“OH! THAT WOULD NEVER HAPPEN TO ME”

IDENTITY THEFT

DETECTION & PREVENTION

FORENSIC ACCOUNTING CLASS

OWENS COMMUNITY COLLEGE

RONALD W. COON, SR., CPA, DABFA

STUDENTS

Merlinda Baker

Brian Begg

Patrick Brumley

Christine Coutcher

Rana Daniels

Sean Elliott

Stefanie Fox

Joyce Hill

Dawn Nienow

Kristin Rausch

Vickie Rygalski

Nadia Semaili

Scott Whitman

A special thanks goes to the staff at William Vaughn & Co., CPA's for their input and guidance in the preparing of this report.

Table of Contents

DISCLAIMER

Any businesses, trade names, service marks, trademarks, intellectual property, logos, products, services and symbols used in this paper are for ***reference examples only***. Neither this class nor the Instructor, nor the Owens Community College endorses these businesses, trade names, service marks, trademarks, intellectual property, logos, products, services and symbols. The student class also does not represent the preference of one business, trade names, service marks, trademarks, intellectual property, logos, products, services and symbols over another.

Chapter 1

Introduction to Identity Theft

"Oh, that would never happen to me…" These famous last words are spoken by a growing number of individuals per year who are falling susceptible to identity theft in the U.S. You may think you are protected because you take care of your credit cards and do a majority of your business online, however, without an identity theft prevention plan, you are merely falling victim to the "oh, that would never happen to me" fallacy. In fact, did you know that every six seconds someone's identity is stolen? Let's look at a couple of actual stories, even though the names are fictitious to protect them, to help you understand that these things actually happen.

Mary Smith's mother stole her identity by applying for two Capital One credit cards in her name. Her mother charged the maximum amount on both cards. Jane applied for a credit card during this time and was denied. Her mother had let the accounts go delinquent and they were turned over for collections. She pulled her credit report and discovered these fraudulent accounts. She agreed to pay them through the collection agencies because she did not want to press charges on her mother. The collection companies even gave her a discount on the amount that was owed. Mary pulled her credit report some time later and discovered both accounts were not showing paid off. She then called Capital One and learned that this stays with one's credit report for 7 years. Creditors view paying accounts as a person agreeing that they are responsible for the charges. Mary put a fraud alert on her accounts with all three credit reporting agencies.

Vic Tumz was another victim of identity theft. It first started with him not being able to find a job in a field where he should be highly sought after-retail sales. He was constantly rejected and never knew why. He continued to take the issue personally. This man eventually filed for bankruptcy and became homeless. He stayed with friends until he outlived his welcome. He then applied for public assistance and welfare but was turned down because he did not have an address. Eventually he did find a job, but was told he was not needed the day the job was to start. The store told him to contact the Store Protective Association. This was when he found out someone used his identity for their shoplifting crime. His record also showed that he had previously been charged with another shoplifting charge, along with burglary and arson in prior years. Another report showed charges dating back farther of arson, theft, and disturbing the peace. He submitted fingerprints to officials to prove his innocence. Police then gave him a Certificate of Clearance for the crimes. Only this man's wallet was stolen, and he even reported his driver's license, social security card, and military ID stolen. He is still trying to fully clear his name. He now works for his family's business and lives with a friend who helps with his finances.

Ida Braxton's identity was stolen by her own sister. First, she made a court appearance and submitted fingerprints. Police told her this cleared her from the case and she was not guilty. The court appearance was humiliating for the woman. A similar situation occurred when her class was visiting a prison on a trip and had to go through a background check. Her instructor called and informed her she did not pass the background check and could not go on the trip. Her explanation was not sufficient enough. Again, she was humiliated because of her sister's criminal record. Each time her sister was arrested she used Ida's identity. Ida made yet

another court appearance and was again cleared. Ida applied for many jobs and was never hired. Each time she learned of her criminal record, which she believed was cleared. Ida does not want to press identity theft charges on her own sister. She is still unable to secure employment and continues to have her sister's record of a drug addict, prostitute, thief, and more.

The story of Michelle Brown is one of the most amazing stories of identity theft, she had the perfect job as a teacher in Texas, a great loving boyfriend, and finally made her dream come true to buy her own house. However, this lead to the destruction of her perfect credit score and even to the loss of her own personal identity.

Michelle Brown applied for a loan, and would not imagine that her confidential information ended up in the hands of Connie, who was the secretary of the mortgage office, she was a drug addict with critical financial needs, who ended up stealing her credit card number and making purchases online. Is this it? She just bought items online. Unfortunately, Connie started going further and further as time passed by, bought clothes, electronic products, and endless list of many other items. Michelle called the credit card company, wondering the reason why her credit card got declined earlier that day when she tried to use it, and she comes to find out that she already exceeded her limit of $10,000. Of course, she did not make any of those purchases, she called every single agency that would supposedly help her, closed all her credit cards, and problem resolved. But sadly, it is not as easy as it sounds, Connie became obsessed with Michelle, she wanted to look just like her, so she started stalking Michelle, took pictures of her and then took them to a plastic surgeon, and asked him that she wanted her legs to look exactly as in the picture, also Connie changed her color to match Michelle's dark

brown color. Moreover, Connie got a driver's license under the name of Michelle Brown, and decides to buy the same exact car that the actual Michelle owns. How was Connie able to still have access to Michelle's information to make purchases? Easy, she knew Michelle's bank, showed up as "Hello, I'm Michelle Brown, and I do not remember my account numbers". Once all the money is gone, Connie asks her friends for some easy way for money, and ended up transporting drugs, and goes to jail for it, and now the real Michelle Brown is looking in the records as a criminal.

Michelle Brown had to go to every single place, trying to prove that she is the real Michelle Brown, and that she actually did not make those purchases, therefore, she should not be held liable. But still they would not believe her story, "How do we know that you are the real Michelle Brown?"

Finally, Connie gets caught high on drugs, when she makes a call to Michelle asking her for help, policy tracked her call, and she admitted to all the things she did, however, Connie did not think that she hurt Michelle in any way, she said that all she did was to take money from her. Connie took more than just material things from Michelle; she invaded her privacy, life, and made her days so bitter and frustrating. Michelle was left with $50,000 in debt, and she is working on fixing her credit, Connie just got two years in jail. Refer to the letter written by the real Michelle Brown, explaining what a frustrating experience she went through. Michelle's Senatorial testimony appears in the appendix of this paper.

Identity theft can happen to anyone. New York City Mayor Michael Bloomberg was a victim of an attempted identity theft by two thieves. The first attempted to steal $10,000 from Bloomberg's bank account. The second attempted to steal $420,000. Both tried to use forged

checks. It is thought that the two thieves were working together. This was not detected until the second attempt at the theft. Bloomberg was lucky because large checks are held and investigated before being cashed or deposited. The thieves were charged with third-degree grand larceny and first-degree identity theft.

Chapter 2

How Identity Theft Can Happen

As you can see from the true life stories above, the theft of one's identity can be a traumatic, expensive, stressful, and time-consuming experience. You may be thinking, "I'm very careful. Identity theft will never happen to me." However, opportunities can arise multiple times throughout your day for an identity thief to strike. Identity theft occurs when a perpetrator steals your personal identifying information to "take over your credit accounts, open new ones, take out a loan, rent an apartment, access bank accounts, or commit many other crimes using your identity."[1]

Any little bit of information that a thief gathers can be all the information needed to open new credit cards, establish phone or wireless service in your name, open a banking account, take out an auto or home loan, get a driver's license issued with their picture, file for bankruptcy, file fraudulent tax returns, etc. In 2007 "credit card fraud (23%) was the most common form of reported identity theft followed by phone or utilities fraud (18%), employment fraud (14%) and bank fraud (13%). Other significant categories of identity theft reported by victims were government documents/benefits fraud (11%) and loan fraud (5%).[2]"

To have a better understanding of how identities are stolen, the following scenarios are listed as possible avenues an identity thief could take to obtain your personal identifying information.

---

[1] www.equifax.com/credit-information/identity-theft

[2] Federal Trade Commission. "Consumer Fraud and Identity Theft Complaint Data, January-December 2007." 13 Feb 2008. 04 Dec 2008 < http://www.ftc.gov/opa/2008/02/fraud.shtm>

1. A perpetrator could file a change of address in your name with the U.S. Postal Service and have access to your bank statements, mail. etc.
2. Someone could gain access to your social security number by reviewing your driver's license, check, tax returns, etc.
3. A city employee or bystander could search in your garbage for cancelled checks, bank statements or any other important documents in order to obtain confidential information about you
4. Computer savvy individuals could send fraudulent emails promising huge prizes and request that you submit your personal information to be eligible
5. A perpetrator could mail unsolicited checks to you and request that you deposit them in your account, thereby giving the perpetrator access to your banking information and a possible route to withdrawing your funds
6. The thief may call your home and act like they are from your bank or a government agency and request that you provide them with you personal information for identification purposes, giving the thief easy access to your personal identifying information.

