2017

Identity Theft: A Look into Preventing Decades of Damages

Mallory Monaco
Assumption College

Identity Theft: A Look into Preventing Decades of Damages

By Mallory Monaco

Faculty Supervisor: Professor Joseph Alfano, Computer Science

A Thesis Submitted to Fulfill the Requirements of

the Honors Program at Assumption College

April 2017

Table of Contents

1. Introduction

If you could spend a few minutes doing something that would save you $1,500 and 175 hours of time, wouldn't you do it? These are the average losses that result from identity theft victimization (Albrecht, Albrecht and Tzafrir 2011).[1] This is equivalent to 22 eight-hour workdays that a victim may have to take off to resolve the problem. It is a crime that is growing in severity each year. Damages from identity theft can span from noticing a fraudulent charge on one's credit card, to a stranger applying for a car loan in a victim's name, to a person using another's health insurance and changing his or her medical records. And these are only a few of the situations identity theft victims may find themselves facing. Each of these have serious consequences and should not be taken lightly. Beyond the losses of time and money, identity theft can ruin a victim's life for years to come. As noted in Rebecca Kanable's article, "The face of identity theft: recognize it when you see it--and help your community identify it", one woman became a victim of identity theft 10 years ago but still faces its negative effects. Her credit score suffered from the identity theft and, as a result, her mortgage interest rate increased. Unfortunately, identity theft is not a one-time mess; "victimization doesn't seem to end."[2]

Given that the consequences resulting from victimization are not easily resolved, think back to the first question posed. It would be foolish not to take a few extra precautions to protect your identity rather than become one of the already 4.6 million victims in 2017.[3] This thesis will explore medical identity theft, credit card identity fraud, tax return identity theft and the impact of consumer data breaches on identity theft. Additionally it will provide insights into some methods that fraudsters use to commit the theft, and recommendations for preventing the fraud. It is known that rather than protecting oneself after fraud has already been committed, there are fewer damages done in preventing the fraud from ever occurring. With this in mind, our goal is to understand how the theft is committed to attempt to prevent the breaches from happening altogether.

Researching identity theft is important because it affects more people each year. It wastes time and money that could be better used for many other causes, and it creates stress for all who encounter it. Part of the reason it affects so many people (over 15 million each year) is because of its many forms.[3] All identity theft begins with stealing personal information using methods that are fairly easily carried out. For example, a skimmer is a pocket-sized device that can be purchased online and used to scan a victim's cards to obtain his or her card information. A skeptical consumer may be quick to say that she would never give a stranger her credit card because that would be giving fraudsters the opportunity to victimize her. However, when you are out to dinner and the check comes to your table, don't you often hand your card over to a person you met 60 minutes prior? We like to think that we can trust everyone; most people can be trusted. However, news articles entitled, "Waiter charged with credit card fraud"[4] and "Cashier linked to credit card skimming scam, police say"[5] have been all too common in recent years. When a person's card is out of his or her hands in either a literal or figurative sense, fraud is possible. More recently, restaurants have begun to use "ziosks" or tabletop kiosks to allow customers to pay right at the table. Using this technology limits the opportunity for fraud to happen between the time the card is handed over to the waiter and returned to the customer. However, because this method is not always an option, the opportunity for fraud still exists.

Separate from this type of identity theft is medical identity theft. There are several methods that fraudsters use to carry out the theft. One possibility is that a clinic bills an insurance company for services that were not provided to a patient. In this scenario, the office defrauds the insurance company financially. An even more serious form of medical identity theft is when a patient’s identity is stolen so the criminal can use the victim’s medical insurance. The consequences of this theft can be threatening to the patient’s physical and financial health because false usage of insurance can alter the patient’s medical records.

Just as credit card fraud and medical identity theft involve using a victim’s info to obtain their benefits, tax return identity theft is when a fraudster steals a victim’s personal information to file the victim’s taxes with the intention of obtaining the refund. Doing so jeopardizes the victim’s financial security.

The origin of my interest in identity theft began a few years ago when my dad’s identity was stolen. A fraudster used my dad’s social security number to file his tax returns and obtain the money. To see the stress it causes victims and yet the ease with which it is committed is astonishing. Over the last decade identity theft has grown a tremendous amount and it will only continue to grow. Victims fail to recognize that they are vulnerable until they are targeted. The first step in determining how to prevent identity theft is learning what it is and how the fraud is committed. As I am getting older and entering the age of having my own credit card account, car, and eventually home, it is important that I know now how to protect myself so that I do not become one of the millions of identity theft victims in the United States.

In the following chapters we will explore a few of the most common forms of identity theft. These include medical identity theft, credit card fraud, tax identity theft and consumer data breaches. In addition, we will analyze some methods fraudsters use to commit identity theft. Finally, we will provide recommendations based on our research about methods for protecting oneself from being victimized. Preventing identity theft is important because it does more than save time and money; it would restrict potentially life threatening situations from occurring.

2. Medical Identity Theft

The least common, yet still dangerous, form of identity theft is medical identity theft. While some identity theft can cause financial troubles such as difficulty obtaining car loans and mortgages, medical identity theft can result in life threatening consequences. The following chapter will discuss specifically what medical identity theft entails, as well as signs of victimization. In addition it will provide suggestions for actions victims can take to resolve damages in an attempt to prevent future victimization. Learning what medical identity theft entails and how it is committed will help determine how to prevent it.

What is medical identity theft?

Medical identity theft is the use of another's name, health insurance numbers, and other personal information without his or her knowledge to obtain medical services, treatments, prescriptions or other goods.[6]

How do you know if you've been victimized?

If you have been the victim of a criminal offense, you are generally aware of it right away. For example, if a burglar steals a television from your home, it doesn't take long to notice that your several hundred-dollar entertainment system is missing. However, this is not always the case with identity theft. Many times an identity theft victim learns of the crime long after the damage is done. In the case of medical identity theft, signs that one has been victimized include receiving a bill for medical services that you didn't incur, indicating that someone used your insurance, or your Explanation of Benefits or Medicare summary including something that you did not receive.[6] Without one of these signs, a victim would not know that a crime has been committed against them. For this reason, if there is any suspicious activity of these types, it is imperative that it be reported right away before further damage is done. It is also important to keep in mind that people 50 years or older with government issued insurance are at a higher risk of medical identity theft.[7] Given that these people are at a higher risk for victimization, it is especially important that they keep their personal information secure.

What consequences do medical identity theft victims face?

