Identity Theft Protection

History of Identity Theft

Identity Theft is not a new crime, rather it has mutated to include new technology such as ATMs and transactions on the World Wide Web. The first forms of identity theft involved the stealing of a person's identification. Before the advent of credit cards in the 1950s this meant the thieving of a person's passport or social security card. In those days you could not obtain a credit card unless you applied for it in person with photographic identification. This made occasions for identity theft far less frequent but the obtaining of credit much less convenient and fast.

In the early 1980's the credit card became a way of procuring all financial information when the Fair Isaacs Organization developed the FICO system of credit scoring. This system of rating a person's credibility is supplied in the form of a report that also contains other sensitive and private personal and financial information. Once an identity thief gets a hold of your credit report they can often also find ways to access your bank account and credit card account. The automation of both credit card, banking transactions and the Internet has made it easy to steal a person's identity.

The good thing about identity theft in this present day is that there are now more resources to help a cope with the crime. And unlike the first days of the Diner's Club card in the 1950s, you are only liable for the $50 of the stolen amount regardless of what the credit card company does.

What is Identity Theft?

Identity Theft occurs when someone, without your knowledge, acquires pieces of your personal information with the intent to use it to commit fraud. The information is often used to obtain credit, merchandise, and services using the victims' name. Identity theft can also provide a thief with false credentials for immigration and / or other applications. An unfortunate repercussion of identity theft is that very often the crimes committed by the identity theft expert are often attributed to the victim.

Identity Theft Scams

If you want to find out about the latest identity theft scams check the resources on the website of the Federal Trade Commission, the FBI and the websites of your local Business Bureau or Chamber of Commerce as well as possibly contacting your local State Attorney General's Office.

Different types of Identity Theft

There are many different types of Identity Theft – below are three examples.

Application Fraud – Also known as True Name Identity Theft: The thief will use your personal information to open new accounts, apply for credit or in extreme examples in attempt to purchase large items using your Identity. Common examples would be the thief uses your personal information to open a new credit card, establish cellular phone service even open a new checking account in order to obtain blank checks.

Account Takeover: This is where the thief uses your existing accounts, credit cards or bank information to make purchases or withdrawals – stealing your money, good ratings and eventually damaging your credit.

Criminal Identity Theft: This is where your personal information is used by a thief assuming your identity. The thief gives your name and presents counterfeit ID's to law enforcement when questioned concerning a crime. This could be a devastating scenario that puts you at risk for being prosecuted for a crime you didn't commit. As unusual as this may sound, it is a real issue that you need to guard against.

What Identity Thieves desire to acquire:

- Social Security – This is your unique personal identification number which identifies you and serves as a gateway to all your personal financial information.
- Date of Birth – used to verify your unique identity as well as confirm most financial transactions.
- Account Numbers – Can be used to withdraw money or make purchases by phone or online.
- Mother's maiden name – Used for passwords, and verify your identity as well as possibly allow access to your personal financial information.
- Pins and passwords – Allow access to your various banking, credit cards and online accounts.
- Driver's License number – Can be used to obtain fraudulent identification.

How your Identity information is acquired

- **Identity Theft in the Workplace** – Be aware of your workspace, as it is vulnerable to many eyes and hands including colleagues, coworkers, temps, service workers, contractors and after hour facility services.

- **Identity Theft Online** – The Internet has exploded in popularity and so have the cases of identity theft. Here are some of the ways your personal information can be obtained from online use:

    1. **Phishing**: Phishing occurs when thieves use the façade of legitimate company to solicit personal information. For example you might receive an email that looks as if it came from your bank or credit card company asking you to update your information. This allows the thieves to capture your account numbers, username, password and other private information.

    2. **Spyware:** Spyware is software that collects personal data from your computer without your knowledge or permission. It can also infect your computer when you visit certain websites, open software programs you have downloaded or click on email attachments. In Spyware methods there are two different ways it can work: *Backdoor Entry* – Providing thieves with remote access to your computer. *Keystroke logging* – Allows thieves to record your keystrokes on your keyboard, enabling them to capture information such as passwords and account numbers as you type it.

