MITIGATING IDENTITY THEFT

By

Colin Reid

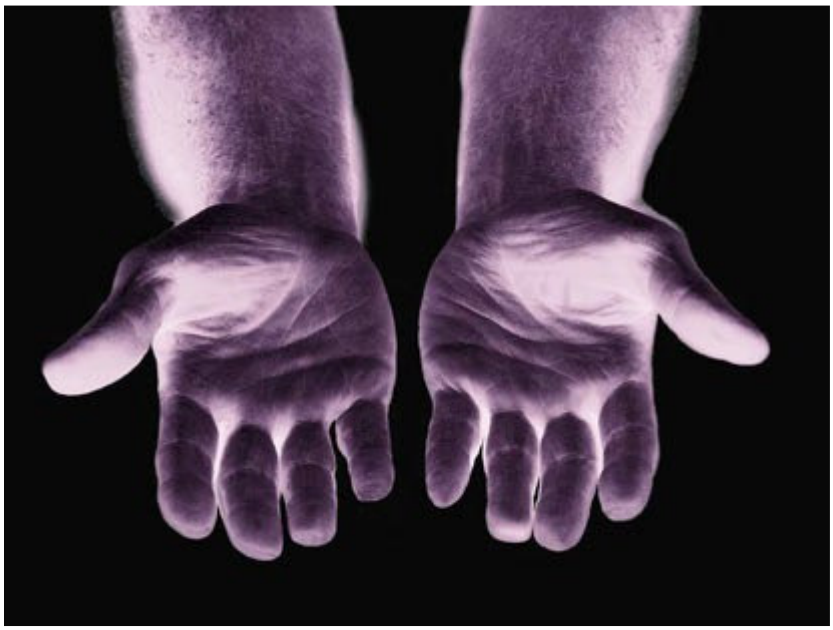


Figure 1. “No Fingerprints” Image provided by ABC News “Medical Mystery”

(This page intentionally left blank.)

INTRODUCTION

According to the FBI, the largest identity theft case started with a dishonest "insider" who worked for an agency that created software to manage credit backgrounds and had access to an infinite supply of personal consumer information. Thirty thousand victims in the United States and Canada and millions of dollars in identity theft losses made this incident the largest identity theft case ever investigated. It is also a dramatic example of the potential of the possibility of becoming a victim of identity theft for all of us consumers.

The crime started with the "insider" Philip Cummings. Phillip worked in Long Island NY as a help desk employee for a company, which provided software for clients. The software was designed for banks and other financial institutions to download consumer credit reports from the three major credit reporting agencies: Equifax, Trans Union, and Experian. Cummings could download just about any consumer credit report he wanted because he had access to the client lists with all of the passwords and codes. He eventually sold these credit reports to a ring of Nigerian criminals. He continued this arrangement for two years after leaving the company due to his vast inside knowledge. Thousands of savings accounts were drained. Credit cards were charged to the limit. New ATM, credit and checks were mailed to the thieves directly.

The FBI combined with help from the Secret Service and the U.S. Post Office got involved when one of the major credit card companies realized that thousands of credit reports were downloaded without anyone's knowledge. Other companies began reporting similar occurrences. The common denominator was phone records that linked Cummings's company. Cummings eventually took a guilty plea. His accomplices' trials are coming up.

Identity theft is becoming a major crime on a global scale. Complaints have grown for seven years in a row according to the Federal Trade Commission. (1) With the few clicks of a mouse, an offender can take your identity from across the world, causing great loss and making it extremely difficulty to repair your good name. A victim will spend on average thirty hours trying to recover from identity theft. (2)

Identity theft covers a wide range of available mechanisms for an offender to steal your information. In modern society, we rely very heavily on technology to help simplify our lives to meet the demand for efficiency. We use credit cards, I-Pass, Lo-jacks, GPS Systems, cellular technology, wireless internet and so on. We use these items to conveniently get though a checkout or a tollbooth without having to fish out money, and receive change. They reduce the need for human intervention, which allows businesses to spend more on advertising and less on

staffing. You now will not have to rely on a bank teller to receive deposits, and manage your finances.

Technology allows us to do a lot from a laptop from the convenience of our homes. These are conveniences, which the public wants to utilize because they can buy us more *time*. That, after all, is what we want - more time to get to the next task at hand. Perhaps they give us more time for our families, or to pursue our interests, or to enhance our income. But there also can be a price associated with these liberties and these conveniences.

There is a certain amount of personal information which is associated with the different conveniences. There has to be some way of ensuring that the person utilizing the service is who they say they are and that the proper party is responsible for the cost or the utilization of the convenience. This information comes in the forms of account numbers, social security numbers, birthdays, maiden names, pass words, encrypted codes, and keys and so on. Once this information gets into the wrong hands, an outside party can become you. They can reap the benefits of almost all you are entitled to, which can be very costly and difficult to rectify.

In this paper, I will show though multiple examples and scenarios that your best protection for safeguarding yourself from becoming a victim of identity theft is common sense. It is rather easy to protect yourself from having your identity stolen. The objective of this paper is to show you how. The following information will be broken down into different methods or types of identity theft and some common sense solutions, which, if followed, will reduce the vulnerability to having your identity stolen. While we will explore some common sense practical strategies to prevent your identity from being stolen, we will also learn what to do to provide minimum loss and recovery in the event your identity has already been stolen.

TYPES OF IDENTITY THEFT

There are numerous ways an identity thief can obtain your information. We will cover each of the different categories of techniques, which will be further broken down into more specific examples.

The different methods of identity theft crimes we will focus on are a direct or physical intervention and electronic. Electronic will be explored more in depth because these crimes cover a range of creative ways via the computer to access your information.

The first and probably the easiest type of identity theft would be a physical identity attack. To understand this type of theft, let's profile an offender.

These thieves have a positive opportunist philosophy, which enables them to seize a vulnerable moment when a person lets their guard down if even for a moment. These attacks are based solely on the victim predator interaction. Understand that the offenders in these types of thefts are getting through life by looking for the opportunity to take advantage of a situation or an unsuspecting person. Crimes which, fall under this category usually occurred when there was an opportunity given to an offender, allowing an offender to utilize some vulnerability. Some common ways a thief might try to steal your information include:

- Taking your purse or wallet.

- Taking your mail. Mail is an easy target as the United States Post office reports they deliver to 146 million homes and businesses a six days a week. (3)

- Diverting your mail through the post office.

- Telephone social engineering attacks.

This is where common sense plays a key role in avoiding becoming a victim. Here are several common sense safeguards to keep in mind to protect your personal information:

- Never leave your wallet or purse unattended. For example, don't leave it in a shopping cart.

- Try to reduce the amount of information you need to carry in your purse or wallet to only what you need to carry.

- Don't sign your credit cards as soon as you receive them. A much better idea is to write: "See photo ID" using a black permanent marker. Although realistically a store clerk will not even look at your signature (although they should), and internet purchases only require an electronic signature, it is common sense to add a little more security for the few times the signature is actually checked. (4)

- Beware if someone asks to swipe your card for you. Devices called "skimmers' are one way of a counterperson to copy the information on the magnetic strip. (5)

- Check your credit card statements for any fraudulent purchases. Report anything wrong immediately to the credit company's fraud or loss prevention department.

- Do not print unnecessary information like social security numbers on your checks.

- Do not print your driver's license number on your checks because the will force a clerk to ask for a physical license.

- Don't carry your birth certificate.

- Don't carry your social security card. An identity thief considers your social security card a most sought after piece of information. (6) The social security number is used to open other fraudulent accounts.

- Avoid carrying your health insurance card when your patient ID number is typically your social security number.

- Pick up your mail on a regular basis. If your mail is constantly containing too much personal information, a P.O. Box will help to secure the information. It is not uncommon to divert your mail simply by using a change of address form at the post office.

- Mail your bills directly. Don't leave them on your porch for the mail carrier to pick up.

- If you store you personal documents or account statements at home, use a secure place of a locked cabinet.

- Invest in a shredder and use it.

- Memorize pins; don't write them down.

- Never give your personal information to anyone on the phone unless you know exactly with whom you are speaking, especially if you did not make the call.