As a result of the medical identity theft, victims often experience negative effects to their insurance policy rates, credit reports and medical files. The unfortunate truth is that once a person becomes a victim, they have to deal with the negative consequences that result for many years to come. The damages and situations involved in cases of medical identity theft are often startling. In one mind boggling example, Linda Weaver received a medical bill for the amputation of her foot but, "she did not need to look down at her two very intact feet to know this was bunk".[7] In this case an identity thief pretended to be Linda as he or she had the surgery. Initially, Linda likely experienced anxiety knowing that someone used her identity to get an expensive and difficult surgery. And yet, this isn't the only reason to be worried. Identity theft can result in both medical consequences and financial hardships that can make living conditions difficult to maintain. In another example, Joe Ryan was billed for a $44,000 colon surgery that he did not receive.[7] This extreme financial burden resulted in the cancellation of his credit cards, damaging effects to his credit score and his future ability to obtain loans, and foreclosure on his home.[7] Overall, the one case of victimization likely ruined Joe's financial health that he spent time building up over several years. While these financial consequences are life changing, the medical hardships that result from identity theft may be considered to be even more damaging. This is because medical identity theft can cause life or death consequences. The act of stealing a person's medical identity results in the victim's medical records being merged with the perpetrator's files. This has very serious implications for the victims' future physical health.

Because the criminal who used Linda Weaver's identity has diabetes, Linda's record now reads that she suffers from the disease.[7] If Linda needs surgery in the future, the doctor may wrongly give her insulin. Similarly, the fraud could result in, "the wrong blood type listed in the file, not documenting a heart condition, and allergies or intolerance to certain medication"[7] all of which can cause incorrect treatment come time the victim needs a medical procedure done themself.

From a financial perspective, medical identity theft can be very costly to a victim. According to Stephanie Armour's article entitled, "The Doctor Bill From Identity Thieves-Crooks use stolen personal data for medical care, drugs; victims get the tab*",* "The Ponemon survey found that 65% of victims reported they spent an average of $13,500 to restore credit, pay health-care providers for fraudulent claims and correct inaccuracies in their health records."[8] $13,500 is a large sum of money to pay for something that you didn't even incur yourself. If the unsettling fact that your medical records have been tampered with doesn't induce too much anxiety, the thought of giving up $13,500 probably will. That money could be used toward much more important expenses such as a child's education, paying off loans, a mortgage, or even your own expensive medical bills rather than cleaning up a stranger's wrongdoing. As a follow up question, one may wonder why it is the victim's responsibility to pay the cost of the fraud. Unfortunately, "unlike in financial identity theft, health-identity theft victims can remain on the hook for payment because there is no health-care equivalent of the Fair Credit Reporting Act, which limits consumers' monetary losses if someone uses their credit information."[8] The Fair Credit Reporting Act (FCRA) is an act which, "promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies"[9] and gives people the right to know what is in their file and if their file has been used against them. Because there isn't a health-care equivalent of the FCRA, it is even more difficult to reverse the negative affects of medical identity theft including paying for the criminal's expensive surgeries.

While Linda Weaver and Joe Ryan's cases negatively impacted their quality of life, an even more extreme case of medical identity theft happened to Anndorie Cromar. Cromar received a call in 2006 from Alta View Hospital in Sandy, Utah to inform her that her newborn baby tested positive for methamphetamine.[8] The disturbing part of this case is that the child was not Cromar's baby. Instead, "someone had stolen her identification, gone into labor, delivered a baby girl and left the infant at the hospital."[8] Reversing the confusion was not an easy task. Cromar had to go to court to have her name removed from the baby's birth certificate and it took several years for her to resolve.[8] This case highlights how unexpected the consequences of medical identity theft truly are as well as the time it takes to resolve the inaccuracies.

How can a victim resolve the consequences incurred?

While victimization can be quick to occur, it is not an easy fix. It can take months for a victim to attempt to correct their medical records and reverse billing notices.[8] To further the issue even more, because of federal medical privacy laws, a victim is not allowed to fully examine their medical records if a thief's health information is mixed with theirs for the sake of the privacy of the perpetrator's records. This seems very counterintuitive when a perpetrator has altered the victim's records. Unfortunately for the victim, "Federal medical-privacy laws bar a person's access to someone else's data, even if the information is in their own files, medical experts say."[8] This is most definitely a flaw in the system, but regardless it is an additional obstacle that victims must deal with in attempt to resolve the situation.

Once identity theft is identified, victims should act quickly to prevent more damage from being done. First, they should try to get copies of their medical records. As was mentioned in the previous section, a victim may have trouble getting their medical records due to privacy laws that will protect everyone, even the criminals who have stolen one's medical identity. However, if a provider refuses to give you copies of your records in order to protect the identity thief's privacy rights, the victim has the right to appeal it. He or she should, "contact the person the provider lists in its Notice of Privacy Practices, the Patient representative, or the ombudsman."[6] If the victim still hasn't received their records within 30 days, he or she should complain to the U.S. Department of Health and Human Services' Office for Civil Rights.[6] Next, the victim should contact anyone the perpetrator may have obtained medical services or goods from in his or her name. This includes doctors, clinics, pharmacies, and any other related entity. The victim should keep detailed records of all those interactions.

Another step is to obtain an Accounting of Disclosures. This is a record kept of all those who were given copies of your records. It includes when the information was sent, who it was sent to, and why it was sent. In addition to tracking who obtained your records, it's important to correct the inaccuracies in your files. Victims should get copies of their medical records and review them for accuracy and report any errors. Additionally it is important to notify health insurers and the 3 credit reporting companies of the fraud, order copies of credit reports, and put a fraud alert or security freeze on credit files so they cannot be further tampered with.[6]

Because of Health Insurance Portability and Accountability Act regulations that protect your medical records, it is difficult to update medical records. Therefore, prevention is much easier than dealing with the negative consequences that a victim suffers from when they don't protect themselves. Overall, the victim has to put in the effort to resolve their issues. It may take time and effort, but it is up to them to fix the fraud.[8]

Who is committing the theft and how?