As you are able to ascertain from the list above, identity thieves are creative individuals with an almost endless list of tactics to employ in order to gain access to your information, and it is not easy to keep up with what they will do next. Everyday identity thieves come up with different tactics to steal people's identity, and if serious steps to combat their tactics are not taken, the number of victims will increase even more than what we have already seen in the past few years.

How do you know when someone is after your identity? No one can answer that question for sure, but what you can do is to understand how your identity could be stolen and what preventative measures you can take to better protect yourself. Although an identity thief can strike anywhere or at anytime, our research has identified five common areas where

identity theft occurs. Perpetrators can gather your personal information from your home, your workplace, in public, from third parties, and online.

Chapter 2.1 – Identity Theft At Home

Like most consumers, you probably feel your home is one of the least likely places an identity thief could gather your personal identifying information and use it for their benefit. Thoughts such as “who would ever look through my trash” or “my neighborhood is safe, that would never happen here” are the exact reasons some homeowners are careless with their information. Homes are the primary target identity thieves strike.

In order to better protect yourself and your information from theft, it is necessary to understand where your daily habits leave you susceptible to identity theft. How would you answer the following questions?

1. Do you shred your gas, electricity, and phone bills in the garbage?
2. Do you shred your bank, credit card statements, and pre-approved credit offers?
3. Do you keep your tax information in a secure location?
4. Do you forward your mail to your new address upon moving?
5. Do you have your mail held at the post office when out of town?
6. Do you know all the contents of your wallet and would be able to recognize if something was missing?
7. Are your passwords and ATM codes unique and not easily identifiable by merely looking at the contents in your wallet?
8. Are your passwords a combination of letters, numbers and special characters?
9. Do you change your passwords frequently?
10. Are your bills and other important documents out of view of visitors allowed in your home?
11. Do you secure the data located on your computer when it is being serviced?
12. Do you have your hard drive completely erased before you dispose of it?
13. Do you delete email documents from unknown sources?
14. Do you have virus protection installed on your computer?

15. Are the virus definitions on your computer updated automatically and frequently?

If you answered yes to all fifteen you are making a good effort at protecting you identity at home. If you answered no to any of the questions or feel as though your identity theft prevention plan could use some work, take a look at some helpful tips:

1. Remove your mail as soon as it arrives
2. Never put mail in your home mailbox for the mailman to pick up.
3. Always go to the local post office to deposit your mail, not just the corner box as it could be compromised by a thief.
4. DO NOT use an unlocked mail box; make sure it is always locked no matter where you live.
5. DO NOT write your account number on the outside the envelope for any mail.
6. Try to rent a P.O. Box, that way you can keep your home address as private as possible from all the unwanted mailing.
7. Consider deleting your home address from public viewing in the white pages or yellow books online.
8. If going on vacation/or out of town, have mail stopped until you return. Call the United States Postal Service at 1-800-275-8777 or your local post office to have a vacation hold put on your mail. In most cases, the Post Office will have you fill out a card for their records to hold your mail until you return.
9. If going on vacation/or out of town, have your newspaper service stopped or arrange to have it picked up by a friend or neighbor so it is not obvious to a thief that you are not home.
10. Leave a light on when you leave your home and advise neighbors that you will be away. Thieves can steal personal information as well as property.
11. Store all important papers in a safe place. Important papers include items such as insurance policies, deeds to your home, birth certificates and social security cards.
12. File all bills in a safe place before and after you pay them.

13. Anytime you need to dispose of any important documents, such as bank statements, old bills etc., be sure to shred them. Don't just put them in your trash. Thieves may rummage through your garbage to get your personal information.
14. When you receive pre-approved credit card applications by mail, do not throw them away in the trash, shred them. You should also considering opting-out of these types of offers by calling the Federal Trade Commission at 1-888-567-8688. (Do not be alarmed if they ask you for your Social Security Number, since this is necessary to match to their files).
15. Have your name taken off the direct mail lists. An easy way to accomplish this is to write a letter to Direct Marketing Association, Mail Preference Service at PO Box 643 Carmel, NY 10512.
16. Opt out of national telemarketing lists, to reduce unwanted calls from telemarketers, by contacting the Telephone Preference Service, Attention: Dept 9301664, Direct Marketing Association at P.O. Box 282, Carmel, NY 10512.
17. When someone calls to solicit some product or service, never give out any personal information. If you are interested in that product or service, take the party's number and call back, so you can verify the party is who they say they are.
18. Keep your income tax forms and records in a secure place as there is a great deal of information on them and your W-2. If you decide to rid yourself of these documents, be sure to shred them; do not simply throw them away in your garbage bin.
19. If you do not receive your regular bank statement, utility bills, or credit card bills as usual, investigate. Don't wait until later to find out there is a problem that could have been avoided.
20. You should check your credit report at least twice a year due to the fact that more and more identities are being stolen each year and the sooner you catch it, the better your chances you have at stopping the problem before it become debilitating.
21. If you are on the phone with the bank, cell phone provider, and you are prompted to provide some personal information, make sure you are in a private area, and nobody is

around to eavesdrop. The information you provide could be useful to some predator lurking around.

22. If you have credit cards that you have not used in the past six months, you should consider cancelling them. An open credit card is a perfect target for a thief to convert for his/her own benefit.
23. If the option of direct deposit is available to you, use it instead of having pay checks sent to you.
24. Never have new checks mailed to you, pick them up from the bank if you can.
25. If you get an email, letter in the mail or a call from your so called “bank”, asking you for personal data to update your information in the system, this is definitely a SCAM! You should call your bank immediately about this matter as soon as possible.
26. Do not believe in prizes unless they are written and explained in detail on an authenticated document, that way you can read it carefully and take into consideration whether you want to participate or not.

A larger amount of business is being conducted now by using social security numbers as an identifier. Therefore, the following tips are provided so that you can safeguard your social security number from potential identity thieves.

1. Leave your social security card at home. Memorize the number and don’t carry it with you.
2. Store it in a safe place along with your other family member’s cards. Even a child’s Social Security Number can be used for identity theft.
3. Never have your Social Security Number put on your checks or your driver’s license. Do not include it on anything that it doesn’t need to be on.
4. Shred any document with your Social Security Number on it that you no longer need. Always keep any such paperwork in a safe place at home.
5. When giving out your Social Security Number for any reason, be sure to ask the following questions: Why do you need it? How will you use it? What will happen if I

don’t give it to you? How do you plan to safeguard my Social Security Number once you have it? Who will have access to my Social Security Number? If you don’t get good and complete answers to these questions, think again about why you are being asked for it. Maybe it is not something you really want to do, or you need to further investigate the situation.

Chapter 2.2 – Identity Theft at Your Place of Employment

Your place of employment is another place that identity thieves are likely to target. Many workplaces are susceptible to identity theft simply because of the large number of people that pass through the business' doors each day. "Your workspace is vulnerable to the prying eyes and hands of many people, including colleagues, coworkers, temps, service people, contractors, and after-hours employees."[3] People who have the legal right to be at your place of employment, people who you are unfamiliar with and have never met before could potentially be an arms reach away from your personal identifying information. If your personal belongings or personnel file is not secure, you could be vulnerable to having personal information stolen. Consider the following questions when determining if you are properly safeguarding your personal identifying information at work.

1. Do you keep personal information secured at your workplace?
2. Does your workplace shred business documents?
3. Do you deny discussing personal information over the phone to "representatives" from financial institutions while you are at work?
4. When discussing personal information do you limit access to your co-workers?
5. Do you limit the storage of any of your personal data on your computer at work?
6. Is your personal information (Social Security Number, date of birth, etc) secured in the Human Resource department with limited access by your co-workers?

If you answered yes to all six questions listed above, you are making a good effort at protecting you identity at work. However, if your personal security plan at work could use some attention, here are some additional tips:

[3] http://quamut.com

1. Keep all valuables secure at your worksite. Lock up or take your purse, wallet, laptop and other valuables with you if you are leaving your worksite.
2. Lock up personal documents in your desk or file cabinet, out of site of co-workers, or leave them at home.
3. Assume that your work computer is being monitored. Do not use your work computer to access password-protected personal accounts, do your online banking, send emails containing personal information, or store documents containing personal information.
4. Find out about the security policies at your workplace. Who has access to your personnel file? Are the personnel files stored in a secure location?

Chapter 2.3 – Identity Theft Online

There are situations where you do not even need to be present for your personal identifying information to be converted for another person's benefit. With its increased use, the Internet has created many more creative ways identity thieves can steal personal information. Phishing, spyware, fraudulent shopping sites, and wireless snooping are among the ways information can be gathered.