- Watch for shoulder surfers at the ATM. Also beware of an ATM machine that acts dysfunctional. In some cases, a couple of paperclips can prevent your card from being returned from the machine, allowing a thief to recover your ATM card later after you leave.

- Request free copies of your credit reports from all three credit bureaus. (We will cover this later.)

- Secure a photo copy of both sides of your credit cards and passport so that in the event these articles are stolen you will be able to call of the necessary phone numbers to immediately cancel those items. (7)

- Stay informed with up-to-date available information on avoiding having your identity stolen. The thieves are constantly seeking out new and creative ways to steal your information, so it is common sense to stay on top of them.

ELECTRONIC IDENTITY THEFT

We've covered how an offender might physically get your personal information. With a little awareness and common sense you can greatly reduce the likelihood of becoming a victim of this kind of thievery. Now, let us turn our attention to the other kind of identity theft: crimes committed through electronic means.

Let's explore some ways an offender might be able to use an e-mail to trick a potential victim into divulging their personal information. The following are several examples of what a deceptive e-mail could look like:

In Figure 2, an email entitled "You've got an E-Greeting" has possibly reached 7 million PC's around the world. The offenders are using a list which has your e-mail address. The list was provided compliments of one of your friends or a co-worker who thought he or she was really sending you a Hallmark. As you walk through the instructions to open, reply or resend the "e-card" you load a worm into your pc, which could allow someone access to your files.

Worms, another form of malware, are self replicating programs which consume bandwidth and cause harm to a network. Originally created to seek out dormant machines on a network and assign it a set of instructions and fix vulnerabilities, their functionality is now used to backdoor a computer making it a zombie, controlled by the author of the worm. This is somewhat unlike a virus, which usually targets only a single computer and corrupt or modify its files.

Malware is another name for software that is malicious. Malware are programs designed to be used in deceptive ways. It can report information about you to an unwanted party such as your browsing habits, disrupt your computer, or instruct your computer to attack another computer. Malware takes on many disguises but what it usually has in common is that it enters a machine or network without the owner's consent. Figure 3 below shows how malware affects your computer.

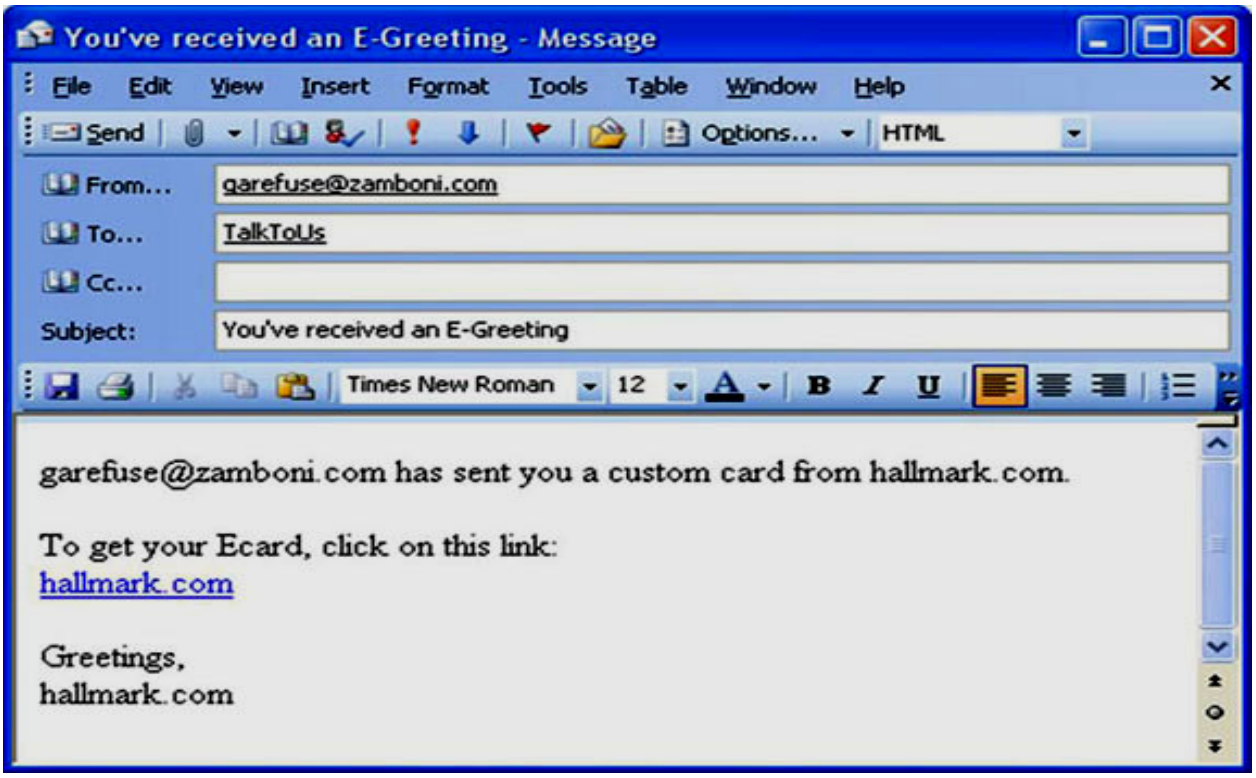


Figure 2. A Fake E-Greeting- Image provided by MSN tech and gadgets- PCWorld "In Pictures: How to Spot an E-Mail Scam"

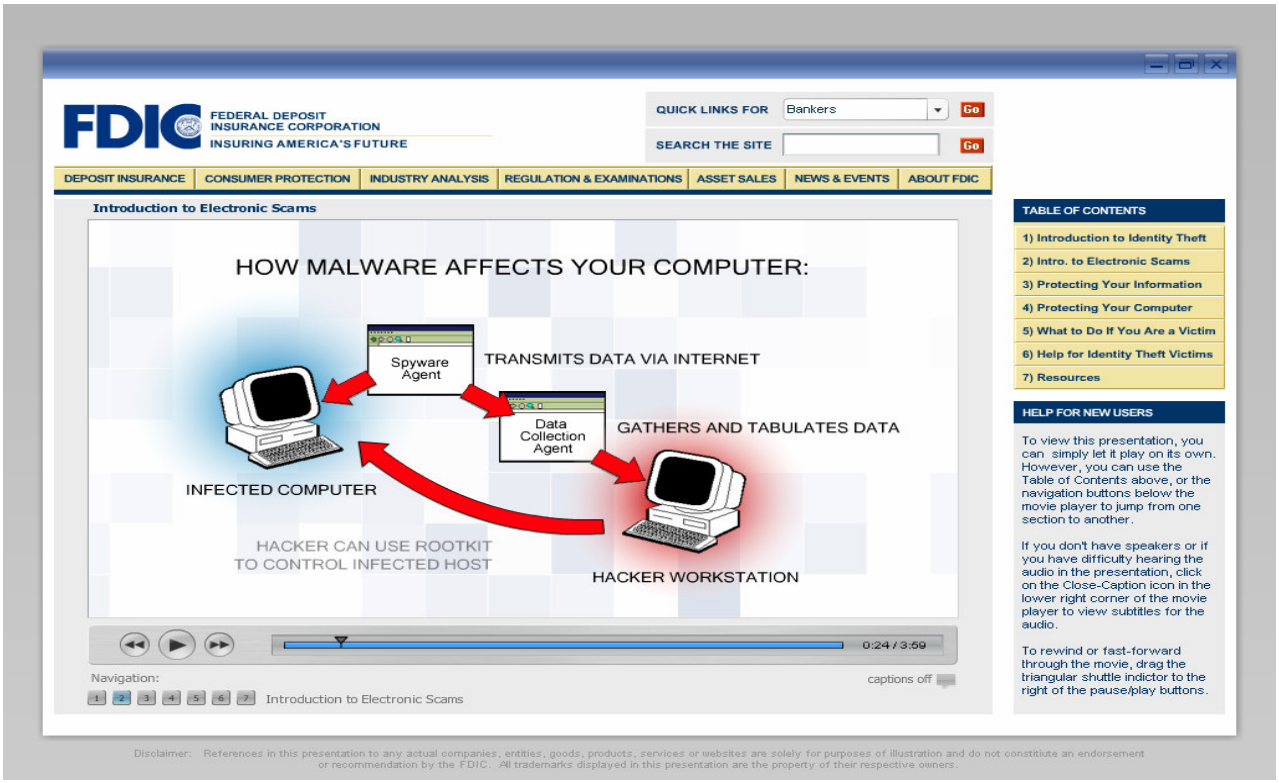


Figure 3. How malware affects your computer diagram- Image provided by FDIC CD-ROM “How to Guard against Internet Thieves and Electronic Scams-Don’t be an On-Line Victim”

