Identity Theft

What You Don't Know Can Hurt You

Anita Koch
Identity Theft Risk Management Specialist

with Perry Sylvester

Identity Theft: What You Don't Know Can Hurt You

What Insurance Professionals Should Know About Identity Theft

Dedication

To all the representatives of LegalShield and IDShield, in honor of their dedication to serving and protecting individuals, families, small businesses and their employees from the ramifications associated with all of the various forms of identity theft.

To my husband, Mike Koch, for his support during the countless hours spent studying, researching, and writing **Identity Theft: What You Don't Know Can Hurt You.**

What Insurance Professionals Should Know About Identity Theft.

Table of Contents

Foreword

Like most people, I would prefer to not even think about identity theft, let alone actively try and educate myself about the matter. My sense was, "Who has the time to learn about this stuff?" Fortunately, I met identity theft expert Anita Koch. From my conversations with her, I came to understand that the possibility of having to spend up to 600 hours—that is, I believe, **15** (count 'em, *fifteen*, as 'five-less-than-twenty') **40-hour work weeks**--to correct the mess made by an identity thief is not just a remote threat, something that happens to "the other guy," but a very real, dare I say, *common* risk.

Given the likelihood and potential severity of the risk, the idea of spending some time to learn how to protect myself seemed, well, a little less burdensome. Like the UCLA basketball coach John Wooden said, "*If you don't have time* to do it right, when will you *have time* to do it over?" It is for this reason I was delighted to be able to help make this information report available to the general public. Anita provides an outstanding overview of the challenge personal identity theft presents to all of us. She does not, however, stop at informing us about the risk; she takes the additional step to show us how to take action to protect ourselves or, if we have already become a victim, how to start piecing our reputations back together.

Perry Sylvester

American Education Systems, LC
14 Belleview, Mt. Clemens, MI 48043
www.BestInsuranceContinuingEducation.com

Preface

It was the early 1990's and my husband, Mike, and I were small business owners. We had a credit card used for the purchase typical business items (office supplies, fuel, furniture, etc.). I kept the books and made sure that adequate funds were set aside to pay the balance in full every month. It was a total shock when I opened the statement one month to find that it was almost *10 times* what it should have been! There were dozens of out of state charges for thousands of dollars. How could this have happened?! Neither of us had lost our credit card nor had we been in the city where the purchases were made in years! Even though we were not, ultimately, held liable for the charges, the situation certainly caused me many sleepless nights and a few extra gray hairs.

Due to that experience, I was very interested to learn more, and accepted the invitation to a LegalShield seminar regarding a service to help those who found themselves victims of identity theft. That was the beginning of my journey. With a background as a teacher, it became my mission to educate people about the fact that there is much more to identity theft than just the financial aspect and what they could do to protect themselves from the growing crime of identity theft.

Many companies have spent millions of dollars claiming to have "the answer" to identity theft, but the truth is that there is *no way* to stop this crime from happening – our data is irretrievably "out there." I believe it was important for the public to be aware of the *facts* regarding identity theft and understand what they are getting when they purchase an identity theft protection service.

Many consumers go to their insurance professional for advice, who may or may not have a clear understanding of all the

aspects of identity theft as well as the benefits and shortcomings of the various identity theft protection services available in the marketplace. All of these factors contributed to the writing of this report.

Anita Koch

248-361-9641 akoch@premiersolutionsintl.com **www.AnitaKoch.com**

Introduction

Identity theft has been the ***Number ONE*** reported crime to the Federal Trade Commission since the year 2000. The FTC received *more than two million complaints* in 2012 alone. Nearly one in five of those complaints was related to identity theft, including: the improper use of personal information such as bank account or credit information or the use of someone's Social Security number to commit theft or fraud.

It is important for you to understand that identity theft is *not* just a financial problem. While credit related crimes are certainly one aspect of identity theft, shredding your mail is only a miniscule part of the combating this serious crime. Other forms of identity theft include Medical, Social Security, Driver's License, Character/Criminal, and more. When someone's medical records have been changed, or they face tax issues, or even false imprisonment as a result of someone stealing their identity, that's the time when they *wish* it was as simple as a credit card or bank account issue.

In this report we will do our best to help you understand the various forms of identity theft, who it affects, how the clients of insurance professionals may be impacted, and what are some reasonable steps that can be taken to protect yourself, your family and insurance customers from one of the fastest growing crimes in the world.

If you have further questions, please feel free to contact me!

Phone: 248-361-9641
Email: akoch@premiersolutionsintl.com
Website: www.AnitaKoch.com

How Did We Get Here?

Most people tend to believe that Identity Theft began with the advent of the internet. While it is true that in today's world the internet does play a rather large role in identity theft; that was not always the case.

In the Bible, Genesis 27 may be one of the first recorded tales of Identity Theft. This tells the story of Jacob using goat skin to cover his hands and neck to steal his brother, Esau's identity. By doing this, Jacob was able to receive the blessing that should have been given to the firstborn son.

While on an expedition to Morocco in 1578, the King of Portugal, Sebastian, was killed and a large number of Portuguese people refused to accept his death. Many believed that the king was hiding on some tropical island and would return to claim his throne. This belief encouraged four pretenders to attempt to impersonate King Sebastian. It didn't take long for the two that were of peasant origin to be found out. The third impersonator, Gabriel Espinosa, was somewhat educated and was a bit more effective in impersonating King Sebastian, but he was eventually captured and executed in 1594. In 1603 the fourth and final imposter, Marco Tullio, spoke no Portuguese at all, but was, remarkably, the most successful in impersonating the king. Even though he had a fairly large following, he too was eventually captured and executed.

In 1964, the Oxford English Dictionary was the first to include a definition for the term "identity theft," followed in 1979 by Collins English Dictionary. According to the Federal Trade Commission, "Identity theft happens when someone steals your personal information and uses it without your permission. It's a serious crime that can wreak havoc with your finances,

credit history, and reputation — and can take time, money, and patience to resolve."

Have you heard the name Frank Abagnale? How about the movie, "Catch Me If You Can" released in 2002, which was based on Mr. Abagnale's rather interesting life? Starting as a teenager in 1963, Mr. Abagnale might be considered one of the first, in more recent times, to be involved in identity theft. Abagnale assumed at least eight identities, including a doctor, an airline pilot, a lawyer and more.

The primary difference between him and most of today's identity thief is that Abagnale did not assume someone else's identity, but created new identities for himself. He did, however, defraud many people and a number of institutions out of many thousands of dollars. (Here's a clip from the 1970's show To Tell the Truth featuring Frank Abagnale that you might find entertaining.)

https://www.youtube.com/watch?v=5w9NsxWFYFU

There may be a few of you reading this who at some point during your younger years used "fake id" to get into a drinking establishment before you were legally old enough to do so. Yes, folks … that was a form of identity theft and it seemed to be fairly harmless back then.

