IDENTITY THEFT

WHAT IS IDENTITY THEFT?

Identity theft is a serious crime, which in the past has disabled and disrupted millions of consumers credit ratings and their overall financial well-being. Identity theft occurs when a person wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain.

IDENTITY THEFT

"Every 79 seconds, a thief steals someone's identity, opens accounts in the victim's name and goes on a buying spree."

CreditGUARD of America has produced this booklet for its clients to help them recognize the common signs of identity theft, what to do when confronted with identity theft, their legal rights and prevention methods that are available in the market place today.

IDENTITY THEFT STATISTICS

According to Federal Trade Commission (FTC), 10 million Americans fell victims to some type of identity theft last year. The FTC also noted that an average victim reported $10,020 in losses and invested in more than two years to resolve those cases. Victims also had to spend an average of $500 in out of pocket costs in order to fix their credit. According to CBSNews.com " Every 79 seconds, a thief steals someone's identity, opens accounts in the victim's name and goes on a buying spree." A survey conducted by the FTC also uncovered that 15% of the victims noted that there was a criminal investigation or warrant for their arrest due to their identity theft.

HOW IDENTITY THEFT OCCURS

Most consumers fall victim to identity theft as a result of the Internet. Nowadays, criminals have access to various high-tech computers and software and they can easily gain access to your personal and financial information. This type of theft is called 'Phishing' where criminals mask themselves as legitimate businesses to deceive unsuspecting consumers.

What do these phishing emails look like? These criminals are very clever, often times cutting and pasting the logos, content and company information from the legitimate entity into the email. The phisher will insert false statements to create a sense of urgency with a corresponding link so the consumer can go and "fix" the problem. Here are some of the false statements identity thieves are using:

- "Our company has decided to test for free the security of the email services that you use…Hoping you have understood that we are doing all these for your own safety…we suggest you access the following form."
- "We have detected a slight error in your information…update and verify your information by clicking the link below…if your account information is not updated within 48 hours then your ability to use your [company] account will be restricted."
- "During our regular update and verification of the [type of account], we could not verify your current information…as a result your access to use our services has been limited…To update your account information and start using our services please click on the link below"

If the consumer clicks on the link in the phishing email, it will take them to a dummy website where consumers are encouraged to fill out a form, putting bank accounts, credit card information or other personal data into the hands of the identity thief. This fake website can look exactly like the legitimate business, financial institution, or government agency they're mimicking.

Another popular Internet scam involves fake credit card companies and mortgage brokers who entice customers with low interest rates and obtain personal information. These fake messages are created in such a way that it replicates well establish companies, which customers recognize and trust with their personal information.

OTHER METHODS OF IDENTITY THEFT

Internet based identity theft is only a part of the whole problem. Skilled identity thieves may use a variety of creative methods to gain access to your personal information. In the following section, we will take a closer look at some common identity theft methods and techniques.

Stealing Information from Businesses: Most identity thieves steal personal information by targeting various businesses and institutions that holds valuable personal data.

- Many thieves may already be working for one these companies and may have access to your information with just a click of the mouse.
- Employees who are in dire financial conditions may be enticed to sell information to identity thieves.
- High technology based identity thieves may hack into the company database and steal personal information from the source.
- Thieves can rummage through the company trash dumps and collect whatever personal information that has not been shredded. These types of thievery is called "dumpster diving."

Stealing Information from Victims: Identity thieves might target specific victims who are

likely to be liberal with regards to protecting their identity.

- An unlocked mailbox is an extremely easy target for identity thieves who are looking for important personal information. Thieves can gather information from bank statements, credit card statements, new checks, tax returns and etc.
- They might gather information by “dumpster diving” and collect whatever information you have discarded.
- Wallets and purses also contain highly significant personal information which can be used by identity thieves to commit fraud.
- Your home is also an excellent information source for thieves who can easily gain access to your personal information. It’s a known fact that most families that had experienced house robberies in the past usually face identity theft short time later.

WARNING SIGNS OF IDENTITY THEFT

Once your identity has been stolen or exploited by a thief, you may not realize this occurrence until some common signs begin to appear. Consumers who keep a close vigilance on their personal information might be able to act quickly and reduce the damage before it gets out of hand.

The following are some of the common signs of identity theft:

- Your regular bank or credit card statements fail to appear. In such a situation, the thief might be stealing your statements from your mailbox or has successfully forwarded your statements to another address.
- Your credit report reveals unauthorized accounts that you did not open.
- Your credit card statement includes charges for items you have not purchased or ordered.
- You receive credit denial letters from financial institutions that you did not apply. This usually occurs when someone applies for credit using your personal information.
- You are turned down for a credit card, mortgage or any other type of loan for no apparent reason. The denial could be a result of unpaid loans taken out by identity thieves under your name.
- You receive collection calls and letters from creditors demanding payment on goods and services that you did not purchase.

HOW IDENTITY THIEVES USE YOUR PERSONAL INFORMATION

The identity thieves’ main objective is to acquire maximum amount of funds in the shortest time possible. In order to achieve such a result, the thieves have to be creative and devious to cover up their tracks. The following are some of the common ways identity thieves use your personal information to commit fraud.

- They may go on spending sprees using your credit and debit card account numbers to buy "big-ticket" items like

computers and televisions that they can easily sell.

