What Insurance Professionals Should Know About Identity Theft

What Insurance Professionals Should Know About Identity Theft

By Anita Koch (with Perry Sylvester, in cooperation with American Education Systems, LC)

About This Program

This is a continuing education program designed to provide an overview of essential information pertaining to identity theft. American Education Systems, LC is not engaged in rendering legal or other professional advice, and the reader should consult legal counsel as appropriate. The content of this publication may be affected by changes in law or industry practice; as a result, the information contained within may become outdated. This material should in no way be used as an original source of authority on legal matters.

About The Exam

Paper courses include a "Test Packet," which contain instructions, a disinterested third-party affidavit (i.e. Monitor Form), an Agent/Producer Information Page, a scoring sheet (i.e. Answer Sheet), and the exam/test. *Online* courses integrate the contents of the Test Packet and deliver them to the student directly.

IMPORTANT NOTE: To earn continuing education (CE) credit with a paper version of this course, you are required to follow one of two options:

- **Option 1**

Complete all the enclosed paperwork in the Test Packet and submit the contents to American Education Systems, LC at 7711 Auburn Road, Utica, MI 48317-5220. We will grade the completed exam; upon passing (i.e. score 70% or better), we will update our records and submit the pertinent information to the State of Michigan's authorized representative so the earned credits can be posted to your official record.[1]

- **Option 2**

At no additional cost to you, we also provide you with the option of completing your exam online. This allows for a more rapid conveyance of the completed paperwork to our office and eliminates the uncertainties associated with physical mail delivery. Instructions for completing your test online are found at the conclusion of the text.

About Contacting Our Office

If you have any questions about your course, the process of meeting your CE requirements, or the contents of your course package, feel free to contact us.[2] Our office hours are Monday-Friday, 10 am to 4 pm, and we maintain a toll-free line at 1-800-775-6339. If you need help after hours, you may leave us a message on the office voice mail, and we will contact you at our first availability. You may also want to visit our homepage at www.AmEdSys.com and search the FAQs.

American Education Systems, L.C.
"Helping professionals succeed since 1994"

www.AmEdSys.com www.BestInsuranceContinuingEducation.com
7711 Auburn Rd, Utica MI 48317-5220
586.726.6339 · Fax 586.726.1059 · aes@amedsys.com

[1] If you do not pass your exam on your first attempt, we will forward you a new exam; there is no maximum number of attempts, nor are there additional fees associated with exam retakes.

[2] Please be advised we can only discuss course and exam *process*; we are not permitted to provide comment or direction regarding course *content*.

Table of Contents

Chapter One – Understanding Identity Theft 6

Chapter Two – Identity Theft Laws and Statistics.....13

Chapter Three – Types of Identity Theft.....24

Chapter Four – Identity Theft and Businesses.....34

Chapter Five – Protecting Your Privacy.....41

Chapter Six – What to Do If You Become a Victim of Identity Financial Theft 45

Chapter Seven – Identity Theft Protection Services.....60

Chapter Eight – Role of the Agent.....64

Chapter One – Understanding Identity Theft

"*Heh-heh…they can* have *my identity*!"

"*Identity theft doesn't bother* me. *If someone wants my identity, let them go ahead and steal it*!"

"*My credit is so lousy no one would* want *my identity*!"

These statements and many more like them have been heard for years by those of us in the identity theft protection industry. Even though there are news reports and stories every day about identity theft, credit fraud and other forms of this pervasive crime, many (or even *most* people) still don't understand *The Many Faces of Identity Theft*.

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.

Dealing with identity theft using the "head in the sand" approach is *not* a good practice. Most people would rather not even *think* about the risks involved with identity theft. The possibility of having to spend up to 600 hours (that's ***15 forty hour work weeks***) to correct the mess made by an identity thief, is almost incomprehensible when the average person cannot seem to find even a few spare hours a week for the things they actually *enjoy* doing.

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

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.

A. Historical Overview of Identity Theft

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 kind 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 taking this class 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 in to 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 steps that can be taken to mitigate risk and expedite recovery for victims.

B. Growth of Identity Theft

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 and Sears/K-Mart 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.

Out-of-pocket losses of $1 or more were experienced by about 14% of identity theft victims. About half of these victims suffered losses of less than $100.,,,,

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.

C. The Challenge of Identity Theft

Identity theft has become big business. McAfee Inc. is a cybersecurity firm in Santa Clara, California, and Monica Hamilton, McAfee's marketing director, reports that the number of malicious programs written to steal personal information has grown exponentially from about 1 million in 2007 to an estimated 130 million in 2013.

Innocently swiping a credit or debit card at a trusted retailer could be the beginning of a very big identity theft problem. The hacking of point-of-sale systems is a fast growing and serious problem. Computer programs are used by identity thieves to get into retail systems and steal the numbers from the customer's cards who are making purchases.

And it is simply not possible for any merchant, large or small, to completely protect their customers' information. All computer systems have some degree of vulnerability … from the mom-and-pop stores to the major retail chains.

Hacking into businesses has become much more lucrative to identity thieves since they can steal thousands or even millions of card numbers in one fell swoop. Unfortunately for the business that is hacked, the losses can be staggering. The estimated cost to the business that is breached ranges from $150 to $250 dollars for each card number stolen. Where do those costs come from? Much of it results from legal settlements. In addition, consultants may need to be hired to remove malware and many hours are required by the employees of the company to notify customers of the breach. The consumer ultimately bears these costs via the resulting increase in retail prices and credit-card charges.

In spite of the costs incurred, it is quite expensive for a retailer to pursue the investigation of an incidence of identity theft. Therefore, instead of investing in better measures to prevent data loss in the future, many retailers simply do what is necessary to recover from the damage done by the hackers and hope that the nightmare is not a recurring one.

It is common for identity theft to go unreported. In addition, often very little is done in the way of investigation regarding the identity theft crimes that are reported.

Smaller, local law enforcement entities do not have the expertise or the personnel to investigate the smaller cases of identity theft that may be reported to them. And it is only the gigantic cases that involve hundreds, thousands or millions of victims that merit the attention of Federal agencies.

The cost to investigate identity theft is typically greater than the probability of solving the crime. Consequently, most identity thieves are never caught. As a result, shoplifting a relatively inexpensive item from a store is more difficult and the likelihood of being caught is greater than it would be to steal $100,000 worth of credit card numbers from a retailer. This is one of the primary reasons for the dramatic growth of this crime.