Getting a fake id as a college student today may seem like it's "no big deal" to the 18 year old. Perhaps your child is away from home and on his or her own for the first time and is not quite old enough to get into the spot that "everyone" is going to. However, getting a fake id online could be the beginning of a much bigger problem than underage drinking.

In order to get the fake id, at least some real information will need to be supplied –name, address, a photo … perhaps even a driver's license number may be required. And, of course, payment must be made which gives access to a credit card number,

expiration date and the CSC (card security code) from the back of the credit card. This information is more than enough for identity thieves to wreak havoc for the college student and his or her family.

There was a tremendous increase in identity theft with passage of the Immigration Reform and Control Act of 1986 (Public Law 99-603, 100 Statute 3359). This law requires employers to verify that employees have entered into the United States legally. As a result, a new industry was born for the purpose of providing illegal immigrants with driver's licenses and Social Security cards.

It is a relatively simple process for people who come into the U.S. illegally to buy a set of identifying documents. Of course, these papers are necessary for them to be able to get a job and a paycheck.

Illegal immigrants who purchase identifying documents are not doing so with the intention of harming anyone. They are usually reassured by the sellers that there is no need to worry about the identity they are receiving. They are assured that this identity belongs to a person who passed away, or someone who no longer works in this country. They may even be told that the identity belonged to someone who sold his identity papers or that the information is for someone who never even existed.

The fact is that identity theft has been around for centuries, and there is nothing that can be done to completely eradicate this problem. There are, however, steps that can be taken to mitigate risk and expedite recovery for victims.

Phone: 248-361-9641
Email: akoch@premiersolutionsintl.com
Website: www.AnitaKoch.com

A Growing "Business"

Security analysts are saying that it's no longer a question of "if" but "when," and everyone should prepare to become a victim of identity theft at some point. It is expected that financial identify theft, defined as the misuse of credit-card, bank-account or other personal information to commit fraud (successful or attempted) will surpass traditional theft as the leading form of property crime.

Even the most cautious consumer cannot completely prevent identity theft. Serious data breaches are reported on a regular basis. Customers of TJ Maxx, Michael's, Target, Neiman Marcus, Home Depot, Dairy Queen, Sears/K-Mart and Anthem Health Care were all victims of cyber-attacks, affecting millions.

The U.S. Department of Justice figures report that credit-card data theft is exploding, increasing 50% from 2005 to 2010.

In America in 2013, a new identity fraud victim was hit every two seconds! According to Javelin Strategy & Research's 2014 Identity Fraud Study, the number of victims rose to 13.1 million over the year. This is an increase of more than 500,000 victims over 2012.

Direct and indirect losses from identity theft totaled $24.7 billion in 2012. We have become so familiar with these huge numbers that we are almost immune to them. Let's put it into perspective.

$24,700,000,000 … *$24.7 BILLION DOLLARS*

If you make $100,000.00 a year, that's two hundred and forty-seven thousand *years* of wages! (494,000 Years if you make $50,000 a year.)

If you made a MILLION DOLLARS A YEAR, you would have to work *247 YEARS* to earn that much money!

What's even more shocking is that over the same period of time, losses from other types of theft (i.e. burglary, motor vehicle theft and other property theft) was $14 billion … that's over $10 BILLION DOLLARS ***more*** from Identity Theft than from all other forms of theft *combined!*

The Javelin Strategy & Research's 2014 Identity Fraud Study reports that one out of every three people notified of being a potential fraud victim actually becomes one. Of the consumers who experienced a card breach, 46% became fraud victims that same year. This is an increase from one in four in 2012.

Identity theft victims who had personal information used to open a new account or for other fraudulent purposes were more likely than victims of existing account fraud to experience financial, credit, and relationship problems and severe emotional distress.

The banks and other financial institutions are getting pretty good at detecting Identity theft. (It's to their benefit to do so, since they bear the brunt of the fraud.) The bad news is that, without help, only 8% of Identity Theft victims discover it on their own.

Identity Theft is *big business* so don't expect it to "go away" any time soon. In fact, you can expect it to be around for a very long time to come.

Phone: 248-361-9641
Email: akoch@premiersolutionsintl.com
Website: www.AnitaKoch.com

What the Numbers Tell Us

It was not until the passage of the Identity Theft and Assumption Deterrence Act of 1998 that identity theft was finally recognized as a crime. With the Federal Trade Commission as the lead governmental agency for consumer matters related to this offense, a centralized source for accepting reports and tracking incidence of identity theft was established.

Since inception, identity theft has consistently been the number one (1) consumer complaint reported to the FTC each year. Early reports indicated that identity theft cases ranged from 400,000 to as high as 750,000 per year. However, it is the opinion of consumer advocacy groups that these numbers are not indicative of the true number of cases for several reasons.

Some of the reasons for the under-reporting of these numbers include the following.

1. The statistics are only based on cases officially reported to the Federal Trade Commission.
2. The number of organizations reporting to the FTC database is very limited
3. The definition of "identity theft" differs between reporting organizations. For example, identity theft as defined by law enforcement differs from that of financial institutions.
4. Identity theft laws vary from state to state.
5. Cases involving children and the deceased were not included in the totals.

2003 was the first year that the Federal Trade Commission released a report on the statistics of reported identity theft. On September 3, 2003 the FTC Identity Theft Survey indicated that 27.3 million Americans were victims of identity theft

between 1998 and 2002, including 9.9 million people in 2002 alone.

The Identity Theft Survey of 2003 also showed that the out-of-pocket expenses of consumers who were victims of identity theft amounted to $5 billion. The losses to businesses and financial institutions added up to almost $48 billion dollars.

The most recent Identity Theft Survey covers the year of 2012. According to this document issued by the U.S. Department of Justice:

- Approximately 16.6 million persons or 7% of all U.S. residents age 16 or older, were identity theft victims one or more times in 2012
- Direct and indirect losses due to identity theft totaled $24.7 billion in 2012, an increase of almost 400% since the first survey in 2003
- Most commonly misused information include
    - Existing bank accounts – 37%
    - Credit card accounts – 40%
- When a victim's personal information was used to open a new account or for other fraudulent purposes, the victim was more likely to experience "financial, credit, and relationship problems and *severe emotional distress."*
- 79% of identity theft victims reported some degree of emotional distress
- Moderate to severe emotional distress was reported by 36% of identity theft victims
- Out-of-pocket losses of $1 or more were experienced by about 14% of identity theft victims, with approximately half of those victims suffering losses of less than $100
- 29% of victims spent more than a month to resolve problems associated with identity theft
- Losses attributed directly or indirectly to identity theft totaled $24.7 billion

- 22% of identity theft victims experienced multiple incidents of identity theft
- Households with higher annual incomes were more likely to experience identity theft than those with lower incomes
- Persons between the ages of 18 to 24 and over the age of 65 were more likely to experience identity theft than other age groups
- The most common way victims discovered financial identity theft was by a financial institution notifying them of a problem
- Most victims of identity theft did not know how their information was obtained and 9 out of 10 victims knew nothing about the person who committed the theft
- Less than 10% of victims reported the crime to law enforcement and/or to the FTC

The rate of nine (9) to ten (10) million new victims has remained consistent since the FTC's first survey in 2003. Consumer advocacy groups continue to advise that the numbers are vastly under-reported due to the previously cited factors.

