Identity Theft-Problem on a Rise

AASHIMA BISEN
CHAMELI DEVI GROUP OF INSTITUTIONS
b.aashi30@gmail.com

Abstract— **Identity Theft has become one of the most lucrative criminal endeavours. Identity theft occurs when a criminal obtains enough personal information (driver's license, social security number, credit/debit card number, etc.) to impersonate someone else. While the stolen information can be used for a number of fraudulent purposes, financial gain–purchasing merchandise, stealing money, establishing loans, etc. – is the most common. This Paper is an attempt to explore this, nation's fastest growing crime. It will outline Introduction, Types of Id Thefts, and Tips to avoid Id Theft, Laws for Id theft & also some aspects to its prevention and cure.**

Keywords— **licit, quintessential, Fraudlent,Felon**

I. INTRODUCTION

Some years ago, the term "identity theft" was little used was very unknown to eveyone.But Today, it is one of the widely recognized term that is associated with the act of capturing public, media and government attention and which has become a serious social issue. Nowadays this crime rate has gone to its heights that Often it is described as – "the crime of the new millennium", the "nightmare of identity theft", the "quintessential crime of the information age", i.e. identity theft has become one of the most prevalent types of crime. Its impacts can be financially devastating and personally traumatic. It not only steals one personal identity but also affects the person's surroundings as its effects are long lasting. These not only affects individual victims but also to government, business and society in general.

II. HOW INFORMATION GETS STOLEN?

The Internet is a boon to mankind but at the same time it has made much easier for criminals to commit crime. Here are some of the methods used by cybercriminals to commit identity theft:

- *Phishing* – Phishing is the act of sending an email to user falsely claiming to be a licit enterprise in an attempt to scam the user. Phishing directs the user to a website that is actually a clone of original website where users are asked to enter all personal details, passwords, Account number.
- *Skimming* – An electronic method of capturing someone's personal information used by identity thieves. The skimmer is a small device that scans a credit/debit card and stores the information contained in the magnetic strip. Skimming can take place during a legitimate transaction at a business.
- *Spyware* – Spyware is used to gather all kinds of personal information, typically without you knowing that anything is happening. Spyware is usually downloaded unknowingly along with free software such as games, screensavers, videos, music, etc. It can also be distributed as an attachment in an email message or disguised as licit software.

Believe it or not, a great deal of identity theft still occurs through old-fashioned stealing. Some criminals will steal wallets, purses, mail or even rummage through your trash in search of any important documents that they can get their hands on.

III .TYPES OF IDENTITY THEFT

There are several types of identity theft. Knowing what to do if you are a victim of identity theft starts by knowing what type of identity theft you are dealing with-:

Financial Identity Theft

When we hear the words "identity theft" we usually think of credit reports and bank accounts. This is called financial identity theft. We hear about data breaches like TJ Maxx (47.5 million credit cards) and Heartland Payment Systems (130 million credit cards) regularly. Our faith in our financial institutions is shaken. Some of us are thinking about stuffing our money in the mattress again. If an identity thief gets access to your bank account, then it may cause financial theft.

Child Identity Theft

Child identity theft occurs when an identity thief uses a child's personal identifying information for personal gain, such as obtaining credit, utilities, employment or to avoid arrest and criminal prosecution. Children are often targeted because the crime is usually not detected until the child reaches adulthood and applies for credit, enabling the thief to use the information for many years.

Medical Identity Theft

This Type of Theft is where someone steals your identity to either obtain medical insurance in your name or use your current medical insurance policy to receive treatment or prescriptions.

Criminal Identity Theft

When a criminal fraudulently identifies himself to police as another individual at the point of arrest, it is sometimes referred to as Criminal Identity Theft. Criminals in this case usually have the some issued documents' of the person or in other words we can say a fake Id.

When dealing with criminal identity theft, expect a lot of skepticism. Police are told "It wasn't me" almost every day. It's also worthwhile to know that many states now have specific laws in place to address identity theft.

Driver's License Identity Theft

This may be the easiest form of ID theft to commit. Your purse/wallet gets stolen, and your driver's license gets to someone who looks like you and in such cases your details can be misuse. This type of ID theft spreads to others, especially criminal identity theft.

