IDENTITY THEFT:

ASSESSING RISK AND PROTECTION AGAINST IT

FORENSIC ACCOUNTING

INSTRUCTOR: RONALD W. COON, SR., CPA, DABFA

SALIHA KHAWAJA

ASHLEY DOWNING

TIM NEWTON

JOSEPH SWANSON

TABLE OF CONTENTS

INTRODUCTION

Picture this scenario: You have spent the last few years building up your credit and saving enough money to buy a house. You go to the bank and apply for a mortgage loan. The bank denies you because of your credit rating. You are confused and frustrated. You log on to one of the credit reporting websites to find out what happened. You look through and realize that there are multiple accounts open in your name that you were not aware of. You have just been the victim of identity theft.

Identity theft occurs when someone uses your personal information without your permission and knowledge to commit fraud or other crimes. Most times, the victims of identity fraud do not even realize they are victims. They only realize when they need money and a good credit rating to get a loan. According to the Identity Theft Survey Report conducted by the Federal Trade Commission in 2003, in total, 12.7% of the survey participants indicated their personal information had been misused from the previous five years. Misuses of information include fraudulent new credit card accounts, taking out new loans, fraud with checking or savings accounts, or when renting an apartment (FTC Identity Theft Survey Report, 4).

It is true that identity theft is on the rise and sometimes you just do not know if you are a victim. Now, it is easier than ever to steal a person's identity because of the advancement of computers and public access to personal data. However, knowledge and awareness can be the key to help prevent such a crime. The federal government and numerous states have passed laws prohibiting identity theft. They are making sure that social security numbers are less accessible by strengthening our processes for issuing new social security number and replacement social security cards. The federal government is also working with other federal and state agencies to find ways to detect and prevent identity theft.

It is our intent to inform the public of the risks involved in our daily lives because of the various behaviors that occur when purchasing items at a store to even how we send our mail. Many people do not realize how easy it can be for a person to steal mail from your mailbox, or obtain your social security number right over the phone, using deceptive techniques. There are certain behavior patterns that can lead to negligence concerning our personal information. We have formed a questionnaire to outline a good portion of those behavior patterns that may lead to some form of exposure to identity theft. This questionnaire deals with social security numbers, online risks, credit card fraud, mail fraud and other types of fraud.

We have listed below a quiz of 25 questions with point values assigned on each answer to the respective questions. The objective here is to add up all of the points and then compare your score to the table following the quiz. We have also presented rationale for most of the questions and answers on this quiz and pointing out the strengths and weaknesses of each response. These patterns address your strengths and weaknesses of your behavior that will either protect you or encourage your identity to be used by someone else.

This quiz will not solve all of the Identity theft cases, though it will make you more educated on how to prevent and protect your identity from being stolen. As mentioned earlier, identity thieves will stop at nothing to secure someone else's identity. No matter how careful you are, your identity still could be stolen from secure places, such as banks, credit card agencies, etc. by someone that was placed in trust of the information and decided to use it illegally.

IDENTITY THEFT RISK QUESTIONNAIRE

Social Security Number:

1. Does your Social Security number appear on any of the following? (Check all that apply).

    a. Checks
    b. Driver's License
    c. Insurance cards
    d. Other forms of ID
    e. None of the above

2. When asked to give out your Social Security number, you:

    a. Never reveal the Social Security number to anyone.
    b. Ask the reason and use for it.
    c. Only reveal the last four digits of the Social Security number.
    d. Give it out freely.

3. Do you keep your Social Security number in your wallet/purse?

    a. Yes.
    b. Yes, but only when it is needed.
    c. No.

4. When documents that have your Social Security number on them are no longer useful to you,

    a. I shred them with a crosscut shredder.
    b. I shred them with a strip shredder.
    c. Burn them.
    d. Tear them up and throw them away.

5. How are your tax returns stored?

    a. In a safe or a locked compartment.
    b. In a file marked "Tax Returns".
    c. Lying around somewhere at home.
    d. I do not worry about this because I do not file taxes.