Phone: 248-361-9641
Email: akoch@premiersolutionsintl.com
Website: www.AnitaKoch.com

The Types of ID Theft

While credit card and bank fraud are the most commonly known types of identity theft, this is a crime that is definitely not limited to the financial arena. In addition, many people think that identity theft only happens to the wealthy. After all, why would anyone be interested in stealing the identity of someone who has little money in the bank?

It may come as a surprise to many, but the harsh reality is that *anyone* can become a victim of identity theft … from college students to senior citizens, identity theft is non-discriminatory and has no respect for age, race, sex or income level.

Financial Identity Theft

Joe T. only had one credit card, an American Express that he paid in full every month. Consequently, he had a difficult time understanding why he was being harassed by a collection agency for a $5,000 balance on a Visa card.

He called the collection agency and the creditor that issued the card. After hours of research, Joe figured out that an application for credit had been sent to his previous address and an identity thief had filled it out. Using Joe's good credit, the thief was issued a Visa card with a $5,000 limit. Of course, it is likely that the thief never intended to pay the bill. Instead, when the card was maxed out, the thief walked away with the merchandise and Joe was left with the bill. The house that Joe wanted to buy had to be put on hold due to the damage that the identity theft had done to his credit score.

Identity theft comes in many forms. The most well-known and well-advertised is Financial Identity Theft. This is the form of identity theft that is affecting more and more individuals and small business owners every year.

Financial identity theft may result in:

- Problems securing a loan
- Harassment from debt collectors
- Reduced credit scores
- Fraudulent Credit Cards being opened in your name
- Debit card or checking accounts being used fraudulently
- Savings accounts depleted
- Investment account fraud
- Loan and Mortgage fraud
- Tax fraud

The use of debit cards is more prevalent today than ever before. The use of debit cards as a means of financial management helps to reduce the overuse of credit cards and the associated interest. However, identity theft can have an even greater impact with debit cards due to the fact that a debit card withdraws money directly from your checking account. If an identity thief gains access to your debit card and you are unaware that your bank account has been depleted, you could end up with overdraft fees and bounced checks. In addition, there may be no way for you to access the missing funds during the time that the bank is investigating your report of the crime.

Identity theft is now being used by car thieves. Using stolen identification the thief then finances or rents a car from a dealer or private seller and then drives off, never to be seen again. The unsuspecting identity theft victim may now end up with damaged credit. Unless they pay for the car or jump through hoops to prove that it wasn't them, the victims may find themselves being harassed by debt collectors for an automobile they never saw.

Cases involving identity theft of brokerage accounts have also become more frequent in recent years. In some instances, the person responsible for the theft is a close family member or friend of the victim – an ex-husband, trusted relatives, or caregiver. Sometimes the perpetrator is a complete stranger

who has been able to hack into the victim's computer and steal that person's brokerage ID and password information.

Rashia Wilson was arrested and sentenced to 21 years in jail after boasting on Facebook to be the "Queen of IRS Tax Fraud." Along with her boyfriend, she filed more than 220 fraudulent tax returns between 2009 and 2012. While she was convicted of stealing more than $3 million dollars, it is speculated the sum may have been closer to $21 million dollars!

It is estimated that between 2003 and 2013, from $99 Billion to $119 Billion was paid by the IRS in incorrect payments for the earned income tax credits alone. In the first six months of 2013, 1.6 million U.S. taxpayers were affected by identity theft. In total for the entire year of 2010 there were 271,000 falsified tax returns, according to the Treasury Department's inspector general. Even though the IRS has discovered many incidents of tax fraud, billions of dollars have been paid in what are, in all likelihood, fraudulent refunds, according to various government reports.

Social Security Identity Theft

Kellie Droste got surprising news from her accountant last month.

An identity thief had stolen the Maricopa, Ariz., resident's personal information and filed a tax return in her name to claim her refund.

"He (her accountant) couldn't file our joint tax return, because someone had already filed a tax return under my Social Security number," Droste said.

Droste reported the fraud and was told it would take at least six months to sort out the matter. Meanwhile, she would have to wait to receive her $2,700 tax refund.

Droste is among thousands of taxpayers victimized by a fast-growing form of identity theft in which stolen personal information is used to file fraudulent tax returns. And although fraudulent tax returns are popular with criminals right now, they represent the tip of the iceberg.

Identity theft is especially prevalent in Arizona, which had more victims per capita than any other state in 2010, with about 149 victims for every 100,000 residents. California, Florida, Texas and Nevada also were leading states for identity theft, according to Federal Trade Commission data.

from Identity Theft Growing, Costly to Victims

A Social Security number (SSN) is a unique number assigned to each individual in the United States. Since 1935, over 420 million different Social Security numbers have been issued. The first three (3) numbers are known as the *area number*. Area numbers assigned before 1972 indicate the state where you applied for your number. The second two (2) digits are called the *group number.* This number originally used to help the Social Security Administration to organize file cabinets into sub-groups as a way to make tracking more manageable. The final four (4) digits are serial numbers issued consecutively from 0001 to 9999.

As a result of business, credit/financial, educational, governmental/military and medical/health care data breaches, it is safe to say that nearly every American's Social Security Number has, statistically, been lost or stolen in the past several years, and the single thing that most identity theft crimes have in common is the misuse of someone's Social Security number.

Prior to 1986, it was common for people to wait until they got their first job to apply for a Social Security number. The Tax Reform Act of 1986 required parents to list the Social Security number for each dependent child over the age of five (5) on their tax return in order to claim that child as a deduction. By 1990 the age was lowered to one (1) and now a Social Security number is required for each claimed dependent regardless of age. Therefore, most parents apply for their child's SSN at birth along with the application for a birth certificate.

Back in 1936, when Social Security numbers were first issued, the public was assured by the federal government that these numbers would only be used for Social Security programs (i.e. tracking your earnings and calculating retirement benefits). However, since that time the Social Security number (SSN) has become the *de facto* national identifier and a person's Social Security number is also often used to confirm an

individual's identity. These two factors make Social Security numbers very desirable to identity thieves.

Due to the dramatic increase in identity theft, it is not necessary to provide your Social Security number in many cases. However, schools, businesses, the military and other governmental agencies continue to use Social Security numbers for a wide variety of purposes outside of Social Security benefits.

If your Social Security number is used by an identity thief to get a job, then that income gets reported to the IRS with your SSN attached. Then when you file your tax return, you don't include those earnings and the IRS records will show that you did not report all of your income. The IRS will then send you a notice of unreported wages.

When someone files a tax return with someone else's Social Security number before the victim, the crime is not discovered until the legitimate tax return is filed.

When two different tax returns are received by the IRS with the same Social Security number, the return is rejected.