In Figure 4, multiple messages are used as a tactic for spreading malware. One of the easiest ways to detect these as malicious e-mails is the use of an IP address instead of a domain name. Figure 4 gives three examples of what some messages could possibly look like

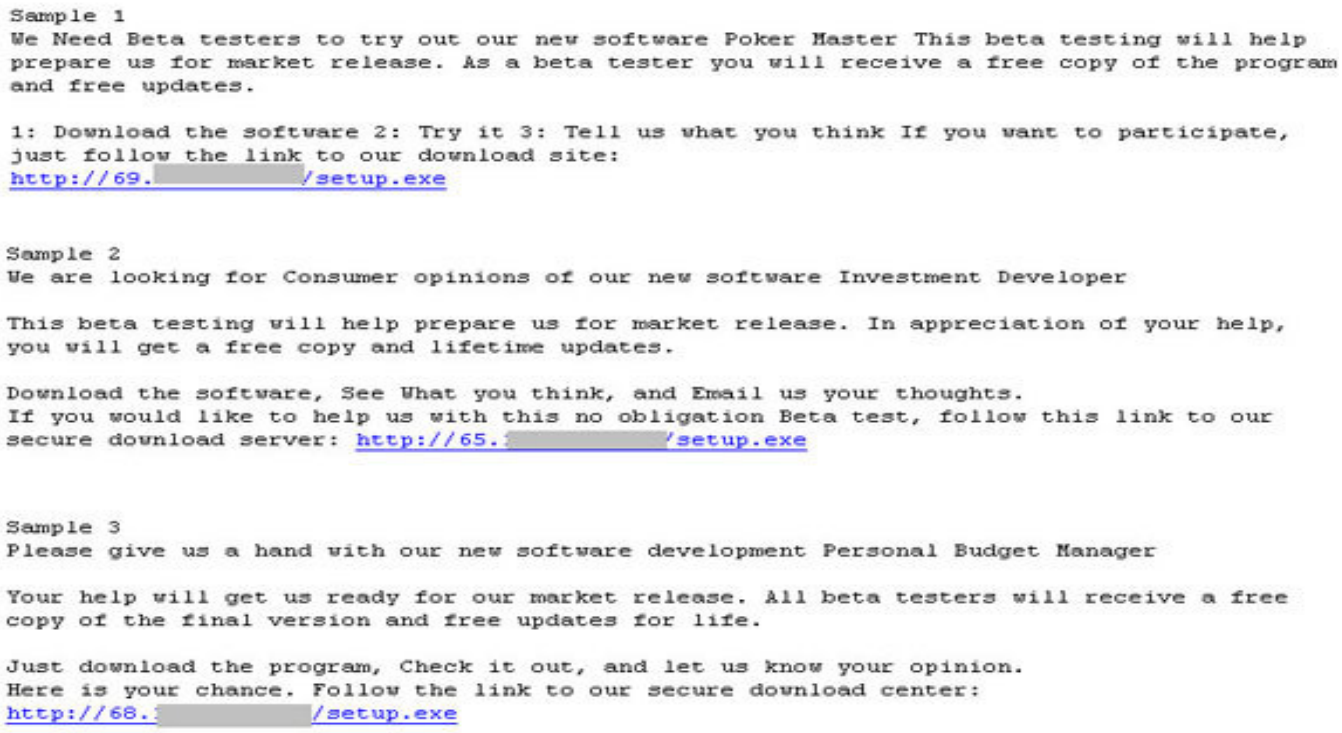


Figure 4. Three examples of tactics to spread malware- Image provided by MSN tech and gadgets- PCWorld “In Pictures: How to Spot an E-Mail Scam”

Figure 5 shows an email about a real product that is available to help keep your information protected while trading files online. “Tor” is a set of tools, which is designed to look like it will help you against the very thing that it will do- spread a worm. The message is clear- “Tor” is a tool, which will give you some anonymity online for web browsing, publishing and other multiple TCP protocol applications. In this case, the ad truly is designed using the actual product’s site to create the counterfeit page. The download is even called ‘tor.exe’.

If you come across a product like “Tor” or any other advertised product in an unexpected email, use common sense. Simply search out the product yourself instead of responding to the ad. You will be able to establish the credibility that the product is the actual product you really want and not a decoy.

Figure 5. –Tor- Image provided by MSN tech and gadgets- PCWorld "In Pictures: How to Spot an E-Mail Scam"

An interesting aspect of the email shown in Figure 6 is it is made to look legitimate because the email address has that personal touch of looking like someone's name. It is also disseminated at an opportune time: it targets football fans during the pre-season that are hungry to win money betting on stats. If you were to click on the email link, you would be sent to the fairly convincing site shown in Figure 7 to get the free software for the games. However, instead you would be loading the StormWorm botnet.

A botnet is a combination of 2 words: A bot or robot (your machine) and net meaning network. The term implies a collection of robots, which run automatically. These are called zombies and are controlled by hackers. This

process is also known as “scrumping” and the botnet’s creator is known as the “bot herder”.

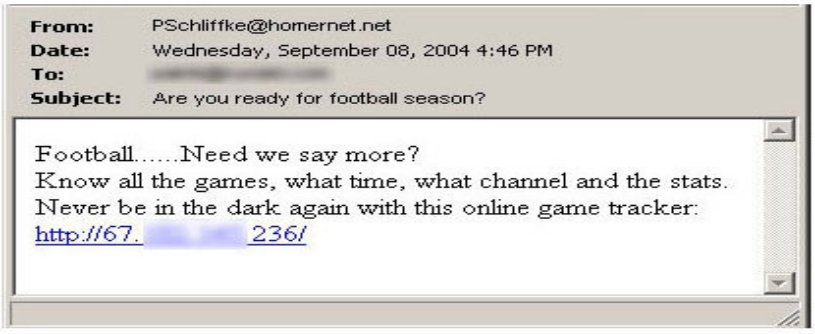


Figure 6. Are you ready for football season? - Image provided by MSN tech and gadgets- PCWorld “In Pictures: How to Spot an E-Mail Scam”

Figure 7. Sports website that loads a botnet worm- Image provided by MSN tech and gadgets- PCWorld “In Pictures: How to Spot an E-Mail Scam”

Figure 8 below shows an alert that is really phishing attack warning the consumer or victim about, ironically, a phishing attack. The email features a link that looks like it will refer to the banks home page, but it doesn’t. In cases such as this one, use common sense when dealing with bank information by typing the banks address instead of using an email link.

