INSTANT IDENTITY ARMOR

Don't Be A Victim - A Multi-Point Plan to Protect You and Your Family From Identity Theft & Fraud

Inside This Report

INTRODUCTION

Don't Be A Victim - A Multi-Point Plan to Protect You and Your Family From Identity Theft & Fraud

In many cases, you don't know your identity has been stolen or your financial accounts have been comprised until your credit card is declined or your bank account gets drained. The panic that rushes through you when you realize what has happened is nothing compared to panic you'll feel when you discover the nearendless nightmare that comes with trying to reverse the damage

There are many safeguards you can take to protect yourself from identity theft and credit card fraud. First and foremost, you must understand what constitutes identity theft and the various methods crooks can use to obtain your identity.

In some cases, you may be unwittingly contributing to the criminal activity by openly displaying your personal information or by being careless with your financial data. In other situations, you may be collateral damage in a large infrastructure security breach that provides financial data on thousands of people within a database to a technologically tsavvy hacker.

By knowing some of the different routes a criminal can take to get your personal information, you can begin to use safeguards to help prevent fraudulent activities and protect your own finances. The safeguards don't have to be large, life-altering security procedures, and they may only require

a few small, simple adjustments to your everyday activities.

Unfortunately, even with all the proper safeguards in place, you can still end up a victim of identity theft. If this happens, there are steps you need to take immediately to mitigate the damage and begin reversing the process. You should be aware that even though you weren't responsible for the theft or at fault for what occurred, the responsibility for cleaning up the mess will fall squarely on your shoulders.

The good news is that with a little luck and swift action, you can take back your life and reclaim control of your finances. The even better news is that by understanding identity theft in detail, you can get fly under a thief's radar and reduce the chance your identity will even be stolen in the first place.

CHAPTER 1: WHAT IS IDENTITY THEFT?

Identity theft is a crime of impersonation where the thief will take your personal information and use it to assume your identity for personal financial gain. Approximately 15 million United States residents have their identities used fraudulently each year with financial losses totalling upwards of $50 billion.

Identity theft can happen to anyone at any time. Today's modern technology and conveniences allow for multiple points of entry for thieves looking to gain access to personal data. Online retailers, smart phones, personal computers, public resumes, and community groups with poor security invite hacking and database breaches to give easy access points to your personal data for thieves.

The best defense is to be aware of the situation, actively work to limit access points, and work diligently to identify any suspicious activities.

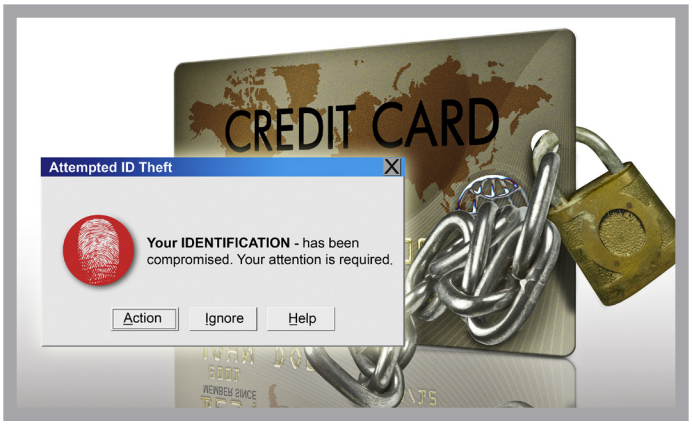
Types of Identity Theft

Although there are many ways to obtain other people's identities and defraud victims, there are typically two main categories of identity theft.

First, there is an account takeover. This type of identity theft is typically the easiest for thieves. In general, a thief will obtain your credit card information (or other comparable financial information) and use it to make purchases. This method is very lucrative for the thief as they can generally quickly reach the credit card's limit and discard the information before you're even aware a theft has happened. Victims typically learn about the fraudulent purchases when they get their monthly statement or when their card is declined because it has reached the maximum allowable limit.

The second type of identity theft is application fraud (also known as "true name fraud"). To do this, a thief must have access to a great deal of personal information about a victim. The thief will then fraudulently use this information to apply for lines of credit in someone else's name. Victims may not learn of this activity until they're contacted by a collections agency for payment, see a surprising new lien on their credit report, or are denied a line of credit due to the fraudulent activity.

Both of these types of identity theft activity are devastating to you and your finances. Even though you can seek redress and may be reimbursed in full for any money that was stolen from you, the hassle and stress of dealing with it all is a situation to avoid.



It Can Affect Anyone

Identity theft can happen to anyone. Thieves do not necessarily take wealth, or lack thereof, into consideration when targeting a victim, nor do they consider your credit score. Essentially, identity theft is a crime of opportunity, and the more you leave yourself open to such opportunities, the more likely it is you'll be targeted.

College students, professionals, unemployed people, and the elderly can all fall victim to security breaches or carelessness at times. Even without carelessness, we are all products of a digital age where much of our personal information is in the hands of numerous other people we can't control.