    3. **Fraudulent shopping sites:** Fraudulent e-commerce sites offering various goods and services through spam or online price comparison sites. Thus when you enter your information for a quote or purchase something this gives the thief your information.

    4. **Wireless Snooping** – Tech-savvy identity theft from connecting to your unsecured wireless networks and stealing your private information directly from your computer.

- **Identity Theft in the Home** – People are often less cautious when it comes to protecting their personal information that can be acquired from their home. Here are some of the ways that your personal information can be stolen from your home:

    1. Steal the Mail – An unlocked mailbox or unattended mailbox makes identity theft easy. In the mail is all the information a thief could want: bank statements, credit card information, car information, personal asset account information, etc.

    2. Access your trash – You trash contains an unbelievable amount of personal information and often it is the information as noted above in the mailbox.

    3. Defraud you by phone – Telephone scams are on the rise such as the popular calling to inform you there has been a possible fraud event on your account and then asking you to "confirm" your personal information to identify and protect you.

- **Identity Theft from Third Parties** – Thieves can sometimes access your information from a third party that has your information on file such as credit companies, employers, restaurants or stores. Here are a few ways your information can be obtained:

    1. Steal records from your employer or past employer – Employees with access to sensitive and secured information.

    2. Dumpster diving in a business's trash – Many businesses may discard documents that are un-shredded thus giving a potential wealth of information for the dumpster diving thief.

    3. Hack into a business's records online – Tech savvy identity thieves gain access to a business's systems because they are using unsecured networks.

    4. Access your credit report illegally – A thief might be able to obtain a copy of your credit report.

How Identity Thieves can Use Your Personal Information

Once your personal information has been acquired you can be exploited in a variety of ways. Below are some of the ways Identity Theft can be used to advance the agenda of the thief and do damage to you the victim:

- **Make Purchases or Withdrawals** – Purchases: A thief will use your credit cards and checks to make unauthorized purchases. These fraudulent buying sprees may include expensive high-end items such as computers and other electronics, which can also then later be resold for cash.

- **Withdrawals** – A thief can withdraw money from your savings, checking or investment accounts via ATM's, checks, online payments or an electronic transfer.

- **Change your address** – A thief can change your address and then can: change your credit card statements and banking statements and thereby preventing you from learning of fraudulent purchases and accounts right away; receive and respond to preapproved credit card offers; receive new credit cards that have been sent to you; receive your tax refund, social security checks or any other mailed income.

- **Open New Accounts** – using your social security number and other identifying information a thief can apply for and obtain new accounts in your name such as: credit card accounts, checking accounts, car loans and other loan accounts. By using a fraudulent address they will prevent you from learning of the accounts existence right away. Then when these accounts become delinquent, a collection company or even a repossession agency being notified of the delinquency will quickly affect your credit report.

- **Establish Services** – such as utilities, cable, satellite, telephone, cell or internet service. Again when the credit goes unpaid your credit will be damaged.

- **Create False Identification** - The manufacturing and even sale of false information is a thriving underground business which supplies thieves the tools they need to create false identities. Thus, your social security information, driver's license information and even passport information can be sold for various different types of fraudulent activities.

- **Get Employment** – As wild as that may sound it's true. Thieves can often secure employment by completely taking over your identity.

- **Receive Social Security Payments** – This is an old but again true scheme, the thief will collect the victim's social security and be able to cash the checks due to the false identification they have already stolen and manufactured.

How to STOP Identity Theft at Work

Remember - Identity Theft at the workplace can be more common than you realize so here are some suggestions to help keep your information safe.

- **Personal Property** – keep your personal property in a secured place at all times. Do not leave your purse, wallet, and laptop, checkbooks, billing statements or other documents on your desk. Rather be aware and keep these items secured when you are away from your desk or even when you have a visitor.

- **Work Computer** – Many companies now monitor and scan the content of employees outgoing emails and internet use and this is usually for security procedures and is perfectly legal. However, be aware your personal information should not be entered onto your work computer as these systems are scanned by employees monitoring the network.

How to STOP Identity Theft Online

Do not use an unsecured computer or computer network. Install the appropriate software to protect your computer, avoid installing software that could potentially harm your computer, protecting your network, practice safe email habits, shop online with caution.