- They may open new credit card accounts in your name. Once they used all available credit and don't pay the balances, the delinquent accounts are reported on your credit report.
- They may counterfeit checks, credit cards, debit cards or authorize electronic transfers in your name and drain your personal bank accounts.
- They may take out an auto loan in your name.
- They may establish phone or wireless services in your name.
- They may file for bankruptcy under your name to avoid paying debts they have incurred under your name.
- They may obtain driver's license issued with their picture while utilizing your name and address.
- They may give your name to the police during an arrest. Once they don't show up for their court date, a warrant for arrest is issued in your name.

HOW TO AVOID BEING A VICTIM OF IDENTITY THEFT

To reduce or minimize the risk of becoming a victim of identity theft, there are some basic steps you can take. In addition to the information that follows, more information on identity protection can be found at the Federal Trade Commission web site.

- The most important preventive method is to review your credit report from each credit reporting agency (Experian, Equifax and Trans Union) at least once a year.
- Remove your name and contact information from marketers' unsolicited mailing lists.
- Terminate unused credit card and bank accounts.
- Avoid carrying your social security card or any other document that carries the number in your wallet, purse, briefcase and etc.
- Shred all documents containing personal information.
- Do not give out your personal information when you are on the phone in a public place where people can listen to your conversation.
- Keep passports, social security, birth certificate and other important personal documents in a safe.
- Only provide your social security number and other personal information to well-reputed and established companies and only when it's absolutely necessary.
- Most companies, institutions and schools use your social security number as the account or the ID number. In such a case, call them and insist that they change it.
- Memorize passwords and PIN numbers instead of carrying them with you.

WHAT TO DO IF YOU ARE A VICTIM OF IDENTITY THEFT

If you suspect any unusual activity in your credit report or you think you may have been a victim of identity theft, the first step should be to immediately place a fraud alert on your

credit report. You can place a fraud alert by contacting one of the credit reporting agencies. After you place the fraud alert, you should close the tampered accounts to reduce further damage. The victim then should file an official police report in the community where the identity theft took place. Keep a copy in case your creditors need proof of the crime. The final step should be to file a complaint with the Federal Trade Commission.

After all the initial steps have been completed, the victim should review his/her credit report from each credit reporting agency. According to U.S. law, the credit reporting agencies must award free copies of credit reports to each victim. The victim should carefully review the credit report to make sure that no additional fraudulent activity is taking place.

CREDIT REPORTING AGENCIES

You can file fraud alerts, change incorrect information and order copies of your credit report by contacting the three primary credit reporting agencies.

EXPERIAN
P.O. Box 2104
Allen, TX 75013-2104
(888) 397-3742
www.exprian.com

EQUIFAX
P.O. Box 740241
Atlanta, GA 30374-0241
(800) 685-1111 (request report)
(800) 525-6285 (report fraud)
www.equifax.com

TRANS UNION
P.O. Box 2000
Chester, PA 19022-2000
(800) 888-4213 (request report)
(800) 680-7289 (report fraud)
www.transunion.com

USING TECHNOLOGY TO COMBAT IDENTITY THEFT

Firewall Software: The most effective method of combating identity theft is to purchase firewall protection software for your personal computer. Without basic firewall protection, hackers can gain access to your personal computer and view sensitive personal information. Most regular firewall software are priced below $100 and hi-end software can run up to $2,000 or more.

Credit Monitoring: Credit Monitoring is a tool that helps you proactively monitor, manage and protect your valuable credit and identity information. This comprehensive service provides protection unlike any other service by helping you detect and respond quickly to fraudulent activities. Potential benefits of credit monitoring services include:

- *Early detection of errors or suspicious activity.* Credit monitoring services usually examine your credit report daily and send you regular alerts to keep you updated.

- *Fraud resolution services.* Most credit monitoring providers offer some form of assistance in cleaning up your credit report when you experience identity theft.

- *Identity theft insurance.* Credit monitoring subscribers can also take advantage of identity theft insurance which guarantees the proper reimbursement amount based on actual damage. Covered expenses may include attorney fees, mailing costs, reapplication fees, phone charges and lost wages for time taken off from work to deal with identity theft recovery.

CreditGUARD of America offers credit monitoring services to its clients upon joining our program. The Coach Credit Scout ™ notifies clients through email alerts every time a change has occurred in their credit report. To view a sample Coach Credit Scout report click on the following link http://creditguardcoach.com/index.php?step=ExampleScout.

KNOW YOUR LEGAL RIGHTS

Understanding your basic legal rights is a significant step in combating identity theft. In 1998, the U.S. government passed the "Identity Theft and Assumption Deterrence Act" which listed identity theft as a federal crime. Under the U.S. federal law, an identity theft victim is not liable for more than $50 if someone uses the victim's credit card without his authorization. Most credit card companies and financial institutions will refund the stolen amount if you notify them in a timely manner. The above protection only applies for credit card fraud.

The Electronic Fund Transfer Act (EFTA) provides consumer protections for transactions involving an ATM or debit card or any other electronic way to debit or credit an account. It also limits your liability for unauthorized electronic fund transfers.

Identity theft victims can also benefit from the Fair Credit Reporting Act (FCRA), which enable them to clean their credit report from fraudulent activities. Under the FCRA, the credit reporting agency and the appropriate financial institution are responsible for correcting inaccurate or incomplete information in your credit report.

If you have any questions or comments regarding this publication, please contact Nemal Perera at 1-800-400-5844 Ext. 160 or email nemal@creditguard.org.