In the previous sections we've reviewed what medical identity theft is, ways victimization is harmful, and how to resolve negative implications of victimization. However, we haven't yet explored who is committing the theft and how they do so. It was found by a police officer that identity theft causes similar trauma to that experienced by victims of repeated physical assault.[10] Therefore, attempting to eliminate this damage should be a priority in our society. In order to make progress in lessening the impact of identity theft, we must learn how the fraud is committed. Years ago the main methods of committing identity theft included dumpster diving and hacking. Dumpster diving is the physical act of rummaging through one's garbage for mail, receipts or anything that may give away valuable personal information for use in a fraudulent scheme. Hacking is a criminal's use of a computer to steal another's information. While these methods are still in use, a common way medical identity theft is committed today is by insiders. In hospitals and doctors offices, it isn't required by law that medical files be locked.[7] Even if it were a law, insiders will always have access to patient files anyway. This makes it easy for someone on the inside to steal records. Some then sell those records on the black market. While a resume may sell for $0.07 on the black market, medical records go for $50-$60.[7] Additionally, while a credit card number may sell for $6-$7, a social security number, insurance or Medicare/Medicaid number sells for $50. Your medical information is so valuable that fraudsters put a lot of effort into crafting a plan to obtain it. In some cases, criminals have organized fake clinics to obtain the information. They enticed elderly patients into visiting a clinic by promising free gifts and free transportation. When the patients got to the clinic, "Phony doctors performed superficial examinations on the victims and then submitted fraudulent medical claims in their names to the tune of over 1.1 million."[7] However, it isn't necessarily as difficult to get the information as the previous scheme makes it seem. While a patient is receiving care, their purses, wallets and personal items are often unsecured in the hospital rooms. This is an open opportunity for the information to be stolen. Additionally, patient wristbands also include valuable information such as social security numbers.[7] It isn't too difficult to obtain this valuable information when it is left in plain sight.

When an insider commits identity theft, they are breaking their position of trust. In a similar manner, fraud may happen between family members. In one example, a patient used her brother's medical insurance out of desperation. The brother was not an accessory to the crime, but instead a victim.[11] Other times it is the health-care providers themselves who are the perpetrators of the crime. In one case, Dr. Kenneth Johnson wrote and sold prescriptions for drugs on the black market.[8] For these reasons we have to be especially careful in assessing who we can trust with our information.

What steps are being taken to prevent medical identity theft?

In order to prevent medical identity theft in the future, action must be taken on both an individual and societal level. On an individual level, it is important to do things with common sense. The rule of thumb when it comes to fraud is that if something sounds too good to be true, then it usually is.[7] Keeping this in mind, it is important that victims don't fall for scams promising free medical services. These are likely fake clinics looking to obtain your information. Also common sense, patients should protect their medical insurance card like they would a credit card. Byron Hollis, managing director of the Blue Cross and Blue Shield Association's (BCBSA) National Anti-Fraud Department warns that "an insurance card is like a Visa card with a $1 million spending limit."[7] And if you are sharing information online, make sure the URL reads, “https:” as “s” stands for secure. Doing these few easy things may help protect the security of your identity.

On a societal level, there are state and federal laws that protect patients and their medical records. HIPAA, the Health Insurance Portability and Accountability Act of 1996 includes regulations on healthcare access, portability and renewal, preventing healthcare fraud, and research. The main purpose of HIPAA is to, “encourage electronic transactions of medical information and heightened safeguards to protect the security and confidentiality of medical information.”[7]

While medical identity theft is very serious and needs to be addressed in order to be prevented, there are not many laws which address its prevention which gives patients a false sense that it is not as big a problem as it truly is.[11] For example, the Federal Trade Commission (FTC) issued the Red Flags Rules in 2008, which made the development of medical identity theft prevention programs a requirement of hospitals. This was a step in the right direction for future prevention. However, these rules were revoked for some hospitals in 2010, no longer requiring the prevention techniques. [11]

Some hospitals are attempting to lessen the fraud and protect their patients by using biometric screening to confirm patient’s identities. These include biometric identifiers such as palm detection scanners which convert the scan into a number that is saved in the patient’s file. Using this software helps protect the identities of those patients. Some hospitals have put good effort torward using biometric identifiers and techniques as simple as photo identification requirements to combat the fraud.[8]

Medical identity theft is a scary threat to the well being of innocent people. Without learning more about its prevention, we are enabling it to grow.

3. Credit Card Fraud

Similarly to medical identity theft, the negative results of credit card fraud victimization can cause decades worth of financial damages. Credit card usage is common in most consumers' daily lives. According to the 2016 U.S. Consumer Payment Study, 40% of consumers in the study prefer to pay with their credit card instead of debit card or cash.[12] It was apparent from the study that people are concerned with security features of certain cards with 74% of consumers selecting the credit card with the most security features. Security features in a card were more important to the consumers than the rewards that the card had to offer. Despite the consumer's desire for security in credit card transactions, credit card fraud continues to grow each year. In AnnaMaria Andriotis' article, "Banking & Finance: Credit-Card Fraud Keeps Rising", it was said that "more consumers became victims of identity fraud last year than at any point in more than a decade despite new security protections implemented by the credit-card industry."[13] Despite the heightened security from 2015 to 2016, new account fraud increased by 40% and account takeover rose 20%.[13] Additionally, in 2015 it was estimated that 4.5% adults in the U.S. were card fraud victims. This is equivalent to $8 billion worth of fraud loss.[14] While we can estimate the current prevalence of the fraud, we cannot know exactly how much fraud takes place each year due to the fact that not all fraud is accounted for. This is because some banks and credit card companies that are hit with the fraud are too embarrassed to report it in fear that they will be thought of as a company with security problems.[15]

What is credit card fraud?

So what exactly is the fraud? "Credit card (or debit card) fraud is a form of identity theft that involves an unauthorized taking of another's credit card information for the purpose of charging purchases to the account or removing funds from it."[16] This form of credit card fraud is called account takeover, which is when an existing account is tampered with. Application fraud, another form of credit card fraud, is the use of someone's personal information to create a new credit card account.[16] In one example, Chernoh Jalloh was arrested at a traffic stop after it was discovered that he had more than ninety fraudulent credit and debit cards in his car, twenty-three of which had his name on them. He committed the fraud with the use of a device that would fraudulently encode the magnetic stripes on cards. The cards were associated with $40,000 worth of fraudulent transactions.[17] In just this one example of fraud, many innocent victim's lives were impacted for years to come.

What methods do fraudsters use to commit credit card fraud?