It may seem that the answer to Social Security identity theft would be to simply change your SSN much like you would change a credit card or driver's license number. However, this is very rarely allowed by the Social Security Administration. The drawbacks to changing your Social Security number include:

- a loss of your credit history
- a loss of your academic records
- a loss of professional degrees and/or certifications
- difficulty in opening a bank account
- difficulty in leasing or renting a home or apartment
- difficulty in establishing new lines of credit

Driver's License Identity Theft

Driver's License Identity Theft happens when someone gets your driver's license information and uses it with their picture. Now if they get a DUI, they don't need to worry about showing up for court because the warrant will be issued for YOU. Or the thief may decide to write a few bad checks.

Character/Criminal Identity Theft

> "It began on a drive to class when he was pulled over for a broken turn signal. After running a check on his driver's license, the officer told him his license was suspended and he was going to jail. Derrick was baffled. "I had no idea the nature of the charge or why I was being arrested. I told the officer he must be mistaken." His car was towed and he was taken to jail where he learned there was an outstanding speeding ticket in Mississippi under his name and driver's license number."
>
> *from* Identity Theft Stories: AllClear ID Helps a Customer Arrested Twice for Crimes He Didn't Commit

Character/Criminal Identity Theft is closely related to Driver's License and Social Security Identity Theft and may result from either or both.

Privacy Rights Clearinghouse is a California non-profit consumer advocacy & awareness group dedicated to helping to empower consumers to take action to control their own personal information by providing practical tips on privacy protection. They say that "criminal identity theft occurs when an imposter gives another person's name & personal information … to a law enforcement officer during an investigation or upon arrest." Personal information may include such things as a driver's license number, date of birth, Social Security number, or the identity thief may even falsely use their victim's name and other personal information without showing any photo identification.

The identity thief may be cited for a misdemeanor or a moving traffic violation and is expected to appear in court … which, of course, he does not do. The identity theft victim may subsequently be unexpectedly detained pursuant to a routine traffic stop & then subsequently arrested due to the bench warrant that was issued in the victim's name.

If the identity thief is involved in a more serious crime, such as a DUI or a felony, then a criminal record may have been created when the identity thief was arrested. The arrest is then recorded in the county and state criminal records database, ultimately ending up with the National Crime Information Center (NCIC) that maintains the national crime index database.

Some victims may learn of (the criminal identity theft) when they are terminated from or denied employment. When the employer used the victim's name to conduct a background check, criminal history was revealed under the victim's name. By law, the victim is informed by the employer that the criminal history is the reason they are being fired or are not being hired. Now it is up to the victim to clear their name with the criminal justice system. This can be a very long process and the assistance of an attorney may be required.

Medical Identity Theft

Brandon Reagin didn't realize someone had snatched his medical identity until his mother called to tell him he was the lead suspect in a car theft in South Carolina in 2005. The 22-year-old marine had lost his wallet more than a year earlier while celebrating with friends after completing boot camp at Parris Island, near Beaufort, S.C. After his training, he was posted to California. But in South Carolina, Reagin lived on, as an impostor used his military ID and driver's license to not only test-drive new cars and then steal them but also visit hospitals on several occasions to treat kidney stones and an injured hand, running up nearly $20,000 in medical charges. Reagin found out about the unpaid hospital bills when he asked for a credit report following the car theft. 'It was horrible,' he says. 'And what made it worse is that no one really knew what to do when it first started happening.'

from Medical Identity Theft Turns Patients Into Victims

One of the fastest growing areas of identity theft is Medical Identity Theft – the fraudulent use of someone's personal information for the purpose of illegally obtaining medical services, devices, insurance coverage or reimbursement or prescriptions. With the ever-increasing cost of health care in the United States, medical identity theft is actually becoming commonplace.

When someone else uses *your name* to obtain health benefits or prescriptions, the thief may incur large medical bills that may or may not be covered by your medical insurance. If they are given the coverage, you run the risk of reaching your insurance coverage limit. If they are not covered, you may be faced with thousands of dollars in unpaid medical bills. It is then left up to you to prove that it wasn't you who received the services.

Since there is no clear cut process for challenging false medical claims or correcting inaccurate medical records, the result could be damaged credit due to unpaid charges and years of working to clean up the mess.

Medical identity theft could result in your medical records being changed. Perhaps the thief is a different blood type or they have diabetes and you don't. Not only could you lose your health coverage because of the false information in your medical record. … It could be life threatening! According to James Pyles, a Washington, D.C. attorney who has dealt with health insurance issues for more than forty years, "It's almost impossible to clear up a medical record once medical identity theft has occurred. If someone is getting false information into your file, theirs gets laced with yours and it's impossible to segregate what information is about you and what is about them."

In an article entitled <u>There is an Epidemic of Medical Identity Theft</u> dated September 13, 2014, **USA Today** states:

"Within the past few weeks we have seen the hacking of the Affordable Care Act's HealthCare.gov as well as a massive data breach at Community Health Systems, a hospital chain with medical facilities in 29 states in which the records of 4.5 million patients of Community Health Systems' hospitals including names, addresses, birth dates and Social Security numbers were stolen."

Medical Identity Theft can haunt you for years. Once you report that the person who received the medical treatment or procedure is not you, the files are sealed due to privacy laws, and medical databases are notoriously slow to update.

Synthetic Identity Theft

In the first half of 2014, a man by the name of Deon Mimbs pled guilty to withdrawing almost $2 million from banks by using fake personal and business identities. "He did this a number of times, in effect creating a small army of synthetic identities," said prosecutor Warren Kato of the Los Angeles District Attorney's Office. "He used these identities to form fake companies, he used 'the army' to create fake customers who would generate fake charges for these companies."

A variation of Identity Theft which has recently become more common is Synthetic Identity Theft, in which identities are completely or partially fabricated. The most common technique involves combining a real social security number with a name and birth-date other than the ones associated with the number.

This is the "latest thing" in the world of identity theft. The thief will take parts of information from many victims and combine it. The new identity isn't any specific person, but all the victims can be affected when it's used.

Synthetic Identity Theft is more difficult to track as it doesn't show on either person's credit report directly, but may appear as an entirely new file in the credit bureau or as a sub-file on one of the victim's credit reports.

Synthetic Identity Theft primarily harms the creditors who unwittingly grant the fraudsters credit. However, collection agencies have the ability to perform what is known as a "Social Search" which looks for an individual's Social Security number. Once the SSN is linked to a current address which is then linked to the delinquent account or accounts, the innocent victim could be pursued by collection agencies.

Individual victims can be affected if their names become confused with the synthetic identities, or if negative information in their sub-files impacts their credit ratings.

