retrieve home-delivered mail, especially when placed in an outside mailbox that is accessible to the public. The vast popularity of the Internet is a major concern of identity theft. This exciting technology seems to be embraced without reservation by the world. Many people blindly believe that what is posted on the Internet must be true ??“ especially advertisements that appeal to the base level of financial hording, whether it is saving or making money. Stolen identities using the Internet are rising at an alarming rate.

Digital identity is made up of user names, passwords, IP addresses, birth dates, social security numbers, personal identification numbers (PINS),

mother??™s maiden names, etc. This information can be used for all Internet transactions, especially financial transactions. For the unsuspecting casual internet user, they can stumble upon a link that will promise them much money with very little work involved or they receive an alert that a bank account is in jeopardy. The user is directed to click on a link to fix the problem and then unknowingly, they have given the thieves all the information needed to enter the user??™s bank account and wipe it clean. Phishing, or spoofing, comes in the form of an email that looks similar to a legitimate web site requesting personal information.

Approximately three percent of phishing scams may be successful. Research has shown 57 million adults have experienced a phishing attack, 1. 78 million could have fallen victim to the scam, and the cost of phishing is 1. 2 billion dollars.

The best deterrent for these scams is to click on only links that are known, without a doubt that the email is coming from a reputable business. A legitimate internet site has the users name in the body of the email (instead of a generalized greeting), and the link being sent does not redirect to another web site that looks similar to the original business page. Social security cards are the greatest risk for total identity theft. Keep them in a safe place, other than a wallet or purse. Carry only the identification needed and nothing more. Always keep wallets and purses secure. All personal information should be stored in a secure location. Know where your identification is at all times, including while at home, work, in the car, or even with family and friends.

It is a good idea to make copies of your personal identification in case something should happen to it. Most often by the time a person is aware of the theft; serious financial damage has already taken place. Detecting Identity Theft in a timely manner is fundamental to limiting the damage and improving the chances of catching the criminal that committed the crime. Being vigilant about monitoring your personal information is essential to your success of recovery if you become a victim. There are many ways to monitor and detect your personal information. One of the first things that should be examined routinely is a credit report from a primary credit monitoring agency. The three major credit agency??™s to contact are Equifax, Trans Union, and Experian. Upon accessing these credit reports, look for unexplained debt or accounts that look unfamiliar.

Report any information you deem fraudulent to the credit agency. Another source that can be used is a company called True Credit, Inc. This company will contact its customers via e-mail alerts anytime someone tries to run a credit check, open a new account or contact the credit agency with changes regarding your credit. Closely examine your bank and credit card statements every month for errors that are unexplainable. Contact these agencies to inform them of the error so it can be investigated and resolved. Make copies checks written when paying bills and monitor when the amount has been deducted from your account. If the money is not deducted from your account in a timely manner or if the account, contact the receiving agency immediately to resolve the issue.

Finally, being turned down for a credit card or a loan when you are certain you have above average credit is a sure sign something is amiss. Contact

these agencies immediately to inquire about the denial of credit and take advantage of the free credit report opportunity provided with the denial letter. The only way to insure that your identity remains secure is to monitor the activities involving purchases and bill paying. Routinely check your credit report for suspicious activity that cannot be explained and always keep a copy of checks and receipts for several months as proof of payment. These simple practices will keep you informed of monthly activities concerning your accounts and the security of vital personal information. Although most individuals would never imagine having their identity stolen, the fact is there were 10 million victims of identity theft in 2008 in the United States (Javelin Strategy and Research, 2009). Would you know how to defend yourself against an identity thief According to www. spendonlife.

com, 2009 Identity Theft Statistics, there are seven target areas for identity thieves.??? Credit Card fraud (26%),??? Utilities fraud (18%)??? Bank fraud (17%)??? Employment fraud (12%)??? Loan fraud (5%)??? Government fraud (9%)??? Other (13%)A victim of identity theft should follow four steps-of-action in order to defend their identity, as stated on www. spendonlife. com. ? Place a fraud alert on your credit reports. ? Close accounts you believe have been tampered with or opened fraudulently.? File a complaint with the Federal Trade Commission (FTC).

? File a report with your local police or police in the community where the identity theft took place. Let us look at each step in further detail. The first step of defense in the event of suspicious activity of any personal account or information is immediately contact the three consumer credit reporting agencies; TransUnion, Equifax, and Experian. You need only contact one of

the three agencies, they in turn will contact the other two for you to place a fraud alert. An initial fraud alert is will stay on your credit report for at least 90 days, and an extended fraud alert will stay on your credit report for seven years. You can choose which alert is best for your situation.

Once the alert has been placed, it is strongly suggested you request a free copy of your credit reports from each agency to verify all information such as, name or initials, social security number, all addresses, and employers. Secondly, close any accounts that appear to have been tampered with, opened, or used without your consent. Once you have found the fraudulent information, you can get it removed most effectively by explaining the issue in an Identity Theft Report with cover letter. Thirdly, file a complaint with the Federal Trade Commission. Filing a complaint with the FTC is simple and they are easily accessible by telephone (toll free), internet and by mail. By contacting the FTC, not only do you give valuable information to other law agencies across the nation to help the fight of identity theft, but you also will attain certain protections from collection companies for several years to follow.