In the previous example, Jalloh used a device to commit $40,000 worth of credit card fraud. This is one of the many ways criminals commit this type of identity theft. Methods range from high-tech hacking or technological techniques to simpler physical dumpster diving. One tool that has aided identity theft recently is the Internet. In the article entitled, "Digital defense begins at home", Todd Shipley, the president of the High Technology Crime Investigation Association says, "Looking at digital crimes can be daunting, because every crime can have some sort of Internet tie-in."[18] As technology and the Internet has grown in recent times, so has the ease with which fraudsters can obtain a victim's personal information. As mentioned in the article, "How to protect and minimize consumer risk to identity theft", the Internet makes obtaining a victim's personal information such as credit card numbers much easier.[1] If information is put online or within the memory of a technological device, it is available to be hacked and stolen. This is a concept that many authors and researchers of identity theft agree upon. In Matthew Lease and Todd Burke's article, "Identity Theft A Fast-growing Crime", they write about the methods fraudsters use to obtain personal information. One of those methods pertains to identity thieves who use the Internet to find information to steal identities. A particularly unsettling assertion was that "Computerized information services may not safeguard the personal information adequately nor screen purchasers of computerized information appropriately, creating the opportunity for an identity thief to commit fraud."[19] It seems as though we cannot trust our information anywhere online without worrying that it will end up with dangerous people ready to take advantage of others. Many researchers agree that because the use of the Internet and technology continues to rise, using the Internet can aid identity theft.

Practically any informational article that is written about identity theft includes specific methods that fraudsters use to steal personal information and identities. These include posing as a legitimate employee, dumpster diving, and skimming.[1] Some additional methods that fraudsters use include very simple acts as well as some more complicated methods. Fraudsters may steal wallets, purses, mail, or "shoulder surf" during purchases to obtain personal information.[1] More complex methods include getting information from a business or employer or attempting to trick a person on the Internet.[1] A common technique called phishing is, "a high-tech scam that uses spam or pop-up messages to deceive consumers into disclosing credit card numbers."[1] The perpetrator may create a pop up that appears to be reliable which asks the victim to confirm account information. They attempt to trick even the most skeptical users into giving information.

In Jane Crossley's article entitled "Credit Card Fraud", she writes, "In 2008, card-not-present fraud accounted for 54% of fraud losses."[20] Just as one might expect, card-not-present fraud are transactions where a physical credit card does not need to be present at the time of purchase, such as during an online purchase. For this reason, "it is the path of least resistance."[14] Fraudsters know that fraudulent card-not-present transactions are harder to detect, which is why many decide to commit their crime in this way.

Also, the fact that more consumers now shop online adds to online credit card fraud. Not only does an increase in online shopping make for more opportunities to commit online credit card fraud, it also makes it more difficult for merchants to decipher which transactions are fraudulent and which are legitimate.[14] Merchants should be concerned with catching fraudulent transactions because they are responsible for paying for the fraud. However, they must also deliver products to customers in a timely manner.[14] After all, if the customer is not satisfied, the company won't have any legitimate orders to fill. According to a survey by Consulting Firm Javelin Strategy & Research, "More than 7.5% of online merchants' revenue is eaten up by the cost of actual fraud and costs associated with fraud-prevention tools."[14] This is a significant amount of merchant's revenue that is unnecessarily wasted on paying for a fraudster's lifestyle. Not to mention that consumers are also hit with higher interest rates and higher prices of products to offset the negative effect on a merchant's cash flow.[15] Because of this negative impact on the economy, multiple technological advancements have been tested in an attempt to prevent further increases in the crime.

What is being done to prevent the fraud?

New technology has been introduced to the world of credit card and debit card purchases in the last few years. Coupling tokenization techniques with EMV (Europay, Mastercard, and Visa) cards has attempted to control credit card fraud. Tokenization is a strategy implemented with mobile wallets in which the unique information of a credit or debit card, such as its account number, expiration date, and security code, is replaced by a set of numbers that can be used to confirm the consumer's identity without relaying the private card information to the merchant.[14] In the case that the data is stolen, the tokenization number will be compromised rather than the shopper's account number. Therefore, the card information is kept safe. Additionally, the U.S.

now uses EMV credit cards to further protect purchases. As opposed to magnetic stripe cards which can be compromised forever if the information is stolen once, EMV cards are very difficult to copy.[21] This is because unlike the magnetic stripes which hold the card information, the chips don't contain any of the card's data. Even if a fraudster is able to obtain the chip's data, it is useless to them.[21]

While the cards have many protective benefits, they also cause inconveniences that form disagreements as to whether or not these cards should be used. Some say that the new cards are beneficial to use because they add additional precautions so it is more difficult for the card information to be compromised. Others argue that the cards don't make shopping much safer because using the chip cards online or by phone is the same as using a credit card with a magnetic stripe. They also dislike the fact that inserting the card into the chip reader takes more time for validation in the system than the time it takes to swipe the magnetic swipe through the reader.[21] On the other hand, mobile pay options can help the economy as they may translate to quicker payment and therefore quicker service at fast-food restaurants or coffee shops. This would positively affect sales.[22]

Using the EMV credit cards with chips may benefit consumers because it is more difficult to compromise the card's information. In the article entitled, "New credit card chip technology puts businesses on the hook for fraud", Paul Muschick writes, "While cardholders aren't liable for fraudulent charges, they still suffer the headache of canceling compromised cards or recouping drained bank accounts. So they have an interest in making sure the best technology is used."[21] In the past, the bank or payment issuer would be liable to cover whatever fraudulent charge was made. However, as of October 2016, a new mandate requires the party that is less EMV compliant to take responsibility.[22] In making cards with chips, credit card companies are trying to bypass the use of the magnetic stripe in the future. For now, the cards will have the chip but they will continue to have the magnetic stripe as well.

Others think that rather than being an extra precaution, the EMV cards are just a hassle. They argue that using the cards requires more time at checkout which will likely cause backed up lines at the store and a less pleasant shopping experience without protecting the consumer much. Malware could potentially be produced that may compromise your credit card data even with the use of the chip.[23] In addition, Jason Oxman's article says that 50 percent of all fraud is committed online.[24] Since the method for using the EMV card for online or over the phone orders will be the same as using a magnetic stripe credit card, fraud will still occur. It currently takes approximately three seconds to swipe a card with the stripe, while using the chip card at checkout takes about eight seconds for verification. This causes people to feel inconvenienced.[21]

Overall, the use of the EMV cards poses a debate about whether or not they are helpful and safer to use in comparison to the current magnetic stripe cards. They cause disagreements because the use of the cards is something that is currently affecting consumers and employees alike. The reasons people dislike the new cards are considered reasonable, as are the arguments for adopting the EMV cards.