Since consumers are not usually held liable for fraudulent credit card purchases, banks have become increasingly vigilant to guard against suspicious purchases. Businesses are not given the same safeguards as individuals and are, consequently, often stuck with the bill. That can spell disaster for small to medium size businesses.

This is especially true businesses that market their merchandise online where the liability for fraud shifts from the issuer of the card to the merchant. When a merchant in a brick and mortar storefront accepts a credit card, and the charge is authorized, and assuming the merchant conforms to regulation, the merchant will get paid, even if a stolen card is used. In a 'Card Not Present' sale, the seller is usually held liable for credit card charge backs, even when the card issuer (bank) has authorized the transaction.

Millions of stolen credit card numbers are for sale on websites that are hidden from the average consumer. You can be sure, however, that these sites are readily accessible to identity thieves. According to Signifyd fraud analyst Mark Bahl, thieves are able to shop for the type of card and desired credit limit they want. One website even offered to emboss the stolen data on blank plastic cards essentially creating cloned credit cards.

Bahl explained, "If you say I want to buy a credit limit on Visa, they'll upload that to you. And all you have to do is pay $140 bucks and now you have $10,000 at your disposal."

When it comes to credit card fraud, everyone is pointing a finger at someone else (processors, banks, VISA/MasterCard, and the merchants). No one wants to takes the blame for identity theft.

Identity theft has become such a lucrative crime, with minimal risk and minimal consequences, that organized crime organizations (often outside of the United States) have become involved. Low paid employees may be recruited to steal client information from their employer. A small USB drive can hold a large amount of data and if the database to which the employee has access is large, this information can quickly add up to a fairly significant source of income for the dishonest employee.

It is common for an identity theft case to cross the boundaries of several different jurisdictions, and each jurisdiction usually has different law and penalties as well as differing jurisdictional policies and procedures. As a result, cooperation between jurisdictions becomes quite challenging. The identity theft victim may live in one state and the identity thief in another.

The theft itself may take place in yet another state or states. This means that there was no crime actually committed in the victim's home state. Smaller identity theft crimes that cross multiple jurisdictional lines are often given little or no attention due to these types of complications.

Once a person has become a victim of identity theft, it is even more important for them to closely monitor their personal information for signs of additional fraudulent activity. Even after the initial identity theft has been discovered and the resulting fraudulent activity resolved, the possibility of being a victim again is quite high.

Chapter Two – Identity Theft Laws and Statistics

"In one notorious case of identity theft, the criminal, a convicted felon, not only incurred more than $100,000 of credit card debt, obtained a federal home loan, and bought homes, motorcycles, and handguns in the victim's name, but called his victim to taunt him -- saying that he could continue to pose as the victim for as long as he wanted because identity theft was not a federal crime at that time -- before filing for bankruptcy, also in the victim's name. While the victim and his wife spent more than four years and more than $15,000 of their own money to restore their credit and reputation, the criminal served a brief sentence for making a false statement to procure a firearm, but made no restitution to his victim for any of the harm he had caused. This case, and others like it, prompted Congress in 1998 to create a new federal offense of identity theft."

~ U.S. Department of Justice

A. Federal Laws

Identity Theft and Assumption Deterrence Act

The Identity Theft and Assumption Deterrence Act became effective On October 30, 1998. This act prohibits "knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law."

(See http://www.ftc.gov/node/119459)

Prior to the enactment of this law, only the financial institutions that had granted credit and suffered monetary losses were considered to be the "victims" as opposed to the person whose identity was stolen. When there is a conviction, this law allows the *true* victim of this crime to seek restitution.

This Act also established the Federal Trade Commission as the central agency to assist identity theft victims and provide guidance on how to resolve the problems caused by the theft. In addition, training for law enforcement and the maintenance of a nationwide database of identity theft complaints was made available to law enforcement as well as giving criminal law enforcement agencies a place to refer identity theft complaints. The FTC also provides identity theft education for businesses and consumers. The nation's primary identity theft website

(www.consumer.gov/idtheft) which provides critical resources for consumers, businesses and law enforcement is maintained by the Federal Trade Commission.

In most cases, the punishment for a person convicted of this offense is a maximum term of twenty-five (25) years' imprisonment, a maximum fine of $250,000, and any personal property that was used or was intended to be used to commit the crime may be seized and forfeited.

Identity Theft Penalty Enhancement Act of 2004

As more Americans began to use the internet to shop and manage their personal finances, President George W. Bush signed legislation to amend the federal criminal code and create the new Federal offense of "Aggravated Identity Theft." This act added two years to prison sentences of those convicted of specified felony violations in which the criminal "knowingly transferring, possessing, or using, without lawful authority, a means of identification of another person." Five years were also added to the sentences on those who were convicted of using false identification in the commission of "terrorist acts."

Identity Theft Enforcement and Restitution Act of 2008

This Act amended the federal criminal code to allow for restitution to compensate the identity theft victims for the time required to rectify the intended or actual harm incurred due to the theft. In addition, offenses for identity theft or aggravated identity theft against organizations were included (expanded from protecting only natural persons).

Prosecution for computer crimes where changed to eliminate the requirement for computer fraud offenses to cross state or national borders. The requirements that damage to the unauthorized access of a victim's computer must be at least $5,000 before prosecution was also removed. New criminal offenses were enacted for attacks on ten (10) or more computers used by a financial institution or the federal government during a one-year period.

This Act gave the Department of Justice more tools with which to combat identity theft and cyber crime.

Fair Debt Collection Practices Act of 1977 (FDCPA)

This Act protects consumers by prohibiting debt collectors from using deceptive or unfair practices when debts have been placed for collection. Household, family and personal debts are covered under FDCPA. It is common for the initial discovery of identity theft to occur because

the victim receives a collection notice or telephone call. Therefore, it is important to be familiar with the rights and responsibilities of the consumer under FDCPA.

Even though the Fair Debt Collection Practices Act (FDCPA) does not expressly address identity theft, it does set forth procedures that a debt collector is required to follow when they receive a notice of identity theft from a consumer. Debt collectors are required to cease collection activity until verification of the debt has been provided by the collector, if the consumer provides a written notice of dispute within thirty (30) days of receiving the validation notice (Section 809 of the FDCPA). According to case law, it is not necessary for a notice of dispute to contain the word "dispute." The consumer is typically advised by the collector that if the debt is not disputed *in writing* within thirty (30) days, the debt will be considered valid.

