# Identity theft essay sample

Sociology, Identity

Identity theft is a major crime that happens to millions of people every year. People whose identities have been stolen can spend months and years trying to clean up the mess the thieves have made of a good name and credit record. There are many different types of identity theft and ways to deal with it. Identity theft is very serious and stolen identities are used to commit many other crimes. Some of the specific types of identity theft besides personal identity theft, include tax related identity theft, business related identity theft, child identity theft, and medical identity theft. Identity theft can cause serious challenges for individuals and businesses and there are several steps to take to help clear up identity theft as well as steps to follow to prevent identity theft from occurring again.

According to the Transunion website, “ Identity theft is the fastest growing crime in America. The number of identity theft incidents has reached 10 million a year and every minute about 19 people fall victim to identity theft” (TransUnion LLC). Identity theft is a very serious problem and unfortunately is happening to many people everyday. According to a book, “ Take Charge” written by the U. S. Department of Homeland Security and U. S. Secret Service, “ The Identity Theft and Assumption Deterrence Act enacted by Congress in October 1998 makes identity theft a federal crime. Violations of the federal crime are investigated by federal law enforcement agencies, including the U. S. Secret Service, the FBI, the U. S. Postal Inspection Service, and the Social Security Administrator’s Office of the Inspector General. Federal Identity theft cases are prosecuted by the U. S. Department of Justice” (U. S. S. S. 491).

Under the law, “ identity theft take places when someone knowingly transfers, possesses or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet or in connection with, any unlawful activity that constitutes a violation of federal law or that constitutes a felony under any applicable state or local law”(U. S. S. S. 491). Some of the types of personal information that identity thieves use include social security numbers, credit card numbers, cellular telephone serial numbers, or any other piece of information that can be used to identity a specific individual.

Once identity thieves have a person’s personal information they can use it to drain a person’s bank account, run up charges on a credit card, get medical treatment with a person’s health insurance as well as many other things. The Federal Trade Commission is an independent federal agency of the U. S. federal government that maintains fair and free competition; as well as enforcing anti-trust laws and educating the public about identity theft. According to their website some of the ways identity thieves get a person’s information include, “ getting it from businesses or other institutions by stealing records or information while they’re on the job, steal your mail also known as “ dumpster diving”, get credit reports by abusing employer’s authorized access to them, steal debit/credit card numbers by capturing the information in a data storage device in a practice known as skimming, steal your wallet or purse, steal personal information through email or phone by posing as legitimate companies known as phishing”(FTC).

Once an identity thief obtains a person’s personal information there are many things they can do with the information. Some of the common things identity thieves use a person’s personal information include, opening a credit card in their name, may call credit card issuer to change the billing address on credit card account, establish phone or wireless service, open bank accounts, counterfeit checks, file for bankruptcy under a person’s name to avoid paying debts that they’ve incurred, buy a car, get identification in a person’s name with their own picture such as a driver’s license, as well as many other things.

The federal trade commission’s website suggests some of clues that someone has stolen information as well as what to do if identity theft happens to a person. Some of the clue’s listed on the site are, “ seeing withdrawals from bank account that you can’t explain, don’t get your bills or other mail, merchants refuse checks, debt collectors call you about debts that aren’t yours, you find unfamiliar accounts or charges on credit report, medical providers bill you for services you didn’t use, health plan rejects legitimate medical claims, IRS notifies you that more than one tax return was filed in your name, you get notice that your information was compromised by a data breach at a company where you do business or have an account” (FTC). If a person loses important personal information or are victims of identity theft, there are steps they can follow to help them repair the damage. If a person is a victim of identity theft, they place an initial fraud alert, order credit reports, and create an identity theft report.

The three national credit reporting companies keep records of everyone's credit history and if a fraud alert is placed, the credit reporting company can contact the other companies and it can make it harder for an identity thief to open more accounts in someone's name. After the initial fraud alert, the Federal Trade Commission recommends ordering your credit report so a person can look over all of discrepancies that might have occurred to get them removed. The Federal Trade Commission then recommends creating an identity theft report, " An Identity Theft Report gives you some important rights that can help you recover from the theft. To create one, file a complaint with the FTC and print your Identity Theft Affidavit. Use that to file a police report and create your Identity Theft Report"(FTC). By filing an identity theft report, it can help get fraudulent information removed form a person's credit report, stop a company from collecting debts that result from identity theft and help a person recover from the identity theft.