Even cautious people may be unwittingly exposing themselves to criminals. Online shopping, social media, automated teller machines, and smart phones all lend themselves as tools to thieves. Additionally, people regularly lend their personal information to strangers in the form of resumes, displayed IDs, mailing information, and public internet usage. The routes into your personal life are virtually endless for a truly determined thief.

Not even your children are safe

Having a child should be one of the happiest moments in any persons life. It is also one of the scariest and nerve wracking. The moment that child is born you are fully responsible for not just your own life but also the life of a new born person that you will help mold into the best person they can be. In all of the commotion and joy of bringing a new life into the world you are also faced with some harsh realities. You have to think of the cost of childcare, school supplies, clothes, buying their first car, starting a college fund, and so on.

One thing you may not think of is the fact that as soon as that child is issued a social security number they instantly become a possible victim for identity theft and if a child's identity is stolen it could be much much worse than having your own taken. Children's Social Security numbers are 51 times more likely to be stolen than an adult's.

Why is that?

Often the first time a person checks their credit isn't until they are at least 18. The crime goes unnoticed for years, usually not detected until the child attempts to obtain credit, applies for a job, college or government benefits. By then, the damage is done. Identity theft is the fastest growing crime and our children are the ones most at risk.

Consider the following statistics from a joint report based on research conducted by AllClear ID and the Carnegie Mellon Cylab:

- Youngest victim only five months old
- 54% under the age of 12
- Largest debt: $725,000
- Two-year-old in bankruptcy
- Nine-year-old in debt collections)

When you have children, make sure that you protect their identity as well as your own.

Who are the Regulating Bodies in Charge?

The Federal Trade Commission (FTC) is charged with consumer protection. They work to educate the American public about deceptive trade practices, including identity theft. It's the FTC's job to track and identify the number of identity thefts and the monetary values of the losses.

Within the FTC is a unit called the Bureau of Consumer Protection (BCP). It works in conjunction with the Federal Bureau of

Investigations, the Office of the Attorney General, local law enforcement bodies, the Securities and Exchange Commission, and others to protect consumers from fraudulent activities and to protect financial institutions from the activities as well . Depending on the nature of the crime, its severity, and its duration, other law enforcement bodies may play a role in capturing the thief, recouping losses, and preventing future instances of the theft. While a few bodies may claim responsibility for controlling the crime, many groups play a hand in its prevention.

CHAPTER 2: METHODS OF IDENTITY THEFT

Identity theft occurs in many ways. As technology advances to make daily life more convenient, thieves advance in order to take advantage of the willing use of these conveniences. Thus, you must stay aware of the latest technologies and the latest techniques that thieves are using to obtain information.

Obtaining Information from Mail

One of the oldest methods of obtaining personal and financial information is to sort through someone's trash. As disgusting as it may be, this is a highly effective method of obtaining valuable information. Similar to dumpster diving, a thief may actually open a mailbox and remove the mail. Victims with roadside mailboxes are more susceptible to this fraud. Credit card bills, phone bills, statements, unsolicited loan information, and more contain very valuable personal information that can be used for account takeovers and application fraud.

For some of the pieces of mail, a thief only needs to respond to the notices and notify the company of a new address. Once they have provided this information, they begin the process of using the victim's line of credit.

In other cases, a thief may actually approach the post office and pretend to be the victim. The thief will then attempt to change the mailing address of the person. In this way, the thief may be able to buy a little more time before the victim and the authorities are alerted to the crime.

The Use of ATMs and Checks

Thieves today are especially skilled at monitoring PIN numbers from a distance. With or without the physical debit card, thieves are able to use ATMs against a victim through a process called "skimming." Skimming devices may be improvised or they may be elaborate purchased devices that attach to an ATM card reader. These devices allow the thief to collect multiple card numbers. The skimming devices may also perform one of two functions: either disrupt the customer's ability to use the machine successfully; or quietly collect card information.

Devices that interrupt transactions are typically easier to identify. They are often attachments to the machine that function similarly to how the machine would function regularly but display an error message after all your information has been entered. A more discreet skimmer will simply capture card information and be nearly undetectable. Outside of ATMs, these sorts of skimmers work on any type of card reading device.

Consumers should manually inspect ATMs and card readers on gas pumps for any loose pieces, odd looking attachments, or possible skimming devices.

Thieves will also create counterfeit checks with a victim's information or may alter checks that belong to you. Additionally, thieves may also open a checking account in a victim's name and use it to write bad checks and incur debt.