Use Software that protects your computer:

- **Up-to-date operating system (OS):** Check for and install upgrades for your operating system – such as Microsoft Windows, Linux or Mac OS.

- **Up-to-date web browser:** Use the latest version of your web browser like: Microsoft Internet Explorer, Netscape or Firefox to make sure your computer has the most updated security patches and encryption capabilities. Almost all browsers offer security settings which you should set to High. The browser should alert you when it detects unauthorized downloads or other potentially malicious activity.

- **Antivirus software** – A computer virus is a malicious program that will replicate itself and infect multiple computers at a time. Some viruses will steal personal information and email it to identity thieves. A good antivirus software program will detect, delete and quarantine any suspicious computer codes or software that it finds in a scan. The best protection is to scan the computer daily and update the antivirus software daily.

- **Antispyware software**: Antispyware software defends and protects your computer from spyware and deletes it whenever it is detected that it has been downloaded and installed without you knowing it.

Avoid Software that can harm your computer:

- Do not click on pop-ups: Clicking on some pop-ups can install spyware onto your computer – avoid clicking on pop-up windows while on the Internet.

- Download Cautiously: Download files from people or web sites that you know or trust.

- File Sharing: File sharing programs allow you to swap files with computer users around the world. If you utilize file sharing make sure your antivirus and antivirus software are up-to-date before you download anything from a file-sharing network.

Using Email:

- To combat phishing and email scams – never respond to emailed requests asking you to verify an account number, PIN or password. Do not provide personal or financial information via email unless you initiated the contact. Never respond to or buy something advertised by spam or other solicited email.

- Do not open attachments or links from people you do not know.

- To visit a web link a friend has sent you type the URL into the address bar of your browser.

- Make sure your antivirus software is set to scan incoming email.

- Another good idea is if you need to send and receive personal or financial data via email then consider investing in encryption software to encode the information.

How to Shop Online Safely

- Shop with companies you are familiar with that you know to be reputable
- Shop and order products and services from sites that keep your information secured. Looks for "https" or a small padlock icon that will often be displayed on the site. These are both indicators that these sites use encryption software to help encode and keep your information secure. One thing to note – sometimes tech savvy thieves will try to make their sites "look" safe so they might have a fake padlock symbol displayed. Often you can double-click on the icon to see whether the certificate is from a legitimate authority such as VeriSign, Thawte or Entrust – for example.
- Do not store your personal information – such as your credit card numbers or even address if possible.
- Using a Credit card instead of a Debit card is also a good way to hedge against identity theft because often credit cards have more legal protections than debit cards. For example, the Federal Law and The Truth in Lending Act, limits liability for fraudulent credit card charges to $50.00. However, liability for unauthorized use of an ATM or Debit card is often determined by how quickly your report the card missing or unauthorized.

How to Protect a Wireless Network

Since wireless networks are less secure, then you need to take the extra precautions to protect your information. If your wireless network is set up without configuring security features, then anyone within a range of your network can use your internet connection. To secure the wireless network you need to implement some settings on your wireless router. Here are some suggestions:

- Change the routers default user ID and password
- Enable 128-bit encryption
- Change your default Service Set Identifier (SSID)
- Disable SSID broadcasting

- Turn on MAC address filtering

How to STOP Identity Theft at your Home

In order to help protect yourself from Identity Theft at your home here are a few suggestions about how to secure your mail, documents and other personal information.

Protecting your Mail

- Do not leave your mail unattended – if you are going to be away for an extended period then arrange to have your mail secured at the post office.
- Consider mailing sensitive information from the post office or a well trafficked mailbox.
- Have new check orders sent to the bank – do not have blank checks sent to the mailbox.
- Fill out change of address forms promptly
- Avoid filling out Pre-Approved credit card offers – these are often a large source of identity theft. You can chose to opt out by calling 888.567.8688
- Keep track of your billing and statement cycles – if a bill or statement is missing then call your creditor immediately.

How to Avoid Phone Fraud

Do not give out personal information on the phone unless you initiated the call. Legitimate companies will never call to verify passwords or account numbers.