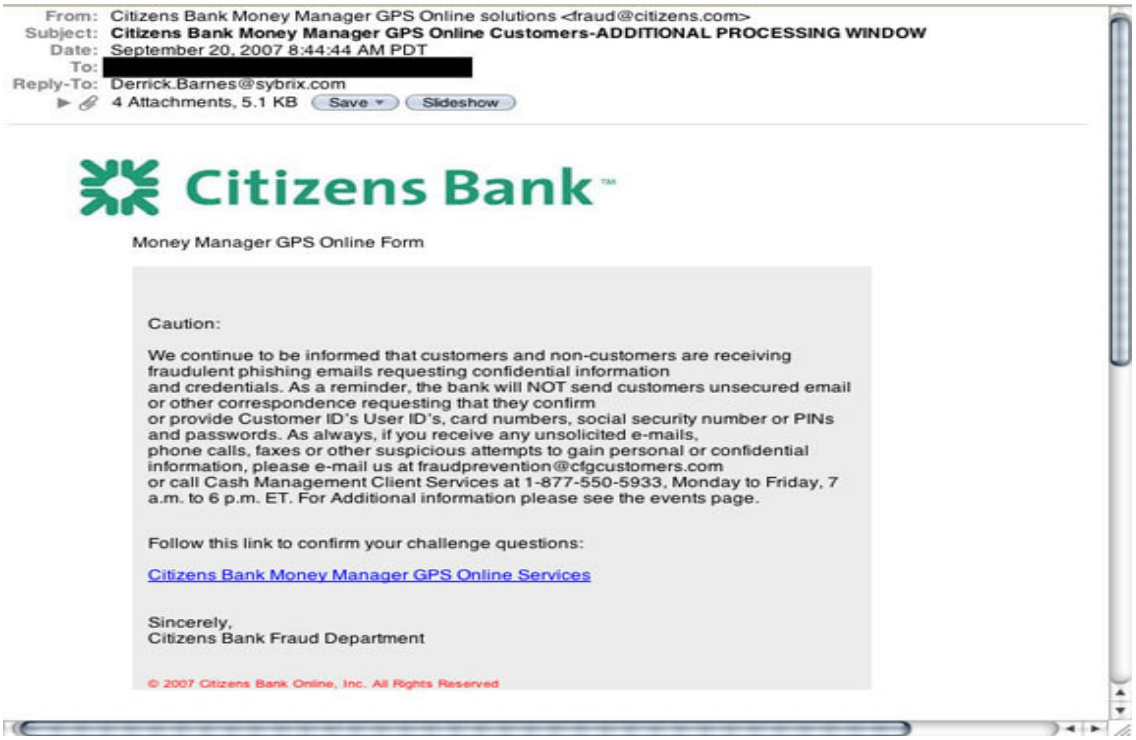
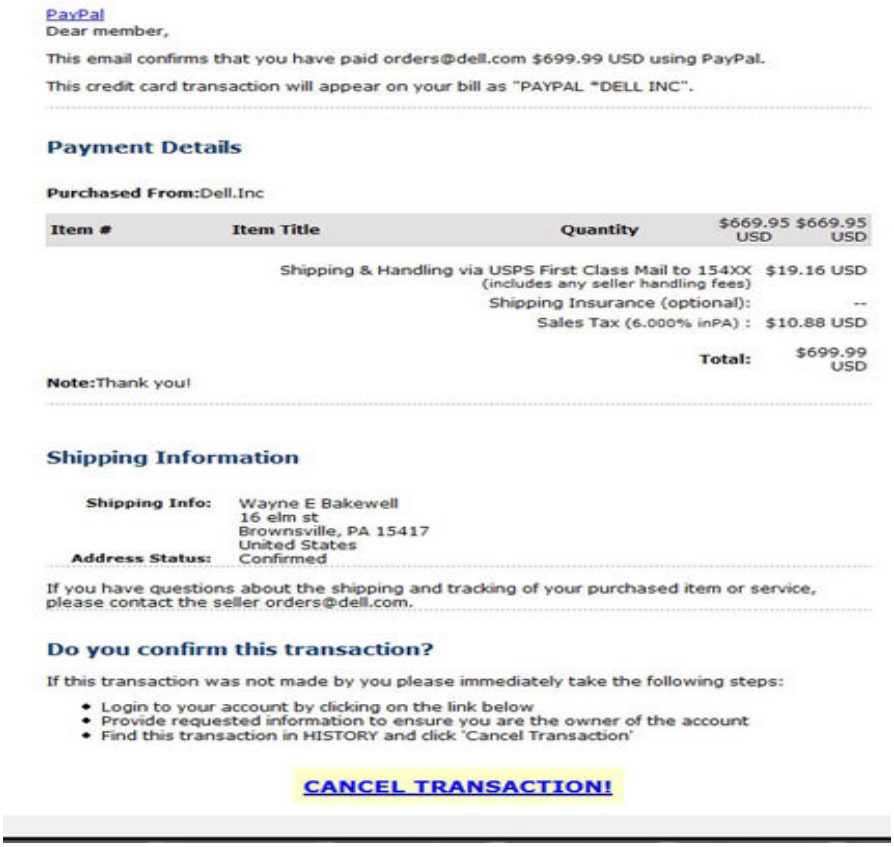


Figure 8. Citizens Bank Warning- Image provided by MSN tech and gadgets-PCWorld "In Pictures: How to Spot an E-Mail Scam"

The notice in Figure 9 below gives you the option of canceling a transaction for purchasing a laptop computer which you never ordered. By canceling the order, you are automatically railroaded into giving up more personal information like confirming your PayPal account number and so on. Once again, an IP address is offered instead of a domain name, a telltale sign that something is amiss.

In this mystery shopper phishing assault shown in Figure 10, most of the links really do go to EBay. However, one or two, like Respond Now link, switch the phishing page with the Google the URL. This clever attack succeeds because so much of the page does look legitimate.



PayPal
Dear member,

This email confirms that you have paid orders@dell.com $699.99 USD using PayPal.

This credit card transaction will appear on your bill as "PAYPAL *DELL INC".

Payment Details

Purchased From: Dell.Inc

Item #	Item Title	Quantity	$669.95 USD	$669.95 USD
		Shipping & Handling via USPS First Class Mail to 154XX (includes any seller handling fees)		$19.16 USD
		Shipping Insurance (optional):		--
		Sales Tax (6.000% inPA) :		$10.88 USD
		Total:		$699.99 USD

Note: Thank you!

Shipping Information

Shipping Info: Wayne E Bakewell
16 elm st
Brownsville, PA 15417
United States

Address Status: Confirmed

If you have questions about the shipping and tracking of your purchased item or service, please contact the seller orders@dell.com.

Do you confirm this transaction?

If this transaction was not made by you please immediately take the following steps:

- Login to your account by clicking on the link below
- Provide requested information to ensure you are the owner of the account
- Find this transaction in HISTORY and click 'Cancel Transaction'

CANCEL TRANSACTION!

Figure 9. Cancel PayPal Transaction- Image provided by MSN tech and gadgets- PCWorld "In Pictures: How to Spot an E-Mail Scam"

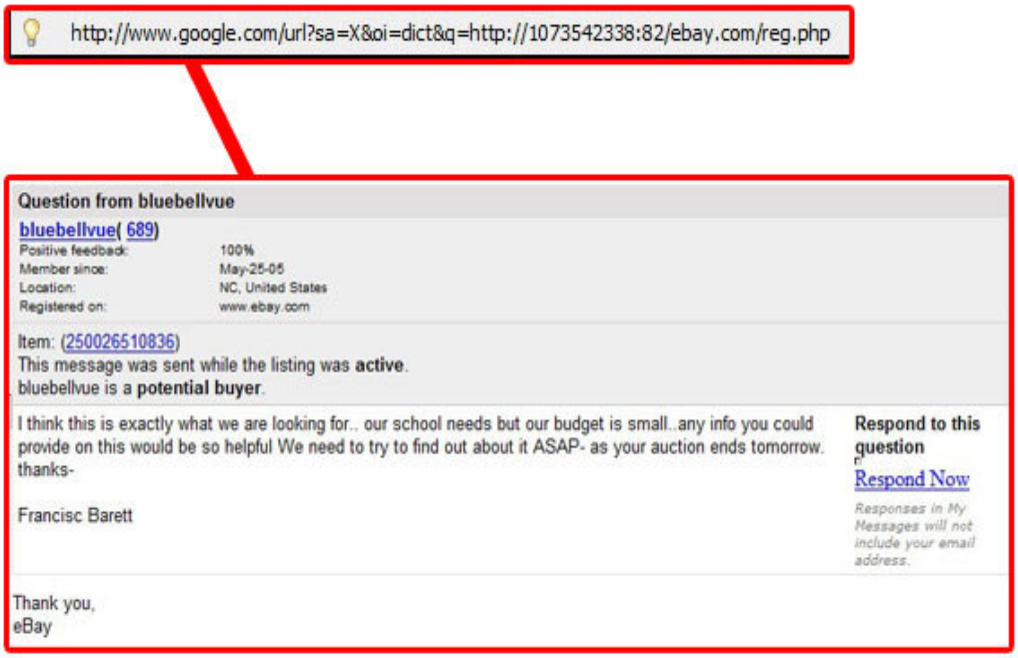


Figure 10. Google URL- Image provided by MSN tech and gadgets- PCWorld "In Pictures: How to Spot an E-Mail Scam"

If you value your reputation at eBay. The scam in Figure 11 could easily get you to respond out of fear of tarnishing your reputation and credibility. Like the email advertising the fake football site, this email preys upon the emotions of the victim, waiting to cash in when the victim lets his guard down.