Child Identity Theft

> Angie Brackin didn't know anything was wrong until she got a phone call asking why her son, Adam, hadn't reported thousands of dollars in income from working in a factory.
>
> "I said, 'Well, that's impossible. Adam is in school today and he's only in fourth grade,'" Brackin said.
>
> Turns out someone had stolen Adam's social security number just months after he was born. …. Over the past 14 years, Adam's social security number was used to rent homes and apartments, to secure jobs, to title eight different cars, and to run up thousands of dollars in unpaid bills.
>
> The freshman at Covenant Christian High School and his mother have now spent several years trying to put an end to the identity theft.
>
> from Targeting Children: the Young Victims of Identity Theft

Child Identity theft is one of the fastest growing sectors of the identity theft "industry," and the numbers are staggering. Although it's difficult to estimate exactly how many children lose their identities, since the crime can go undetected for years, the FTC states that 5% of identity theft cases target children, which translates into 500,000 kidnapped child identities per year, and growing.

Why are our kids, the very people we most want to protect, so vulnerable? Because they have unused, unblemished credit profiles. Richard Power, Distinguished Fellow, Carnegie Mellon CyLab, recently published the first ever Child Identity Theft

Report based on identity protection scans of over 40,000 U.S. children. It is extremely alarming that 10.2% of the children in the report had someone else using their Social Security numbers. That figure is fifty-one (51) times higher than the rate for adults of the same population.

Richard Hamp, Assistant Attorney General of Utah, who specializes in Identity Theft, is quoted as saying, "The fact is, Social Security Numbers are being sold on the street every day by the thousands." Criminal, financial and other forms of identity theft are being perpetrated on children as well as adults every day.

The TODAY Show told us about:

- Egan, who is only 2 years old, but he already owes thousands of dollars in credit card debt and has declared bankruptcy.
- Nine year old, Riley, is in default on utility bills. Her Social Security number was stolen even before she was born.
- After having her identity stolen at the age of three (3), seventeen (17 year old Caitie from Scottsdale, Arizona is up to her *eyeballs* in debt … including owing $600,000 dollars in mortgage loans and another $100,000 in car loans and credit cards.

A recent study of 27,000 children found that 10% of them had their social security number tied to mortgages, loans, credit card accounts & even vehicle registrations. And what group of children are the *most targeted?* Kids UNDER 5!

For parents, cleaning up the mess made of their children's identity by the thieves can take years and can haunt the children for most of their lives.

Phone: 248-361-9641
Email: akoch@premiersolutionsintl.com
Website: www.AnitaKoch.com

Protecting Your Privacy

Although there is nothing that can be done to completely *stop* identity theft, there are steps that can and should be taken to reduce the possibility of becoming the next victim. This section will cover some of those steps.

Credit Reports

Everyone is entitled to a free copy of their credit report from each of the three (3) credit bureaus (Experian, TransUnion and Equifax). Reviewing your credit reports *at least* once a year is an important step in protecting your privacy and keeping your credit safe. If you have not looked at your credit reports recently (or ever), it is recommended that the first time you request them get all three.

Carefully review all three reports and, if you find any items that you do not agree with, dispute them. Once you have completed this process, get into the habit of checking a report from each credit repository every four (4) months. It's a good idea to put a reminder on your calendar or in your planning device so that you remember to take the time to regularly check your credit reports.

There are many credit monitoring services available today. The advantage of having one of these services is that you are alerted when something changes on your credit report. You may choose a service that monitors a single bureau or select a service that will alert you to changes in any one (1) of the three (3) credit repositories. Should you receive an alert, it is important that you take action quickly. If suspicious activity has taken place, follow the steps outlined in the section entitled "If You Have Become A Victim ..."

There are two (2) types of inquiries that may occur on your credit report: soft inquiries and hard inquiries. While there are other circumstances that could warrant a soft inquiry, the most common occurrences happen when you check your own credit score, you're "pre-approved" for a credit card, or an employer looks at your credit report as part of a background check. Soft inquiries do *not* impact your credit score. Checking your own credit score will not lower your credit score.

A hard inquiry occurs when you apply for some type of loan or a credit card and the financial institution checks your credit report prior to making a decision on whether or not to give their approval. Hard inquiries can stay on your credit report for up to two (2) years and your credit score may be lowered a few points when a hard inquiry occurs. Due to the fact that multiple hard inquiries over a short period of time can lower your credit score significantly, you should keep the number of hard inquiries to no more than one (1) or two (2) a year.

Financial Accounts

Financial institutions are required by law to provide you a copy of their Annual Privacy Notice which includes their Privacy Policy. The Privacy Policy is a document that will inform you as to the information that is being collected about you and how that information is being used. You have the right to "opt-out" (choose not to participate) and thus prevent the sale of your personal data to third parties. If you fail to opt-out, you have unwittingly given your permission to share your personal information with other non-affiliated third parties.

The incidence of credit card data theft has grown by 50% over the five (5) year period from 2005 to 2010. The number of malware programs designed to gain access to your financial data has grown dramatically from 1 million in 2007 to about 130 million in 2013.

There is a lot of important information that is being transmitted via the internet due to the fact that so many people are making purchases, paying bills and doing their banking online. Here are some steps that can be taken to help keep your personal information safe:

- Use your credit card rather than a debit card for online purchases as you have better protection under federal law.
- Change your logins and passwords regularly (monthly is recommended).
- Do not store logins and passwords on your computer. It is particularly important that you clear your logins and passwords if you are working on a public computer.
- Phishing is used by identity thieves to gain access to confidential information by hiding behind a name that you trust, such as your bank or businesses that you have done business with in the past. Before you respond to any request for personal data into any website, be sure to verify who is asking and why they need it. Directly contact the company that is asking for the information should you be suspicious of any request.
- Review your bank and credit card statements regularly. Verify any purchases that you believe to be fraudulent.
- Monitor your credit report. You are entitled, by law to a free credit report from each of the three (3) credit repositories, Experian, Equifax and TransUnion every year. Request a credit report from one of the credit bureaus every four (4) months. When you receive it, check it carefully for any accounts or lines of credit that you did not open.
- If you don't own a shredder … buy one. Make it a habit to shred any documents that contain your personal information before throwing them away. Remember, even junk mail may contain some of your personal information.

Internet / Online

Malware programs are MALicious softWARE programs that are used to gain unauthorized access to computers, collect sensitive information and/or disrupt the operation of the computer. Malware is also known as a computer contaminant and comes in many forms. The following are some of the current forms of malware … the list is likely to continue to grow.

- Computer viruses (replicating program that performs some kind of harmful activity to the infected computer)
- Spyware (gathers data without the knowledge or consent of the computer's owner)
- Adware (inserts advertisements to generate revenue)
- Worms (replicates itself for the purpose of spreading to other computers)
- Trojan horses (gives unauthorized access to the affected computer)
- Rogueware (masquerades as an authentic well-known program in order to steal data, money, etc.)
- Ransomware (limits access to the infected computer system)

Smartphones are common in today's world. However, most smartphones do not have the same protection as your home computer or laptop … especially when a public Wi-Fi system is being used. If you are using free Wi-Fi when it's available, it is wise to manually connect and avoid the use of automatic connecting. Turning off the sharing capabilities of your phone when in public places is also recommended.