If a consumer notifies a collector that the debt is the result of identity theft and refuses to pay, that is sufficient notice that the consumer disputes the validity of the debt and triggers the collector's duties under Section 809.

Fair Credit Reporting Act of 1970 (FCRA)

When a consumer disputes a debt, The Fair Credit Reporting Act (FCRA) also places duties on debt collectors. Section 623 of the FCRA says that, if a consumer disputes the accuracy of information furnished by the debt collector, it becomes the responsibility of the collector to notify the Consumer Reporting Agency (CRA) of the dispute. Upon receipt of a valid notice of a dispute directly from a consumer, the debt collector must take these four steps:

1. A reasonable investigation with respect to the disputed information must be conducted.
2. All of the information provided by the consumer with the notice of dispute must be reviewed.
3. The investigation must be completed and the debt collector must respond to the consumer within thirty (30) days of receiving the dispute.
4. If it is determined that the disputed information is inaccurate, the entity that furnished the data must correct the inaccuracy with each Credit Reporting Agency to which the inaccurate information was provided.

The Fair Credit Reporting Act also requires debt collectors to have reasonable procedures in place to respond to identity theft notifications received from Credit Reporting Agencies. These procedures are meant to prevent more false information from being reported. Blocked information must be prevented from being refurnished.

If a consumer submits an identity theft report directly to a collector stating that information maintained by the collector is the result of identity theft, the information is *not* to be given to the Credit Reporting Agencies, unless the debt collector knows or is informed by the consumer that the information is correct.

If a debt collector is notified that any information related to the debt in question may be the result of identity theft, the collector must also notify other relevant parties (i.e., creditor) that the information may be the result of identity theft. Also, should the consumer request it, the debt collector is required to provide the consumer with all the information to which he/she would otherwise be entitled to if he/she had disputed the debt.

Fair and Accurate Credit Transactions Act (FACTA) OF 2003

In addition to the granting of additional rights to consumers, specific provisions are designed to assist victims of identity theft and fraud. One of the rights given to consumers under this Act is the ability to obtain a free copy of the individual's Personal Credit Report from each of the three (3) Credit Reporting Agencies once every twelve (12) months. Due to the fact that many creditors report to the Credit Reporting Agencies, it is wise for consumers to request one report from each credit bureau approximately once every four (4) months. However, it is important for consumers to be aware that creditors my attempt to hold them liable for negligence for failing to notify creditors of fraudulent accounts in a timely manner. More frequent monitoring of consumer credit files helps to avoid this situation.

Fraud Alerts

A call needs to be placed to any one of the three (3) Credit Reporting Agencies to report fraud and that CRA must tell the other two (2). An initial fraud alert makes it more difficult for an identity thief to continue to use the victim's identity for fraudulent purposes. Placing a fraud alert results in:

1. An Initial Fraud Alert being placed at all three (3) credit bureaus for a period of ninety (90) days.
2. The automatic "opt-out" for two (2) years of pre-approved credit and insurance offers.
3. A free copy of the person's credit report from each of the credit bureaus for review.

For credit to be extended while the Fraud Alert is in place, the credit grantor must take reasonable steps to confirm the identity of the person applying for credit. It is likely that the fraud victim will be contacted to verify his/her identity, therefore it is important to be certain that each of the Credit Reporting Agencies (Experian, TransUnion and Equifax) has the current contact information for the affected party.

At the consumer's request, an "extended" Fraud Alert may be placed for a period of seven (7) years. This alert can be removed before the end of the seven (7) year period by the consumer upon written request and proof of identity.

Military service personnel who are on active duty may request an "Active Duty Alert" to be placed on their credit file for at least twelve (12) months. This alert may be removed prior to the end of the twelve (12) month period upon written request and proof of identity.

"Red Flags Rule"

Many businesses and organizations are required to put a written identity theft prevention program in place under the Red Flags Rule. These programs are meant to detect identity theft by the "red flags" that occur in the day-to-day operation of a business. The written identity theft prevention program is also a means to take steps to reduce the possibility the occurrence of identity theft and to mitigate any damages that may result. In general, adherence to this program can help businesses to detect suspicious activity and minimize the costly consequences of identity theft.

The *Four (4) Basic Elements of an Identity Theft Prevention Program under the "Red Flags Rule"* for Businesses include:

1. Reasonable policies and procedures must be implemented to identify "suspicious patterns or practices, or specific activities that indicate the possibility of identity theft" (Red Flags) that may occur in the day-to-day operation of the business. These "Red Flags" will vary according to the type of business.
2. Once the "Red Flags" have been identified, a program needs to be developed for the detection of the "Red Flags."
3. Once a "Red Flag" has been detected, the Identity Theft Prevention Program must detail the specific, appropriate actions to be taken.
4. The IDT Prevention Program must also spell out how the business intends to keep the program current as new identity theft threats are identified.

To What Businesses does the "Red Flags Rule" Apply?

1. Financial Institutions
    a. State or national banks
    b. Federal savings and loan associations
    c. Mutual savings banks
    d. State or federal credit unions
2. Creditors

A creditor is defined as "person that, directly or indirectly, holds a transaction account belonging to a consumer." (This does *not* apply to a professional who directly bills his or her clients for

services at the end of the month. However, anyone who *lends money* as a regular and ordinary part of their business practices, *is required to adhere* to the "Red Flags Rule.")

A business owner should answer the following questions to determine if their business is a "creditor" under the Red Flags Rule.

If the answers to the following questions are "No," the Red Flags Rule does ***not*** apply to this business/organization.

a. Does the business/organization regularly
    i. bill customers or defer payment for goods and services?
    ii. arrange or grant credit?
    iii. take part in deciding whether or not to extend, renew or set the terms of credit?

If the answer to ***all*** of the following questions is "No," the Red Flags Rule does ***not*** apply to this business/organization.

b. In the ordinary course of business, does the business/organization regularly
    i. obtain or use consumer reports with regards to a credit transaction?
    ii. supply information to Credit Reporting Agencies regarding credit transactions?
    iii. give loans (advance funds) to/or for an individual who must repay the loan/funds with either pledged property or cash?