Online Risks:

6. Do you update on a regular basis:

    a. Operating Systems.
    b. Web Browser.
    c. Firewalls.
    d. Anti-virus software.

7. Do you download software:

    a. From any site.
    b. Sites you know and trust.
    c. I do not download free software.

8. When I receive a pop-up message:

    a. I close the pop-up message immediately.
    b. I respond to those that interest me.
    c. I respond to them all.

9. When giving out personal information (SS#, credit card number, bank account number):

    a. I do not give out my personal information over the Internet.
    b. I log onto sites that I have previously visited and know are secure.
    c. I give out this information regardless of the site.

10. On the one-time offers that are “too good to be true”:

    a. Yes, they are too good to be true, but there must be a catch.
    b. Yes, this is a once in a lifetime offer.

11. When you shop online:

    a. I do not shop online.
    b. I go to sites that I have had success with in the past.
    c. I shop at any site.

12. When I go to a new site to shop:

    a. I do not shop online.
    b. I check for any safety and security policies before I shop.
    c. I shop at any site.

13. When paying for merchandise:

a. I do not shop online.
b. I use a money order
c. I pay by credit card
d. I pay by an online check
e. I pay by check.

Credit Card Fraud:

14. How many debit and/or credit cards do you carry in your wallet or purse?

a. All the cards I own.
b. Only a select few that I know I will need.
c. I do not have a debit and/or credit card.

15. Is the pin number on your debit and/or credit card:

a. Part of my social security number.
b. Part of my date of birth.
c. Part of my address.
d. Some other number that can be identified in wallet or purse.
e. A completely unrelated number.
f. I do not have a debit and/or credit card.

16. When you receive your debit and/or credit card, do you:

a. Sign the back of the card immediately.
b. Make reference to secondary form of ID.
c. Leave it blank.
d. I do not have a debit and/or credit card

17. When you use your debit and/or credit card to make purchases:

a. I keep all necessary receipts safely and securely.
b. I know where my card is throughout the transaction.
c. I verify the amount of the transaction.
d. I do not have a debit and/or credit card.

18. When using the ATM:

a. I use the first one available.
b. I have certain machines I would trust and use.
c. I do not have a debit and/or credit card.

19. On your debit and/or credit card statements:

a. I make the necessary payments.
b. Quickly review the statement and make the necessary payments.
c. Reconcile the receipts against the charges on the statement and make the necessary payments.
d. I do not have a debit and/or credit card.

Mail:

20. How do you receive your mail?

a. In my mailbox.
b. In a locked location.
c. In a P.O. Box.

21. How do you send mail?

a. In my mailbox.
b. Drop them off in a mailbox.
c. Drop them off at the post office.

22. When receiving a Pre-Approved credit card application, do you:

a. Fill it out and hope for the best.
b. Throw it away as junk mail.
c. Tear it up and throw it away.
d. Shred it.

23. If you do not receive your bank statement, credit card statement on a regular basis, do you:

a. Wait until the next statement arrives.
b. Wait until the next statement arrives and reconcile both of them.
c. Investigate the reason for the non-receipt of the statement.

Other:

24. Do you review your credit report?

a. At least once a year.
b. At least once every two to three years.
c. When it becomes necessary.
d. I have not reviewed it yet.

25. While on vacation or away for an extended period of time, do you:

a. Have mail put on hold at the post office
b. Have someone trustworthy watch over the homestead.
c. Stop the delivery of newspapers.