On-Line:

1. Do you decline to place personal information on social networking sites like MySpace or Facebook?
2. When you are asked by your financial institution to update information, do you decline to click on the link provided in the email? (This could be a phishing scam. Phishing uses legitimate company names and facades to solicit personal information from you directly.)
3. Do you check that a website is secure when you use the computer to conduct online banking, bill payment, or online shopping? (Check the website for https//, since this is designed to alert you that the website is secure.)
4. Do you use a secure area on your computer to store financial account numbers and details?
5. Do you have spyware protection on your computer?
6. Do you regularly (at least once a month) run a full spyware check? (Spyware is a software program that collects personal information from your computer without your knowledge or consent.)
7. Do you have passwords on your credit cards, bank and other accounts?
8. Are your passwords a combination of letter, numbers and special characters?
9. Do you change passwords frequently?
10. How secure is the data on your computer when being serviced?
11. Do you have your hard drive completely erased if you are disposing of it?

12. Do you open email documents from unknown sources?
13. Do you have virus protection installed and update the virus definitions automatically?

If you answered yes to the above thirteen questions, you are making a good effort at protecting your information online. However, knowing how identity theft can happen is only half the battle. Knowing how identity thieves gain access to your personally identifying information can aid you in preventing identity theft. Here, we will provide some ways to prevent identity theft online.

Online security is more important to the consumer than ever before, with greater online commercial activity. This means that thieves possibly have more chances at getting privileged information. It is important to take preventative measures when conducting e-commerce, online banking, and other activities that include your personal information. Do not share any kind of information with anybody over the internet. For example: do not post any information on Facebook or MySpace that you would not want a stranger to know. Do NOT give out personally identifying information over instant messaging services (MSN messenger, AOL Instant Messaging); even if you know the person. You never know who could be around to intercept the confidential information intended only to be received by your friend.

When shopping online, it is important to make sure that you are buying from the business you are intending to purchase from. Know how you got to the page where you are submitting your purchase information. Did you get there from a suspect link in an internet search or email you received? These are just a few of the questions that one must ask while conducting business online. Another very important thing to consider while submitting important personal information is whether the website being used starts with “https”, rather

than the standard “http”. This signifies that the internet site is using a secure socket layer, which means that there are security measures in place to help prevent others from seeing your information.

A good practice to help keep your identity safe is to do your online shopping, online banking, and other activities that require personally identifying information online at home on a hard-wired internet connection. This will prevent others from seeing what you send and what is being sent to you. It will also prevent the thief from sending fake web pages to you.

Another good way to help prevent information from being stolen is updating your software, whether it is the platform (e.g. Windows, Apple, and UNIX) that you are using or browsers (e.g. Firefox, Internet Explorer, Safari) that you use. Users can update their computers easily using updates found in the system or software. These updates will fix potential holes within the programs that hackers could use to get personal information.

Using anti-spyware software along with anti-virus software is a must. The anti-spyware software will help prevent people from spying on your internet activities, while the anti-virus software can help prevent virus that pull your personal information from your computer.

It is also important to change passwords on a regular basis, as this provides an extra layer of security to help prevent hackers from hacking into your online accounts. It would also be helpful not to use password reminders, which automatically save your passwords, on those websites that hold your personal information, as this can allow easy access to people who might be around your computer on a regular basis. If you must use these password reminders then it would be equally useful to lock your computer when you are away. Do NOT create PIN numbers or passwords that contain the following: the last six or four digit numbers of your

Social Security try to use a mix of upper and lower case letters, and make sure it will be easy for you and only you to remember. Add an additional pass code to your accounts. For example, every time I call my cell phone provider, in addition to giving them the last four digits of my Social Security, I give them a pass code I made up myself, easy to remember and that nobody could ever figure out.

Chapter 2.4 – Identity Theft in Public

An even less secure area where your personal information is accessible to identity thieves is when you are out in public, either at the grocery store, a high school basketball game, or merely walking down the street. There are a variety of ways that your information could be stolen in public. Wallet and purse theft is probably the one that you automatically think of, however, shoulder surfing and skimming are two other common ways that thieves can gain your information in public. Have you had someone look over your shoulder while at an ATM?

Protecting your identity in public may be harder than you thought. Below are some questions to help identify if you are properly safeguarding your personal identifying information.

1. If you lost your wallet or purse and had it returned, would you look to determine if anything was missing?
2. Do you ensure that your tax professional signed and filled in all appropriate areas required of them on your tax return?
3. Does your tax professional keep copies of your returns and require that your documents are secure?
4. Would you decline to execute a blank tax return for your tax professional?
5. Do you secure your Social Security card in a safe place, not including your wallet?
6. Do you ensure that your SSN is not printed on your checks, insurance card, or driver's license?
7. Do you deposit outgoing mail in secured mailboxes only?
8. Do you decline to confirm personal information over the phone to where others can hear?
9. Do you check to make sure that people around your personal identifying information are not messing with their phone while they are close to you? (Note, they may actually be taking a photograph of your personal information.)

10. Do you ensure that your credit card, driver's license or other personal information are never out of your site?
11. Do you know and trust the person doing your taxes?
12. Is your credit/debit card always within sight when you are paying for purchases? (Note: If someone walks away with your card they may be stealing your card number)

If you answered yes to all twelve questions listed above, you are making a good effort at protecting you identity in public. Below are additional ways to help you combat identity theft in public.

1. Safeguard yourself and your purse or wallet at all times. Always know what is in your purse or wallet so that if stolen, you know what credit card company/companies to call, etc. Avoid carrying sensitive personal information, such as your birth certificate, social security card, checkbook, or passport unless necessary.
2. When leaving the house only take the credit card or debit card you plan on using, and leave any others at home in a safe place.
3. Be sure to sign any credit card as soon as received and also put on it to have another form of ID checked when being used.
4. When you give a sales associate your card, watch what is being done with it and it should be in full sight at all times. Question what that party is doing if anything seems suspicious.
5. Any card that requires a pin number, make sure it is unique, not something such as you or your child's birth date, part of your address, part of your SSN, etc.
6. Never have a pin number written down and in your purse or wallet. Memorize it.
7. Keep all of your receipts from any use of your credit/debit cards, and double check the amounts with your purchases either just after purchase or when you get home.
8. Try to use traveler's checks instead of personal bank checks.

9. Check your monthly statements against all of your receipts also, to make sure there are no duplicate or unauthorized charges. This would apply to your checking account monthly statement also.
10. If using an ATM, be aware of your surroundings and use one you are familiar with. If it is in a public place such as a mall, make sure no one is watching over your shoulder.

.

Chapter 2.5 – Identity Theft via Third Parties

The last arena where thieves can gain access to your information is from third parties. Though you can implement all the precautions outlined in the preceding sections, you could still be at risk of identity theft from a third party. A third party is anyone who has your personal identifying information on file. Third parties include your employer, your tax professional, restaurants or businesses you patronize, your bank or your credit card company.

Perhaps the best way to protect yourself from third party identity theft is to be aware of ways perpetrators can access your information. Perpetrators use many of the same means to gather your information via third parties as they would directly from you. These tactics include:

1. Stealing: Third party theft usually involves stealing records from your employer or other business that has access to your personal information. The thief could be an employee at that business who uses the information gathered to commit fraud themselves or to sell this information to others.
2. Dumpster Diving: While dumpster diving in your personal garbage can be prevented by shredding your personal documents, it can be more difficult to safeguard your information in business refuse. Encourage your employer to enact a policy that all papers with people's private information are shredded before being discarded.
3. Bribing employees who have access to the records: Thieves may pay cash to business employees who have access to or are willing to sell personal information.
4. Hacking into business records: Thieves could gather personal information from unsecured business networks. Educate yourself on your employer's online security policies.
5. Gaining access to your credit report illegally: Obtaining credit reports under false pretenses, such as posing as a lender or potential employer, is another way third party theft can occur.

Stealing, dumpster diving, paying employees for information, accessing business records, and are all ways identity thieves use third parties as ways of gathering information. Third party theft could be theft of business records from your financial institution or workplace. It could be hacking into unsecured networks of businesses. It could even be a thief posing as someone else (a potential employer, lender, etc.) to get your credit report or other records. Protecting yourself from third party identity theft is virtually impossible. However, limiting the number of people and companies who have your personal information and knowing the early warning signs of identity theft are your best protection from third party identity theft.