Telephone Scams

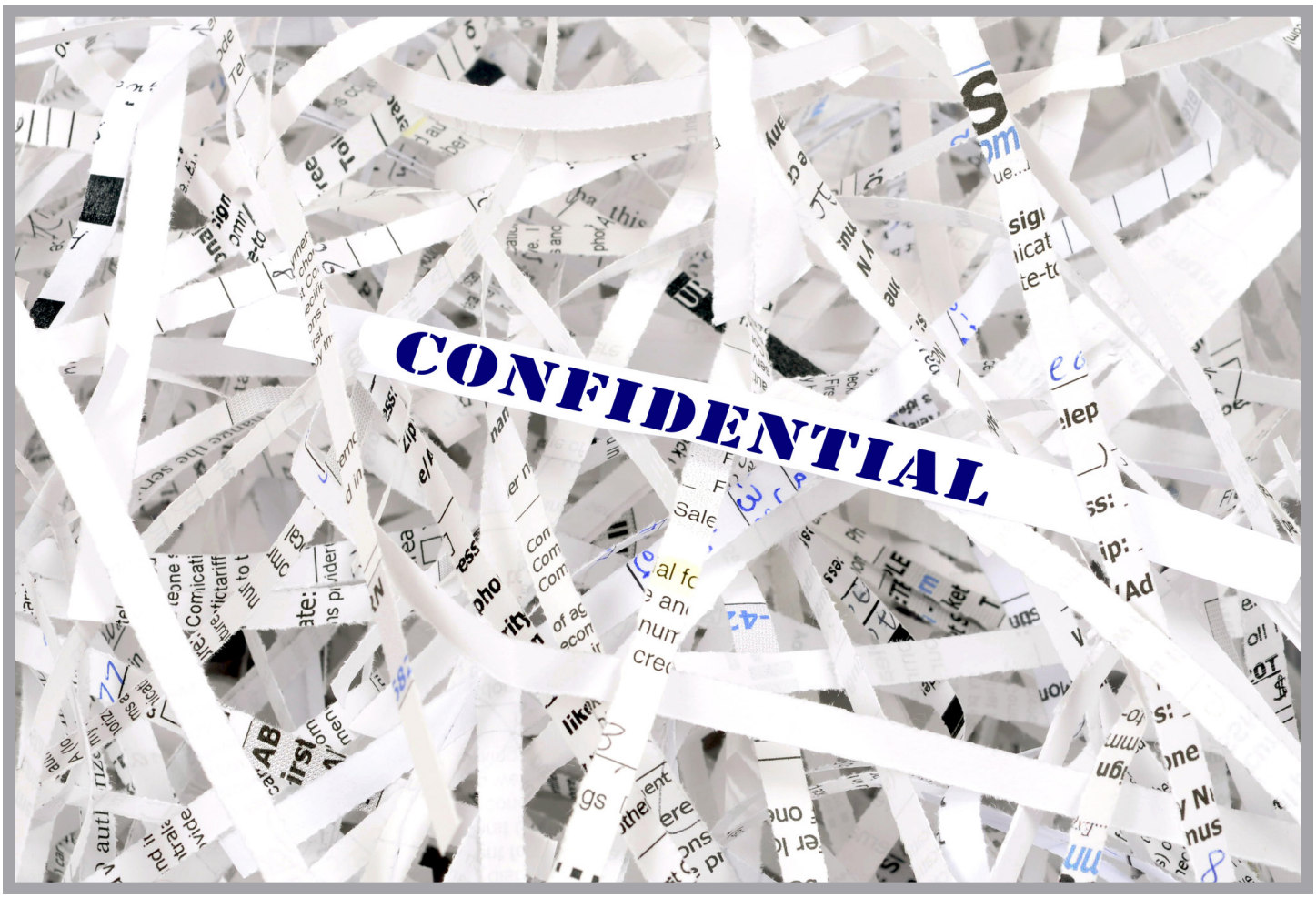
Similar to credit card fraud, thieves may also use your identity and credit information to open a telephone service account in the victim's name. This type of fraud is relatively easy to rectify but can still be a hassle. More likely, victims of telephone fraud have been scammed by a scam artist soliciting a donation for a fake charity or soliciting personal information in order to obtain the victim's identity.

Separately, the integration of smart phones and online capabilities make these mobile devices highly susceptible to hackers and thieves with the right tools. With the amount of personal data stored and transmitted through smart phones, thieves with a little technological savvy can hit the identity theft jackpot.

Every year, hacker conferences draw large crowds of computer savvy geniuses into hotspots to attempt to infiltrate the latest and greatest technology. These conventions offer substantial cash and gift prizes for security breaches. Every year, the tech companies discover they have a long ways to go before they build impenetrable devices. In fact, many of these tech companies realize that the farther they advance with their technology, the farther tech-savvy thieves advance as well.

Online Activities

In today's day and age, people are increasingly transmitting personal and financial information through online forums. Activities like online shopping, social media usage, online banking, public internet usage, and phishing scams are common activities that open you up to identity theft and financial ruin. Due to the vast online economy, thieves take advantage of this modern convenience and use it to their advantage.



Public wireless internet access creates a hotbed of opportunity for thieves and scam artists to target individuals and capture their information. Thieves may be able to tap directly into a wireless device or even plant malware or malicious content directly onto a website or email. Once an unsuspecting victim like you clicks the link, the thief has access to your computer and may plant tracking devices that will monitor your activities, passwords, habits, financial information, and much more.

CHAPTER 3: PREVENTING IDENTITY THEFT

As overwhelming as it may seem, there are steps that you can take to protect yourself from identity theft. Being aware of the problem is the first step, and taking action is the second.