Federal Privacy Laws

Identity theft affects individual victims, businesses and governmental agencies and legislative efforts must take all of these into consideration, while taking into consideration what issues may come up in the future regarding identity theft. Crimes that are now be considered identity theft were considered to be False Personation, or "the crime of falsely assuming the identity of another to gain a benefit or avoid an expense."

Family Educational Rights and Privacy Act of 1974 (FERPA)

This law protects the privacy of student education records and applies to all schools that receive funds from the United States Department of Education. FERPA gives parents or students over the age of eighteen (18) the right to:

- Inspect and review the student's education records maintained by the school.
- Request that school records believed to be inaccurate or misleading to be corrected or amended. Should the school decide not to amend the record, the parent or eligible student may request a formal hearing. After the hearing, if the record is still not amended by the school the eligible student or parent has the right to include a statement regarding the contested information in the file.

- FERPA allows the release of information without the consent of the parent or eligible student under the following conditions (34 CFR § 99.31):
    - School officials with legitimate educational interest;
    - Other schools to which the student is transferring;
    - Specified officials for audit or evaluation purposes;
    - Appropriate parties in connection with financial aid to a student;
    - Organizations conducting certain studies for or on behalf of the school;
    - Accrediting organizations;
    - To comply with a judicial order or lawfully issued subpoena;
    - Appropriate officials in cases of health and safety emergencies; and
    - State and local authorities, within a juvenile justice system, pursuant to specific State law.

The student's name, address, telephone number, date and place of birth, honors and awards and dates of attendance may be included in a Directory unless the parents or eligible student requests that this information not be disclosed.

Schools must notify parents and eligible students about their rights under the Family Educational Rights and Privacy Act on an annual basis.

Driver's Privacy Protection Act of 1994 (DPPA)

This federal law limits the times when a state department of motor vehicles may disclose to the general public, including the media, personal information contained in a person's motor vehicle record. This includes the individual's photograph, Social Security Number, driver's license number, name, address, telephone number and medical or disability information. Certain entities such as the police and courts are exempt.

Health Information Portability and Accountability Act of 1996 (HIPAA)

HIPAA is the most significant development in U.S. health care in recent history. The initial purpose was to ensure and improve the continuity of health insurance coverage for workers changing jobs. To facilitate this objective, "Administrative Simplification" provisions were included that required the Department of Health and Human Services (HHS) to implement national standards for the transmission and protection of health information. These national standards are far-reaching in scope, and HIPAA affects nearly every aspect of the United States health care system.

Under the HIPAA Privacy Rule federal protections are provided for individually identifiable health information held by covered entities and businesses associated with those entities. Patients are also given a collection of rights with respect to that information. The Privacy Rule

is balanced to insure that the disclosure of health information needed for patient care and other important purposes is facilitated.

The HIPAA Security Rule specifies a series of administrative, physical, and technical safeguards for covered entities and businesses associated with those entities. These safeguards are in place to assure the confidentiality, integrity, and availability of electronic protected health information.

HIPAA covered entities and their business associates are required to provide notification following a breach of unsecured protected health information in accordance with the HIPAA Breach Notification Rule.

The Office for Civil Rights enforces the HIPAA Privacy Rule, which protects the privacy of individually identifiable health information; the HIPAA Security Rule, which sets national standards for the security of electronic protected health information; the HIPAA Breach Notification Rule, which requires covered entities and business associates to provide notification following a breach of unsecured protected health information.

The HIPAA Privacy rule regulates the security and confidentiality of patient information. The U.S. Department of Health and Human Services published a final Security Rule in February 2003, which sets national standards for protecting the confidentiality, integrity, and availability of electronic protected health information.

Gramm-Leach-Bliley Financial Modernization Act of 1999 (GLBA)

The primary purpose of the Gramm-Leach-Bliley Act is to protect the privacy of consumer information held by "financial institutions" - defined as "companies that offer consumers financial products or services like loans, financial or investment advice, or insurance.

The GLBA requires companies to safeguard sensitive data and to provide privacy notices that explain the information sharing practices of the company to their customers. The customer/consumer then has the right to limit some, but not all, of the sharing of their personal information.

The Privacy Notice is a written description of a company's Privacy Policy. It must be a "clean, conspicuous and accurate statement" of the privacy practices of the company.

The information contained with the Privacy Notice should include:

- what information is collected regarding consumers and customers
- with whom the information collected is shared
- how the company safeguards and protects the information collected

The Privacy Notice must explain that the customer or consumer has the right to say "no" to the sharing of certain information with the financial institution's affiliates. The consumer/customer may Opt-Out of having their information shared with certain third parties and the Privacy Notice must offer a reasonable way to do so.

B. State Laws - Michigan

Identity Theft Protection Act of 2004

Michigan's Identity Theft Protection Act includes protecting a broad range of "personal identifying information" that can be used to specifically identify an individual. The definition of "identity theft" was expanded by this act to include the fraudulent use, or attempted use, of the personally identifying information of another person to commit an illegal act.

An identity theft victim has the right to file a police report and may file criminal charges against the identity thief in the jurisdiction where the victim lives. Courts may impose a fine of up to $25,000 and, an additional five (5) years may be added to the sentence of a person convicted of identity theft who has also been convicted of and served time for an underlying fraud crime. An identity thief may be prosecuted up to six (6) years after the identity theft or after the identity thief has been identified.

This Act also protects the personally identifying information of a deceased person so that criminals who attempt to misuse the information of a deceased person may be punished under this law.

Michigan Identity Theft Legislation Links
http://www.michigan.gov/documents/legislative_links_126649_7.pdf

C. Identity Theft Statistics

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 ages between 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.

Chapter Three – Types of Identity 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 respecter of age, race, sex or income level.

A. 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 2001, 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.

B. 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."

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 call 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 and government 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 and 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

The "Sixty Minutes" report entitled Biggest IRS Scam Around: Identity Tax Refund Fraud was first aired on September 21, 2014. In part, this report states:

"This is how it works. Someone steals your identity, files a bogus tax return in your name before you do and collects a refund check from the IRS. It's so simple, you would think it would never

work, but it does. It's been around since 2008, and you'd think the IRS would have come up with a way to stop it, it hasn't. Instead the scam has gone viral, tripling in the past three years."

I 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).
    - copy of your Social Security card
    - copy of your driver's license
    - copy of your passport
- Record the dates of calls made and letters sent.
- Keep copies of all letters sent in your personal files.

C. 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.

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.

D. 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."

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 such 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, there 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.