ANSWER POINT VALUES

1. a. 4 b. 3 c. 2 d. 2 e. 0
2. a. 0 b. 1 c. 2 d. 5
3. a. 3 b. 1 c. 0
4. a. 0 b. 2 c. 2 d. 4
5. a. 0 b. 2 c. 2 d. 2
6. a. Y=0 N=1 b. Y=0 N=1 c. Y=0 N=2 d. Y=0 N=4
7. a. 4 b. 2 c. 0
8. a. 0 b. 3 c. 4
9. a. 0 b. 2 c. 5
10. a. 0 b. 5
11. a. 0 b. 2 c. 5
12. a. 0 b. 2 c. 5
13. a. 0 b. 1 c. 2 d. 3 e. 4
14. a. 3 b. 2 c. 0
15. a. Y=3 N=0 b Y=2 N=0 c. Y= 2 N=0 d. Y=1 N=0 e. Y=1 N=0 f. 0
16. a. 2 b. 2 c. 3 d. 0
17. a. Y=0 N=2 b. Y=0 N=2 c. Y=0 N=1 d. 0
18. a. 3 b. 1 c. 0
19. a. 3 b. 2 c. 1 d. 0
20. a. 3 b. 2 c. 0
21. a. 3 b. 2 c. 0
22. a. 3 b. 3 c. 2 d. 1
23. a. 4 b. 3 c. 1
24. a. 1 b. 2 c. 3 d. 4
25. a. Y=0 N=3 b. Y=1 N=3 c. Y=0 N=4

Your Total_____pts.

See the chart on next page to see how your behavior patterns affect your risk to identity theft.

RISK RATING SCOREBOARD

0-30	31-60
If you are in this range then you are doing a good job at protecting your identity. There still is always a chance at something happening but you have the least amount of risk involved. After taking the questionnaire you will be able to do little things that you may have never thought of before to reduce your risk even further.	If you fall into this tier you are heading in the right direction. If your score was in the thirties you are doing a good job and with a few adjustments to your behavior you could get into the first tier. If your score is in the fifties you are not doing bad, you are doing some things right. Although a few more changes should improve your risk factor.
61-89	**90 +**
Being in this tier is not that hopeless, unless your risk score was in the eighties. You will need to improve certain behavior patterns to protect your identity. By taking this questionnaire you should be aware of your vulnerabilities that can lead to your identity to be abused. Looking at the area in which your score is high will give you an idea as to what changes to your behavior should be made.	If you fall into this tier you have to change your lifestyle when it comes to how you protect your identity. With a score this high you are a walking target so to say. You should go back through this questionnaire and see what changes in your lifestyles you would have to make in order to have a lower risk.

RATIONALE AND EXPLANATION FOR IDENTITY THEFT QUESTIONNAIRE

Social Security Numbers:

1. The most common type of fraud is the theft of a wallet or purse. Normally, it contains the person's driver's license, checks, insurance card, and other forms of identification. Many times, a person has his/her social security number appearing on any one of these items. There is a growing trend to eliminate the social security number from different forms of identification.
   - (a) Checks are rated very risky at (4) with a social security number because it has all the information needed for identity theft. It also has the bank account number.
   - (b) Driver's license is rated highly risky at (3) because it has the name, address, and sometimes a social security number.
   - (c) Insurance cards sometimes have the social security number on them, but not all thieves know that. This is why insurance cards are at an elevated risk of (2).
   - (d) There are other forms of identifications that may have the social security number on them, which also make it risky. This has an elevated risk of (2).

2. It is a very smart idea to never give out a social security number to anyone, unless it is for a legitimate reason. If you are asked for a social security number, get a phone number to call them back before you reveal it.
   - (a) If a social security number is never revealed, it has no risk (0).
   - (b) Even when a person asks the reason and the use of the social security number, there is still a small risk involved. The reason for this is because the individual asking for it might have the wrong intentions. This has a minimal risk involved at (1).
   - (c) Sometimes the last four digits of the social security number are used for confirmation. However, that does not mean that the person asking for it will be misrepresenting the use for it. So there is an elevated risk involved at (2).
   - (d) Many times people do not realize the risk of revealing their social security number freely to others. It is very risky behavior, thus, it is rated (5).