Protecting Mail

This may be one of the most simple protection measures that you can implement to protect yourself from harm. Before discarding mail, be sure to shred any pieces of paper with any identifying information. For maximum security measures, shred any and all documents that are directed to you.

Document shredders are available in a wide variety of prices and security options. Basic shredders are small, inexpensive, and shred in a linear pattern. More

expensive shredders can shred multiple pages simultaneously, and perform in a cross-cutting manner (instead of having strips of paper, this shredder creates diamond-shaped confetti). With a cross-cutting shredder, you eliminate the risk of shredding a document in a way that is easy to piece back together. Also, with linear cuts, it is possible that an entire strip of paper may contain just enough information for an identity thief to do damage.

An added security measure is to place a lock on your mailbox. The lock may act as a deterrent to theft. Additionally, you will notice immediately if the lock has been tampered with and will be able to alert authorities before damage incurs.

For maximum security, you can purchase a post office box or a UPS box and have all of your vulnerable mail routed to that address. If you travel often, you can use these boxes as your primary address so that your mail doesn't accumulate at home and indicate that you're away.

Key Tips for Protecting Mail

- Remember that bills typically arrive on a monthly basis. Be diligent in anticipating the mail, and alert the appropriate company if a bill fails to arrive on time.

- Always opt out of pre-approved credit card offers. For a five year opt-out plan, contact 1-888-5-OPT-OUT. For a permanent opt-out option, visit www.optoutprescreen.com, initiate an online request, and fill out the Permanent Opt-Out Election form. The number and website are operated by the major credit bureaus.

- You should always arrange for a trustworthy neighbor, family member, or friend to pick up your mail when you're away for an extended period of time.

PIN, Debit Cards, and Credit Cards

As technology advances, so does the methods of thieves. It is not paranoid, silly, or overprotective to take protective measures to secure the integrity of these cards and PINS. While you may not be able to keep a watchful eye on your cards at all times (ie, when a waiter takes a card to the back to finalize payment), you can still take steps to protect yourself.

First and foremost, you should consider using a credit card with optimal security features instead of debit cards for transactions. In general, credit card companies understand the prevalence of identity theft and credit card theft. They have advanced their security protocols and their reimbursement procedures leading to a quick and efficient system for consumers. In case of theft, you will find that working with credit card companies requires less hassle and is quicker for reimbursement than trying to resolve the situation with a bank.

Next, you should consider using bank tellers instead of ATMs. Although it is

slightly more time consuming to withdraw money this way, it eliminates the risk of ATM skimmers and over-the-shoulder peekers. While it may not be completely feasible to do this all the time, you should at least evaluate the machine for suspect attachments or signs, such as a sign indicating that you should "swipe here" before entering your card into the machine's card reader.

Also, carry only the cards necessary. That way, if a pickpocket steals your wallet, or if you accidentally leaves your purse somewhere, you'll only have a short list of companies to notify, and the damage can be minimized.

New credit card technologies also bring some added hazards. The unique benefit of being able to "wave" a card at a card reader instead of "swiping" it also means that thieves may have card readers that can read these types of cards as you walk past (these devices are known as Rogue RFID Scanners). To protect against these types of scanners, you can buy RFID protective sleeves, wallets, and even pocket liners. They create an impenetrable barrier that prevents thieves from gaining access to your data.

Finally, request an annual credit report from each of the credit reporting bureaus (Experian, TransUnion, and Equifax). According to recent statistics, only one out

of five people invoke this simple protection . Thoroughly review each and every entry on the report. If something suspicious is on the report, contact the credit bureau for inquiry. If it cannot be resolved by the bureau, directly contact the company listed on the report. If it still cannot be resolved, proceed through the appropriate channels to dispute the entry, and flag the reports for unauthorized activity with all three of the credit reporting bureaus.

Key Tips for Protecting PINS, Debit Cards, and Credit Cards

- Keep PIN information private. Do not provide this information to anyone, and protect the information from the prying eyes of strangers.
- Beware of strangers that may try to "help" while at the ATM.
- If a card is not immediately returned upon completing or canceling the transaction, contact the financial institution immediately.
- Always review banking and credit card statements to ensure all transactions were authorized and accurate.
- Know the reimbursement and insurance limits for each account. Never have more money in an account than the financial institution is willing to reimburse for if theft or fraud were to occur.
- Know the timelines for reporting yourself as a victim of identity theft to be fully reimbursed for damages.
- Physically inspect ATMs and gas pumps for odd attachments and possible skimming devices. Any loose fittings could compromise the machine.

Be Smart

Protect Personal Information

Only provide personal information on a need-to-know basis, and seriously reconsider any public announcements of such information. Social media sites, personal blogs, resumes posted online, dating websites, etc. all provide a wealth of personal information that can be used to steal identities. Consider each and every instance of personal information, and evaluate whether or not it is necessary for that information (or portions of it) to be made public. Zealous protectors of their identity can even have a little fun with this piece of protection. Consider creating an alternate name for places with public announcements, like restaurants and mechanic shops.