E. 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.'"

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 There is an Epidemic of Medical Identity Theft 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.

F. Synthetic Identity Theft

In the first half of 2014, a man by the name of Deon Mimbs plead 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 individual's Social Security number. Once the SSN is linked a current address

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.

G. 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.

Targeting Children: the Young Victims of Identity Theft

Child Identity theft is one of the fastest growing sector 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?* Kid 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.

Chapter Four – Identity Theft and Businesses

"The term 'business identity theft' is frequently used to describe a wide variety of scenarios involving the fraudulent or unauthorized use of a company's identity, including the following:

Identity thieves in New York used financial information obtained from corrupt bank employees to cash counterfeit payroll checks that were designed to look like they belonged to the victim organizations, which included corporations, hospitals, and government agencies.1

In California, criminals rented office space in the same building as a legitimate business, ordering corporate credit cards or retail merchandise in the businesses' name, and then disappeared by the time the business realized that its identity has been stolen. 2

A Nevada man claimed that the identity of his business was stolen after a company changed the name of the businesses' officers through filings with the Secretary of State's office, then sold the business to a third party. 3

In New Jersey, a company accused a former employee of corporate identity theft after the employee posed as the company on various social networking and business-related sites, all the while posting negative information about the company. 4

Large companies such as eBay, Microsoft, and VISA, have dealt with business identity theft carried out through "phishing" schemes where fraudulent emails purporting to be from legitimate, recognizable businesses seek personal or financial information from recipients. 5

In Tennessee, criminals have been creating phony web sites that impersonate the identity of legitimate car dealerships and advertise low prices in order to scam people into making deposits for vehicles that do not exist. 6

In Georgia, criminals purchased a cell phone, registered it under the name of "Georgia Powers" (which showed up on caller ID), and convinced a number of elderly people – who thought they were speaking with the utility company "Georgia Power" – to divulge their credit card data. 7 "

A. Protecting PII – Personally Identifiable Information

Defining PII and PIFI

The United States General Services Administration defines PII as " any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual."

In more general terms, Personally Identifiable Information is any data, sensitive or non-sensitive, that can distinguish one person from another, i.e. identify a specific individual.

Information that is non-sensitive may be procured from public records, telephone books, corporate websites and directories. Transmission on non-sensitive PII may be sent in unencrypted form without resulting in harm to the individual.

Should Sensitive PII be disclosed, harm could result to the individual whose privacy has been compromised. Therefore, it is important that Sensitive PII should be *encrypted* in databases and when being transmitted.

Personally Identifiable *Financial* Information (PIFI) is any type of Personally Identifiable Information related to or linked with a person's finances; such as credit card and bank account numbers. PIFI is typically information made available by a consumer to his or her financial institution that would not be given to the public.

It is this Personally Identifiable Financial Information that is protected by the Gramm-Leach-Bliley Act. The GLB requires financial institutions to notify their clients as to the privacy policies and practices that they have in place to protect the nonpublic personal information in their possession. Customers must be informed what is being done to avoid the disclosure of PIFI to third parties without the consumer's consent.

According to the U.S. GSA, examples of PII include but are not limited to:

- Name
    - Full name
    - Maiden name
    - Mother's maiden name
    - Alias
- Personal identification number

  - Social Security number (SSN)
  - Passport number
  - Driver's License number
  - Taxpayer Identification number
  - Financial account number
  - Credit card number
- Address information
  - Street address
  - Email address
- Personal characteristics
  - Photograph (especially of the face or other identifying characteristic)
  - Fingerprints
  - Handwriting
  - Biometric data (retina scan, voice signature, etc.)
- Information about an individual that is linked or able to be linked to one of the above
  - Date of birth
  - Place of birth
  - Race
  - Religion
  - Weight
  - Activities
  - Geographical Indicators
  - Employment information
  - Medical information
  - Education information
  - Financial information

Identity Theft and PII

Millions of records have been compromised in recent years involving Personally Identifying Information (PII). When this information is put in jeopardy, it harms both the individual and the organization involved with the security breach. Identity theft is, of course, one of the potential consequences to the individuals. The organization involved is also damaged due to loss of public trust, the legal liabilities associated with the breach, as well as the costs involved in remediation.

The U.S. GSA defines an Information Data Breach as an incident "when PII is viewed, leaked, or accessed by anyone who is not the individual or someone authorized to have access to this information as part of his/her official duties."

One of the first steps that an organization should take in regard to protecting PII is to know what information they are collecting that fits the description on PII. Once your organization is clear on what constitutes PII, the collection, retention and use of PII should be limited to that which is strictly necessary for business purposes.

Comprehensive Policies and Procedures should be developed by any organizations that use, collect and retain PII. In addition, all employees should receive appropriate and regular training regarding the organization's Privacy Policies and Procedures. This is especially important for those employees who will access or use the PII held by the organization.

B. Clients/Customers and Identity Theft

A security breach can happen to any business … large or small. How you respond in the case of a security breach will dramatically affect your business from then on. How you handle the situation will affect your company's reputation and your client's level of trust going forward.

The Ponemon Institute "conducts independent research on privacy, data protection and information security policy." Their 2014 Cost of Data Breach Study: United States revealed the following.

- The cost of a data breach has increased from $188 to $201 per record from 2013 to 2014.
- The number of customers who terminated their relationship with a company after a data breach has increased.

A data breach can also result in the loss of consumer trust, reduced traffic to a once profitable website accompanied by a decrease in sales.

It is important for every business to have a written policy in place to respond to a security breach. Having a plan in place will help you to take action quickly and effectively.

According to Betsy Broder of the Federal Trade Commission,

"The best thing that any institution that has consumer information can do is to develop a plan based upon the threats that currently exist, and then continually reevaluate it. … It is essential for any financial institution or other entity that has this sensitive consumer information, to continually reassess data security. … We expect companies to us reasonable data security practices that are appropriate for the type of information that they collect. … We expect companies to be aware of what the tools are that they can use to ensure protection of this information. … We expect companies to use appropriate and reasonable data security that is geared toward the type of information that they collect and that they use."

Information on the steps to implement such a plan will be introduced in a following segment.

C. Employees and Identity Theft

As an employer, it is to your benefit to make sure that your employees are aware of the ramifications of identity theft and what they can do to prevent it from happening in the work place. It is important that all companies, large and small, have a *written* security policy in place.