Chapter 3

Prevention Programs

Taking the previous steps to prevent becoming a victim of identity theft can make it a lot harder for thieves to steal your identity. It can also be a very time consuming, costly and tedious process, and there is still a chance that your identity may be stolen. There are several identity theft protection programs that can be purchased for added security. They are specialists in identity theft prevention and will take action to protect your information. These companies do all the leg work for you in protecting your identity for a small monthly fee. Fees range from $2.00 to $14.99 a month. Some of the most popular and most comprehensive programs are LifeLock, TrustedID and Identity Guard. A comparative matrix of what these services offer is available at the following website: http://www.consumercompare.org/identity_theft_protection_services/compare.php?kw=gcrcid3+identity%20theft&gclid=CP7Eo-aHtJYCFQ0xawodziDALg

Most programs offer special features that protect your identity. Fraud alerts will be set on all three of your credit bureau reports, Experian, Equifax and Trans Union. The fraud alerts will notify you of any suspicious activity or any inquiries on your credit reports. One of the most popular ways a thief steals your information is through pre-approved credit offers that are not properly destroyed. The identity theft protection program will remove your name from any pre-approved credit offer and any junk mail list. They will also order your credit reports once a year and send them to you for your review.

One of the bonus features some of the programs offer is wallet and purse protection. The program will contact your bank, credit card and document issuing companies to have them

cancel your accounts and replace the lost or stolen items. This feature saves the consumer a lot of time and ensures that no accounts or documents go unreported as stolen or lost. You will also be notified if your name is associated with an unknown address. This alerts you if a thief has changed your address to obtain personal and financial information. The protection program can also monitor criminal websites to see if your name is being sold or traded.

Your entire family can become a victim of identity theft. Some protection programs offer extended coverage for children and students. Most minors do not have an active credit file. The program will monitor the child's file to ensure one is not created illegally.

If you are enrolled in one of these programs and your identity is stolen, the company will take action to recover your identity. The average out of pocket expense of identity theft victims range from $400 to $1500 which includes lost wages, travel expenses, legal fees, postage, photocopying, telephone cost and other expenses that may incur. Some programs will reimburse you for these fees and pay lost wages, up to $500 a week. If you need the assistance of an attorney, accountant or any other professional to repair your identity, the cost will be covered by the identity theft program. Keep in mind that you are not legally responsible for paying any fraudulent debt incurred by a thief. Your true cost may be being denied credit, a new job or even being incarcerated because a thief has used your identity for illegal activities. Some protection programs will cover loss up to $2,000,000 to restore your identity.

There are several identity theft protection programs that offer a 30 day free trial period. Research the different products to find out which one is right for you.

Chapter 3.1 - Credit Card Identity Theft Programs

All major credit card companies offer some form of identity theft protection as an added service to owning their credit card. The additional benefit is charged to the card owner on their billing statement. The costs are generally $9.99 - $15.99/month.

The features of credit card identity theft protection programs are pretty universal amongst all the different credit card companies. Benefits/services generally include:

1. Free 30 day trial.
2. Monthly credit score tracking.
3. Monthly credit reports from the three national credit bureaus.
4. Daily monitoring of credit reports with an email alert when changes are detected
5. Toll free access to fraud resolution representatives.
6. Alerts when an activity is detected including when new accounts opened in customer's name, new applications for credit are filed, address changes, public record changes, and potentially negative information on credit files.
7. Card and document registration service in case they become lost or stolen.
8. Identity theft insurance with amounts varying by company. Some companies offer $5,000/occurrence, others offer $25,000/occurrence. Insurance covers legal costs and lost wages associated with restoring the customer's credit. Please note that due to New York state law restrictions, identity theft coverage cannot be offered to residents of New York.

The identity theft protection that is provided by credit card companies can also be provided by other identity theft services at similar costs. These other services offer monitoring credit card related activity as well as monitoring of public records, customer's social security numbers, bank accounts, and medical records.

Chapter 3.2 - Home insurance policies

State farm, Allstate, Geico, Nationwide, American Family, and Progressive homeowner insurance policies have identity theft coverage. All of these companies have the same type of coverage with an average cost of $25.00 year with no deductible and they all cover the following fees:

1. Cost of obtaining credit bureau reports.
2. Fees when reapplying for loans, grants or other credit instruments.
3. Phone, postage, and shipping fees.
4. Notary and filing fees for costs you incur to correct your identity and credit records.
5. Certain legal fees resulting from identity fraud.
6. Up to $1,000 for deductions or service fees from financial institutions and other costs to regain control of your personal identity.
7. Up to $5,000 combined for lost wages and child and elder care expenses.

Some of the companies allow you to access a consumer fraud specialist to help you set up credit reporting and monitoring for a fee. Unfortunately this program is a reimbursement program. So you must have the money to spend to recover your identity before the insurance will reimburse you.

Chapter 4

Combating Identity Theft

Identity theft is a very serious crime, due to the fact that it involves the loss of money as well as the person's identity. Sometimes, we make it easy for the predator to have access to our personal information. We should always keep in mind that we could be the next victim; therefore, it is a must to learn what to do if your identity is taken. Did you know that more than half of identity theft is committed by people you know? Now when we refer to identity theft, we have to look to a large variety of identity theft frauds such as: credit cards fraud, phone or utilities fraud, bank fraud, etc.

In order to be able to prevent yourself from becoming a victim, it is important to know how these thieves commit the crime and be aware for any red flags.

There is an endless list of things that identity thieves do, and honestly it is not easy to keep up with what they will do next. Everyday they come up with new tactics to steal people's identity, and if we do not take serious steps to fight against them, the number of ID theft victims will continue to increase. How could we prevent Identity Theft? This could be easy if we strictly follow every single of the following steps, in order to save ourselves from becoming the next victim?

The attorney general website has a "checklist" of what to do when you first discover that your identity has been stolen. Throughout all of these procedures it is recommended that you hold onto all of your correspondence in order to maintain a record of what you have done. One of the first things to do is report the theft to all three of the major credit reporting

agencies. Contact their fraud departments and have a “fraud alert” placed on your credit report. A fraud alert does not prevent credit cards from being taken out under your identity, but the credit card company will call you to verify that you actually are obtaining a new card since there is an alert in your credit report.

It is also a good idea to get a copy of your credit report so you can see what credit accounts have been attributed to your name without your authorization. With your credit report in hand you can easily identify what creditors you need to contact, and what accounts need to be closed. It is also advised that after clearing up the problems on your credit report that you obtain another credit report a few months later. This second report is to verify that the changes you tried to make have actually happened.

The next step you should take is to file a police report with your local police department or sheriff. Some creditors will want to see proof of the crime actually happening, so by filing a police report you will have that evidence for them. This will make closing your accounts easier, because most creditors like to see proof that the theft did occur.

You should also dispute the bills that arise as a result of your identity being stolen. If this involves disputing charges with a credit card company be sure to write the address for “billing error” disputes and not the bill payment address. Cooperate with them, and your credit rating should not be affected. You should not let yourself be coerced into paying fraudulent bills, and no legal action should be brought against you. If any merchant, financial institution or collection agency suggests otherwise you should report them to government regulators. (where, who, phone numbers address)

If a loan, credit, or utility service was fraudulently opened under your name you can obtain a copy of the application that was filed to acquire the service. This may help you to figure out what information was stolen and used. It could even help catch the thief, because if you know what information was used you should know who has access to it.

It is also a good idea to file a complaint with both the Federal Trade Commission (FTC) and your state's office of the attorney general. The FTC has a form that you can fill out and submit on-line. Most states have on their attorney general websites forms there that can be filled out and submitted on-line. The purpose of registering your complaint is so that the FTC and attorney generals can investigate the case. The more complaints that are filed; the more information that is made available to the people investigating the case, and hopefully with all the information they can catch the thieves.

There is also a way to place a security freeze on your credit report. A security freeze prohibits a credit reporting agency from releasing any information contained in a consumer's credit report without the express permission of the consumer. The consumer must request a security freeze by mailing one to one of the credit reporting agencies. If the consumer is a victim of an identity theft this service is free, but if the consumer is not a victim, the credit reporting agency may charge up to $5.00 to perform such a service.

If the identity theft was perpetrated using a drivers license number then the Bureau of Motor Vehicles in the state your drivers license is issued should be contacted.

Identity theft is a growing problem in our society today. Minimizing the damage is the objective once your identity and/or personally identifying information have been jeopardized or

stolen. It is important to be organized and persistent while trying to stop the person who stole your identity. The following guidelines will help.

1. Keep comprehensive records by comprising a simple matrix to chart your course of action. Pertinent information should include the name of contacted agencies, agencies phone number, and address, date you contacted the agency, contact person, and important comments.
2. Follow-up all phone calls in writing. Use certified mail return receipt requested on all outgoing mail.
3. Maintain copies of all correspondence. Do not send any originals in the mail.

When you realize that your identity has been stolen, you should take these next five steps immediately.