Social media sites can do more than just publish personal information that can lead to identity theft. Some of the information posted on social media sites may provide thieves with enough information to let them enter your home and take physical property as well. When you post information about your vacation plans and check-ins, it acts as an open invitation for unscrupulous individuals to enter a vacant home. Think about it, your name and address can easily be found but just about anyone and the majority of social media users leave their profiles open to the public. If someone has your name and address and you constantly update your status and you check in at a movie theater or restaurant that instantly lets a thief know that they have free reign to your home for at minimum an hour and a half.

Be ultra-secure and leave that information offline.

Also, ensure that all personal accounts require passwords in order for changes or inquiries to be made. Create unique passwords for each account and memorize them. Discuss the privacy policy for companies that hold all personal accounts, and gain a thorough understanding of how they may use personal information (opt-out of information distribution when necessary).

It is important for you to remember never to copy important information such as birth certificates, social security cards, credit cards, driver's license, etc. at large public copy machines.Every image processed through a large copy machine is stored on an internal hard drive which can easily be accessed by anyone with even a limited amount of computer skill. Protect Online Information

Do not open or respond to suspicious emails, and install anti-virus software along with a firewall to prevent online intruders from tracking personal internet activities. Also, consider that email is not a very secure method of information transmission, and be wary of trading information through it. Research the latest trends in internet scams, and be on the alert for these activities and tip offs. Finally, consider creating a separate email account that contains no personal information and is only used for suspected spam (such as special offers, sign up promotions, etc.).

Protect Smart Phones and Data

Smart phones hold a vast amount of personal data and are incredibly easy to crack into, especially if you don't even have a superficial passcode. Smart phone users should never store their account passwords

and account information in their smart phones. However, you could devise a clever scheme in order to encrypt your passwords in a way that only you could understand.

Many smart phones also utilize a remote wiping service. That way, if you lose your phone, you can log into a computer (or even through another smart phone), enter your smart phone information, and the remote wiping service will clear out any and all information from your phone. While this may not help to return the phone to you, it will certainly protect you from the troubles of identity theft.

Tech-savvy thieves may also have access to state-of-the-art technology that is able to transfer data and information by merely placing the device near a smart phone. This furthers the importance of not keeping confidential information on a phone that can be easily compromised.

Notify the Proper Authorities of Suspicious Behavior

Always notify the proper authorities or companies of suspicious behavior. The Better Business Bureau, the Attorney General, or even the local FBI may be appropriate. In other cases, consider who the suspicious person or company is claiming to be, and contact the actual company to notify them of your concerns.

For example, if you get an email claiming to be from FedEx that requests personal information, you should contact the FedEx headquarters. Let them know that this is occurring, and provide them with all of the relevant information. Not only can they help track down the perpetrator, but they will likely appreciate it.

Key Tips for Being Smart About Security

- Keep a low profile on social media sites.
- Do not distribute personal information online.
- Keep all social media sites on their optimal security and privacy settings, and do not connect with people that are not trustworthy.
- Make all passwords unique and different.
- Create dummy email addresses and telephone numbers to use for non-personal forms.
- Be hyper-vigilant with protecting smart phones and their data.
- Maintain a passcode or password on all electronic devices.
- Install a remote wiping system for all smart phones.
- Be aware of the proper authorities that will need to be contacted in case of an emergency.
- If passwords of data must be stored on a smartphone, create a complex coding system for storing the information so that the information is impossible for anyone to decipher other than you.

- Protect the integrity of passwords, credit card numbers, and financial information.

- Be aware of your surroundings when using ATMs. Do not trust that strangers will not look at the screen while typing the PIN.

CHAPTER 4: WHAT TO DO WHEN IDENTITY THEFT OCCURS

Even with all of the precautions and procedures in place, identity theft and credit card abuse may still occur. Whether you triggered the criminal activity through some sort of neglect, or the criminal was able to infiltrate another institution to gain access to your identity (ie, hacking into a dating website to obtain personal information), the activity has occurred and you must now deal with the aftermath. Once this happens, there are a few steps that you must take to mitigate or reverse the damage.

Before any action is taken to identify the leak or to mitigate the financial damages, immediately contact your credit bureau or financial institution to notify them of the suspicious activity. It is possible that the suspicious activity may be a mistake on behalf of the financial institution and no further action will be needed.

Alternatively, the financial institution may deem that the suspicious activity is, in fact, a security breach and the confidentiality of your personal and financial information has been compromised. In this instance, you will need to contact the local law enforcement agency to begin filing a report.

Steps to Take in Recovering a Lost Identity and Line of Credit

First and foremost, you should report the crime to police and the appropriate authorities immediately. Contact the local police department and file a criminal complaint. You should request a copy of the report as well. You can use the report to help substantiate the fraud claim with financial institutions or relevant credit companies.

Also, you should report the crime to all three of the credit bureaus. Write down any and all information that can assist you with making the claim. Include the date and time of the call, the names of each and every person that you speak with, and any reference numbers that they may provide. You will need to ensure that your credit reports reflect the identity theft claims.