You can create an even stronger culture of security by regularly holding training for employees about identity theft and information security. The company's written security policy should, of course, be reviewed, allowing time to answer questions regarding any areas that may be unclear. A comprehensive training program should include *all* employees, not just full time. Part-time employees, those who work at satellite offices, temporary and seasonal help should all be included in the training programs.

After attending ask every employee to sign a statement acknowledging that they have attended the training. In addition, an agreement to follow your company's confidentiality and security standards for handling sensitive data should be signed by each employee.

What happens when an employee becomes a victim of identity theft? What, if any, impact would this have on the company/business that they work for? It has been reported that a serious case of identity theft can take up to 600 hours to resolve … that's fifteen (15) forty-hour work weeks!

When an employee tries to handle an Identity theft issue by themselves, the problem can last from a few weeks to many months. Since most bank, creditors and other affected institutions are usually open when the employee is at work, most of the hours spent resolving the problem are on company time.

It should also be noted that when an employee is affected by identity theft, they are often very upset and annoyed by the situation. This may result in their disrupting the other employees around them by discussing their situation. Identity Theft can be a very *emotional experience* for affected employees and their sense of being violated may be extreme.

When employees feel valued by the business they work for, they tend to be happier and more loyal to the company. Identity theft poses a very high risk to an employee's financial health. In addition, there may consequently be an effect on physical health due to the stress related to being a victim of identity theft. One of the ways that employers can show that they care about their employees and to mitigate potential stress is by offering an identity theft protection service as a voluntary employee benefit.

D. Business Owner(s) and Identity Theft

Due to the fact that a business owner's personal information, credit and finances are often closely linked to their business, the risk to the owner, a key executive, or an officer of a corporation is significantly increased when it comes to identity theft. In the case of smaller, privately held or family owned businesses, the separation between the business and the business owner may be almost undetectable. When the business and business owner are practically one in the same, what impacts the business impacts the owner and vice versa.

Business identity theft, therefore, exposes the business owner to additional risks. Business and commercial bank accounts are *not* protected in the same way as personal bank accounts when it comes to identity theft.

Part 205 of Federal Reserve Regulation E "establishes the basic rights, liabilities, and responsibilities of consumers who use electronic fund transfer services and of financial institutions that offer these services." While this federal regulation spells out the requirements whereby banks must reimburse individual consumers for fraudulent losses, it does *not* apply to business and commercial accounts.

Business and commercial bank accounts are covered by the Uniform Commercial Code (UCC). The Uniform Commercial Code is a set of legal rules and regulations that govern business or commercial transactions and dealings.

When it comes to identity theft, in particular fraudulent banking activities, business bank accounts have less protection, shorter time periods for reporting fraudulent activity as well as significantly higher liability than that of an individual consumer. In addition, individual banks have the ability to further reduce the fraud reporting timelines. By amendments to the bank's commercial banking agreements, some banks are even disclaiming certain obligations to the business entirely.

The bottom line is that when it comes to the protection of a commercial bank account from the ravages of identity theft, the responsibility is left squarely on the shoulders of the business owner and the business entity.

E. Business Entity and Identity Theft

Business identity theft is *not* the same as a security breach or the loss of customer or client information. Even though business identity theft is often referred to as ”corporate or commercial identity theft” any type and any size organization or business can potentially become a victim of this crime. This includes single owners and DBA’s, partnerships and LLCs, not-for-profit organizations, public and private schools, local governments, as well as corporations, large and small.

Business identity theft happens when the *business entity* itself is being impersonated by an identity theft criminal. The thief may then use the identity of the *business entity* to establish lines of credit that can then be used to purchase gift cards, electronics, other equipment or materials which can subsequently be sold or exchanged for cash.

When this happens to a business entity, the business’s credit rating may be damaged or the business may reach the credit limit. This could, in turn, result in loss of working capital for the business.

Chapter Five – 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.

A. 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 and alert, it is important that you take action quickly. If suspicious activity has taken place, follow the steps outlined in Chapter Six (6).

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 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 this 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.

B. 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.

C. 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 indicated 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 ant 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 checks 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 protections 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.

D. 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.

Chapter Six – What to Do If You Become a Victim of Identity Financial Theft

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 that 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 to resolve. In addition there may be costs incurred and above all, persistence and patience will be required to get back to pre-theft status.

A. 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

B. Request a Credit Freeze

You may also request that a credit freeze be place 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

Credit Freeze Letter Example #1

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 John. J. Doe, 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.

[*Your signature*]

[*Your name*]

Credit Freeze Letter Example #2

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 John. J. Doe, 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 will pay the fee of $10 for placing the freeze by:

[*Indicate form of payment used (i.e. check, money order, credit card) and include payment information for processing*]

Sincerely,

[*Your signature*]

[*Your name*]

C. Order Your Credit Reports

Each of the credit reporting agencies is required to provide you with a free credit report once you have placed and 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.

D. Create 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 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

(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:

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.

MEMO FROM FTC TO LAW ENFORCEMENT

To: Law Enforcement Officer

From: Division of Privacy and Identity Protection / The Federal Trade Commission

Re: **Importance of Identity Theft Report**

The purpose of this memorandum is to explain what an "Identity Theft Report" is, and its importance to identity theft victims in helping them to recover. A police report that contains specific details of an identity theft is considered an "Identity Theft Report" under section 605B of the Fair Credit Reporting Act (FCRA), and it entitles an identity theft victim to certain important protections that can help him or her recover more quickly from identity theft.

Specifically, under sections 605B, 615(f) and 623(a)(6) of the FCRA, an Identity Theft Report can be used to permanently block fraudulent information that results from identity theft, such as accounts or addresses, from appearing on a victim's credit report. It will also make sure these debts do not reappear on the credit reports. Identity Theft Reports can prevent a company from continuing to collect debts that result from identity theft, or selling them to others for collection. An Identity Theft Report is also needed to allow an identity theft victim to place an extended fraud alert on his or her credit report.

In order for a police report to be incorporated in an Identity Theft Report, and therefore entitle an identity theft victim to the protections discussed above, the police report must contain details about the accounts and inaccurate information that resulted from the identity theft. We advise victims to bring a printed copy of their ID Theft Complaint filed with the FTC with them to the police station in order to better assist you in creating a detailed police report so that these victims can access the important protections available to them if they have an Identity Theft Report. The victim should sign the ID Theft Complaint in your presence. If possible, you should attach or incorporate the ID Theft Complaint into the police report, and sign the "Law Enforcement Report Information" section of the FTC's ID Theft Complaint. In addition, please provide the identity theft victim with a copy of the Identity Theft Report (the police report with the victim's ID Theft Complaint attached or incorporated) to permit the victim to dispute the fraudulent accounts and debts created by the identity thief.