A Virtual Private Network (VPN) uses the internet to provide secure remote access by offsite users to their organization's network. You may also wish to consider the utilization of a VPN connection for your smartphone as an added layer of protection when using public Wi-Fi.

More people today are aware of the need to make sure that if they are transferring sensitive data over the internet that the website is "secure." This can be verified by looking for the letter "s" after the http in the web address or URL. The appearance of a locked padlock is also used by some web browsers (i.e. Internet Explorer) to indicate that encryption is being used by that site.

Having multiple passwords – different for each password protected website that you visit – is certainly a good idea. However, keeping track of all those passwords can be a daunting task.

Basic firewalls typically come with the computer operating system. A firewall puts up a barrier between your computer and the internet. The information "packets" that are being sent back and forth, to and from your computer, are monitored to determine if they meet a certain set of criteria. Those that do not, are blocked. A basic firewall may only monitor incoming data. More sophisticated firewalls also check outgoing data and can keep your computer "invisible" when you're online.

In order to combat online threats, it is wise to protect your computer against viruses by using antivirus protection. Antivirus software is designed to detect, prevent and take the appropriate action to disable or remove malicious software programs from your computer.

Antispyware software is used to protect against malware other than viruses. Most software professionals recommend that both anti-virus and anti-spyware protection programs should be installed on your computer. Your operating system may come with a level of protection for both. In addition, there are free antivirus and antispyware programs available as well as paid versions.

Medical and Health Related

Health and medical information is particularly sensitive when it comes to identity theft, and health information is protected by Federal Law (HIIPA). Health care providers, insurance companies and governmental programs such as Medicare and Medicaid are required to adhere to these guidelines and most health information that is held by these organizations is covered under these laws.

While there are circumstances when your medical information must be shared with other parties, the law sets limitations on this sharing. In addition, it is required that you give written permission before your information can be shared with your employer or for marketing purposes.

There must be appropriate safeguards in place to protect the information in your medical records. These safeguards must address the physical records as well as electronic. In addition, every health care provider must have someone on staff who has been appointed as a privacy officer. This is the person clients would speak with should there be concerns.

Phone: 248-361-9641
Email: akoch@premiersolutionsintl.com
Website: www.AnitaKoch.com

If You Have Become a Victim …

No one really *expects* to become a victim of identity theft, yet we know that it can happen to anyone. Financial identity theft is often the means by which victims first become aware of the fact that they have a problem. The best way to limit the damage caused by identity theft is to take action *as soon as possible.* Resolving an identity theft issue takes time. In addition to the time it will take, there may be costs incurred and above all, persistence and patience will be required to get back to pre-theft status.

Social Security Identity Theft

If you become a victim of Social Security Identity Theft, here are the basic steps to follow:

- Contact the IRS Identity Protection Specialized Unit immediately at (800) 908-4490.
- Report the fraud.
- Request and complete IRS ID Theft Affidavit Form 14039 or you may use a copy of your police report.
- Send the police report or affidavit along with proof of your identity (one of the following).
    - o copy of your Social Security card
    - o copy of your driver's license
    - o copy of your passport
- Record the dates of calls made and letters sent.
- Keep copies of all letters sent in your personal files.

Driver's License Theft/Misuse

If you discover that your driver's license is being misused or someone uses your name and birth date to get a driver's license number, you may need to change your DL number. If you lose or

suspect that your driver's license has been stolen the following steps should be followed.

- While not required, it is recommended that your report a stolen driver's license to the Michigan Secretary of State and/or to law enforcement – especially if yours was an *Enhanced Driver's License (EDL)* to prevent anyone from using your license for border crossing.

- The Secretary of State can provide you with a Driver License Alert. (https://www.michigan.gov/documents/driver license alert request form 17623 7.pdf)

When this form is filed, a flag is placed on your driving record to notify law enforcement that someone else could be using your name and identification during a traffic stop and may keep fraudulent traffic violations off your record.

- You can replace your lost or stolen Michigan driver's license on-line or in person. Go to www.dmv.org/mi-michigan/replace-license.php for further instructions.

Create an Identity Theft Report

See **Appendix 1** for detailed instructions on how to complete this important task.

Place an Initial Fraud Alert

Once you have been notified or you realize that you have become a victim of identity theft there are certain steps that should be taken as quickly as possible to mitigate the damage caused by this crime. It is important to follow a system, remain organized, and document the steps you take in the process.

The first step is to place an Initial Fraud Alert with one (1) of the three (3) credit repositories. The company that you call is required to notify the other two (2) of your alert.

Begin tracking your progress by recording the date you contacted the credit bureau and how they were contacted (by telephone or mail). Create a file to keep copies of any written correspondence related to your case. Make note of date, time and the person you spoke with if your contact was made via the telephone.

There is no charge to place a fraud alert on your credit file and your initial alert will remain in place for ninety (90) days.

Experian	**1-888-397-3742**
TransUnion	**1-800-680-7289**
Equifax	**1-800-525-6285**

Request a Credit Freeze

You may also request that a credit freeze be placed on your credit file *with each credit bureau*. Once a credit freeze has been put in place, you must give your consent before your credit report will be released to any potential creditor. Michigan is the only state that has not yet adopted security freeze laws to protect victims of identity theft. However, Experian, TransUnion and Equifax offer a voluntary security freeze to identity theft victims.

There is no charge for a victim of identity theft to place a security freeze with any of the credit bureaus. As a Michigan resident who is a victim of identity theft, you will be required to send a written request to have the fees for placing a security freeze waived.

Written requests for a credit freeze should be sent by certified mail, return receipt requested to each credit bureau. Your name, current and former addresses for the last two (2) years (five years for TransUnion), along with your Social Security number and date of birth should be included with the request. Experian requires that a copy of a government identification card (driver's license, state ID card or military ID card) be included. Experian and Equifax require a copy of a utility bill, insurance or bank statement showing *your name* and current mailing address. If you are not an identity theft victim and are requesting a credit freeze, the $10.00 fee may be paid by check, money order or credit card. TransUnion requires payment by credit card only.

Should you want to apply for a loan or insurance, authorize a potential employer to conduct a background check, or open a new line of credit, the freeze will need to be lifted, at least temporarily. A charge of $10 per credit reporting agency will be required to lift the freeze, either temporarily or permanently.

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
P. O. Box 9554
Allen, TX 75013

TransUnion
Fraud Victim Assistance Department
P. O. Box 6790
Fullerton, CA 92834-6790

Order Your Credit Reports

Each of the credit reporting agencies is required to provide you with a free credit report once you have placed an initial fraud alert. After you have placed the fraud alert, each credit bureau will explain your rights and how you can get a free copy of your credit report.

You should request that only the last four (4) digits of your Social Security number be shown on your credit report.

Make sure to make copies of letters that you send to request these reports and keep them in your files along with the dates and times of any telephone conversations.