Regardless of one's opinion on the chip card's pros and cons, the fact of the matter is that using chips makes it more difficult for fraudsters to create counterfeit cards. It is said that the technology of a magnetic stripe card is comparable to the technology of a cassette tape.[22] It is embarrassing to think that we trust our bank accounts and future financial stability to the technology of many years ago. And while technology is expensive to implement with the most basic systems ranging from $500 to $1,500, it may be worth using if it is effective in preventing damaging consequences.[22] Adding a layer of protection to a magnetic stripe card brings us to the use of chip cards and mobile wallets. A mobile wallet is the mobile version of a chip card.[22] It was necessary that the U.S. adopt EMV technology when we did because other countries used it before us. This resulted in fraudsters coming to the U.S. to commit the crime since they knew it would be easier to get away with in America.

In addition to tokenization and the use of EMV cards, some banks are now using the location of customers to verify that their purchases are legitimate. The thought is that a customer's phone is likely with them when they are making a purchase with their card. Therefore, their location is used to confirm that the transaction is legitimate.[14] This is not a foolproof method for tackling the fraud in our country as not all customers have cellphones, not all of them carry their phones with them at all times, and not all banks have all of their customers' numbers. However, it is a start.[14] At this point, customers have to opt-in to use this system of protection.

Overall, the struggle that is being worked through is trying to prevent fraud without accidentally affecting legitimate transactions or disrupting the sales process of a business. The idea sounds much simpler than the actual complex task at hand.

What can I do to protect myself from credit card fraud victimization?

While the above explains the technological attempts at preventing credit card fraud, there are things each consumer can do to protect themselves as well. One simple step that can be taken to prevent the likelihood of credit card fraud is to remove oneself from being sent preapproved credit cards. While being sent the cards in the mail may seem harmless and routine, it can result in fraud if it ends up with a fraudulent party. Dumpster divers are able to commit fraud by collecting personal information that the victim has thrown away and put curbside to be collected. Since the curb is public domain, this act is also legal. If a perpetrator comes across a preapproved credit card that was thrown away without being shredded, he or she can easily fill it out and get the card sent to any address without the victim's knowledge of the fraud. A simple solution to this would be to insist that all personal information and pre-approved credit cards are shredded prior to being thrown away. However, fraudsters are tricky people and they have learned to illegally intercept mail prior to a victim knowing that they were due to receive it. In this scenario, the scammer could take the pre-approved credit cards from the mailbox and fill out the applications without the victim's knowledge that they were sent one.[25] Additionally, to keep your card information safe, avoid giving it out over the phone or lending it to a roommate or child. Look at your bank statements when you receive them and compare their validity with your receipts.[26]

If you report fraud when you notice it, you aren't liable for any more than $50.[26] While this isn't a life changing consequence, it is still important to protect yourself from the theft because of the negative impact it can have on your credit score. This is where the real harm is done. If a fraudster tarnishes a credit score, it is not easily or quickly reversed. This concept is highlighted well in a story mentioned in Rebecca Kanable's article, "The Face Of Identity Theft". In her article, Kanable writes,

> "One woman became a victim of identity theft 10 years ago and did everything she could to straighten out 'her' bad credit scores. When she finally was able to get a loan to purchase a new home, her mortgage interest rate was higher because of her low credit score. Every month she writes a check for her mortgage she's paying the price of identity theft. With identity theft, victimization doesn't seem to end."[2]

If victimization doesn't end once your identity has been stolen, it is important to avoid being targeted in the first place.

Overall, advancements are being made to prevent future credit card fraud. There is still a lot of progress to be made in terms of technological advancements, but we are on the starting path to achieving prevention of future credit card fraud.

4. Tax Identity Theft

What is tax identity theft? How is it committed?

Similar to medical identity theft and credit card fraud is tax-related identity theft. Also called tax-refund fraud, this identity theft involves a person's private information being stolen and fraudulently used against them for the benefit of the perpetrator. Specifically, it is using the information to file the victim's taxes with the hope of obtaining their refund.[27] This damaging fraud can be done with basic information and a social security number. Fraudsters are often willing to risk a lot for the benefits they will receive from committing the fraud. Some thieves create fake W-2s using a victim's employee identification number.[27] Others have gone so far as to pretend to be executives of a company to get victims' W-2s. Additionally, W-2s are sold on the dark web for $4-$20.[28]

So how do people know they've been victimized? Generally it isn't until one attempts to file their taxes and receives a notice that their social security number has already been used to file taxes that year that a person realizes he or she is an identity theft victim.[29] For example, Joe Garrett, a tax official for the state of Alabama, fell victim to identity theft in 2015. Garrett's fraud was found to be committed through TurboTax, the website he uses for his own tax returns. A fraudster opened a second TurboTax account in Garret's name using his social security number. When he questioned why he didn't hear about the second account from TurboTax, a representative replied that individual accounts cannot be discussed under certain privacy laws.[28] Our society has constantly been trying to make technical advancements in order to have the most efficient systems and processes. However, "Mr. Garrett said efforts to speed and automate the tax-refund process have made it far easier for criminals to commit quick, anonymous fraud."[30]

For this reason it is necessary to reassess what is best for tax-filers with both the pros and cons of each advancement.

A similar situation involves increased security. There have been many measures put into place this year to enhance the security of tax filers in order to protect their identity as they move forward with filing their taxes. However, with the positive effects of having more security come the negative aspects including false positives. In 2016 $9 billion or 1.2 million legitimate returns were delayed due to extra security precautions.[28] While the security is in place to benefit tax filers, it doesn't come without a cost. The same was discussed in the previous chapter with the discussion of whether EMV cards are worth the wait. In each of these situations it is important to realize that nothing that is worth developing comes without a cost. It is necessary to weigh what is most important for people as a whole. In this case, some may say that the delayed legitimate payments are worth experiencing until we figure out how to avoid tax identity theft. Others will likely disagree.

What is the scope and severity of tax identity theft?

The unfortunate news is that just one source of fraud opportunity can lead to a lot of damages. For example, a hospital worker stole 600 patients' personal information.[27] With it, the worker filed 29 fraudulent tax returns and was able to get $226,000 worth of refunds. Just one criminal and one glitch in the hospital's security system resulted in headaches for many people. The ease with which one person can harm many people is the main reason that this fraud is dangerous. Many times, CPAs find their client's tax fraud before the client finds out about it. In 2016, "59% of CPA tax practitioners said one or more of their clients were victims of tax identity theft during the year."[29] While this number has decreased from 63% in 2015, it is still a high statistic. Of those 59%, 95% said less than 5% of their clients were victims. While this is promising, it is still concerning.[29]

Elaborate schemes aren't always the preferred methods used to commit the fraud. Susan Pemberton and Cynthia Sibert of Nassau County put advertisements on Craigslist for job opportunities and apartment rentals that appeared to be legitimate. Instead, the duo collected the social security numbers, names, birthdates, and addresses of those who expressed interest. With the information that they collected, the two filed over 250 tax returns and opened loans and credit cards in the victims' names.[31] While we like to think that people have our best interest in mind, it is important to remember that there are many self-centered people or some who are desperate for money to the extent that they are willing to harm others for their benefit. Because of this, we need to protect ourselves and our personal information.