1. Close all credit card accounts, bank accounts, and any other accounts you feel have been compromised. First call the company to alert them of possible theft or theft already perpetrated.
2. Call one of the three consumer reporting companies to set a fraud alert on your credit report. The agency you contact will in turn contact the other two companies with your request.
    - **Equifax:** 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241
    - **Experian:** 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9532, Allen, TX 75013
    - **TransUnion:** 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790
3. Contact all agencies who distribute identification cards. The type of identification involved would be any state or federal identification such as a driver's license or social security card.

4. File a police report. If you have property stolen make an initial report and follow up once fraudulent activity occurs.
5. File a complaint with the Federal Trade Commission. According to the FTC, "By sharing your identity theft complaint with the FTC, you will provide important information that can help law enforcement officials across the nation track down identity thieves and stop them. The FTC can refer victims' complaints to other government agencies and companies for further action, as well as investigate companies for violations of laws the agency enforces. You can file a complaint online at www.ftc.gov/idtheft. If you don't have Internet access, call the FTC's Identity Theft Hotline, toll-free: 1-877-IDTHEFT (438-4338); TTY: 1-866-653- 4261; or write: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Be sure to call the Hotline to update your complaint if you have any additional information or problems."[4]

To identify fraudulent occurrences keep an eye on your credit report, credit/debit card statements, and bank statements. By saving receipts from your card purchases, you will be able to recognize charges you may not have made.

After you complete the recommended immediate steps, you are now ready to handle individual theft occurrences.

[4] www.ftc.gov

Chapter 4.1 - Credit Report

To correct fraudulent information on a credit report, the Fair Credit Reporting Act set up guidelines to follow. The consumer reporting companies and the business providing the information to the consumer reporting company are equally liable in correcting any fraudulent information on the report. The law requires the consumer to involve both companies in the correction process. The Federal Trade Commission has provided a complete guide, which provides assistance in correcting a credit report.

Consumer Reporting Company Obligations

Consumer reporting companies will block fraudulent information from appearing on your credit report if you take the following steps: Send them a copy of an identity theft report and a letter telling them what information is fraudulent. The letter also should state that the information does not relate to any transaction that you made or authorized. In addition, provide proof of your identity that may include your SSN, name, address, and other personal information requested by the consumer reporting company.

The consumer reporting company has four business days to block the fraudulent information after accepting your identity theft report. It also must tell the information provider that it has blocked the information. The consumer reporting company may refuse to block the information or remove the block if, for example, you have not told the truth about your identity theft. If the consumer reporting company removes the block or refuses to place the block, it must let you know.

TABLE 1

Sample Letter for Blocking of Credit Report Information

Date

Your Name

Your Address

Your City, State, Zip Code

Complaint Department

Name of Consumer Reporting Company

Address

City, State, Zip Code

Dear Sir or Madam:

I am a victim of identity theft. I am writing to request that you block the following fraudulent information in my file. This information does not relate to any transaction that I have made. The items also are circled on the attached copy of the report I received. *(Identify item(s) to be blocked, by name of source, such as creditors or tax court, and identify type of item, such as credit account, judgment, etc.)*

Enclosed is a copy of the law enforcement report regarding my identity theft. Please let me know if you need any other information to block this information on my credit report.

Sincerely,

Your name

Enclosures: *(List what you are enclosing.)*

The blocking process is only one way for identity theft victims to deal with fraudulent information. There's also the "reinvestigation process," which was designed to help all

consumers dispute errors or inaccuracies on their credit reports. For more information on this process, see How to Dispute Credit Report Errors and Your Access to Free Credit Reports, two publications from the FTC. [5]

Information Provider Obligations

Information providers stop reporting fraudulent information to the consumer reporting companies once you send them an identity theft report and a letter explaining that the information that they're reporting resulted from identity theft. But you must send your identity theft report and letter to the address specified by the information provider. Note that the information provider may continue to report the information if it later learns that the information is not the result of identity theft.

If a consumer reporting company tells an information provider that it has blocked fraudulent information in your credit report, the information provider may not continue to report that information to the consumer reporting company. The information provider also may not hire someone to collect the debt that relates to the fraudulent account, or sell that debt to anyone else who would try to collect it.

[5] www.ftc.gov

Chapter 4.2 - Credit Cards

Credit card fraud is one of the most common types of theft perpetrated against the consumer. The Fair Credit Billing Act institutes and monitors actions taken for credit card billing error. The consumer is protected and by law is only held liable for $50.00 of unauthorized credit card charges, when you take immediate action. The Federal Trade Commission outlines what must be done to benefit from this law, and provides a sample letter.

1. Write to the creditor at the address given for "billing inquiries," NOT the address for sending your payments. Include your name, address, account number, and a description of the billing error, including the amount and date of the error. See Table Two.
2. Send your letter so that it reaches the creditor within 60 days after the first bill containing the error was mailed to you. If an identity thief changed the address on your account and you didn't receive the bill, your dispute letter still must reach the creditor within 60 days of when the creditor would have mailed the bill. This is one reason it's essential to keep track of your billing statements, and follow up quickly if your bills don't arrive on time.

You should send your letter by certified mail, and request a return receipt. It becomes your proof of the date the creditor received the letter. Include copies (NOT originals) of your police report or other documents that support your position. Keep a copy of your dispute letter. The creditor must acknowledge your complaint in writing within 30 days after receiving it, unless the problem has been resolved. The creditor must resolve the dispute within two billing cycles (but not more than 90 days) after receiving your letter.

For more information, see Fair Credit Billing and Avoiding Credit and Charge Card Fraud, two publications from the FTC at www.ftc.gov.

TABLE 2

Sample Dispute Letter For Existing Accounts

Date

Your Name

Your Address

Your City, State, Zip Code

Your Account Number

Name of Creditor

Billing Inquiries

Address

City, State, Zip Code

Dear Sir or Madam:

I am writing to dispute a fraudulent (charge or debit) on my account in the amount of $_____. I am a victim of identity theft, and I did not make this (charge or debit). I am requesting that the (charge be removed or the debit reinstated), that any finance and other charges related to the fraudulent amount be credited, as well, and that I receive an accurate statement.

Enclosed are copies of (use this sentence to describe any enclosed information, such as a police report) supporting my position. Please investigate this matter and correct the fraudulent (charge or debit) as soon as possible.

Sincerely,

Your name

Enclosures: (List what you are enclosing.)

Chapter 4.3 - Banking Fraud

State laws provide protection when a thief commits fraud with stolen or counterfeit checks with Federal law addressing criminal electronic withdrawals. The Federal Trade Commission offers comprehensive advice to resolve banking fraud.

Fraudulent Electronic Withdrawals

The Electronic Fund Transfer Act provides consumers protection from transactions involving an ATM or debit card, or another electronic way to debit or credit an account. It also limits your liability for unauthorized electronic fund transfers.

You have 60 days from the date your bank account statement is sent to you to report in writing any money withdrawn from your account without your permission. This includes instances when your ATM or debit card is "skimmed" that is, when a thief captures your account number and PIN without your card having been lost or stolen.

If your ATM or debit card is lost or stolen, report it immediately because the amount you can be held responsible for depends on **how quickly** you report the loss. If you report the loss or theft within two business days of discovery, your losses are limited to $50. If you report the loss or theft after two business days, but within 60 days after the unauthorized electronic fund transfer appears on your statement, you could lose up to $500 of what the thief withdraws. If you wait more than 60 days to report the loss or theft, you could lose all the money that was taken from your account after the end of the 60 days. **Note:** VISA and MasterCard voluntarily have agreed to limit consumers' liability for unauthorized use of their debit cards in most instances to $50 per card, no matter how much time has elapsed since the discovery of the loss or theft of the card.

The best way to protect yourself in the event of an error or fraudulent transaction is to call the financial institution and follow up in writing by certified letter, return receipt requested so you can prove when the institution received your letter. Keep a copy of the letter you send for your records.

After receiving your notification about an error on your statement, the institution generally has 10 business days to investigate. The institution must tell you the results of its investigation within three business days after completing it and must correct an error within one business day after determining that it occurred. If the institution needs more time, it may take up to 45 days to complete the investigation but only if the money in dispute is returned to your account and you are notified promptly of the credit. At the end of the investigation, if no error has been found, the institution may take the money back if it sends you a written explanation. For more information, see Electronic Banking and Credit, ATM and Debit Cards: What To Do If They're Lost or Stolen. [6]

Fraudulent Checks and Other "Paper" Transactions

In general, if an identity thief steals your checks or counterfeits checks from your existing bank account, stop payment, close the account, and ask your bank to notify Chex Systems, Inc. or the check verification service with which it does business. That way, retailers can be notified not to accept these checks. While no federal law limits your losses if someone uses your checks with a forged signature, or uses another type of "paper" transaction such as a demand draft, state laws may protect you. Most states hold the bank responsible for losses from such transactions. At the same time, most states require you to take reasonable care of

[6] http://www.ftc.gov/bcp/edu/pubs/consumer/credit/cre07.shtm

your account. For example, you may be held responsible for the forgery if you fail to notify the bank in a timely manner that a check was lost or stolen. Contact your state banking or consumer protection agency for more information.