Tax-Related identity theft is very prevalent in the United States and is an ongoing problem. According to an article from the American Institute of CPA's written by Patti Burquest, " The Treasury Inspector General for Tax Administration (TIGTA) reported that the IRS identified more than 1. 1 million incidents of tax identity theft related to 2011 returns. Moreover, Beth Tucker, deputy commissioner for Operations Support, stated that for the first 10 months of 2012, the IRS protected, through enforcement efforts, close to $20 billion of revenue related to fraudulent refunds"(AICPA Burquest). The article then moved on to discuss the ways that tax identity theft can occur and how it is discovered. One of the ways tax related identity theft happen is by income being reported to the IRS but not earned by the taxpayer. In this

case, the thief uses the victim’s social security number to file a fraudulent tax Form W-2 and reports wages that were never earned or withheld.

The second way it is discovered is by multiple returns filed under one social security number, in which case the thief files early in the filing season in an attempt to gain a refund before the true taxpayer files his or her tax return. The third way tax related identity theft is found is by IRS notices and collection activity. In this case, the thief may send out a fake letter telling the victims that they are not required to file a return. Tax related identity theft has become a huge problem in the United States, and the Internal Revenue Service has created ways to help stop and prevent it from occurring. The Internal Revenue Service has established a special unit that focuses on identity theft, which is called the IRS Identity Protection Specialized Unit. When a person becomes a victim of tax related fraud, the unit is trained to help taxpayers with any identity theft issues. The IRS will electronically mark a taxpayer’s account when identity theft is reported and individuals then receive an identity protection personal identification number.

The AICPA article written by Patti Burquest stated, “ The IP PIN procedure began in late 2011 as a trial program, with the IRS issuing approximately 54, 000 IP PINs. For 2012, the number of IP PINs issued increased to 250, 000 with a further increase to 600, 000 expected for the 2013 filing season” (Burquest). The number of IP PINs tripled in one year and is expected to almost triple again next year, which is really astonishing and shows what a huge problem identity theft really is. In the closing statements of the article

written by Patti Burqest, she wrote about how the IRS is making identity theft a key emphasis area for 2013 and how they plan to devote many resources to prevention, protection, and prosecution of tax related identity theft cases. While the Internal Revenue Service has taken steps to assist victims of tax related identity theft, there are still some struggles it faces and taxpayers face many problems when trying to deal with their identity theft issues.

In the Journal of Accountancy, an article written by Alistair Nevius on May 8 2012, stated, “ Treasury Inspector General for Tax Administration (TIGA) reviewed IRS data from 1. 1 million identity theft cases, and discovered the IRS is not effectively providing assistance to victims of identity theft and current processes are not adequate to communicate identity theft procedures to taxpayers, resulting in increased burden for victims” (Nevius). Some of major problems discussed in the article were how the IRS does not handle the cases in a timely fashion, communication with IRS is limited, as well as the guidelines about identity theft are conflicting and not consistent. The TIGA made some recommendations for the IRS that they agreed to which include, “ establishing accountability for its Identity Theft Program, implement a process to ensure that IRS notices are not sent to the address listed on identity thief’s return, ensure taxpayers are notified when the IRS has received their identifying documents, create a specialized unit in the Accounts Management function to exclusively work on identity theft cases, and ensuring programming is adjusted so that identity theft issues can be tracked and analyzed for trends and pattern’s” (Nevius).

Although tax related identity theft is major crime and problem, the IRS is agreeing to take the steps it needs to stop and prevent it from happening. Tax related identity theft might become less frequent if the IRS continues to focus on ways to prevent and combat against it from happening. In a recent article on the AICPA website, " IRS's Identity Theft Liaison Pilot Program with Law Enforcement expands to 50 States", published on March 29, 2013, spoke about how the IRS is expanding its Law Enforcement Assistance Program on Identity Theft to all fifty states and the District of Columbia. In this program, state and local law enforcement officials with evidence of fraudulently filed tax returns and permission from the victims to disclose their tax return information can help to investigate the frauds and prosecute.