For additional information on Identity Theft Reports or identity theft, please visit www.ftc.gov/idtheft.

E. 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 it contains 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.

F. 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

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

NOTICE TO FURNISHERS OF INFORMATION / OBLIGATIONS OF FURNISHERS UNDER THE FCRA

The Federal Fair Credit Reporting Act (FCRA), 15 U.S.C. 1681y, imposes responsibilities on all persons who furnish information to consumer reporting agencies (CRAs). These responsibilities are found in Section 623 of the FRCA, 15 U.S.C. 1681s-2. State law may impose additional requirements on furnishers. All furnishers of information to CRAs should become familiar with the applicable laws and my want to consult with their counsel to ensure that they are in compliance. The text of the FCRA is set forth in full at the Web-site of the Federal Trade Commission (FTC): www.ftc.gov/credit. A list of the sections of the FCRA cross referenced to the U.S. Code is at the end of this document.

Section 623 imposes the following duties upon furnishers:

ACCURACY GUIDELINES

The banking and credit union regulators and the FTC will promulgate guidelines and regulations dealing with the accuracy of information provided to CRAs by furnishers. The regulations and guidelines issues by the FTC will be available at www.ftc.gov/credit when they are issued. Section 623(e).

GENERAL PROHIBITION ON REPORTING INACCURATE INFORMATION

The FCRA prohibits information furnishers from providing information to a CRA that they know or have reasonable cause to believe is inaccurate. However, the furnisher is not subject to this general prohibition if it clearly and conspicuously specifies an address to which consumers may write to notify the furnisher that certain information is inaccurate. Sections 623(a)(1)(A) and (a)(1)(C).

DUTY TO CORRECT AND UPDATE INFORMATION

If at any time a person who regularly and in the ordinary course of business furnishes information to one or more CRAs determines that the information provided is not complete or

accurate, the furnisher must promptly provide complete and accurate information to the CRA. In addition, the furnisher must notify all CRAs that received the information of any corrections, and must thereafter report only the complete and accurate information. Section 623(a)(2).

DUTIES AFTER NOTICE OF DISPUTE FROM CONSUMER

If a consumer notifies a furnisher, at an address specified for the furnisher for such notices, that specific information is inaccurate, and the information is, in fact, inaccurate, the furnisher must thereafter report the correct information to CRAs. Section 623(a)(1)(B).

If a consumer notifies a furnisher that the consumer disputes the completeness or accuracy of any information reported by the furnisher, the furnisher may not subsequently report that information to a CRA without providing notice of the dispute. Section 623(a)(3).

The federal banking and credit union regulators and the FTC will issue regulations that will identify when an information furnisher must investigate a dispute made directly to the furnisher by the consumer. Once these regulations are issues, furnishers must comply with them and complete an investigation within 30 days (or 45 days, if the consumer later provides relevant additional information) unless the dispute is frivolous or irrelevant or comes from a "credit repair organization." The FTC regulations will be available at www.ftc.gov/credit. Section 623(s)(8).

DUTIES AFTER NOTICE OF DISPUTE FROM CONSUMER REPORTING AGENCY

If a CRA notifies a furnisher that a consumer disputes the completeness or accuracy of information provided by the furnisher, the furnisher has a duty to follow certain procedures. The furnisher must:

Conduct an investigation and review all relevant information provided by the CRA, including information given to the CRA by the consumer. Sections 623(b)(1)(A) and (b)(1)(B).

- Report the results of the CRA that referred the dispute, and, if the investigation establishes that the information was, in fact, incomplete or inaccurate, report the results to all CRAs to which the furnisher provided the information that compile and maintain files on a nationwide basis. Section 623(b)(1)(C) and (b)(1)(D).
- Complete the above steps within 30 days from the date the CRA receives the dispute (or 45 days, if the consumer later provides relevant additional information to the CRA). Section 623(b)(2).
- Promptly modify or delete the information, or block its reporting. Section 623(b)(1)(E).

DUTY TO REPORT VOLUNTARY CLOSING OF CREDIT ACCOUNTS

If a consumer voluntarily closes a credit account, any person who regularly and in the ordinary course of business furnishes information to one or more CRAs must report this fact when it provides information to CRAs for the time period in which the account was closed. Section 623(a)(4).

DUTY TO REPORT DATES OF DELINQUENCIES

If a furnisher reports information concerning a delinquent account placed for collection, charged to profit or loss, or subject to any similar action, the furnisher must, within 90 days after reporting the information, provide the CRA with the month and the year of the commencement of the delinquency that immediately preceded the action, so that the agency will know how long to keep the information in the consumer's file. Section 623(a)(5).

Any person, such as a debt collector, that has acquired or is responsible for collecting delinquent accounts and that reports information to CRAs may comply with the requirements of Section 623(a)(5) (until there is a consumer dispute) by reporting the same delinquency date previously reported by the creditor. If the creditor did not report this date, they may comply with the FCRA by establishing reasonable procedures to obtain and report delinquency dates, or, if a delinquency date cannot be reasonably obtained, charged to profit or loss, or subjected to any similar action. Section 23(a)(5).

DUTY OF FINANCIAL INSTITUTIONS WHEN REPORTING NEGATIVE INFORMATION

Financial institutions that furnish information to "nationwide" consumer reporting agencies, as defined in Section 603(p), must notify consumers in writing if they may furnish or have furnished negative information to a CRA. Section 623(a)(7), The Federal Reserve Board has prescribed model disclosures, 12 CFR Part 222, App. B.

DUTIES WHEN FURNISHING MEDICAL INFORMATION

A furnisher whose primary business is providing medical services, products, or devices (and such furnisher's agent or assignees) is a medical information furnisher for the purposed of the FCRA and must notify all CRAs to which it reports of this fact. Section 623(a)(9). This notice will

enable CRAs to comply with their duties under Section 604(g) when reporting medical information.