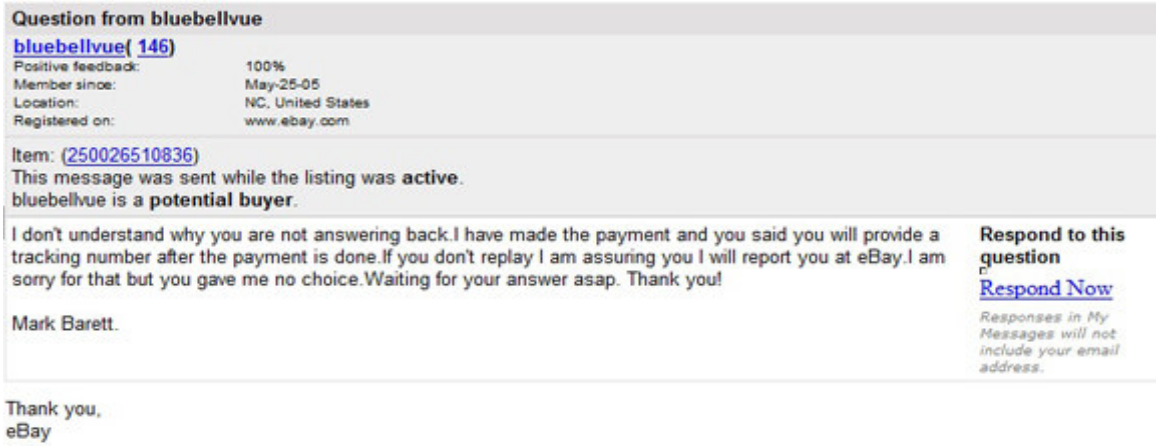


Figure 11. Threatens Your Good Name- Image provided by MSN tech and gadgets- PCWorld "In Pictures: How to Spot an E-Mail Scam"

Figure 12 advertises a rather unlikely scenario that some fall for nevertheless. It is not likely that someone pretending to be an agent from the IRS is going to email you to tell you that you have overpaid on your return. Once you start responding with your social security number and other information to "verify your identity", you have given away far too much information.

The example of Figure 13, shows how easy it is to utilize what is public information and use it as the means to trick an unsuspecting victim (in this case an alumnus), to give a credit card to get a good deal from an old "classmate". This attack preys on a person's desire to reconnect with his or her past. Nostalgia is a powerful emotion, and the person who is perpetrating this attack is counting on your desire to relive the past beating out your good common sense.

We have seen several examples of how attackers can use email and websites to snare sensitive information from a victim. All of these approaches share one thing in common. They attempt to make you let your guard down by offering you something that will likely be of intense interest to you. As we shall emphasize repeatedly in this paper, your strongest ally in defending yourself against these kinds of attacks is to use common sense.

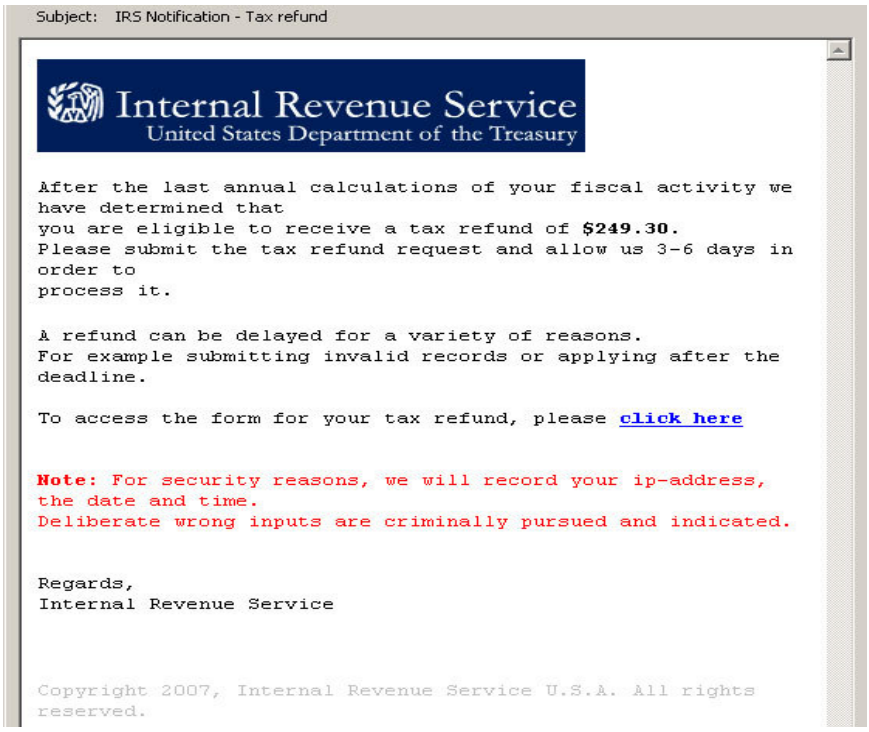


Figure 12. Letter from the IRS- Image provided by MSN tech and gadgets- PCWorld "In Pictures: How to Spot an E-Mail Scam"

.

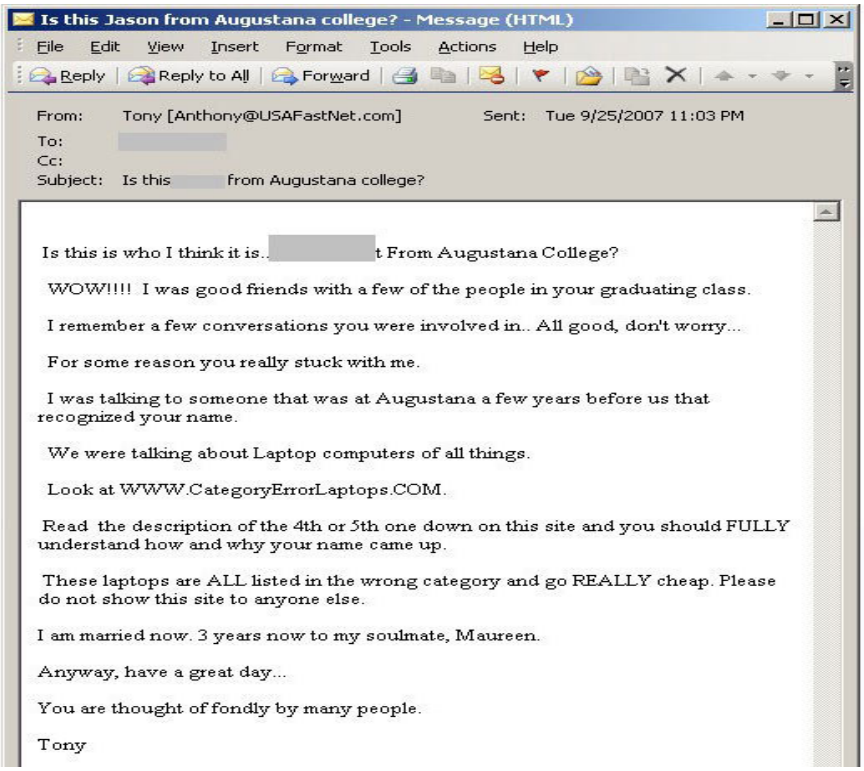


Figure 13. Using the familiar to lure a victim- Image provided by MSN tech and gadgets- PCWorld "In Pictures: How to Spot an E-Mail Scam"

What to Do If Identity Theft Strikes

When you have a monster under your bed or in your closet, at least you know what you are dealing with, because you can detect it. Becoming a victim of identity theft can be a very unnerving situation because you don't know what to expect, to what degree the damage has grown, and when and where this monster will strike again. But when you use a little common sense, you can start protecting yourself and begin minimizing the damage if it occurs. This section will focus on the steps you can take to rectify the damage if identity theft strikes you.

Some key things to remember if you become a victim include:

1) Don't panic. Panicking never helped anyone through anything.

2) If you think you might have become a victim, under the Truth in Lending Act, you typically will not be responsible for more than $50.00 in unauthorized charges per credit card. Most financial institutions will not hold you liable for charges that they would consider fraudulent.