Once this has occurred and you has seen the new report with the claim, be sure that they implement the heightened security measures. In the future, the credit bureau will seek your permission before allowing an entity to open any new credit accounts. Be sure to check in with the credit bureau periodically to determine if anyone is continuing to try to use your identity and lines of credit under your name.

You will need to document each and every step that they take during this process. It's best if you have a notebook or file folder dedicated specifically to this issue. You'll need to include any and all information that you possibly can about the situation. Include names of all the people and companies you contact, as well as any expenses you incur. Make copies of all disputed documents with notes, and keep these copies in your notebook or file.

You'll also need to cancel all of your credit cards, and request that the credit card companies issue you completely new cards. At this time, discuss the security breach with the credit card company and ask that they implement heightened security measures. Remember to document the time and date of the call as well as the name of the person you spoke to and copies of relevant documents.

Do the same for bank accounts. Close the accounts, and open new ones. Discuss the security breach with the bank, and be sure to ask if they can open a new account that has the same benefits as your existing account (there may be cases where the bank has changed some of their customer features, such as free checking or reimbursed ATM fees). Ask the bank to implement any heightened security measures that they may have for identity theft situations.

Once these new accounts have been opened, create new PINS and passwords for each and every account. Be sure to create unique passwords for each account. If new accounts are not necessary, be sure to at least change the passwords for all accounts.

Also, contact all utility companies (including cell phone providers) to notify them of the theft. Implement security measures for these accounts as well. In many cases, they will implement a password that will be necessary for any interactions with the account.

The Federal Trade Commission is also a great resource. They can assist victims of the crime, and help with the resolution of any financial issues that have resulted from identity theft.

Now, this notebook will be full of sensitive information. Keep it under strict lock and key. Sturdy safes with locks are a great option. The safe should also be stored in a secure and inconspicuous location. A built-in safe would be an ideal situation for this circumstance, but that may not be possible. Nonetheless, a locked safe located in an inconspicuous location may be the best course of action for protecting the notebook.

It would be best to maintain these records for five to seven years, depending on state and federal reporting requirements. Once the time has passed and it is safe to assume the issue has been successfully and completely resolved, you should completely destroy the records through the use of a cross-cut shredder or incinerator.

Identify the Leak

First, use the mechanism for discovering the unlawful activity as the first clue to untangling the great web. Was this information discovered in a credit report? Did a credit card company contact you and alert you to suspicious activities? Did the victim uncover the activity in a monthly statement? Consider the source, and start from there to determine the root of the leak.

Once the source has been identified, begin following the trail. If it was identified through a credit report, contact the company listed for the entry. If it was identified through a credit card statement, analyze the first few entries of unauthorized charges. If a bank or credit card company alerted you to suspicious activities, contact the bank or company and ask for more details.

Continue following the trail until it runs cold. In some cases, an errant restaurant employee may have copied the credit card information. In other cases, a skimmer could have been placed on the card reader at the gas pump. Or, perhaps, someone had all your personal information and applied for a line of credit under your name.

Once the trail runs cold, consider what actions you have taken that could have led to that beginning point, and how you can prevent it in the future. It may be as simple as using a credit card in the future, paying in cash, or placing a lock on the mailbox. It may also be a more complicated fix, such as removing all your personal information from all public forums or implementing a security procedure for discarded personal mail.

When uncovering the paper trail, be sure to document all the activities and instances of suspicious activity. You should be able to provide this information to the proper authorities that are investigating the fraudulent activity. Chances are, if the thief is doing this to you, they are doing it to others as well.

By keeping immaculate records, you can aid the police investigation, solidify a case against the thief, preserve evidence that may be useful for recovering lost funds, and uncover information that may be useful to other victims of the same perpetrator.

Again, these records should be stored in a secure location, preferably a locked safe in a secure location. The records should be destroyed once it's determined that the issue has been successfully and completely resolved.

CHAPTER 5: LIABILITY AS THE VICTIM OF IDENTITY THEFT

As the victim of identity theft, you will need to jump through a lot of administrative hoops to get your finances back in order. Fortunately, credit bureaus and financial institutions are well-rehearsed in this crime and willing to help. Nonetheless, it is your responsibility to ensure that all goes well, everything is in order, and all fraudulent activities are reported in a timely manner.

Although you may not have done anything wrong and may not be responsible for the activities of the criminal, you're still responsible for your own finances and must meet certain obligations and requirements if your wish to be reimbursed for the monetary loss.

Know Reporting Timelines

Timelines are incredibly important in identity theft cases. As a consumer of a financial institution, you should be well aware of any reporting timelines for fraud for all your personal accounts regardless of whether or not you are a victim of identity theft. Timelines are important to know and understand because they may determine the reimbursement amount and timeframe. Timelines may also protect you from legal liability that may result from any losses that the financial institution may incur.