You can contact major check verification companies directly for the following services: To request that they notify retailers who use their databases not to accept your checks, call: TeleCheck at 1-800-710-9898 or 1-800-927-0188 or Certegy, Inc. (previously Equifax Check Systems) at 1-800-437-5120. To find out if the identity thief has been passing bad checks in your name, call SCAN at 1-800-262-7771

If your checks are rejected by a merchant, it may be because an identity thief is using the Magnetic Information Character Recognition (MICR) code (the numbers at the bottom of checks), your driver's license number, or another identification number. The merchant who rejects your check should give you its check verification company contact information so you can find out what information the thief is using. If you find that the thief is using your MICR code, ask your bank to close your checking account, and open a new one. If you discover that the thief is using your driver's license number or some other identification number, work with your DMV or other identification issuing agency to get new identification with new numbers. Once you have taken the appropriate steps, your checks should be accepted.

Note: The check verification company may or may not remove the information about the MICR code or the driver's license/identification number from its database because this information may help prevent the thief from continuing to commit fraud.

If the checks are being passed on a new account, contact the bank to close the account. Also contact Chex Systems, Inc., to review your consumer report to make sure that no other

bank accounts have been opened in your name. Dispute any bad checks passed in your name with merchants so they don't start any collections actions against you.

Fraudulent New Accounts

If you have trouble opening a new checking account, it may be because an identity thief has been opening accounts in your name. Chex Systems, Inc. produces consumer reports specifically about checking accounts, and as a consumer reporting company, is subject to the Fair Credit Reporting Act. You can request a free copy of your consumer report by contacting Chex Systems, Inc. If you find inaccurate information on your consumer report, follow the procedures under Correcting Credit Reports to dispute it. Contact each of the banks where account inquiries were made, too. This will help ensure that any fraudulently opened accounts are closed.

For help contact Chex Systems, Inc. at 1-800-428-9623; www.chexhelp.com; Fax: 602-659-2197 Chex Systems, Inc. Attn: Consumer Relations, 7805 Hudson Road, Suite 100, Woodbury, MN 55125.

Where to Find Help

If you have trouble getting a financial institution to help you resolve your banking-related identity theft problems, including problems with bank-issued credit cards, contact the agency that oversees your bank (see list below). If you're not sure which of these agencies is the right one, call your bank or visit the National Information Center of the Federal Reserve System at www.ffiec.gov/nic/ and click on "Institution Search."

Chapter 4.4 – Helpful Agencies to Contact if Your Identity is Stolen

Below is a listing of agencies you should consider contacting if your Identity is stolen. Please note that this is not an exhaustive list, and you should contact your local law enforcement agencies for further direction.

Federal Deposit Insurance Corporation

The FDIC (www.fdic.gov) supervises state-chartered banks that are not members of the Federal Reserve System, and insures deposits at banks and savings and loans.
Call the FDIC Consumer Call Center toll-free: 1-800-934-3342; or write: Federal Deposit Insurance Corporation, Division of Compliance and Consumer Affairs, 550 17th Street, NW, Washington, DC 20429. (For more information see FDIC publications Classic Cons... And How to Counter Them, A Crook Has Drained Your Account. Who Pays? , and Your Wallet: A Loser's Manual).

Federal Reserve

The Fed (www.federalreserve.gov) supervises state-chartered banks that are members of the Federal Reserve System. Call: 202-452-3693; or write: Division of Consumer and Community Affairs, Mail Stop 801, Federal Reserve Board, Washington, DC 20551; or contact the Federal Reserve Bank in your area. The Reserve Banks are located in Boston, New York, Philadelphia, Cleveland, Richmond, Atlanta, Chicago, St. Louis, Minneapolis, Kansas City, Dallas, and San Francisco.

National Credit Union Administration (NCUA)

The NCUA (www.ncua.gov) charters and supervises federal credit unions and insures deposits at federal credit unions and many state credit unions.

Call: 703-518-6360; or write: Compliance Officer, National Credit Union Administration, 1775 Duke Street, Alexandria, VA 22314.

Office of the Comptroller of the Currency (OCC)

The OCC (www.occ.treas.gov) charters and supervises national banks. If the word "national" appears in the name of a bank, or the initials "N.A." follow its name, the OCC oversees its operations. Call toll-free: 1-800-613-6743 (business days 9:00 a.m. to 4:00 p.m. CST); fax: 713-336-4301; or write: Customer Assistance Group, 1301 McKinney Street, Suite 3710, Houston, TX 77010. (For more information see OCC publications: Check Fraud: A Guide to Avoiding Losses, How to Avoid Becoming a Victim of Identity Theft, and Identity Theft and Pretext Calling Advisory Letter 2001-4)

Office of Thrift Supervision (OTS)

The OTS (www.ots.treas.gov) is the primary regulator of all federal, and many state-chartered, thrift institutions, including savings banks and savings and loan institutions. Call: 202-906-6000; or write: Office of Thrift Supervision, 1700 G Street, NW, Washington, DC 20552.

The road to identity theft correction can be frustrating but stay diligent and persistent in your fight. The Federal Trade Commission offers other remedies to help the consumer achieve winning results.

WORKS CITED

Author Unknown. “Her Mother Stole Her Identity.” May 2000. 27 Oct 2008. < http://www.privacyrights.org/cases/victim14.htm>

Author Unknown. “I’m Burdened with My Sister’s Criminal Record.” May 1999. 27 Oct 2008. <http://www.privacyrights.org/cases/victim3.htm>

Author Unknown. “The Story of Bronti Kelly” 18 Oct 2008. <http://www,myidfix.com/identity-theft-stories.php>

Carter, Steve. “Indiana Identity Theft Guide” IndianaConsumer. 2008. 15 Oct 2008 <http://www.indianaconsumer.com/ebook-idtheft/index.asp>

Cox, Michael. “Identity Theft Information for Michigan Consumers – 2006 Update.” MichiganGov. Oct 2006. 19 Oct 2008 <http://www.michigan.gov/ag/0,1607,7-164-34739_20942-80479--,00.html>

Equifax. 2008. 10 Oct 2008 <www.equifax.com/credit-information/identity-theft/>.

Federal Trade Commission. “Consumer Fraud and Identity Theft Complaint Data, January-December 2007.” 13 Feb 2008. 04 Dec 2008 < http://www.ftc.gov/opa/2008/02/fraud.shtm>

Federal Trade Commission. 2005. 10 Oct 2008 <http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.shtm>

Federal Trade Commission. 2008. 12 Oct 2008 <http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/deter.html>

Identity Theft Resource Center. 2008. 1 Oct 2008 <www.idtheftcenter.org/>

Identity Theft Resources Center. “Fact Sheet 101 – ID Theft Test.” IDTheftCenter. Aug 2005. 11 Oct 2008 <http://www.idtheftcenter.org/artman2/publish/c_theft_test/ID_Theft_Test.shtml>

Identity Theft Resources Center. “Fact Sheet 104 My Wallet or PDA was Lost or Stolen.” IDTheftCenter. Feb 2008. 11 Oct 2008 <www.idtheftcenter.org/artman2/publish/v_fact_sheets/Fact_Sheet_104.shtml>

Identity Theft Resources Center. “Fact Sheet 118 PC Perfect – information Safety Quiz.” IDTheftCenter. Feb 2007. 11 Oct 2008 <www.idtheftcenter.org/artman2/publish/c_theft_test/Fact_Sheet_118_PC_Perfect_-_information_Safety_Quiz>

Indiana Consumer. 2007. 6 Oct 2008 <http://www.indianaconsumer.com/idtheft/victim_kit.asp>

McQuillan, Alice. “Bloomberg Victim of ID Theft.” WNBC. 2 Oct 2007. 18 Oct 2008. <http://www.wnbc.com/news/14254295/detail.html>

Partner, Malaney J. “Tips for Choosing a Tax Preparer.” Internal Revenue Service. 4 Oct 2008. <www.irs.gov/individuals/article/0,,id=133088,00>

Pennsylvania Office of Attorney General. 2008. 17 Oct 2008 <http://www.attorneygeneral.gov/idtheft>

Quamut. 2008. 6 Oct 2008 <www.quamut.com>

Stein, Julie. “How Your Identity Can Be Stolen.” Quamut. 29 Sept 2008 <www.quamut.com/quamut/preventing_identity_theft/>

Stop ID Fraud. 2008. 14 Oct 2008 <www.stop-idfraud.co.uk/index.htm>

West Virginia Attorney General’s Office. 2008. 9 Oct 2008 <http://www.wvago.gov/identitytheft.cfm>

Wikipedia. 13 Feb 2008. 1 Oct 2008 <en.wikipedia.org/wiki/Shoulder_surfing_(computer_security)>

APPENDIX:

Instructions for Completing

The ID Theft Affidavit

To make certain that you do not become responsible for any debts incurred by an identity thief, you must prove to each of the companies where accounts were opened in your name that you didn't create the debt. The ID Theft Affidavit was developed by a group of credit grantors, consumer advocates, and attorneys at the Federal Trade Commission (FTC) for this purpose. Importantly, this affidavit is only for use where a new account was opened in your name. If someone made unauthorized charges to an existing account, call the company for instructions.