3. The social security number should be kept in a safe place at all times. Keeping it in a wallet or purse is a very risky behavior because of the uncertainty of theft at any time.
   - (a) Keeping it in wallet or purse at all times is highly risky and is rated at (3)
   - (b) Carrying the social security card only when needed is less risky, however there is always the possibility of it getting stolen or lost. So it is rated at (1).

4. It is a good practice to either keep documents that have the social security number on them in a safe place or dispose of them properly.
   - (a) Shredding such documents with a cross cut shredder has no element of risk (0) because trying to put together such pieces would be nearly impossible.
   - (b) Using a strip shredder has an elevated risk at (2) because some thieves might take the time to put together such pieces.
   - (c) Burning is a good way to dispose of documents, but it still has an elevated risk at (2) because, many times, the ashes leave imprints.

- (d) Tearing up such documents is very risky behavior at (4) because a thief can easily put together torn pieces.

5. Tax returns should always be stored in a safe place.
   - (a) Storing returns in a safe or locked compartment has no element of risk involved (0).
   - (b) A file marked "tax returns" is a giveaway to the social security number, and so it has an elevated risk rating of (2).
   - (c) Having tax returns lying around somewhere in the house has an elevated risk of (2).
   - (d) There could be some W2 forms or other tax related form lying around that could have the social security number on it. Additionally, not filing for taxes could be a criminal offense and could put you at odds with the Internal Revenue Service. Thus, it has an elevated risk of (2).

Online Risks:

6. Sometimes not updating certain software or anti-virus controls on the computer can lead to identity theft.
   - (a) Operating system is the least risky at (1), but it is still important to keep it up to date because an older system is more susceptible to viruses and hackers.
   - (b) Keeping a Web browser up-to-date is also necessary because it gives some anti-virus protection as well as pop-up blockers. Thus it is also rated at (1)
   - (c) Firewalls are very important to the safety of the material on the computer. It prevents certain sites to corrupt the computer and keeps hackers out, which makes the firewall the first line of defense. Not updating a firewall carries an elevated risk at (2).
   - (d) Anti-virus software is very beneficial when downloading materials from different sites. Updating is very important, otherwise, risk of viruses infecting the computer can become very high at (4).

7. Downloading software from the Internet is not always safe.
   - (a) Downloading from any site, is very risky at (4) because not every site on the Internet is trustworthy.
   - (b) Sites that you know and trust is mildly risky at (2) because there is always a remote chance that the site has been corrupted since the last time it was visited.
   - (c) Not downloading software from the Internet has no risk or (0).

8. Pop-up messages can be very dangerous because they deal with phishing for information from the computer. In most cases the messages have attached files or viruses, like Trojan horses, that are loaded into your computer when the message is opened.
   - (a) This is one of the safest behaviors because these pop-up messages are closed right away (0).
   - (b) Responding to the pop-up messages that are of interest can still be highly risky at (3) because you never know if these ads contain one of those files.
   - (c) Responding to all of the pop-up messages is very risky at (4) because they can be an open invitation for identify theft or corrupt your computer in more ways than one.

9. Giving out personal information over the Internet is not always safe because you may never know who is on the other end receiving this vital information.
   - (a) If personal information is never given on the Internet, then there is no risk involved (0).
   - (b) Using sites that you have used before is safer, however, there is always a chance that the site has been corrupted since it was last visited. This gives it an elevated risk of (2).
   - (c) Using any site is very risky at (5) because not every site is safe and secure. It would be wise, if you are visiting a new site, check to see if the site has a security endorsement.

10. Sometimes there could be once in a lifetime offers that sound "too good to be true."
   - (a) If it is understood that there must be catch to these types of offers, and nothing was done, then there is no risk involved (0).
   - (b) If it is believed that it is a once in a lifetime offer, then one could find himself involved in various types of Internet scams and this constitutes as highly risky behavior (5).