How to Detect Identity Theft

If you are a victim of Identity Theft it is critical that you take action immediately, acting fast can help contain the damage saving you time, money and frustration. It is essential to be able to recognize the major signs of identity left.

- Lost Belongings – If your belongings are lost or stolen then you should assume that your identity is at risk and act immediately.
- Missing Mail – Keep track of your monthly bills, statements or other sensitive items that you expect to receive in the mail. Be aware and watch for missing: Bank statements, Credit Card bills, Boxes of new checks, Pay stubs, Tax forms, Tax refund checks, Social Security Earnings and Benefits Statements, Social Security checks, etc.
- Unauthorized Purchase and Accounts – Look for unexpected charges, unauthorized transactions, unfamiliar accounts.
- Calls from collection agencies – for unfamiliar outstanding debts.
- Attempts at repossession – A lender attempting to repossess something you do not own.
- The IRS contacts you – correspondence that may indicate that you have filed duplicate returns or haven't reported all your earnings.
- A Loan or credit application is refused – You may be unexpectedly turned down for credit or a loan due to a poor credit rating.

How to Repair your Credit after Identity Theft

Here are some basic guidelines to helping you start the process of cleaning up your credit and reclaiming your identity.

Write to the Credit Bureaus

To accelerate the process of repairing your credit, send a letter to each of the three credit reporting agencies. This letter is often referred to as an Identity Theft Report. Here are some things to include in your letter:

- Reference the phone call that you already made to place a fraud alert on your file.
- State clearly that you are a victim of identity theft and that you're writing to request that all fraudulent information be removed from your report.
- Be as specific as possible about which information should be removed. Include a copy of the credit report on which you indicate each instance of fraud.
- Include copies of your police report, ID Theft Affidavit, and any other documents that support your case.

Send your letter by Certified Mail Return Receipt Requested. The addresses of the fraud divisions for the three credit reporting agencies are:

EQUIFAX
PO Box 740256
Atlanta, GA 30374

EXPERIAN
P.O. Box 9556
Allen, TX 75013

TransUnion
P.O. Box 6790
Fullerton, CA 92834

Fair Credit Reporting Act (FCRA), the credit reporting companies are required by law to take the following two steps:

Block all allegedly fraudulent information from appearing on your credit report.

Investigate the fraudulent information you've reported. They must inform the companies that originally provided the information (creditors, lenders, etc.) that you are disputing the charges. Those companies are required to investigate and report back the findings to the credit bureaus.

**Follow up with the credit bureaus after to make sure the information is being reported correctly.

More Steps to Take to Help You Recover from Identity Theft

Unfortunately, the process of repairing your Identity can be a lengthy one, so here are some additional steps to take in order to reclaim your credit and Identity.

As you move through the process it is important that you keep a thorough paper trail; keep all documentation, correspondence and detailed records of everyone you talk with.

It would be a wise decision to also send all reports via Certified Mail Return Receipt Requested.

Take Action Quickly!

As soon as you realize you have been victimized by Identity Theft you should:

- File a Police Report
- Put a Fraud Alert on your credit report
- Notify all your accounts of possible fraud and Identity Theft
- Close all compromised accounts

- Consider changing credit card numbers and passwords
- Complete ID Theft Affidavits – www.consumer.gov/idtheft/pdf/affidavit.pdf
- Contact check verification systems if your checking accounts were compromised –
    1. Certegy – 800.437.5120
    2. ChexSystems – 800.428.9623
    3. Scan – 800.262.7771
    4. TeleCheck – 800.710.9898
- Contact DMV if your driver's license or state identification was stolen
- Contact Social Security if your card or number was stolen
- If you Passport was stolen contact – State Department's Passport Services at 202-955.0430

To Your Success,

Brokers Choice of America

**As with any financial transaction make sure to consult your CPA or tax attorney as well as your Financial Advisor for the most appropriate information as it applies to you individually. This article is written only to provide a basic understanding of the above concept.*

Disclaimer: BCA Universities are a trademarked marketing name of a course offered by BCA Marketing. BCA Universities are not accredited by any organization of higher education nor are any courses approved for C.E. (Continuing Educating) credits for any professional license.