Social Security Identity Theft

There are millions of people working in America who don't want to pay taxes. It may be an illegal immigrant , a deadbeat parent, or a paroled criminal trying to shake their past. Your SSN may be the most valuable piece of personal information a thief can steal.

While the Social Security Administration isn't required to tell you about all these jobs, the IRS will want you to pay the taxes. This can be a tough battle, too. For a non-government agency, the IRS has unbelievable power. Expect a lot of hoops to jump through here. Although it's gotten easier over the past few years, the process is still time consuming.

Synthetic Identity Theft

This is the "latest thing" in the ID theft world. The thief will take parts of information from many victims and combine it. The new identity isn't any specific person, but all the victims can be affected when it's used.

IV. PREVENTION TACTICS

Prevention is the major aspect of Id theft. Consider the following question: would you rather prevent id theft or detect and recover from it? The same question considered in a different context: would you rather place a lock on your door to prevent a thief from stealing your stuffs or notice they have been stolen and go through the process of filing reports with the police, insurane company etc,to recover from theft? The obvious choice is to prevent it.

First of all, you need to recognize all of the sources of information that identity thieves could use against you. Listed below are some of the most common:

- Public records (tax documents, court proceedings, etc.)
- Bills
- Social media sites
- Credit/Debit card receipts
- Newspaper and magazine subscriptions

Remember, identity thieves are always looking for a chance to get a breakthrough and steel your identity on your single mistake or carelessness. As long as you remain vigilant in securing your identity, you can avoid becoming a victim. Listed below are some tips and information that will help you do just that:

- Install up-to-date anti-virus and anti-spyware software on your computer.
- Be responsible over every bank statement, and keep them under close watch.
- Turn on your computer's firewall. If you connect to the Internet via a wireless network, make sure it's encrypted to prevent outside access.
- Be wary of what sites you visit when using public Wi-Fi.
- Use unique, hard-to-guess passwords for all online accounts.
- Avoid opening emails from unknown senders.
- Since identity theft isn't strictly a digital crime, you need to take steps to protect your sensitive documents at home too. Consider investing in a professionally installed monitored alarm system if you don't already have one installed. There are lots of sites out there to choose from

like SelectHomeSecurity.com and many others, so do your homework if that’s the way you want to go.

V.STEPS TO TAKE IF YOU ARE VICTIMISED

Even if you are very careful about your personal and financial information you still can become a victim. But if you are diligent about checking your banking accounts, monthly bills, and review your credit report periodically, you will detect identity theft early. Early detection makes the process of correcting accounts and credit problems much easier. The following steps should be taken immediately if you uncover that your identity has been stolen:

- Place a fraud alert. This is an important step in regaining your good name and good credit.
- If you’ve been victimized, close those accounts that have been under attack immediately.
- Review your credit/debit regularly and if you find some disputes then inform the company as soon as possible.
- Enquire your bank if you discover checking or savings account discrepancies.
- File a complaint with the Federal Trade Commission.
- File a report with your local police or the police where the identity theft took place.
- Contact the local post office if you suspect your mail has been redirected do to an identity thief submitting a change of address form.
- Contact the Social Security Administration if you suspect your Social Security Number has been used fraudulently.
- Keep account of the time of money you spent and also the amount of money you spent.

VI. THE ROLE OF TECHNOLOGY IN PREVENTING IDENTITY THEFT

In an ever evolving technological age, let’s examine the role technology plays in preventing identity theft and tips to safeguarding information stored on your computer.

- *Use of antivirus software*- Viruses can often cause your computer to send out files or other stored information.

- *Use a firewall*-A firewall can be used to limit an application’s access to your computer. Hackers can take over your computer and access the sensitive information stored on it.

- *Encryption of the files you store on your PC*-Encryption uses keys to lock and unlock data while it’s being transmitted over the Internet, so that only the intended recipient can view the data. Encryption is also used to protect email messages and attachments stored on your PC. You can verify if websites use encryption to transmit your personal information. In Internet Explorer this is done by checking the yellow lock icon on the status bar.

- *Use of authentication*-Authentication is the method used to identify you via username and password when accessing personal information on your PC or online.