11. Shopping online is growing to be one of the latest trends and it can be convenient, but risky.
   - (a) If you do not shop online at all, then there is no risk (0).
   - (b) If you shop at sites you have been to before is a good practice, however, there is always a chance that the site is not secure, so it carries an elevated risk of (2).
   - (c) Shopping at any site, regardless of the security features of that site, is very risky behavior (5).

12. When you shop at a new site online do you
   - (a) If you do not shop online at all, then there is no risk (0).
   - (b) Do a bit of research on the website you are using and read up on their safety and security policies before you place an order. By doing this, you lower your risk factor at (2) than if you shop at just any site.
   - (c) Use any site that you find and put your risk factor very high at (5) because you are not being careful at what you are doing. A little investigation goes a long way.

13. Buying merchandise online is risky because personal data is being submitted.
   - (a) By not shopping online, there is no risk here (0), however see other questions for in-store risks.
   - (b) Sending in a money order for Internet purchases poses very little risk at (1), but some sites may still require sending in payment before shipment which means that you may be taking a chance on not receiving the goods purchased.
   - (c) Using a credit card carries some risk (2), depending on that site's security features. Larger and more popular sites tend to be more secure, but they are also more targeted by hackers. You also have other remedies available when using a credit card.
   - (d) Submitting checking account information is highly risky at (3) than a credit card because there are no extra security features on checking accounts like the security code on credit cards. One can also use stolen checking account information from the Internet and print his/her own checks.

- (e) Paying by check is also highly risky at (4), because you taking a chance of the check going through the mail.

Credit Card Fraud:

14. Carrying lots of credit and/or debit cards can pose a real threat in the case of a theft.
    - (a) Carrying multiple credit cards in the wallet or purse can be dangerous if they were to be stolen. The cards have the possibility of getting run to the limits, before the victim is able to report it. This makes it highly risky at (3).
    - (b) Having just one or two cards minimizes the loss involved if the wallet or purse is stolen, so there is an elevated risk involved at (2).
    - (c) There is no risk here (0), as there are no credit cards involved.

15. Most debit and/or credit cards have security features like pin numbers. However, if the pin numbers can be identified with certain items in a wallet/purse, then this poses a great threat.
    - (a) Using part of the social security number is highly risky at (3), because if a thief has stolen credit card or bank information, they may already have the social security number or could be working on acquiring it.
    - (b) Birthdays are not coveted as much as social security numbers, however there are still risky to use, since they can be discovered, thus, it carries an elevated risk at (2).
    - (c) Addresses may not be that hard to find out, but a thief will usually try other numbers first, before resorting to the address. This carries an elevated risk at (2).
    - (d) There is always a possibility that a thief can figure out the pin number for a credit/debit card from the contents of a stolen wallet/purse as a last resort. This still carries an elevated risk of (2).
    - (e) Using an unrelated number carries little risk because a stolen card will be harder to use and it gives the victim more time to call the credit card company or bank to cancel the card. However, there is still always a chance that such a number can be found out, thus, it carries a risk rate of (1) because the thief still has a 1 in 10,000 chance of getting it right.
    - (f) There is no risk here (0), as there are no credit cards involved.

16.
    - (a) Signing the back of your credit/debit card leaves no chance for the thief to sign it, but does allow a thief to try to match your signature. This has an elevated risk of (2).
    - (b) Many people make reference to another form of identification such as a picture ID on the back of the card, but, unfortunately, many cashiers do not even check for this. Past studies reveal that there is a 1 in 7 chance of this happening. Thus, it is rated at (2)
    - (c) Leaving it blank allows a thief to sign your signature anyway they want, creating an easy match. This is highly risky at (3)
    - (d) There is no risk involved here (0), as there is no credit card.

17. Keeping a record of transactions and knowing where a card is during transactions will lower the risk of identity theft.
    - (a) Keeping all receipts safe and secure allows for accurate record keeping, and little risk of someone getting a credit card number off the receipt. If the answer was NO, it carries an elevated risk rate of (2).