While many companies accept this affidavit, others require that you submit more or different forms. Before you send the affidavit, contact each company to find out if they accept it. If they do not accept the ID Theft Affidavit, ask them what information and/or documentation they require.

You may not need the ID Theft Affidavit to absolve you of debt resulting from identity theft if you obtain an Identity Theft Report. We suggest you consider obtaining an Identity Theft Report where a new account was opened in your name. An Identity Theft Report can be used to (1) permanently block fraudulent information from appearing on your credit report; (2) ensure that debts do not reappear on your credit reports; (3) prevent a company from continuing to collect debts or selling the debt to others for collection; and (4) obtain an extended fraud alert.

The ID Theft Affidavit may be required by a company in order for you to obtain applications or other transaction records related to the theft of your identity. These records may help you prove that you are a victim. For example, you may be able to show that the signature on an application is not yours. These documents also may contain information about the identity thief that is valuable to law enforcement.

This affidavit has two parts:

- Part one — the ID Theft Affidavit — is where you report general information about yourself and the theft.
- Part two — the Fraudulent Account Statement — is where you describe the fraudulent account(s) opened in your name. Use a separate Fraudulent Account Statement for each company you need to write to.

When you send the affidavit to the companies, attach copies (NOT originals) of any supporting documents (for example, driver's license or police report). Before submitting your affidavit, review the disputed account(s) with family members or friends who may have information about the account(s) or access to them.

Complete this affidavit as soon as possible. Many creditors ask that you send it within two weeks. Delays on your part could slow the investigation.

Be as accurate and complete as possible. You may choose not to provide some of the information requested. However, incorrect or incomplete information will slow the process of investigating your claim and absolving the debt. Print clearly.

When you have finished completing the affidavit, mail a copy to each creditor, bank, or company that provided the thief with the unauthorized credit, goods, or services you describe. Attach a copy of the Fraudulent Account Statement with information only on accounts opened at the institution to which you are sending the packet, as well as any other supporting documentation you are able to provide.

Send the appropriate documents to each company by certified mail, return receipt requested, so you can prove that it was received. The companies will review your claim and send you a written response telling you the outcome of their investigation. Keep a copy of everything you submit.

If you are unable to complete the affidavit, a legal guardian or someone with power of attorney may complete it for you. Except as noted, the information you provide will be used only by the company to process your affidavit, investigate the events you report, and help stop further fraud. If this affidavit is requested in a lawsuit, the company might have to provide it to the requesting party. Completing this affidavit does not guarantee that the identity thief will be prosecuted or that the debt will be cleared.

If you haven't already done so, report the fraud to the following organizations:

1. Any one of the nationwide consumer reporting companies to place a fraud alert on your credit report. Fraud alerts can help prevent an identity thief from opening any more accounts in your name. The company you call is required to contact the other two, which will place an alert on their versions of your report, too.
   - Equifax: 1-800-525-6285; www.equifax.com
   - Experian: 1-888-EXPERIAN (397-3742); www.experian.com
   - TransUnion: 1-800-680-7289; www.transunion.com

   In addition, once you have placed a fraud alert, you're entitled to order one free credit report from each of the three consumer reporting companies, and, if you ask, they will display only the last four digits of your Social Security number on your credit reports.

2. The security or fraud department of each company where you know, or believe, accounts have been tampered with or opened fraudulently. Close the accounts. Follow up in writing, and include copies (NOT originals) of supporting documents. It's important to notify credit card companies and banks in writing. Send your letters by certified mail, return receipt requested, so you can document what the company received and when. Keep a file of your correspondence and enclosures.

   When you open new accounts, use new Personal Identification Numbers (PINs) and passwords. Avoid using easily available information like your mother's maiden name, your birth date, and the last four digits of your Social Security number, your phone number, or a series of consecutive numbers.

3. Your local police or the police in the community where the identity theft took place. Provide a copy of your ID Theft Complaint filed with the FTC (see below), to be incorporated into the police report. Get a copy of the police report or, at the very least, the number of the report. It can help you deal with creditors who need proof of the crime. If the police are reluctant to take your report, ask to file a "Miscellaneous Incidents" report, or try another jurisdiction, like your state police. You also can check with your state Attorney General's office to find out if state law requires the police to take reports for identity theft. Check the Blue Pages of your telephone directory for the phone number or check www.naag.org for a list of state Attorneys General.

4. The Federal Trade Commission. By sharing your identity theft complaint with the FTC, you will provide important information that can help law enforcement officials across the nation track down identity thieves and stop them. The FTC also can refer victims' complaints to other government agencies and companies for further action, as well as investigate companies for violations of laws that the FTC enforces.

You can file a complaint online at www.consumer.gov/idtheft. If you don't have Internet access, call the FTC's Identity Theft Hotline, toll-free: 1-877-IDTHEFT (438-4338); TTY: 1-866-653-4261; or write: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580. When you file an ID Theft Complaint with the FTC online, you will be given the option to print a copy of your ID Theft Complaint. You should bring a copy of the printed ID Theft Complaint with you to the police to be incorporated into your police report. The ID Theft Complaint, in conjunction with the police report, can create an Identity Theft Report that will help you recover more quickly. The ID Theft Complaint provides the supporting details necessary for an Identity Theft Report, which go beyond the details of a typical police report.

DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER GOVERNMENTAGENCY

Victim Information

(1.) My full legal name is _____
(First) (Middle) (Last) (Jr., Sr., III)

(2.) (If different from above) When the events described in this affidavit took place, I was known as_____
(First) (Middle) (Last) (Jr., Sr., III)

(3.) My date of birth is _____ (day/month/year)

(4.) My Social Security number is_____

(5.) My driver's license or identification card state and number are_____

(6.) My current address is _____

City _____

State _____ Zip Code _____

(7.) I have lived at this address since _____ (month/year)

(8.) (If different from above) When the events described in this affidavit took place, my address was_____

City _____

State _____ Zip Code _____

(9.) I lived at the address in Item 8 from _____(month/year) until _____(month/year)

(10.) My daytime telephone number is (_____)_____

My evening telephone number is (_____) _____

DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER GOVERNMENTAGENCY

How the Fraud Occurred

Check all that apply for items 11 - 17:

(11.) □ I did not authorize anyone to use my name or personal information to seek the money, credit, loans, goods or services described in this report.

(12.) □ I did not receive any benefit, money, goods or services as a result of the events described in this report.

(13.) □ My identification documents (for example, credit cards; birth certificate; driver's license; Social Security card; etc.) were stolen/lost on or about _____. (day/month/year)

(14.) □ To the best of my knowledge and belief, the following person(s) used my information(for example, my name, address, date of birth, existing account numbers, Social Security number, mother's maiden name, etc.) or identification documents to get money, credit, loans, goods or services without my knowledge or authorization:

_____ Name (if known)
_____ Address (if known)
_____ Phone number(s) (if known)
_____ Additional information (if known)
_____ Name (if known)
_____ Address (if known)
_____ Phone number(s) (if known)
_____ Additional information (if known)

(15.) □ I do NOT know who used my information or identification documents to get money, credit, loans, goods or services without my knowledge or authorization.

(16.) □ Additional comments: (For example, description of the fraud, which documents or information was used or how the identity thief gained access to your information.)

_____
_____
_____
_____
_____
_____

(Attach additional pages as necessary.)

Victim's Law Enforcement Actions

(17.) (check one) I □ am □ am not willing to assist in the prosecution of the person(s) who committed this fraud.

(18.) (check one) I □ am □ am not authorizing the release of this information to law enforcement for the purpose of assisting them in the investigation and prosecution of the person(s) who committed this fraud.

DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER GOVERNMENTAGENCY

(19.) **(**check all that apply) I □ have □ have not reported the events described in this affidavit to the police or other law enforcement agency. The police □ did □ did not write a report. In the event you have contacted the police or other law enforcement agency, please complete the following:

_____(Agency #1)

_____(Date of report) (Report number, if any)_____

_____(Phone number)

(Email address, if any)_____

_____ (Agency #2)

_____ (Date of report) (Report number, if any)

_____ (Phone number) (email address, if any)

Documentation Checklist Please indicate the supporting documentation you are able to provide to the companies you plan to notify. Attach copies (NOT originals) to the affidavit before sending it to the companies

(20.) A copy of a valid government-issued photo-identification card (for example, your driver's license, state-issued ID card or your passport). If you are under 16 and don't have a photo-ID, you may submit a copy of your birth certificate or a copy of your official school records showing your enrollment and place of residence.

(21.) Proof of residency during the time the disputed bill occurred, the loan was made or the other event took place (for example, a rental/lease agreement in your name, a copy of a utility bill or a copy of an insurance bill).(Officer/Agency personnel taking report)(Officer/Agency personnel taking report)

DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER GOVERNMENTAGENCY

(22.) A copy of the report you filed with the police or sheriff's department. If you are unable to obtain a report or report number from the police, please indicate that in Item 19. Some companies only need the report number, not a copy of the report. You may want to check with each company.

Signature_____ date signed _____(Notary)

[Check with each company. Creditors sometimes require notarization. If they do not, please have one witness (non-relative) sign below that you completed and signed this affidavit.]

Witness:_____(signature)(printed name)

_____(date)(telephone number) certify that, to the best of my knowledge and belief, all the information on and attached to this affidavit is true, correct, and complete and made in good faith. I also understand that this affidavit or the information it contains may be made available to federal, state, and/or local law enforcement agencies for such action within their jurisdiction as they deem appropriate. I understand that knowingly making any false or fraudulent statement or representation to the government may constitute a violation of 18 U.S.C. §1001 or other federal, state, or local criminal statutes, and may result in imposition of a fine or imprisonment or both.

DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER GOVERNMENTAGENCY

I declare (check all that apply): As a result of the event(s) described in the ID Theft Affidavit, the following account(s) was/were opened at your company in my name without my knowledge, permission or authorization using my personal information or identifying documents:

Fraudulent Account Statement

Creditor Name/Address (the company that opened the account or provided the goods or services) Account Number Type of unauthorized credit/goods/services provided by creditor (if known) Date issued or opened (if known) Amount/Value provided (the amount charged or the cost of the goods/services) During the time of the accounts described above, I had the following account open with your company:

Billing name _____

Billing address_____

Account number _____

Example: National Bank22 Main Street Columbus, Ohio 2272201234567-89 auto loan 01/05/2002 $25,500.00

• Make as many copies of this page as you need. Complete a separate page for each company you're notifying and only send it to that company. Include a copy of your signed affidavit.

• List only the account(s) you're disputing with the company receiving this form. See the example below.

• If a collection agency sent you a statement, letter or notice about the fraudulent account, attach a copy of that document (NOT the original).Completing this Statement

DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER GOVERNMENTAGENCY

Identity Theft Victim Stories:
Verbal Testimony by Michelle Brown

Posted: July 2000

U.S. Senate Committee Hearing on the Judiciary Subcommittee on Technology, Terrorism and Government Information -- "Identity Theft: How to Protect and Restore Your Good Name"
July 12, 2000

Senator Jon Kyl, Chairman
Senator Dianne Feinstein

Verbal Testimony by Michelle Brown

“Mr. Chairman and Members of the Committee,

I am pleased to be in your presence today and I genuinely thank you for the opportunity to elevate the invasive crime known as identity theft. This is a topic that I am unfortunately, intimately familiar with.

My name is Michelle Brown. I am 29 years old and have been working in the disciplined field of international banking for the last 7 years. I am an ambitious and hard-working individual; I'm certain that I am much like any of your cousins, your nieces, your daughters. I believe that I strongly represent any average, respectable citizen of the United States. However, there is one clear-cut issue that separates me from nearly the rest of the population: I have lived and breathed the nightmare of identity theft. I will tell you first-hand, this is a devastation beyond any outsiders' comprehension, a nearly unbearable burden that no one should ever have to suffer.

Imagine establishing credit at age 17, and building a perfect credit profile over the next 11 years. Imagine working consistently since age 15, helping to finance your education at an accredited University to advance your future success in life. Imagine never having been in trouble with the law. Imagine the violation you would internalize as you realize some vile individual you have never met nor wronged, has taken everything you have built-up from scratch to grossly use and abuse your good name and unblemished credit profile.

That's precisely what happened to me. I discovered this new blackened reality on January 12, 1999, when a Bank of America representative called me inquiring about the first payment on a brand new truck, which had been purchased just the previous month. I immediately placed fraud alerts on my credit reports, cancelled all credit cards, and even placed a fraud alert on my Driver's License number. From that day forward, I unearthed the trail of this menace's impersonation and attempted to work with the current faulty system to protect myself from any further abuse. **The system clearly failed me.**

To summarize, over a year and a half from January 1998 through July 1999, one individual impersonated me to procure over $50,000 in goods and services. Not only did she damage my credit, but she escalated her

crimes to a level that I never truly expected: she engaged in drug trafficking. The crime resulted in my erroneous arrest record, a warrant out for my arrest, and eventually, a prison record when she was booked under my name as an inmate in the Chicago Federal Prison.

The impersonation began with the perpetrator's theft of my rental application from my landlord's property management office in January 1998. Immediately, the perpetrator set up cellular service, followed by residential telephone and other utility services, attempted to obtain timeshare financing and department store credit cards, purchased a $32,000 truck, had nearly $5,000 worth of liposuction performed to her body, and even rented properties in my name including signing a year lease. Not only did this person defraud the Department of Motor Vehicles in obtaining a duplicate drivers' license (with my name and number) in October 1998, but she even presented herself as me with this identification to the DEA and before a federal judge when she was caught trafficking 3,000 pounds of marijuana in May 1999.

She remained a fugitive for almost 6 months while still assuming my name-- and was finally turned in by an acquaintance in July 1999.

Months later - in September 1999 - I was stopped at LAX's Customs after returning from a vacation in Mexico (after she was already in prison). While I explained my innocence to several agents in a stream of tears, and as I attempted to clearly distinguish this Michelle Brown from the "other Michelle Brown" with a criminal record, I was blatantly treated with strong suspicion. I was, as is typical for an identity fraud victim, guilty until proven innocent. I was finally let go after an hour, after the police were called to vouch for me. This situation reinforced my fear that I may be wrongly identified as the criminal, which could end up with my arrest, or worse yet, being taken into custody to serve time in jail. After having seen so many inefficiencies and blatant errors in the system, I feel no assurance nor can I receive any concrete evidence from authorities that this type of insane mix-up would **never happen again**.

It was tormenting to know someone was in essence living the good life at my expense, and I was left in the dust with the taxing chore of proving my innocence. The restoration of my credit and my good name was a seemingly never-ending process. I was forced to make literally thousands of phone calls, fill out various forms, submit all sorts of documents, and have many documents notarized. Without a doubt, I was entirely consumed with the whole painstaking process. I gained nothing from putting over 500 hours into the chore of restoration; all in all, it was an exhausting waste of a good person's time and a massive drain on my life and energy. At one point, I even feared my safety after I learned that the perpetrator had previously been linked with a convicted murderer. The whole identity fraud experience was, by far, the darkest, most challenging and terrifying chapter of my life.

I faced many difficulties in clearing my name, and I still face the fear that I will forever be linked with the perpetrator's criminal record. I have encountered widespread inefficiency and general insensitivity at nearly every turn, and know that there are most definitely not enough dedicated resources and governmental authorities to assist victims and to simplify the burden on the innocent's life.

Clearly changes need to be made. The Government not only needs to promote initiatives to shorten and simplify restoration of one's name and credit, but also to facilitate early detection and termination of an abused name, and most importantly, to deter criminals from the lure of such an easy crime by enforcing swift and severe punishment.

I think that Senator Feinstein's Identity Theft Prevention Act of 2000 is definitely a positive initiative and will put the legislation in the right direction to fight this crime. I support the two corresponding bills and recommend the enforcement of such initiatives.

I came here today because I feel responsible to limit the abuse of other innocent's names and their lives. I

know how terribly tormenting it is to be a victim. I am living proof that identity theft is a very real crime, with very real victims, and true life-altering consequences. It's astounding that my life-long discipline to be a law abiding citizen, and to have the diligence to establish perfect credit, was reversed so easily, so quickly, simply because I represent the perfect victim in a criminal's eyes. This crime is clearly on the rise, and no one at this time is completely protected from becoming the next victim.

I realize the scenario of becoming an identity fraud victim seems entirely far-fetched and implausible to many of you. I know the feeling. I was once in your shoes**.**

I thank you for your time and for the opportunity to present my story and views today. I hope it is clear now that many changes need to effect to the current system to combat this crime and protect victims. This fact is crystal clear in my mind.

Thank you.

Michelle Brown “