DUTIES WHEN ID THEFT OCCURS

All furnishers must have in place reasonable procedures to respond to notifications from CRAs that information furnished is the result of identity theft, and to prevent refurnishing the information in the future. A furnisher may not furnish information that a consumer has identified as resulting from identity theft unless the furnisher subsequently knows or is informed by the consumer that the information is correct. Section 623(a)6). If a furnisher learns that it has furnished inaccurate information due to identity theft, it must notify each consumer reporting agency of the correct information and must thereafter report only complete and accurate information. Section 612(a)(2). When any furnisher of information is notified pursuant to the procedures set for the in Section605B that a debt has resulted from identity theft, the furnisher may not sell, transfer, or place for collection the debt except in certain limited circumstances. Section 614(f).

The FTC's Web site, www.ftc.gov/credit, has more information about the FCRA, including publications for businesses and the full text of the FCRA.

Chapter Seven – Identity Theft Protection Services

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.

A. 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.

B. 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 care 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 call, 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.

C. 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, 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.

D. 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.

Chapter Eight – Role of the Agent

William Benson is in the midst of a financial nightmare. His ex-wife and her current partner opened new credit cards in Benson's name and racked up $22,000 in charges. In addition, they got a loan and purchased a car, but neglected to make the payments. To make matters worse, they leased an expensive apartment in his name and then moved to another state. Mr. Benson has called his insurance agent to see if he has any coverage that will help him out.

As an insurance professional, your clients are looking to you for advice and solutions in protecting themselves, their families and their businesses against the growing risk of identity theft.

A. Property & Casualty Agent

Identity theft coverage is typically available as an endorsement on a homeowner's policy. Many of these endorsements only offer limited coverage for credit card losses. Some are meant to reimburse your client for lost wages, postage, notary fees, etc.

When a business gathers and stores personal information, whether on paper or electronically, that business is at risk for a data breach. Retail merchants, medical facilities, financial institutions and other businesses are looking to protect themselves against losses related to a data breach. As a result, the purchase of cyber insurance policies increased by twenty percent (20%) from 2013 to 2014 according to the tracking done by New Your insurance brokerage firm, Marsh LLC.

Cyber insurance policies are designed to provide coverage for the costs related to a data breach, including:

- Providing credit monitoring services for customers
- Hiring public relations experts to mitigate any damage to the company's reputation
- Retaining investigators to determine the source of the breach

Policies may also include access for the business owner to resources to help reduce the likelihood of the occurrence of a data breach. In addition, assistance may be provided to ensure that a plan is in place including proper procedures to be followed should a breach occur.

Coverage may also be included to protect the business from the liability associated with a data breach. This may include help with the charges for legal defense from lawsuits resulting from the breach as well as the cost of any settlements, judgments or civil awards that may be legally obligated as a result.

It is up to the Property and Casualty Agent to have a clear understanding of the impact that identity theft can have on his or her clients. It is also important to know what is and is *not* covered by the policies and/or endorsements that are being sold to your customers.

Commercial clients may also be interested in offering identity theft protection services that include *restoration* services (instead of to resolution services as discussed earlier) as an employee benefit to keep employees on the job and focused on their jobs should the employee become a victim of identity theft.

B. Life Agent

According to Identity Management Institute (IMI) life insurance fraud is costing the industry approximately $70 billion a year. Life insurance agents should counsel their clients review their life insurance policies regularly and be sure that the beneficiary is who they intended it to be. Policy holders should be cautious in their response to any unexpected phone calls, emails or correspondence regarding their life insurance policy. Any requests for information should be verified by the client with the policy issuer.

When marketing life insurance it is important for agents to be aware of the fact that a large part of life insurance fraud is related to identity theft. You may wish to educate your clients and offer the added protection of in identity theft plan to their life insurance policy.

One of the questions a life insurance agent may ask is whether or not the client, or prospective client, has an updated Last Will and Testament. Statistics tell us that over 70% of Americans do not have this important document. A Last Will and Testament specifies who raises young children as well as who receives the person's property. Without this document in place (intestate), you leave these critical decisions in the hands of the state in which you reside.

Life insurance agents may wish to inform their clients of the fact that identity theft protection services that include a legal services plan often include a Last Will and Testament, Living Will and Medical Power of Attorney as part of the membership.

C. Health Agent

According to the Identity Theft Resource Center, 2013 was the first year that data breaches in the medical industry surpassed all other sectors. There were more data breaches that year in the health care industry than in business and government combined.

Following is the percentage of the total reported breaches in 2013 by category.

- Health/Medical 43.8%
- Business 34.4%
- Government/Military 9.1%
- Educational 9.0%
- Financial/Credit 3.7%

Offering identity theft protection services in addition to traditional benefit offerings has become more common. Identity theft protection does, of course, help the employees who are affected by this pervasive crime. However, these services also benefit the employer by helping to reduce the time the employee has to spend to get back to pre-theft status. Stephanie Ward, vice-president and account manager at Corporate Synergies Group Inc., a prominent health insurance brokerage and consulting firm, stated that identity theft protection has gone from an offering given to only one or two clients to, "Now it's something we are including in all of our proposal information."

In addition to the financial loss that may be experienced by victims of identity theft, emotional distress is also a consequence of the crime. Victims may have to deal with the effects of a negatively impacted credit report that can require hundreds of hours to resolve. Depending on the type of identity theft, victims may be subjected to criminal investigation or even arrest based on fraudulent information. The stress associated with employees dealing with the effects identity theft may also cause an increase in the use of medical benefits, thus increasing claims and costs to the employer.

D. Voluntary Benefits Agent

More employers than ever before are adding voluntary services as part of their benefits package. At one time voluntary were primarily used to keep and attract, motivate and retain the best

employees. In today's market, voluntary benefits are often used to offset coverage gaps created by the higher deductibles used to control premiums.

In addition, a Hartford study reported that employees who are offered voluntary benefits are more satisfied with their benefits than those who are not. While many of these benefits are medically related, identity theft protection and legal benefit plans continue to grow in popularity.

Voluntary benefits also help to add value and differentiate the agent or broker from his or her competition by enhancing employer-client relationships. Typically, these benefits are at no direct cost to the employer and are paid 100% by the employee through payroll deduction.

The bottom line is that offering voluntary benefits, in particular identity theft protection services combined with legal service plans, helps employees, employers and insurance professionals.

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.

If you have further questions, please feel free to contact her:

Phone: 248-361-9641

Email: akoch@premiersolutionsintl.com

Website: www.AnitaKoch.com