Many financial institutions have security protocols in place for identity theft and fraudulent activities. If you fail to report the fraudulent activity within the timelines, the financial institution may adjust your reimbursement and recovery rate. The financial institution may also take an extended period of time to reimburse you if you report the crime after the recommended timeline.

The financial institution may also incur a significant loss based on the theft. Although you may be reimbursed in full, your financial institution may not see reimbursement from the criminal. In this case, the financial institution may seek redress through some other means. If you failed to alert the financial institution to the theft in a timely manner, then you may be subject to a lawsuit filed by the financial institution. Regardless of whether or not you win the suit, you'll need to hire an attorney and the fees will be costly.

Know Reimbursement and Recovery Limits

You should also be aware of their reimbursement and recovery limits. Some financial institutions only reimburse you for a specific number of times in a specific time span. Other institutions may have a set dollar amount.

The policies and procedures for reimbursement and recovery vary greatly between the financial institutions. Some may have clauses that stipulate reimbursement is dependent on reporting within a specified timeframe, and other policies may have more stringent clauses.

Smart consumers will only keep enough money in their accounts that if theft were to occur they would be reimbursed in full. The bottom line is that financial institutions have significant leeway in helping you through this process or hindering you through this process. It is of the utmost importance that you know and understand the stipulations of your policies.

Be Aware of Protocols Regarding Fees that Result From Theft

Financial institutions may also have policies and procedures in place to address fees that result from theft (such as overdraft fees). When theft occurs, you should contact the financial institution and immediately address the issue. You should also immediately inquire about the protocol to ensure that fees are not assessed on the account as a result of the theft.

During this time, it would be advisable to inquire which aspects or damages on the account are your responsibility, and which aspects will be reimbursed (as well as the process for reimbursement).

Credit Card Liability

Federal law limits your liability to $50 in the case of credit card theft. However, if you report the credit card theft prior to it being used by the thief, then you can't be held liable for any unauthorized charges that occurred after you reported it. Credit card companies may provide further reimbursement as a customer benefit .

This brings a warning of a different nature. There are companies or sales people that will try to sell "loss protection" insurance for identity theft, including credit card theft. At times, these salespeople will claim that you are responsible for any charges made by the thief if you do not have loss protection insurance. This is untrue.

ATM and Debit Card Liability

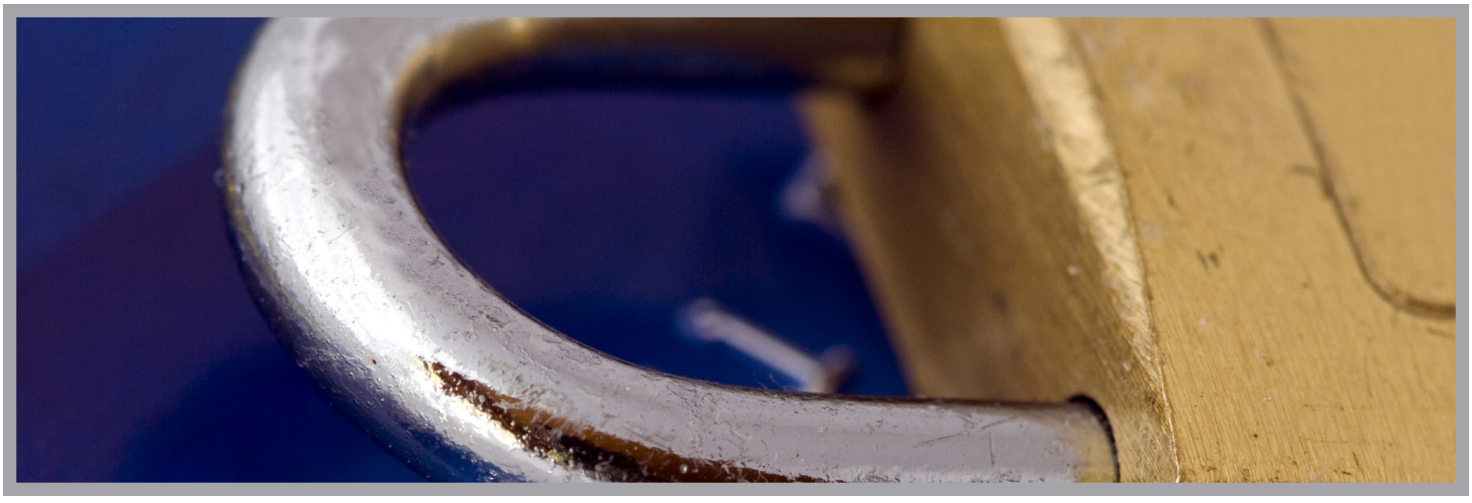
While federal law allows for limited liability for ATM and debit card theft, the liability is vastly different than that of credit card fraud. If you report the loss within the first two business days of discovery, the liability is limited to $50. If the report is made between two and sixty days of discovery, the liability can be up to $500. If the victim waits more than sixty days, you may not be entitled to any reimbursement for lost funds.

Again, some financial institutions may have voluntary reimbursement amounts that are better than the federal law stipulates. Every consumer, regardless of whether or not they are a victim, should be aware of the liability limits that are established by their financial institution.