Fourth, and finally, file a report with your local, state, or federal law enforcement agencies. For best results, take a copy of your printed Federal Trade Commission ID Theft Complaint Form and a cover letter with any supporting documentation to the local authorities. Also, attach a copy of your Identity Theft Report from the FTC. If you cannot file a report face-to-face, you have the opportunity to file over the Internet or telephone. In addition to filing the report, you will want a copy of the official police report. If there is an instance where you cannot obtain a copy of the official police report, sign

your Complaint and write the police report number in the “ Law Enforcement Report” section on the form.

(Be sure to attach only copies and not any originals). If you feel you have been a victim of identity theft, take your first action and defend yourself as soon as possible. Contact any of the three consumer reporting companies to review your free credit report.

There is no financial limit to what an identity thief will take from you. Businesses are vulnerable to the consequences of stolen identities, as well. 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 (Campana, 2006). Business leaders should know where private information is stored and track all who have access to it. Every business should have a good understanding and knowledge of the laws that are in place regarding the protection of non-public personal information.

Violating these laws will result in large fines, civil liabilities, and possibly imprisonment. The Fair and Accurate Credit Transactions Act Disposal Rule (FACTA) requires that reasonable measures are put in place to protect against unauthorized access or use of consumer information. This rule applies to individuals such as landlords, businesses, and any entity that possesses consumer information. The Gramm-Leach-Bliley Act Safeguards Rule requires financial institutions such as banks, credit unions, 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 to implement policies and procedures to maintain the security and confidentiality of non-public personal information (Campana, 2006). The Health Insurance Portability and Accountability Act, more commonly known as HIPAA, is the rule that protects the privacy of individually identifiable health information whether in paper or electronic forms. The rule also permits the disclosure of personal health information needed for patient care and other important purposes.

All businesses should be knowledgeable about the rules that apply to their type of business. Policies and procedures should be developed and implemented and employees should be properly trained to follow them. A responsible business owner will be proactive in taking steps to prevent a breach of non-public personal information. Senate Bill 164, signed into law in March of 2006 by Governor Jim Doyle of Wisconsin, states that companies must inform customers of a data breach, which typically occurs when computer systems are hacked, when dishonest employees sell information, or when businesses simply lose information. Governor Doyle made this comment when signing the bill, ??? Getting consumers??™ personal information is the first step in identity theft, and if consumers don??™t know whether their information has been compromised, they can??™t take steps to protect themselves.??? In an article written by Joe Vanden Plas (2006) for the Wisconsin Technology Network, he made this statement, ??? The bill likely to have the greatest impact on businesses is SB 164, which gained unanimous support in both houses of the Legislature.

If there has been a security breach that leads to the theft of personal information, companies must inform victims of the breach in the manner in which they usually communicate, whether that is by e-mail or traditional mail.??? It is clearly the main responsibility of businesses to protect non-public personal information. Although this bill only applies to Wisconsin at this time, it is believed it will be adopted by all states in the near future. The Aberdeen Group, a leading provider of fact-based research, has estimated that $221 billion a year is lost by businesses worldwide due to identity theft.

The effects of identity theft to a business cannot be ignored. Preparation (Deter), planning (Defend) and recognizing (Detect) potential risks are essential to protect against it. Taking the appropriate steps to protect non-public personal information is a good start to the minimizing the business risks of identity theft. References2009 identity theft statistics (2002-2009). Retrieved May 24, 2010, from http://www. spendonlife. com/guide/identity-theft-statisticsBecker, G. and Posner, G.

(2006, September 17). The Becker-Posner Blog. Retrieved from http://becker-posner-blog. com/archives/2006/09/deterring_ident. htmlCampana, J.

, (2006, September 19). Identity theft: The business time bomb. Wisconsin Technology Network. Retrieved from http://wistechnology. com/articles/3332/eHow.

(2010, May). How to Detect Identity Theft. Retrieved from http://www. ehow. com/how_2189966_detect-identity-theft. htmlFederal Trade Commission. (2010, May).

Defend, recover from identity theft. Retrieved May 24, 2010, from http://www. ftc. gov/bcp/edu/microsites/idtheft/consumers/defend. htmlFederal Trade Commission.

(n. d.) Fighting Back Against Identity Theft. Retrieved fromhttp://www. ftc. gov/bcp/edu/microsites/idtheft/consumers/deter.

htmlFederal Trade Commission. (2010, May). Identity Suspicious Activity. Retrieved fromhttp://www.

ftc. gov/bcp/edu/microsites/idtheft/consumers/detect. htmlIdentity theft statistics. (n. d.) Retieved May 19, 2010, from http://www. spamlaws. com/id-theft-statistics.

htmlInternet ID Theft Statistics Show How Online Identity Theft Works. (2005-2007). Retrieved from http://www. guard-privacy-and-online-security. com/internet-id-theft-statistics. htmlSocial Security Administration. (2009, August). Identity Theft and Your Social Security Number.

ICN 463270Understanding health information privacy.(n. d.). Retrieved May 29, 2010, from http://www. hhs.

gov/ocr/privacy/hipaa/understanding/index. htmlWalker, J., (2009, August 25). How identity theft affects a company.

Retrieved from http://www. a1articles. com/index. php