Keep in mind that this should not represent identity theft as almost a victimless crime. Some people have been arrested after having their identity stolen because their identity was used to facilitate larger crimes. People can spend a lot more than 30 hours cleaning up their credit reports. According to the Secretary of State's Office, on the average it can take 30 hours to fix your credit report. For some, however, it can take months or even years. Subsequently, victims are denied car loans, credit cards and mortgages. (8)

Use common sense to keep the damages to minimum. Start by trying to identify what information has been taken. If you are being contacted by your credit card company and it is not a sales call, find out what it is they are contacting you about. It is always good to communicate with your credit card company to let them know the type of activity they should see on the card. It is in their best interest to communicate with the cardholder because typically the banks, which endorse the credit card company, are responsible for the activity in the end. In most cases, the cardholder is exempt from the financial responsibility of a stolen card but again, it does affect your credit, takes time, and can be a frustrating process.

When traveling, it is also important to give your credit card company notification if you plan to use the card. This does two things: It helps the credit card company get a better feel for your spending profile, which might allow the card company insight to offers you might want to take advantage of, and also you

won't have to go through the embarrassment if your card is turned off and you actually needed it for an emergency outside normal business hours.

Communicating with the credit card company can also prevent any activity uncharacteristic of your profile. For example, if you were to purchase a recharge of your Starbucks gift card in Berwyn Illinois at 11:00 a.m. and someone claiming to be the card holder is buying a brand new set of Firestone 16" whitewall tires in Juatulco, Mexico at 1:21 P.M., it is likely the credit card company might catch it because of the times and your history shows you typically let the card company know if the activity will seem out of character.

If you discover fraudulent activity on you credit card again, don't panic. It could possibly be an internal error at the card company. Regardless, make certain the card is deactivated and get a name of the person you are speaking with, id number and time of deactivation. You can do these things online but you might feel more at ease with human intervention for a positive confirmation the account is deactivated.

First, find out if you still have the card in your possession. At times, people don't realize at first that their card has been stolen because they are not aware that their wallet or purse, containing the card(s) was lost or stolen. The victim also could have been the target of a residential burglary at home and not even realized it because they are at work. Burglars that find credit cards have a tendency to go to a local gas station to fill up because they can pay at the pump and not have to present any secondary identification. They know that as soon as the card is reported stolen, they could be caught trying to use it if they wait too long. Time is critical for them to get the most use out of the card quickly and with anonymity. Find out the locations of the fraudulent activity and make a timeline of the locations, making sure a loved one hasn't been using the card. The local police can help with talking to the credit card company(s) for that information.

As a reminder, it is important to know what time zone your card company is recognizing and compare that time to your time zone in the event you live in Chicago and your card company is in New York. The timeline also helps the police investigation with possible video footage of the offender using your card in a retail store. It could show his vehicle information, dispel a suspect's statement of his whereabouts at the time, and other information to catch and charge a subject with identity theft. The timeline showing when a victim leaves his home and the first charge is made gives investigators a window of when the burglary occurred. This window is critical because it generates information about the incident, and raises new questions. (For example, did the offender use ambient light, to commit the theft, or did it happen during the time the landscape company was working at your home).

What becomes challenging is at times the credit card company will want report numbers to coincide with the fraudulent usage. If the attempts to use the card

are in different districts, you might have to report to multiple agencies. Although there might be a lead investigating agency, you still might have to do your own compiling of incident reports for the credit card company.

Try to notice anything unusual like if the first fraudulent purchase was possibly not far from somewhere where you might have lost the card. Try to remember if you merely set the card down to use it, or if maybe someone has your identity. It is possible that you have your card, but someone has found your account number through another source.

There are many incidences of an identity theft offender simply stealing the trash from a dumpster and finding multiple account numbers from various carbon copies. It is important to destroy the carbons during the transaction. If the business is not using an electronic swipe card reader (which most are), do not be afraid to ask for your information back to ensure proper disposal.

If you are not sure what the means were of how an offender used your card information, start planning a list of all of your creditors so they can be notified as early as possible. You might not fully be aware of how much information the offender has, but you reduce the risk if you act fast.

If you become a victim of identity theft, and you are not sure to what extent you need to start a contingency plan. Here are some guidelines for setting the contingency plan.

-Make sure your records are accurate.

-Have a strategy when you contact a company. Don't be afraid to keep a supervisor on the phone until you have exhausted everything you need to know to fix the problem. Write a list of questions and have them ready.

-Write down the names of everyone you speak with, the dates and outcomes.

-Follow up everything in writing. Use certified mail, return receipt requested.

-Check with other state law enforcement resources to see if there are other available to assist you if you are a victim.

-File a report with the Federal Trade Commission. (FTC)
Your information can help law enforcement help others who might be a victim using similar circumstances, and held aid in tracking an offender.

-Keep all copies of correspondence, police reports, and supporting documents accessible when speaking with the other agencies.

-Get a filing system started to organize your documents.

-Always keep the originals. Only send out your copies of supporting documents.

-Keep your paperwork safe for a long time after you are able to resolve the issue, since problems could crop up later on.

The FDIC offers free downloads to provide a victim with helpful tools and ideas to organize your case. The first step of the contingency plan is to start with a creditor contact sheet, which is shown below:

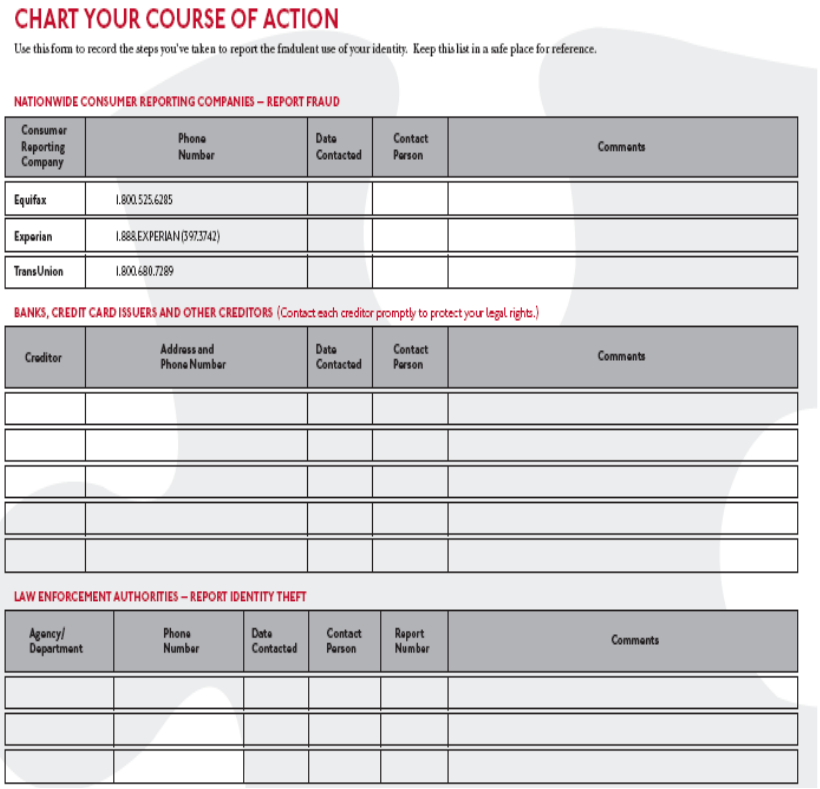


CHART YOUR COURSE OF ACTION

Use this form to record the steps you've taken to report the fraudulent use of your identity. Keep this list in a safe place for reference.

NATIONWIDE CONSUMER REPORTING COMPANIES – REPORT FRAUD

Consumer Reporting Company	Phone Number	Date Contacted	Contact Person	Comments
Equifax	1.800.525.6285			
Experian	1.888.EXPERIAN (397.3742)			
TransUnion	1.800.680.7289			

BANKS, CREDIT CARD ISSUERS AND OTHER CREDITORS (Contact each creditor promptly to protect your legal rights.)