- (b) If a card is out of sight during a transaction, someone could be writing down the number or making an imprint so they can use it in the future. Knowing where the card is at all times minimizes the risk. If the answer was NO, it carries an elevated risk rate of (2).
- (c) By not verifying the amount of the transaction, a cashier may have overcharged for something not received, or they may have kept or stolen a product for themselves. This is why it is so important to verify the amount of the transaction. If the answer was NO, the risk involved is (2).
- (d) There is no risk here (0), as there is no credit card.

18. Even some ATMs carry risks for fraudulent activity.
    - (a) Using an unfamiliar ATM is highly risky (3) because it is unknown which one could possibly be fraudulent. There are products that thieves temporarily install on an ATM that can visually observe or digitally record transactions that could obtain card and pin numbers.
    - (b) Using a trusted ATM, such as the one at the bank, minimizes the risk of information being stolen. However, there is always the chance that someone may have tampered with it, which gives it a minimal risk rate of (1).
    - (c) There is no risk here (0), as there is no debit card involved.

19. Sometimes not going over a debit and/or credit card statement poses a risk for identity theft.
    - (a) Just making the necessary payments on the debit or credit card without looking at the statement is a very huge risk. The assumption is that the person looks at what is due and pays the amount. This is highly risky at (3) because there may be items on the statement that were not purchased by the user.
    - (b) Quickly reviewing the statement carries an elevated risk at (2) because not everything on the statement may be correct.
    - (c) Reconciling receipts and making the necessary payments carries a minimal risk at (1) because there is always mail fraud and the remote chance of information being duplicated.
    - (d) There is no risk here (0), as there is no debit card involved.

Mail:

20.
    - (a) Receiving mail in a mailbox is highly risky (3) because someone could steal it out of the mailbox. Sometimes it is possible that dishonest employees would not deliver the mail, and instead, open it themselves.
    - (b) Receiving mail in a locked location has an elevated risk (2) because there is always that dishonest person.
    - (c) Receiving mail in a P.O. Box carries no risk at (0), however, there is still a remote chance of improprieties during the delivery process.

21.

- (a) When placing outgoing mail in the mailbox that just gives a person a chance to steal the mail out of the box and get personal information. This is highly risky at (3)
- (b) Dropping mail off in a mailbox still carries an elevated risk (2) because someone could break into the mailbox.
- (c) Dropping mail off at the post office carries no risk of (0), however, there is still a remote chance of improprieties during the delivery process.

22. Almost everybody has received a pre-approved application in the mail.

- (a) Filling out Pre-Approved credit card applications is highly risky (3) because of the uncertainty of scams.
- (b) Throwing away a pre-approved application is also highly risky (3) because someone could go through the garbage, fill it out and send it in the victim's name.
- (c) Tearing up a pre-Approved credit card application has an elevated risk of (2) because someone can go through the garbage and get all the personal information.
- (d) Shredding such mail carries a minimal risk (1) because some thieves would go through the trouble and put together such pieces.

23. It is very important to receive statements on a timely basis because of the sensitivity of the information involved.

- (a) Waiting until the next month's statement to arrive and reconciling both at the same time is highly risky at (3) because someone could have utilized your account that you may be unaware of.
- (b) Waiting until the next statement arrives is very risky at (4) because you would not be able to reconcile the statement to ensure that your balance matches the statement balance.
- (c) Investigating the reason of non-receipt of the statement is a proactive approach to find out why you have not received the statement. However, it still has a minimal risk at (1) because someone may have gotten a hold of your account information.

Other:

24. It is recommended to review your credit report at least once a year, but if you notice symptoms of identity theft, it is a good idea to review it sooner.