How can the fraud be prevented altogether?

According to a survey included in Paul Bonner's article entitled, "CPAs contend with tax ID theft", CPAs who attempted to resolve cases of theft ranked their attempts at resolving the theft an average of 2.7 on a scale of one to five with one being considered very difficult.[29] In the last five years, identity theft has shown up as number one on the IRS' list of "dirty dozen" tax scams multiple times including in 2016. It seems that the IRS has recently understood the importance of prevention. Paul Bonner's article, "Tax ID theft victims may obtain copies of fraudulent returns" reads, "Acknowledging that taxpayers victimized by stolen identification tax refund fraud may have a compelling concern to determine just what information about them was stolen and how it was used, the IRS said it will provide copies of fraudulent returns for the current tax year and up to six previous tax years."[29] This is a step in the direction of prevention because previously the returns were not allowed to be released. Additionally, the fraud is decreasing overall because of the security summit, “a group of federal, state and tax-prep industry officials convened by IRS commissioner John Koskinen in 2015.”[28] Overall, methods are being tested to make the system as efficient as possible. The IRS used data analytics with filters to attempt to make the process of selecting cases of tax identity fraud efficient and accurate. In testing just three elements, the IRS was able to prevent 24,000 returns from being incorrectly flagged as potentially fraudulent.[32]

The IRS is using more and more security measures in the process of identifying fraud each year. They have suggested using more verification requirements for certain software, they launched an Identity Theft Tax Refund Fraud Information Sharing and Analysis Center, and they created the security summit. Despite all that the IRS is trying to do to protect taxpayers, some of the responsibility also falls on the taxpayers themselves. The IRS.gov website article entitled, “Identity Theft Remains on ‘Dirty Dozen’ List of Tax Scams; IRS, States, Tax Industry Urge People to be Vigilant Against Criminals”, reaches out to taxpayers and suggests that they protect their information in any way possible. This includes protecting computers with virus protection and firewalls, encrypting tax files on one’s computer, and being careful about where and to whom you distribute valuable personal information.[33] Knowing the basics about victimization, such as the fact that the IRS will not email a taxpayer, can be simple information that saves a person time and money in the long run.[34]

What should you do if you become a victim of tax-refund fraud?

Claiming your refund once you’ve been victimized is possible. However, it is a lengthy and time consuming process which generally takes a minimum of six-months.[35] So what should you do if you find yourself in this situation? Some recommendations include closing your financial accounts, contacting the three credit bureaus (Equifax, Experian and TransUnion), filing a police report, contacting the social security administration, and putting a fraud alert on your account.[35] Additionally, if you think you may be a victim of tax identity theft, it is a good idea to file an Identity Theft Affidavit (IRS form 14039) to put an alert on the account.[35] This form will help anyone who thinks fraud has occurred and it will be given more time to exercise additional security precautions. If you decide to file that form, "When the IRS receives the affidavit, it will flag the taxpayer's account with a marker indicating that a tax return filed under the taxpayer's name could be fraudulent. In some cases the IRS will issue that taxpayer an identity protection personal identification number. This IP FIN must be included on the tax return for the tax year for which it was issued or the tax return will be automatically rejected."[35]

Tax identity theft shouldn't be taken lightly. While the IRS is working to protect each of us from becoming victims, we need to do the foundational work in securing our private information so we don't make it easy for the fraud to be committed against us.

5. Identity Theft and Consumer Data Breaches

Over the last few years, consumer data breaches have been especially prominent. It seems as though we are always hearing of a new story on the news about a large corporation that we visit frequently losing to hackers due to a lack of cyber security. These include Home Depot, Anthem, Target, Sony, and Citibank, just to name a few.[40] With each of these large companies losing to hackers, innocent customers' emails and credit/debit card information have been compromised. In John Jesitus' article entitled, "Data breaches a near certainty", Jennifer Searfoss, Esq. writes that because of our reliance on the internet, the loss of data to hackers isn't just a possibility, "It's a certainty. It's just a question of when, and of what nature."[36] The Internet's role in our lives has greatly increased over the last decade. Just as was discussed earlier in this thesis with its affect on credit card fraud is its impact in data breaches. There are very smart cybercriminals everywhere who know how to manipulate systems. As people whose lives operate on Internet use every day, we need to understand that everything that we put out online can be stolen in an instant. Even those who don't use the Internet recreationally are at risk of their information being hacked given usage of servers by hospitals and medical clinics. While it is true that even those who don't use the Internet for recreational purposes can have their medical identities stolen due to data breaches, the following case brings to light that it is our responsibility to protect our private information to the best of our ability. The Anthem data breach, which involved criminals stealing information from December 2014 through January 2015,[37] resulted in 78.8 million current and former customers' personal information such as names, birthdate and social security numbers being stolen.[38] Many people noticed that they were victimized closely following the time of that breach. While it's difficult for anyone to surely state that the resulting fraud was caused by the Anthem hack, it's probably not entirely a coincidence.

In response to the hack, many Anthem customers complained to the company. Because it is hard to say whether the victimization occurred due to a lack of personal security or due to the breach, Anthem responded by requesting to search the victim's computers to analyze whether they had properly protected their own information.[39] It was said in Tim Greene's article, "Anthem to data breach victims: Maybe the damages are you own darned fault" that once this was requested, many customers revoked their complaints.[39] This could be because they knew that they did not properly protect themselves, they didn't want someone snooping around on their computer, or they didn't want to give up their computers for a period of time. For this reason, it is important to protect your own information online and on paper because if it falls into the wrong hands, there can be serious consequences.