Creditor	Address and Phone Number	Date Contacted	Contact Person	Comments

LAW ENFORCEMENT AUTHORITIES – REPORT IDENTITY THEFT

Agency/ Department	Phone Number	Date Contacted	Contact Person	Report Number	Comments

Figure 14. FDIC creditor contact sheet- Image provided by FDIC CD-ROM "How to Guard against Internet Thieves and Electronic Scams-Don't be an On-Line Victim"

Ask for a fraud alert to be placed with the 3 major credit companies. You only need to notify one company for the other two to be notified. The three main companies are:

1) Equifax 1-(800) 525-6285 www.equifax.com P.O. Box 740241 Atlanta, GA 30374-0241

2) Trans Union 1(800) 680-7829 www.transunion.com Fraud Victim Assistance Division P.O. 6790 Fulton, CA 92834

3) Experian 1 (888) EXPERIAN (397-3742) www.experian.com P.O. Box 9532 Allen, Texas 75013

A fraud alert comes in two varieties, one which only lasts 90 days and the other which lasts 7 years. The alert serves as a warning to any of the different credit agencies that your identity has been compromised and to not give or alter any of your information during this time.

Once the alert is placed on your credit report, Equifax, TransUnion and Experian are required to block fraudulent information from appearing on your credit account history. Also, once you have placed a fraud alert on your report, you are then entitled to receive free copies of your report while trying to fix the problems. The FDIC page below displays the necessary contact information: http://www.fdic.gov/consumers/consumer/guard/index.html

Figure 15. Federal Trade Commission's information- Image provided by FDIC CD-ROM "How to Guard against Internet Thieves and Electronic Scams-Don't be an On-Line Victim"

The FDIC's "Don't be a Victim Online CD-ROM is an excellent resource for what to do if you become a victim of identity theft. The CD is free and walks the

user through in a step-by-step fashion. Figure16 (Onguard on line) provides another one of FDIC's resources to help spot a scam.

Figure 16 OnGuard Online- Image provided by FDIC CD-ROM "How to Guard against Internet Thieves and Electronic Scams-Don't be an On-Line Victim"

Always check your credit report whenever possible. You are entitled to one free credit report from the three major credit reporting agencies annually. Try to watch for unusual account activity such as that shown in Figure 17.

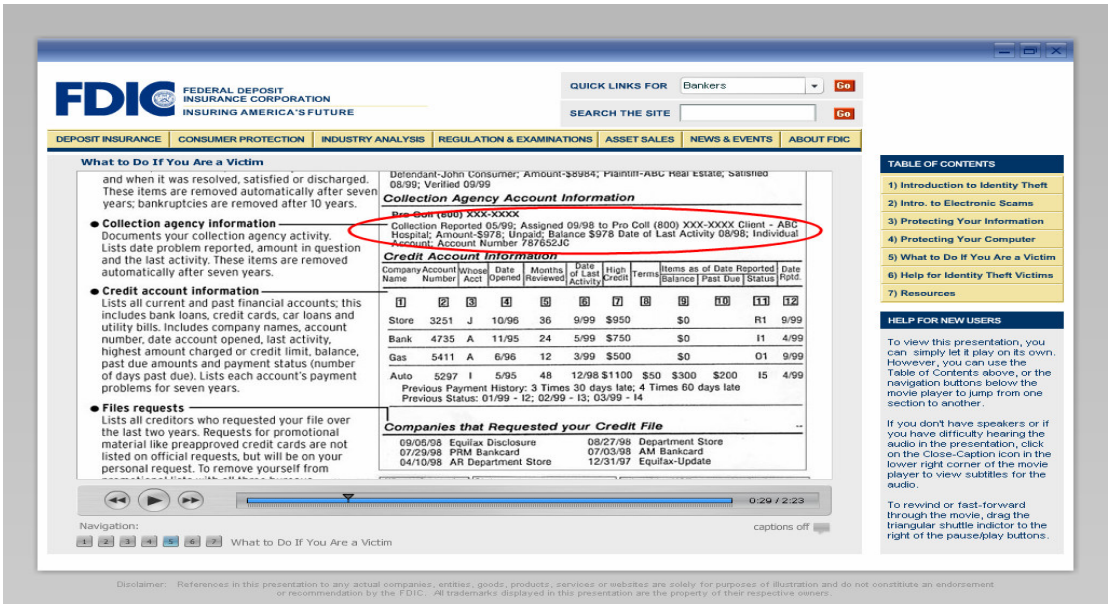


Figure 17 fraudulent collection on credit report- Image provided by FDIC CD-ROM "How to Guard against Internet Thieves and Electronic Scams-Don't be an On-Line Victim"

Common Sense Best Practices on your PC or Laptop

Probably the worst case scenario of getting your information stolen would be getting your laptop stolen, since it is used to handle your accounts, bills, banking, records and so on. The following are some ideas or precautions to help in the event of such a great loss:

1) Invest in theft deterrence software. Canadian based Absolute Software offers "Computrace" for any brand or type of laptop computer. This increasingly popular software is now an industry standard with some of the more recent models of laptop computers and can be requested by the consumer when ordering a new computer. The device is especially critical for companies that loan out their computers to employees.

The Computrace device is an agent which resides on your hard drive. In the event your laptop is stolen, the device begins to make "panic calls" to a location in Canada. The Canadian base is able to get address information relayed from the device, and then the company contacts the local authorities in that jurisdiction to recover the laptop. It is reasonably inexpensive, and thieves do not know it sending the calls. It has proven to be quite effective in law enforcement. Absolute Software's link is http://www.absolute.com/laptop-security-solutions.asp

2) Consider a biometric fingerprint identification system. Failure to provide a proper biometric identification will prevent your laptop from booting up, making it extremely difficult for a thief to bypass but not impossible. Sometimes third party biometric devices can thwarted that function with the operating system but when used in conjunction with encryption makes your information much more secure.

3) Encrypt your files. You can encrypt an entire partition on your hard drive or in some cases, just folders and files. Only parties who have permission are able to read your sensitive information. You send a key to only those who you want to. This key is generated by the author and a pass code of numbers is allocated in the form of a key which unlocks the material. The only drawbacks are sometimes there is a lag of time encrypting and decrypting files and is not truly foolproof if there is a brute force attack an your machine. Depending on the strength of the encryption you use, however, the brute force attack might become infeasible.

4) Use strong passwords. Don't ever give your password to anyone and don't write it down and place it under your keyboard. Make it complicated with numbers and letters to prevent a simple dictionary attack to crack your password. Change your password frequently.

5) Store limited amounts of information on your laptop. Only store what you need to store. If it is a business laptop, only keep the files or data needed for the weekend. Store files on a flash drive because a laptop is a much more likely target for a thief.

6) Set a BIOS password. This will slow down a would-be thief if he or she starts trying to guess your password. It can be set for a lockout after 3 attempts, but understand all the thief has to do is restart the computer to get 3 new guesses. You can also remove the CMOS battery which could clear the Bios information but not all thieves would know how to do this and it is very risky to probe the inside of a computer with a screwdriver.

An Example from an Investigative Perspective

Up to now, we've discussed what identity theft is, how it could happen to you, what to do if it does, and how common sense plays a role in not being victimized. Now we explore how a particular identity theft case played out as a police investigation. This case may provide further insights into how you can protect yourself.

From a law enforcement perspective, these offenses can take many forms. The scam varies from case to case, and each must be investigated individually. As an investigator, you do not want to get tunnel vision from the case last week, but at the same time you have to remember details which could begin to follow a pattern. You have to look for trends, similar circumstances and always keep an open mind about what kind of offender you are looking for. For example, who would gain from using someone else's credit card number to purchase twenty new videogames: the local video storeowner or the victim's thirteen-year-old son Both are possibilities that must be investigated.

Sometimes the cases can be solved when you are not trying to get the answers but when you ask the right questions. You have to identify what the crime is, its severity, who will benefit from the crime, and why. You have to consider whether someone is guilty or is someone else trying to make someone look guilty?

In this process, sometimes, at the end of the day you get lucky and start following the right questions. Sometimes you solve the case just following your gut and a little bit of luck.

This section provides an actual example of a fairly large identity theft scam, which included multiple offenders working together to pull this off. I offer this example from a law enforcement perspective because it shows how an identity theft is thwarted, and reveals another creative avenue for these types of offenders to exploit.