- (a) Reviewing your credit report once a year is recommended, but sometimes symptoms of identity theft can appear sooner. Therefore, there is a minimal risk of (1).
- (b) Reviewing the credit report at least once every two to three years is not very proactive because in the meantime, someone could have taken out thousands of dollars in your name. This carries an elevated risk rate of (2).
- (c) Only reviewing the credit report when it becomes necessary could mean that someone has done a lot of damage to your credit, could put a hold on the your life to overcome it. Therefore, there is a high risk of (3).
- (d) Not reviewing your credit report at all is a very risky at (4) because you are the aware of the activity that has transpired over a period of time. When it comes time to buy a house or get a loan, it would become increasingly difficult because the activity was not monitored and/or corrected on the credit report.

25. There will be some point in time when you will have to leave your residence for an extended period time, such as for vacation or an emergency.

- (a) Having mail put on hold has no element of risk, however, if the answer was NO, then it carries a risk of (3).
- (b) Having someone you trust watching the homestead still carries a risk because you may not be aware of what company the trusted individual may bring. They could confiscate some important documents that could lead to identity theft. If the answer was YES, it carries a minimal risk of (1), and if the answer was NO, then it is highly risky (3)
- (c) If you put a hold on the delivery of newspapers, it gives the homestead a "lived-in" look. Therefore, there is no risk involved. However, if the answer was NO, then it is very risky behavior at (4) and you are inviting trouble.

.

CONCLUSION:

Identity theft is a serious crime and can leave its victims outraged and frustrated. The key is that when you begin to see any indication of identity theft, you must act quickly. Often times, you will have to put your life on hold to overcome it. Once found out, you need to take the proper steps to resolve it. Ignoring the problem or delaying action by even days can result in disaster. Victims of identity theft know how frustrating it can be and how time consuming it is to untangle that sort of mess. It takes some victims almost 10 years to completely rid of all the bad credit that was accumulated. It takes a toll not only on the victim, but the family as well.

It is better to be aware of all of the ways someone could possibly steal your personal information, than to have it happen and wonder how or why. When you become a victim of identity theft whom do you turn to and what do you do? Following is some information to help you recover from identity theft. There are also some prevention tips that may help you stay one step ahead of identity theft. Remember that knowledge and awareness is the key to stop identity theft in the beginning.

RECOVERY TIPS

If you believe that you have been a victim of identity theft, there are four steps that need to be completed. These can be completed in any order. However, all of these need to be done as soon as possible to set a timetable, and, ultimately, to prevent any further problems. You should keep a log of all conversations, mailings, and meetings that have to do with your identity theft recovery. This is in case you will need to reference them in the future.

1. Contact your local law enforcement. You will need to file a police report. Try to bring as much information as you can when filing, including any letters from creditors and possible fraudulent statements to verify your case. You may also need to complete an ID theft affidavit before coming, which was developed by the Federal Trade Commission This form will formally list all known fraudulent accounts. This affidavit may also be required by any of the companies involved.

Ohio has also implemented the PASSPORT program for ID theft victims. This program issues a special card to ID theft victims, which can be used to confirm their identity when necessary. Local law enforcement will contact all other state authorities by placing the victim in the computer, which may help prevent future crimes from occurring.

2. Contact the credit bureaus. You will need to put a fraud alert on your credit report. This will monitor activity on your report and let you know when someone uses your identity. However, this may not prevent any crimes, because the person may have all your information and may pass through any extra verification procedures. Some states allow for a credit freeze, which stops any company from using your credit report, and that way no one can open accounts in your name. This can be effective in large cases, but it may take time to unfreeze, and it may become increasingly difficult to obtain credit for a while.

You are only required to contact one credit bureau; that one will then contact the other two. However, you may want to contact all three to be on the safe side. You should request a credit report and look it over to make sure you document all fraudulent activity. Once a fraud alert is on your credit report, you are entitled by law to receive a free report. It is always a good idea to follow up and verify that the alert has been placed on the remaining two bureaus.

3. **Close any fraudulent accounts**. Contact all of your current creditors by telephone and in writing to notify them of your circumstances. Ask them if they will accept the ID affidavit, if not ask them for their form. See if you can close your accounts, or possibly change account numbers. Review all your recent statements to make sure you have documented all fraudulent activity. Please see the prevention tips on how to keep track of your creditor's information so you will have it when you need it.