- *Use of biometrics*-Biometrics is a type of authentication that uses individually unique physical attributes such as fingerprinting, iris/retina, facial structure, speech, hand geometry and written signatures.

VII. IDENTITY THEFT LEGISLATION

Law enforcement and government agencies take identity theft seriously. They recognize it as a major crime that has a long-lasting impact on the health of the economic system. Because of the seriousness of the crime, specific identity theft laws have been passed at the federal and state levels.

Federal Laws

In 1998, the Identity Theft and Assumption Deterrence Act was passed by the US Congress. Those identity theft laws made identity theft a federal crime for the first time. Under this law, anyone who is found guilty of identity theft can be sentenced to up to 15 years. Plus, depending on how the crime was committed, the criminal could be in violation of many other federal laws, including computer fraud or financial institution fraud.

In 2004, President Bush signed the Identity Theft Penalty Enhancement Act. This law amends all previous laws governing identity theft. This law defined aggravated identity theft and set punishment levels for the crimes that fit into this category. The law defines aggravated identity theft as when a person “knowingly transfers, possess, or uses, without lawful authority, a means of identification of another person” while committing certain felonies.

When someone is found guilty of aggravated identity theft, two years is added to their sentence from the original felony. If the crime has certain terroristic elements, five years is added to the original sentence. The law also allows for even stiffer penalties when someone abuses their position of power or commits the crime at their place of employment.

State Laws

In addition, each state has a set of identity theft laws. The penalties for these crimes vary greatly on a state to state basis. Some states send mixed signals when it is time for punishing an identity thief. For example, Alabama ranks identity theft as a Class C felony while trafficking in stolen identities is considered a more serious, Class B felony. While those categorizations may sound harsh, the maximum prison sentence for a Class B felony is two years and only half that for a Class C felony. In some states, the identity thief could be out on the street before the victim has even cleaned up the mess left behind.

Internet Fraud Laws

Another set of identity theft laws came in 2008 with the passing of the Identity Theft Enforcement and Restitution Act. Prior to the passing of the law, so-called cyber criminals had to cause at least $5,000 in losses before they could be prosecuted. That ridiculous requirement is gone thanks to this law. If, at minimum, ten computers were attacked, the thief can be charged with a felony under this new law.

VIII. CONCLUSION

The rise in the rate of identity theft can be associated to the fact that with progress, there are often problems. As the modernization is increasing we cannot deny the reality that more and more people are using internet for many purposes and due to which more personal information is out in the public thus making it vulnerable for identity thieves to steal. There are several steps that can be taken to protect you from being a victim. Apart from the precautions that can be taken to combat this crime, there are many laws that are dealing with victims and with criminals practicing the crime.

References

1) Howstuffworks. "How Identity Theft Works" URL: http://computer.howstuffworks.com/identity-theft.htm

2) Federal Trade Commission October 2003. URL: http://www.ftc.gov/bcp/conline/pubs/credit/idtheftmini.htm

3) Everett, Cath."Identity Theft: How You can Protect and Survive" http://www.computeractive.co.uk/feature/1156002

4) Microsoft. "Phishing Scams: 5 Ways to Help Protect Your Identity" 8 July 2004 URL:\http://www.microsoft.com/athome/security/email/phishingdosdonts.mspx

5) Identity-theft Scenario

URL: http://www.identity-theft-scenarios.com/identitytheft-punishment.html

6) The White House. "President Bush Signs the Fair and Accurate Credit Transactions Act of 2003" 4 December 2003

URL:http://www.whitehouse.gov/news/releases/2003/12/pr int/20031204-3.html

10) Fight Identity Theft. "Identity Theft Legislation" URL: http://www.fightidentitytheft.com/identity-theft-laws.html

11) The Official Identity Theft Prevention Handbook http://books.google.co.in/books?id=o1d_ILH2PukC&printsec=frontcover&dq=identity+theft+prevention&hl=en&sa=X&ei=Y8oVVK3AA8_IuASznoKYBA&ved=0CB0Q6AEwAA#v=onepage&q=identity%20theft%20prevention&f =false

12) Ways to Protect Yourself from Id Theft http://www.quora.com/What-are-good-ways-to-protect- yourself-from-identity-theft

.