Review Your Credit Reports

Key information to be verified includes:

- Name
- Address
- Social Security Number
- Employment History

If you are aware of personal accounts that have been compromised, contact someone in the fraud department of the affected businesses directly. Any telephone conversations should be documented as to the date and time of the call as well as the name of person you spoke with. Follow up with a confirmation letter sent via certified mail, return receipt requested.

When you receive your credit reports, check to see if they contain any other charges or accounts that you did not open or authorize. Check your credit reports carefully. If you find additional errors on the reports, follow the same procedure as you did earlier, documenting telephone conversations and following up with written correspondence.

Dispute Credit Report Errors

Send letters explaining mistakes on your credit reports to:

- Experian, Equifax and TransUnion
- Each business reporting fraudulent transactions on existing accounts (Attention: Fraud Dept.)
- Each business reporting new accounts opened in your name (Attention: Fraud Dept.)

Request the credit bureaus and businesses to block the disputed information from showing up on your credit report by doing the following.

- Identify yourself with your name, address and Social Security number, including proof of your identity
- Indicate disputed transactions
- Include a copy of your Identity Theft Report
- Ask that disputed/fraudulent information be blocked

Phone: 248-361-9641
Email: akoch@premiersolutionsintl.com
Website: www.AnitaKoch.com

Getting Help

While it is not necessary to purchase identity theft protection services, many consumers are looking for ways to reduce their risk. Regulators have fined several providers of identity theft protection services for deceptive marketing practices.

Like it or not, identity theft is here to stay and it is in the agent and client's best interest to know what differentiates one type of service from another.

Credit Monitoring

Credit monitoring services keep track of your credit report(s). A credit monitoring service will notify you when there is any suspicious activity, such as a delinquency or derogatory report on any of your accounts. You will also be alerted if there are any significant changes in your credit report(s), such as new accounts or lines of credit being opened.

Some people think that credit monitoring is "the answer" to identity theft. It is not. Many consumers look at credit monitoring services as identity theft "insurance." While these programs have some characteristics in common with insurance products, they often do not do the same things as you would expect an insurance policy to do.

Credit monitoring is good, in that it can alert you when there is activity on your credit report. This allows you to take action quickly to clean up and limit the amount of potential damage that can be done by an identity thief.

Companies that have experienced a security breach (i.e. Target, Nordstrom's, Home Depot, etc.) like to offer credit

monitoring services to their potentially compromised customers. This should be seen more as a public relations (PR) move than anything else. It really does not compensate in any way for the fact that a criminal now has possession of the customer's personal data.

Reimbursement Policies

There are consumers who think that a credit monitoring service will reimburse them for any funds that are stolen as a result of identity theft. However, these services act as expense reimbursement programs rather than insurance.

For example, your car insurance will cover the cost of repairing your car in addition to injuries you might suffer as a result of an accident. However, a credit monitoring service does not cover the costs to put your identity back to the way it was before the theft, nor does it pay you for any injuries you may suffer as the result of being a victim. Denis Kelly, president of IDCuffs.com says, "It pays the equivalent of the cost to have your car towed and possibly the shipping costs of a new bumper."

Reimbursement policies do not typically cover "actual losses" … that is the merchandise or funds stolen from existing accounts or from accounts created by the identity thief. The Electronic Funds Transfer Act (EFTA) outlines the process to be followed in order to recover any "actual losses."

Identity Theft Reimbursement policies are designed to give you the money back for expenses you incur associated with restoring your identity to what it was prior to the theft. These policies typically cover things like long distance telephone calls, certified mailing costs, notary fees, the cost of copies of police reports, etc. There may be deductibles involved and should you have coverage from more than one source, you will likely be paid only what the first service does not cover.

Reimbursement policies do not do any of the work for you. The process of making the calls, writing the letters and following up is left in the hands of the victim. Much of the time spent in getting back to pre-theft status must be done during normal business hours. This means that the victim may need to take time off work. Some reimbursement policies may compensate you for the lost pay. However, expect to receive a 1099 if the amount is over $600.

Resolution vs. Restoration

"A close friend of mine had his identity stolen. He was not using any monitoring service and did not regularly check his credit. ID thieves opened accounts, took out loans and got a driver's license in his name. The thieves racked up thousands of dollars in debt. It had physical effects on him and his family. It took him almost a year of constant attention and hard work to get his life back."

~ Tyler Cohen Wood, *Cyber Branch Chief of an Intelligence Agency under the Department of Defense*

What's the difference between a "Resolution" and a "Restoration" service when it comes to identity theft? Basically, it comes down to who does the work … who makes the calls and waits on hold, who writes the letters and does the follow up?

Both services will typically begin with some form of a package of materials along with instructions as to steps to follow. A "Resolution" service will usually provide an 800 number the identity theft victim can call to speak with an Assistance Advisor, Crisis Coach, or Personal Advocate … someone to help the victim through the lengthy process of restoring their identity to pre-theft status. However, the victim is still the person responsible for doing the bulk of the work.

A true "Restoration" service will give the victim the option to sign a Limited Power of Attorney (POA) which will allow a professional to do the bulk of the work of restoration for the

victim. A Limited POA will be used for interaction on the victim's behalf with:

- Experian
- TransUnion
- Equifax
- Department of Motor Vehicles (DMV)
- Federal Trade Commission (FTC)
- Social Security Administration (SSA)
- U.S. Postal Service (USPS)
- Financial Institutions
- Creditors
- Collection Agencies

A professional that has the training and established relationships to work with the various agencies and departments involved in the restoration process is able to put the victim's life back to pre-theft status much faster than would be possible for the victim on their own.

Legal Services and Legal Service Plans

> "Identity theft and financial fraud are rapidly growing and increasingly common crimes, but relatively few resources exist to prepare victim service providers to help victims of these crimes. Although identity theft is considered a nonviolent crime, victims often report that they suffer trauma similar in intensity to that of violent crime—feeling violated, confused about how to get help, and no longer in control of their lives. Added to this emotional trauma is the burden of having to prove one's innocence."
>
> *~ U.S. Department of Justice*

In the 132 page document, "Guide to Assisting Identity Theft Victims" written for attorneys by the Federal Trade Commission, it is recommended that legal counsel be used in special cases when:

- the age, health, language proficiency or economic situation of the victim may create a barrier in disputing and correcting errors in their records

- the victim is being sued by creditors for debts incurred by the identity thief
- the victim is being harassed by creditors attempting to collect debts incurred by the identity thief
- creditors and/or credit bureaus are not cooperating in helping the victim to undo the damage done by the identity thief
- the identity theft case is more complex and/or involves more than just financial identity theft

After assisting the victim initially, it is recommended that a follow up be done in two (2) weeks to see how the victim is progressing in their case.

The cost of retaining an attorney who is proficient in the detailed process of helping an identity theft victim to restore his or her identity to pre-theft status can be lengthy and, therefore, expensive. Some identity theft protection programs include the cost of having legal counsel to assist in this process which, in many cases, is quite beneficial.