The investigation ended last year when my police department received a rash of complaints from local citizens who complained that their identities were stolen and didn't understand how. The victims complained about multiple examples in which their credit was being affected and the activity was very difficult to track. The victims claimed the offenders were somehow opening up new credit accounts, which they never remembered doing, maxing out their credit cards, and purchasing gifts without the card holder's knowledge. The items purchased by the victims account numbers ranged from clothes to computer equipment. The location of the goods being purchased varied from catalogs, major stores on line, telephone orders, and so forth. Included were physical purchases, some caught on surveillance cameras, where an actual credit card was displayed belonging to

the victims. This was also unusual because none of the victims reported any missing or stolen property.

There really wasn't much to go on from an investigative standpoint but these crimes did share one common denominator: all of the victims were male. This really didn't seem like much at first but it did turn out to be a major clue later.

Sometimes these crimes are difficult in law enforcement to solve because of their distributed nature. In some cases the offender(s) might be from another country. Local departments do not have a budget to send someone to another country to make an arrest and bring a criminal to justice. The FBI is typically interested in these cases for statistical purposes. It also has been our department's experience that sometimes not all agencies can work well together on these cases.

For example, when Scotland Yard was asked to help assist in a crime where our offender resided in their jurisdiction, it was explained that they take 100 calls a day about identity theft in London and our case would not be looked into, nor would there be any arrests made. Even after we discovered the identity of the offender and where he lived. Interpol and other agencies which try to govern the international enforcement of Internet laws only have the resources to pursue larger cases, so these types of cases are difficult to take mainly because of manpower. But when the Royal Canadian Mounted Police were contacted, they were very eager to help, and they actively post the most wanted identity theft offenders on their web page including photos when available. The link for RCMP personal information scams is http://www.rcmp.ca/scams/index_e.htm.

The case involving the male victims suddenly took a turn. The illegal purchase of goods that were mailed out had been delivered to a general area in our town where the population was high. Many dwellings had multiple families living in the same apartment. It became difficult to track where every online purchase was being delivered until after the fact. The proceeds were being delivered to different apartments but all in the general vicinity.

The victims had something else in common other than their gender. All of their charge statements revealed four-hundred-dollar purchases. The break finally came when a credit card was used that day to overnight ship a package to one of the apartment buildings in the hot area. It didn't take long for the merchandise to be tracked down in the Fed Ex tracking system, and a brief hold was put on the shipment to put a plan in place. This investigation now had grown to involve the Chicago Police Department and in a combined effort the apartment building was under surveillance. It was learned during that time that the likely offenders were living in the apartment building and had placed the victims name over their name on the doorbell. Fed Ex loss prevention provided us with uniforms, a van, and the stolen packages to make the arrest. Once the offender signed the bogus Fed Ex invoice, all units rushed in for the arrest.

In these physical kinds of cases, there are tangible evidences such as a forgery, and possession of stolen goods. In some cases, you have to make a deal with these types of offenders to go after the larger ones. In this case the offender signed Consent to Search form and the apartment was loaded with large amounts of stolen merchandise which was stacked to the ceiling. It was then learned that multiple families in the area, many of which were new to this country, used their residences as “go-betweens” related to the main perpetrator.

The main offender was an escort service. The madam of the escort service was living in the hot area and had a very enterprising operation using prostitutes to do her dirty work. Her business card appears in Figure 18. During the transaction of these men paying for the services provided by the prostitutes, the prostitutes always requested the actual credit card to be presented for “professional reasons”. Then the prostitutes would get the four digit code on the back of the card, which would go to the madam, who would in turn have all the information needed to order goods over the phone or internet. Meanwhile, it was awkward for our victims to explain these charges, which hindered the investigation.

Typically, with Internet theft cases, it is hard to prove who in the household actually committed the crime of identity theft. It is not always clear who was at the computer during the activity and extremely difficult to prove. In most cases a confession is necessary or a lesser charge is imposed like forgery.

At a local law enforcement level, we fall typically in a first responder category. The victim sometimes isn’t always positive their wallet or purse has been stolen or mislaid. We try to determine by the events which led up to the discovery of the missing property and choose the right course of investigative options.

Once it has been established a person has been the victim of identity theft, police try to assist the victim with preventative measures to minimize the affects of the damage. This process begins right away because it is more important than the investigation at this time. The priority is to reduce the loss. Sometimes time is critical if a thief has stolen someone’s identity. The first order of business is to shut down all credit cards until the items are found, and carefully track any purchases which are unknown to the victim. The locations for a stolen credit card fraudulently being used can tell the police a lot about the offender, which can ultimately lead to an arrest.

In these days of security around buildings becoming more of a priority, surveillance and security cameras are usually a valuable resource in an identity theft investigation. Most offenders do not realize they or their vehicles might have been recorded trying to use a stolen credit card at a gas pump because the pump does not require human intervention.

The electronic thefts are handled with the same strategy –start by minimizing the damage, and work your way out. The investigations sometimes require additional agencies to get involved when jurisdictional circumstances become factors.

Other agencies like the FBI, State Police, and other local agencies provide excellent resources to help victims of identity theft. With all of these agencies cooperating together, we are able to do our fair share of apprehending these types of offenders.

Conclusion

It is almost impossible to completely protect yourself from becoming a victim of identity theft. However, you have options when your identity is stolen. This document presented practical strategies and common sense solutions for protecting and recovering your identity. The main idea is to safeguard your personal information, refrain from panicking, methodically track down your creditors, and resolve the little recovery battles. This will help you eventually win the war.

Using a little common sense helps you avoid falling prey to some of the scams and breaches of security with your personal information. Common-sense caution is your most effective weapon for securing your information, keeping it out of the hands of the bad guys.

Bibliography

1) Forbes.com *More from Forbes .com* Commentary "Prevent Identity Theft "page http://www.forbes.com/opinions/2007/03/08/identity-theft-prevention-oped-cx_td_0308identity.html

2) Authority of the State of Illinois- Secretary of State Department Author: Jesse White Secretary of State "Identity Theft- Don't Become a Victim" Section 5 (May 2007)

3) Postal News United States Postal Service April 23, 2007 "Mail Remains the Most Secure Way to Send and Share Information- White House report issued today outlines steps to combat ID Theft" http://www.usps.com/communications/newsroom/2007/pr07_032.htm

4) About.com: Internet/ Network Security "Ten Tips to Prevent Identity Theft, Tony Bradley, and CISSP-ISSAP #2 http://netsecurity.about.com/od/newsandeditorial1/a/aaidentheft.htm

5) Bank of Internet USA: Preventing Identity Theft BofI .com http:// www.bankofinternet.com/QuickHelp/Preventing_Identity_Theft.asp

6) Utah State University: Preventing Identity Theft Christine E. Jensen MS CFCS June 2004, http://www.utahstateuniversityextension.com

7) Utah State University: Preventing Identity Theft Christine E. Jensen MS CFCS June 2004, http://www.utahstateuniversityextension.com

8) USATODAY.com Act Now to Prevent Identity Theft Sandra Block

9) Figure # 1 "No Fingerprints" Image provided by ABC News "Medical Mystery: No Fingerprints" abcnews.go.com/Health/story?id=2771451&page=1

10) Figure # 2 "You've Got an E-Card"
Figure # 4 "Three Examples of Tactics to Spread Malware"
Figure # 5 "Tor"
Figure # 6 "Are you ready for football season?"
Figure # 7 "Sport site that loads the botnet"
Figure # 8 "Citizens Bank Warning"
Figure # 9 "Cancel PayPal Transaction"
Figure # 10"Google URL"
Figure # 11"Threatens Your Good Name"
Figure # 12"Letter from the IRS"
Figure # 13"Is this ----from Augustina College?"
Images provided by MSN tech and gadgets- PCWorld "In Pictures: How to Spot an E-Mail Scam"

http://tech.msn.com/products/slideshow.aspx?cp-documentid=5617846

11) Figure # 3 “How malware affects your computer”
Figure # 14”FDIC creditor contact sheet”
Figure # 15”Federal Trade Commission information”
Figure # 16”Onguard Online”
Figure # 17”Fraudulent collection on credit report”

Images provided by FDIC CD-ROM “How to Guard against Internet Thieves and Electronic Scams-Don’t be an On-Line Victim”
http://www.fdic.gov/consumers/consumer/guard/index.html