The article states, " Since October, the IRS has pursued more than 670 criminal identity theft investigations and convicted offenders are receiving sentences averaging four and reaching up to 20 years. In January, the IRS participated in a coast-to-coast identity theft enforcement sweep that resulted in 298 indictments, informations, complaints, and arrests"(Journal Of Accountancy). The article also stated how the IRS had other success in identity theft areas, " by stopping $20 billion in fraudulent refunds and 5 million suspicious returns in 2012, up from $14 billion and $3 million in 2011"(Journal of Accountancy). The IRS is taking many steps in the right direction to help victims deal with identity theft and prosecute the criminals who are involved. Business identity theft is another type of identity theft that occurs when a person uses a business's identifying information to obtain credit, goods, services, money or property to commit a felony or misdemeanor.

Business identity theft has become very common and according to “ Preventing Identity Theft in Your Business” a book written by Judith M. Collins, the author states that business identity theft has become increasingly common for three reasons which are, “ Corporate credit card bank and other account statements have more entries than the accounts of an average individual and are more complex and less easily reconciled. Corporate credit accounts usually carry higher dollar amounts. Many employees oftentimes are authorized to use a single corporate account. In this case, the theft and fraudulent use of the account number is less easily detected in the corporation credit card statement than in an individual credit statement that contains fewer account entries”(Collins 135). The most common types of business identity crimes include credit card, bank, retail accounts, and subsidiary fraud. When a person steals a business’s identity it can lead to a subsidiary fraud.

Judith Collins states, “ the theft of a business’s state and federal identifiers has opened the doors to new crimes of business impersonations, such as subsidiary fraud. This is the registration, with a secretary of state, of a fraudulent subsidiary company using a legitimate business’s identifiers. With the payment of a modest registration fee, in some states as little as $25, parasite “ businesses” can be formed and pose as legitimate businesses, incurring never to be paid expenses for goods and services and obtaining fraudulent business loans and other means. Sometimes these entities defraud legitimate company’s by invoicing them for services never rendered or by ordering merchandise that is then sold on the black market”(Collins 136, 137). This statement describes how business identity theft can lead to

other frauds. If a business's identity is stolen, than their customer's information is a also as risk which can lead to more identity theft crimes. Identity theft can also occur in business when there are data breaches which can lead to invidual identity theft.

The Privacy Right's Clearinghouse (PRC) is a nationally recognized consumer education and advocacy nonprofit organization dedicated to the privacy of American consumers. The PRC keeps track of data breaches from companies from the year 2005 to the present. Some of the cases that are on their website are examples of how business identity theft not only effects the business but the consumers as well. In an article in the New York Times, written by Ann Carrns, " A probable factor in the rise in identity theft in 2011, the report found, was an increase in reported data breaches, like those at Sony PlayStation and Epsilon. Fifteen percent of Americans were notified that their information was lost in a data breach in 2011, and those notified of a data breach are almost 10 times more likely to be an identity fraud victim than someone who wasn't notified, Javelin found"(Carrns). The PRC website has the information on the Epsilon data breach as well as many other cases.

Epsilon is an example of business related identity theft. Epsilon is an email service provider for companies, and reported a breach that affected three percent of its customers in April of 2011. According to the PRC website, " A total of 75 companies were affected and these companies may end up paying a combined amount of $412 million in damage control. Epsilon itself could pay $225 million. Some estimate the total cost of the Epsilon breach could run as high as $3-$4 billion in forensic audits and monitoring, fines,

litigation, and lost business for provider and customers. Conservative estimates place the number of customer email addresses breached at 50-60 million. The total of customer emails exposed could reach 250 million”(Databreaches. net/PRC). This is just another way that identity theft can affect businesses and individuals and lead to other frauds and crimes.