There is also an identity theft protection plan that gives the victim access to legal counsel for more than just identity restoration. The legal services plan is available for any and all legal needs that the client might have – including will preparation, traffic tickets, 24/7 emergency access to legal help and more.

Phone: 248-361-9641
Email: akoch@premiersolutionsintl.com
Website: www.AnitaKoch.com

Appendix 1
Creating an Identity Theft Report

There are three (3) steps involved in creating an Identity Theft Report:

1. Submit a report of the identity theft to the Federal Trade Commission via telephone or email. Print a copy of the FTC Identity Theft Affidavit for your records.
2. Take a copy of your FTC Identity Theft Affidavit and file a report regarding the theft of your identity with the police. Get a copy of the police report or a report number.
3. Attach the police report to the FTC Identity Theft Affidavit, creating your Identity Theft Report.

Step 1: Contact the Federal Trade Commission (FTC)

By Phone: (877)438-4338 or
(866)653-4261 (Hearing Impaired – TTY)

Explain the details of what happened to the Federal Trade Commission representative.

Get the Complaint Reference Number from the representative, as well as the password for your FTC Identity Theft Affidavit. (A link will be emailed to you so that you can get your IDT Affidavit.)

Print or save your IDT Affidavit by going to the link provided by the FTC representative, entering your complaint reference number and IDT Affidavit password.

Online: www.ftc.gov/complaint

Go to www.ftc.gov/complaint and complete the IDT Affidavit complaint form with as many details as possible. Click "submit" after carefully reviewing the form and save the reference number. This reference number is necessary whenever you need to update your identity theft complaint, either by phone or online.

By clicking on the words, "Click here to get your completed FTC Identity Theft Affidavit" you will be able to print or save the competed form.

Step 2: File a Police Report

A report may be filed either at the police department where the theft occurred or at your local police department.

Take a copy of your FTC Identity Theft Affidavit with you when you file a Police Report regarding your identity theft case. Once you have filed the police report, get the report number or a copy of the police report.

Keep a copy of the police report for your files along with the police report number. Keep a record of the date(s) you made calls or visits to the police department(s).

Step 3: Create your Identity Theft Report

Attach the completed FTC Identity Theft Affidavit to the police report. Keep a copy of your Identity Theft Report for your files.

Phone: 248-361-9641
Email: akoch@premiersolutionsintl.com
Website: www.AnitaKoch.com

Appendix 2
Sample Documents

Credit Freeze Letter Example

August 21, 2017

TransUnion
Fraud Victim Assistance Department
P. O. Box 6790
Fullerton, CA 92834-6790

To Whom It May Concern:

I would like to place a security freeze on my credit file.

My name is
Samuel J. Smith, Jr.
[Be sure to include your full name, any middle initials, any suffixes such as Jr., Sr.,III, etc., and names by which you were formerly known.]

My current address is
1234 Pine Street, Omer, Michigan 48749.

In the past two (2) years, I have also lived at:
[List all previous addresses. For TransUnion, list previous addresses for the past five (5) years. Include additional sheets of paper, if necessary.]

My Social Security number is: 123-45-6789
My date of birth is: January 1, 1899

I am including a copy of the following:

[Make a list of the supporting documentation that you are enclosing. It is important to remember that the requirements for each credit reporting agency may be slightly different. Be sure you double-check the documentation that is required before sending your request. Remember … never send originals. Send *copies only*.]

☐ I am an identity theft victim.
[If applicable, check the box.]
A copy of my police report is enclosed.

OR

☐ I will pay the fee of $10 for placing the freeze by:

- Check or Money Order (if applicable)
- Credit Card (select one): [Visa] [MasterCard] [American Express] [Discover]

Card number: 1234 5678 9012 3456
Card Security Code (if required): 111 (4 digits for Amex)
Expiration date: 01/2121

Sincerely,

[Your signature]
[Your name]

Sample Dispute Letter
(for Existing Accounts)

[Date]
[Name]
[Address]
[City, State, Zip]

[Company Name]
[Billing Inquiries or Fraud Department]
[Address]
[City, State, Zip]

To Whom It May Concern:

This letter is to dispute fraudulent charge(s) on my account number [Acct. #] in the amount of $_____, dated [Dates appearing on statement]. I request that you remove the fraudulent charge(s) and any related finance or other charge(s) from my account as I am a victim of identity theft and did not make these purchases.

Please update my account and send an updated statement with accurate information. [You may also wish to request that the account be closed.] In addition, it is requested that you stop reporting the fraudulent charge(s) to any and all of the three (3) nationwide credit bureaus with which you correspond.

A copy of my Identity Theft Report is enclosed, along with my credit report and my account statement indicating fraudulent charges due to identity theft. A copy of the Federal Trade Commission's "Notice to Furnishers of Information" is also enclosed, indicating your responsibilities under the Fair Credit Reporting Act.

Thank you for your timely investigation into this matter. Written response as to your findings and actions is expected and appreciated.

Sincerely,

[Name]

Enclosures:
Proof of Identity
Identity Theft Report
FTC Notice of Furnishers of Information
Copy of Account Statement indicating fraudulent charge(s)
[Name] Credit Report showing information to be corrected

Sample Dispute Letter
(for New Accounts)

[Date]
[Name]
[Address]
[City, State, Zip]

[Company Name]
[Billing Inquiries or Fraud Department]
[Address]
[City, State, Zip]

To Whom It May Concern:

This letter is to make you aware of the fact that I am a victim of identity theft and my personal information has been used to open a fraudulent account with your company. Therefore, I request that you close the account immediately and absolve me of all the fraudulent charges on this account. In addition, please take the necessary steps to see that any and all information regarding this account is removed from my credit files.

A copy of my Identity Theft Report is enclosed, along with a copy of my credit report indicating the fraudulent charges to your company due to identity theft. A copy of the Federal Trade Commission's "Notice to Furnishers of Information" is also enclosed, indicating your responsibilities under the Fair Credit Reporting Act.

Your timely investigation into this matter as is the closing of this account and absolving me of all charges is anticipated. Written response as to your findings and actions is appreciated.

Sincerely,

[Name]

Enclosures:

Identity Theft Report
FTC Notice of Furnishers of Information
[Name] Credit Report showing information to be corrected

Phone: 248-361-9641
Email: akoch@premiersolutionsintl.com
Website: www.AnitaKoch.com

About the Author

Anita Koch's first exposure to identity theft occurred in the early 1990's when she and her husband, Mike, were victims of financial identity theft. It was in 2006 that she learned that there were services available to help mitigate the damage and stress caused by this crime. As an educator and consumer advocate, she earned the designation of Certified Identity Theft Risk Management Specialist in 2007 through the Institute of Fraud Risk Management.

"The Certified Identity Theft Risk Management Specialist™ (CITRMS)course is the nation's only professional certification program specifically developed to train and equip professionals to understand and address Identity theft and related fraud. The comprehensive CITRMS course addresses risks and issues for consumers, employees, and businesses / professional practices."

Institute of Consumer Financial Education (ICFE)