Check Liability

There is no federal law that limits your liability due to paper check theft, fraud, or abuse. However, the state laws vary. State laws typically hold the financial institution responsible for these types of fraud with certain parameters.

First, financial institutions and state laws typically hold you responsible for managing



your account for unauthorized transactions. The laws also typically expect you to report any suspicious or fraudulent activity at once. If you don't monitor you account and does not immediately report the activity, then you may be held liable for the theft that occurred. Alternatively, the financial institution may be liable, but may also be allowed to file suit against you for not living up to your responsibilities .

Liability Agreements

Financial institutions always provide liability agreements with their cards and services. The liability agreements may be long, technical, and difficult to read. Nonetheless, they are imperative to read and may be the difference between full reimbursement and no reimbursement. If you are having a difficult time understanding the terms of the liability agreement, contact the financial institution directly, and ask to speak to someone that can assist you with understanding the terms.

Today, these liability agreements are typically in an online form. You simply scroll down to the bottom of the agreement, and click "agree." While this may seem like the most convenient and efficient course of action, it may also lead to trouble. If you do not have time to read the agreement, simply print the document, and set it aside until you have a few spare moments. Be sure to read the information as soon as possible, since many of the terms of service may change throughout the year.

CHAPTER 6: TRENDS FOR 2013 AND BEYOND

In the upcoming years, consumer watchdogs expect thieves and hackers to be more creative with their attempts. Electronic health records are ripe for the picking in the upcoming year as technology is infiltrating new sectors of the American economy and consumers are slowly learning how to adapt to changing infrastructures.

In essence, consumers are becoming savvier and cold-calling the elderly is not as profitable as it once was. Today's scam artists are becoming more adept with the various avenues of infiltration and are targeting markets that may not have been targets before.

Debt collection agencies, non-profit organizations, and governmental entities have large amounts of personal data and financial information. Through these sources, thieves can obtain credit card information and begin running up charges before you have any idea that your information has been breached.

While American financial institutions and government officials have made great strides in raising awareness to the crime amongst the citizen population, we should see a major shift as the targets of fraud become less civilian and more infrastructural.

CHECKLISTS FOR YOUR SAFETY

Social Media

Do not post any personal information that could be used to steal your identity.

Consider the fact that anything you post to social media could be used against you.

Do not publish vacation plans or check-ins.

Refrain from publishing information that could lead someone to guess your passwords.

Keep social media pages private for only your most trusted friends and family.

Smart Phones

Do not store passwords or account information on your smart phone.

Consider that technology changes rapidly, and thieves may have advanced devices that could easily capture information on your phone.

Implement security measures that would hinder a person from being able to use your smart phone account to make purchases.

Do not download applications that you do not know for sure to be trustworthy.

Lock your home screen with a password and implement a remote wiping system.

Online Habits

Be aware that your online habits may not be private when surfing public wi-fi.

Do not download or open suspicious emails or links.

Buy and install anti-virus systems with firewall protection.

Use unique and different passwords for all accounts.

Pay attention to the latest trends in online attacks.

Mail Usage and Disposal

Remember that anyone may at any time dig through your garbage and collect your mail.

Purchase a shredder for shredding documents before discarding them.

Consider using a post office box or UPS box for highly sensitive pieces of mail.

Be aware of your billing cycle, and notify the appropriate companies when something is off cycle.

Purchase a lock for your home mail box.

Liabilities

Know the timelines for reporting suspicious activities.

Know the account limits for quick reimbursement and recovery.

Know the terms of service and liability agreement for each account.

When suspicious activity has been indicated, immediately alert the appropriate entities.

Know the legal liabilities as established through federal and state laws.

QUICK RESOURCES FOR CONSUMERS

Federal Trade Commission
Website: www.ftc.gov
Phone: 1-877-ID-THEFT

Credit Bureaus:

Experian
Website: www.experian.com
Phone: 1-888-397-3742

TransUnion
Website: www.transunion.com
Phone: 1-800-680-7289

Equifax
Website: www.equifax.com
Phone: 1-800-685-1111

Credit Card Contact Information

Visa: 1-800-847-2911

Mastercard: 1-800-622-7747

American Express:
1-800-554-2639

Check Verification Companies

CheckRite: 1-800-766-2748

Chex Systems: 1-800-328-5121

CrossCheck: 1-800-552-1900

Equifax-Telecredit:
1-800-437-5120

NPC: 1-800-526-5380

SCAN: 1-800-262-7771

Tele-Check: 1-800-366-2425

For more consumer information, please visit

Identity Theft Resource Center

www.idtheftcenter.org

Bankrate
www.bankrate.com

Privacy Rights Clearing House
www.privacyrights.org

Fight Identity Theft
www.fightidentitytheft.com

United States Department of Justice
www.usdoj.gov

Published by:

Survival Life, LLC

P.O. Box 91074

Austin, Texas 78709

Website: http://www.survivallife.com

Mail: support@survivallife.com