It isn't completely the fault of the individuals either. The breach was the cause for some people's fraud. This is evident when it was brought up that kids' social security numbers were used fraudulently and that, unlike their parents, the only logical place to retrieve a child's social security number would be through a health insurer.[38]

Methods to protect oneself from being victimized by a data breach

Many of the best ways to protect oneself from being victimized are common sense. If someone shreds his or her personal documents and is careful about personal information posted online, they will be more difficult targets for identity thieves. It is highly recommended for personal information to be protected physically and on all networks. Additionally, software is on the market to protect customer's identities. LifeLock is a membership that can be purchased to protect against identity theft. Similar to insurance for identity theft, LifeLock will monitor your accounts and credit score and if you become a victim they will help recover the damages up to one million dollars. Upon entering their website, the tagline reads, "Don't think it can happen to you? 1 in 4 people have experienced identity theft."[41] In 2010, the United States Census Bureau partnered with LifeLock to protect U.S. citizens when providing their demographics for the Census.[42] The Census requires that all people send their personal information and if they fail to send their information by April, a Census taker will go to their home to obtain the information. This is the source of some identity theft. Fraudsters pretend to be Census takers and collect information necessary to commit identity theft. [42] In partnering with LifeLock, the U.S. Census Bureau attempted to protect U.S. citizens from being targeted by perpetrators looking to take advantage of this opportunity.

6. Conclusion

In conclusion, as patients, consumers, and tax-filers, it is our job to protect our personal information from being stolen and used for another's benefit. While businesses and governmental agencies are working to protect our medical and financial health from being negatively impacted by identity theft, it was made clear in the research that we must put in the effort to keep our valuable personal information private. In an age where use of technology continues to grow, being knowledgeable about each type of identity theft and how fraudsters commit the theft can be very beneficial in protecting ourselves from becoming one of the 15 million identity theft victims each year. [3]

7. Bibliography

1. Albrecht, Chad, Conan Albrecht, and Shay Tzafrir. "How to Protect and Minimize Consumer Risk to Identity Theft." *Journal of Financial Crime* 18, no. 4 (2011): 405-14. Accessed February 3, 2016. http://lib.assumption.edu/login?url=http://search.proquest.com/docview/898415400?accountid=36120.

2. Kanable, Rebecca. "The Face of Identity Theft." *Law Enforcement Technology* 36, no. 4 (2009): 28-33. Accessed February 15, 2016. http://lib.assumption.edu/login?url=http://search.proquest.com/docview/229835006?accountid=36120.

3. "Identity Theft Victim Statistics." Identity Theft and Scam Prevention Services. 2016. Accessed April 13, 2017. http://www.identitytheft.info/victims.aspx.

4. Fay, Anthony. "Waiter Charged with Credit Card Fraud." WWLP.com. September 25, 2015. Accessed February 24, 2016. http://wwlp.com/2015/09/25/waiter-charged-with-credit-card-fraud/.

5. Denny, Dawn. "Cashier Linked to Credit Card Skimming Scam, Police Say." KXAN.com. July 29, 2014. Accessed February 24, 2016. http://kxan.com/2014/05/20/restaurant-cashier-linked-to-credit-card-skimming-scam-police-say/.

6. "Medical Identity Theft." Consumer Information. August 2012. Accessed February 14, 2017. https://www.consumer.ftc.gov/articles/0171-medical-identity-theft.

7. Biegelman, Martin T. "Medical Identity Theft." In *Identity Theft Handbook: Detection, Prevention, and Security*, 97-112. Hoboken, NJ: Wiley, 2009. Accessed March 1, 2016.

8. Armour, Stephanie. "The Doctor Bill From Identity Thieves --- Crooks Use Stolen Personal Data for Medical Care, Drugs; Victims Get the Tab." *Wall Street Journal*, August 08, 2015. Accessed March 14, 2017. http://lib.assumption.edu/login?url=http://search.proquest.com/docview/1702192791?accountid=36120.

9."Fair Credit Reporting Act." *Dictionary of Marketing Communications*. Accessed February 15, 2017. doi:10.4135/9781452229669.n1256.

10. Benibo, Biiaye R, PhD, Valrie, CPA, PhD Chambers, and Betty, Phd Thorne. "Breaking Bad News to Victims of Identity Theft: Lessons from Medical Doctors." *Journal of Accountancy* 222, no. 2 (August 2016): 30-34. Accessed March 14, 2017. http://lib.assumption.edu/login?url=http://search.proquest.com/docview/1809564535?accountid=36120.

11. Mancini, Michelino. "Medical Identity Theft in the Emergency Department: Awareness Is Crucial." *Western Journal of Emergency Medicine* 15, no. 7 (2014): 899-901. Accessed February 20, 2017. PMC.

12. *2016 U.S. Consumer Payment Study*, October 2016. Accessed March 28, 2017. http://tsys.com/Assets/TSYS/downloads/rs_2016-us-consumer-payment-study.pdf.

13. Andriotis, Annamaria, and Peter Rudegeair. "Banking & Finance: Credit-Card Fraud Keeps Rising --- Industry Adds Chips and Other Protections, but Number of Victims Increases by 18%." *Wall Street Journal*, February 02, 2017. Accessed March 14, 2017. http://lib.assumption.edu/login?url=http://search.proquest.com/docview/1863541857?accountid=36120.

14. Sidel, Robin. "Credit-Card Fraud Grows Online." *Wall Street Journal*, October 26, 2016. Accessed February 14, 2017. http://lib.assumption.edu/login?url=http://search.proquest.com/docview/1832121549?accountid=36120.

15. Corbitt, Terry. "Credit Card Fraud." *Credit Management*, March 2003, 31-32. Accessed April 24, 2017. http://lib.assumption.edu/login?url=http://search.proquest.com/docview/228353745?accountid=36120.

16. "Criminal Law." Findlaw. 2017. Accessed February 18, 2017. http://criminal.findlaw.com/.

17. Jeffrey, Jeff. "Credit Card Fraud Scheme Nets 37-month Sentence." *South Carolina Lawyers Weekly*, May 25, 2016. Accessed March 22, 2017. http://lib.assumption.edu/login?url=http://search.proquest.com/docview/1792454001?accountid=36120.

18. Garrett, Ronnie. "Digital Defense Begins at Home." *Law Enforcement Technology* 37, no. 4 (2010): 16-22. Accessed February 3, 2016. http://lib.assumption.edu/login?url=http://search.proquest.com/docview/229777099?accountid=36120.

19. Lease, Matthew L., and Tod W. Burke. "Identity Theft." *The FBI Law Enforcement Bulletin*, August 2000, 8. Accessed February 1, 2016. http://go.galegroup.com/ps/i.do?id=GALE|A65241453&v=2.1&u=mlin_c_assumpt&it=r&p=PPCJ&sw=w&asid=226f8c351e71df1e12a573f38c364ce0.