4. **File a complaint with the Federal Trade Commission (FTC).** This is important as your case now becomes a federal case and the FTC may contact authorities in and out of your state regarding your case. You can do this by calling the FTC at 800-ID-THEFT (800-438-4338), or fill out the form at www.consumer.gov/idtheft.

Here is a list of Credit Bureaus you will need to contact:

CREDIT BUREAU	TO REPORT CONSUMER FRAUD
Equifax Credit Information Services PO Box 7402741 Atlanta GA 30374-0241 www.equifax.com	Call 800-525-6285 and write to Equifax
Experian PO Box 2002 Allen, TX 75013 www.experian.com	Call 888-397-3742
TransUnion P.O. Box 2000 Chester, PA 19022 www.transunion.com	Call 800-680-7289 and write to Fraud Victim Asst. Dept P.O. Box 6790 Fullerton, CA 92834-6790

PROTECTING YOURSELF AGAINST ID THEFT

- Be careful about the information you give out over the phone or on the Internet unless you are *sure* you know whom you are dealing with. If someone calls you, do not assume they are who they say they are. Insist on calling back on a number you know is legitimate.

- Remember that Web sites can be faked. What may look like a legitimate online storefront or contest may simply be a scam to trick you into revealing personal information.

- Take a good hard look at what you are carrying around in your wallet or purse. Carry only the identification information and the number of credit and debit cards that you will actually need. Leave your Social Security card – and anything that bears that number – in a secure place. Your medical insurance card may have your social security number. Make a copy of the card, black out the number on the copy, and carry the copy.

- Make a photocopy of the front and back of everything in your wallet or purse. Put the copy in a safe place so you will have the account numbers and contact numbers in the event you need to cancel credit cards.

- Do not have your SSN or DL# printed on your checks.

- Make sure checks (used and unused), credit cards, bank records, and other personal information is carefully secured in your home or office, particularly if other people, whether workers or roommates, will be around.

- Guard your mail. If your mailbox is left unattended during the day while you are not at home, consider installing a locked mailbox, a mail slot, or using a Post Office Box.

- Hold onto your purse, your wallet, and your checkbook. Do not leave them unattended. If you discover a checkbook, credit card, or personal information missing, take appropriate action to notify your financial institutions.

- If your deposit account information ends up in the hands of the wrong party, consider closing your account and opening a new one with a new account number.

- Shred documents with sensitive/confidential information before throwing them away.

- Secure your trash. Be careful what you throw away. Statements from your doctor, checks on closed accounts, expired charge cards or IDs are treasures to thieves. . Dumpster divers can piece together little bits of information to get what they need to steal your identity.

- If you do not use pre-screened offers for credit, opt out of receiving them. Call 1-888-5-OPTOUT

- Talk to the financial institutions and brokerage firms where you have accounts about placing passwords on them.

- Choose passwords for online financial services wisely. Avoid anything easily guessed or learned via research, such as mother's maiden name, kids' names, and pets' names.

- Take your receipt with you when you leave the ATM.

- Ask about information security and data storage procedures of the companies you do business with, including your doctor's office, dentist's office, and anywhere else that has your Social Security number.

- Give your SSN only when absolutely necessary.

- Know your billing and statement cycles. If something is late, find out why.

- Check your banking, brokerage, and credit card statements immediately after receipt in order to spot bogus charges.

- Cancel all unused credit accounts.

- Be wary of promotional scams, "You are a winner" letters, and requests for help from strangers in foreign countries who promise you riches.

- Be sure that you receive your check orders in a timely manner.

- Obtain a copy of your credit report once a year and take action if there is information about transactions or accounts you did not initiate.

REFERENCES

Federal Trade Commission: Identity Theft Survey Report. http://www.ftc.gov/os/2003/09/synovatereport.pdf. September 2003.