20. Crossley, Jane. "Credit Card Fraud." Credit Management, May 2009, 26-27. Accessed March 14, 2017. http://lib.assumption.edu/login?url=http://search.proquest.com/docview/228314909?accountid=36120.

21. Muschick, Paul. "New Credit Card Chip Technology Puts Businesses on the Hook for Fraud." *McClatchy - Tribune Business News*, October 01, 2015. Accessed March 2, 2016. http://lib.assumption.edu/login?url=http://search.proquest.com/docview/1718223391?accountid=36120.

22. Fry, Meg. "Chipping Away at Credit Card Fraud." *Njbiz* 29, no. 20 (May 16, 2016): 9. Accessed March 22, 2017. http://lib.assumption.edu/login?url=http://search.proquest.com/docview/1797248370?accountid=36120.

23. Camp, Cameron. "EMV Cards Still Prone to Payments Crime." American Banker. January 15, 2015. Accessed March 2, 2016. http://bi.galegroup.com/global/article/GALE%7CA397375970/0ff7ad3abfb794423ac02781d6b212e7?u=mlin_c_assumpt.

24. Oxman, Jason. "EMV Cards: The Beginning of the End for Hackers." American Banker. September 30, 2015. Accessed March 2, 2016.

25. Murphy, Colm. "Identity Theft: Protecting Yourself on the Internet." *Accountancy Ireland* 40, no. 5 (October 2008): 52-54. Accessed February 24, 2016. http://lib.assumption.edu/login?url=http://search.proquest.com/docview/223190815?accountid=36120.

26. "Protecting Against Credit Card Fraud." Consumer Information. July 2012. Accessed February 14, 2017. https://www.consumer.ftc.gov/articles/0216-protecting-against-credit-card-fraud.

27. Dishman, Scott. "Preventing Tax-related ID Theft." *Accounting Today* 31, no. 1 (January 2017): 6. Accessed April 4, 2017. http://lib.assumption.edu/login?url=http://search.proquest.com/docview/1864063456?accountid=36120.

28. Saunders, Laura. "Weekend Investor -- Tax Report: Tax-ID Theft Drops, but Vigilance Still Needed." *Wall Street Journal*, March 04, 2017. Accessed April 9, 2017. http://lib.assumption.edu/login?url=http://search.proquest.com/docview/1873954601?accountid=36120.

29. Bonner, Paul. "CPAs Contend with Tax ID Theft." *Journal of Accountancy* 222, no. 2 (August 2016): 26-29. Accessed April 4, 2017. http://lib.assumption.edu/login?url=http://search.proquest.com/docview/1809564654?accountid=36120.

30. Saunders, Laura. "Even the Tax Man Has a Taxing Time." *Wall Street Journal*, April 16, 2015. Accessed April 10, 2017. http://lib.assumption.edu/login?url=http://search.proquest.com/docview/1673303733?accountid=36120.

31. Callegari, John. "Nassau Women Charged with Craigslist ID Theft." *Long Island Business News*, January 26, 2012. Accessed April 10, 2017. http://lib.assumption.edu/login?url=http://search.proquest.com/docview/919124660?accountid=36120.

32. Cohn, Michael. "IRS Filters Caught $4.1 Bn in ID Theft." *Accounting Today* 30, no. 11 (November 2016): 52. Accessed April 12, 2017. http://lib.assumption.edu/login?url=http://search.proquest.com/docview/1838667782?accountid=36120.

33. "Identity Theft Remains on "Dirty Dozen" List of Tax Scams; IRS, States, Tax Industry Urge People to Be Vigilant Against Criminals." Identity Theft Remains on "Dirty Dozen" List of Tax Scams; IRS, States, Tax Industry Urge People to Be Vigilant Against Criminals. February 3, 2017. Accessed April 10, 2017. https://www.irs.gov/uac/newsroom/identity-theft-remains-on-dirty-dozen-list-of-tax-scams-irs-states-tax-industry-urge-people-to-be-vigilant-against-criminals.

34. Dougas, Christine. "Watch Out: Tax Time Is Prime Time for ID Theft." *USA Today*, 2013, 3B. Accessed March 4, 2017.

35. Jones, George G., and Mark A. Luscombe. "Tax ID Theft: Best Practices for Individuals and Businesses." *Accounting Today* 27, no. 8 (August 2013): 14-15. Accessed April 10, 2017. http://lib.assumption.edu/login?url=http://search.proquest.com/docview/1426016269?accountid=36120.

36. Jesitus, John. "Data Breaches a near Certainty." *Dermatology Times* 38, no. 3 (March 2017): 73-81. Accessed April 23, 2017. http://lib.assumption.edu/login?url=http://search.proquest.com/docview/1881387040?accountid=36120.

37. Bankrate.com - Compare Mortgage, Refinance, Insurance, CD Rates. 2017. http://www.bankrate.com/.

38.Wall, J.K. "Customers of Anthem say ID theft proliferating: but insurer, citing FBI, denies breach to blame." *Indianapolis Business Journal*, July 13, 2015, 1+. *General OneFile* (accessed April 23, 2017). http://libraries.state.ma.us/login?gwurl=http://go.galegroup.com/ps/i.do?p=ITOF&sw=w&u=mlin_c_assumpt&v=2.1&it=r&id=GALE%7CA424990248&asid=315b34f4e8140bb38042cd3e10ff1261.

39.Greene, Tim. "Anthem to data breach victims: Maybe the damages are your own darned fault." *Network World*, April 10, 2017. *General OneFile* (accessed April 23, 2017). http://libraries.state.ma.us/login?gwurl=http://go.galegroup.com/ps/i.do?p=ITOF&sw=w&u=mlin_c_assumpt&v=2.1&it=r&id=GALE%7CA489068912&asid=a589f98aeae3cbe0703a8ec6d85cfa3f.

40. Bankrate.com, Allison Ross •. "11 Major US Data Breaches." 11 Major US Data Breaches. Accessed April 2, 2017. http://www.bankrate.com/finance/banking/us-data-breaches-1.aspx.

41. "Identity Theft Protection - Avoid ID & Credit Fraud | LifeLock." LifeLock. 2016. Accessed March 3, 2016. https://www.lifelock.com/.

42. "LifeLock Partners with 2010 Census to Help Protect Consumers from Identity Theft." *Business Wire*, March 08, 2010. Accessed March 15, 2016. http://lib.assumption.edu/login?url=http://search.proquest.com/docview/219911292?accountid=36120.