# Identity theft

Identity theft refers to the stealing of another individual’s identity to gain financial advantages with their names.

## Victims of the crime

There are many victims of the crime. The victims include people with sixteen years and above; these group of individuals are in a position to earn. The thieves use the information to access one’s bank account. The identity thieves listen to victims’ conversations as they provide their bank information through a telephone. The thieves use the bank information to make false applications for loans, fraudulent bank withdrawals and acquiring particular privileges illegally.

Another group of victims of identity theft are business organizations. Hackers identify crucial information of a company and use it to attain finances illegally. Besides, business corporations have workers that are dishonest. Such workers allow unauthorized personnel to gain access to business’ financial information. Thirdly, some people fall victims to their close relatives. Most victims tend to trust those people that are close to them such as parents and siblings. They disclose their bank account details; such people use the information to open credit accounts. The internet is another factor to increased identity theft; some websites specialize in providing criminals with steps to get particular information that will help them carry out illegal activities (Bilge et al., 2009).

## Prevalence of the crime

According to studies, about nine million citizens of the United States of America are victims of identity theft annually (Bilge et al., 2009). Various behaviors defined the fraud activity. The first one is an analysis of the number of unauthorized use of credit cards. The second way is the number of cases of attempts to open new credit accounts (Bilge et al., 2009). There is an existence of consumer reporting centers that give alerts on any fraud activities in the account of clients. The high prevalence of identity thefts is those police officers are reluctant in arresting the criminals; they believe that it does not easily stop them because of the anonymity.

## Causes of the crime

There are numerous causes of identity theft. One of the causes is the opportunity that occurs when one loses their items. For instance, misplaced credit cards can lead to the identity thieves using the card to steal. The credit card will be a gateway for the thief into the crucial information such address; this will help the thief to get bank details whereby they steal finances from the bank. It, therefore, calls for care of one’s belongings to avoid theft (Romanosky, Telang & Acquisti, 2011).

Besides loss of items, mailbox can lead to identity theft. People forget to have emails that can be locked quickly in case of suspicious activities. Thieves get the personal information from emails of the victims whereby they devise ways to steal from them. The third cause is an unsecured waste; this occurs mostly when people place bank statements and receipts in the trash that is not secured. Criminals get the chance of going through the vital documents and devise ways of stealing one’s finances. Private documents need to be properly shredded to prevent the risks of theft (Romanosky, Telang & Acquisti, 2011).

Another cause is the imposters that pretend to be legitimate business individuals end up stealing victim’s private information. Victims are often lured by promising business deals from scammers. People need to be careful and avoid giving out their bank information through unsecured sources (Bilge et al., 2009).

## How victims contribute to the crime

There are numerous ways through which a person can become a victim of identity theft. Thieves use numerous strategies to steal personal information and use to the detriment of the victim. One of those strategies is becoming used to unsafe surfing. People are usually negligent of the wireless connection they use to browse the internet. At home, for example, people share internet connection with the entire neighborhood. They do not take extra steps to investigate or ascertain digital encryption and security status of the connection. With sufficient digital encryption, it is possible for the internet provider or thieves to access the contents of all computers sharing the network (Potter, 2014). Access to the computer implies that the thief can take any personal information of interest and use it as he/she pleases.

Another way victims contribute to the crime is by failing to activate firewalls and purchase reputable protective software. It is not a surprise to learn that most people run computers without installing antivirus and antispyware protection (Potter, 2014). For those who have protective programs, it is recommended that they keep updating them. However, some consider downloading of updates as time-consuming and something unnecessary. By doing so, the victims invite malicious codes to infect their devices which is an effective method of facilitating identity theft. An additional way to contribute to the crime is by opening attachments from strangers (Potter, 2014). Some people find it irresistible to open pictures, files, and links sent from unknown sources. Some of these files and links are executable and can infect computers with viruses. The viruses have the potential of collecting all information in the computer and be used to facilitate identity theft.

Stuffing wallets and handbags with numerous and important identifying cards and papers is another ideal of contributing to the crime. It is common to carry Social Security cards, insurance information, credit cards, national id, and work id with them (Cassim, 2015). However, there is a possible of losing or misplacing the documents together. If they are lost and found by malicious people, it is possible for a person to become a prey of identity theft. Lastly, victims contribute to the crime by disposing documents with valuable information in the trash without much thought. They fail to shred, burn, or store documents with sensitive information. However, thieves can through the trash looking for credit statements, tax information, and pre-approved credit offers. The information gained from documents collected in the trash or dumpsite can be used to initiate identity theft (Cassim, 2015).

## Methods of prevention

Shop on secure sites only; since online shopping offers convenience to most shoppers, it is important to be cautious not to enter personal information to unscrupulous sites. Shoppers should shop from sites that use encryption and are reputable such as Amazon.com.

Limit paper trail by shredding mails and unwanted documents; every home should have a shredder to shred items such as cancelled checks, preapproved credit card offers, bank statements, receipt for prescriptions that may contain personal information such as social security number. They should be shredded in a way that makes anyone to obtain confidential information from the trash (Elbirt, 2005).

Check credit reports regularly; it is possible for someone to open credit accounts and apply loans using stolen names and social security number. By diverting correspondence to different address, the theft can remain undetected for a long period. It is, therefore, advisable to keep checking credit reports regularly for any discrepancies (Elbirt, 2005).

Avoid revealing information to any unverified sources; whether it is through the internet or over the phone, even the slightest of personal information should not be given to distrusted sources. Regardless of the pressure to answer questions, it is always to request and insist on verifying the identity of the requesting party.

Guard wallets and purses; wallets and bags carrying vital documents should not be left in unlocked cars and in exposed places. When carrying them, they should be held tightly to the body. Also, it is important to limit the number of valuable documents carried in the wallets (Elbirt, 2005).

Protect passwords and PINS; it is important to have strong passwords for all financial accounts and banking services. Additionally, simple passwords that can be easily recovered should be avoided. Also, using the same or similar passwords to different accounts should be avoided (Elbirt, 2005).

Protect personal devices; laptops, tablets, and smartphones should be equipped with software to keep off malware, viruses, and spyware. The software protects and makes alert in case of threats to the devices and any personal information contained therein (Elbirt, 2005).

## Resources available

For those who are unfortunate and become victims of identity theft, they can use some of the established procedures to get help. They can contact the Federal Trade Commission (FTC), relevant financial institutions, and government agencies. FTC is in charge of providing information to victims handling their responses, and coordinating with law enforcement agencies and credit bureaus (OVC, 2010). Victims who believe their Tax Identification Number is insecure can also contact the Internal Revenue Service and file the necessary affidavit. Banks also have procedures for safeguarding cards and accounts of customers who believe they are victims of identity theft. Also, victims can contact the three credit bureaus and alert of the security threats.

## Opinion and conclusion

I believe 50 percent of the instances of identity theft can be prevented if victims were to be cautious of their personal information. Some people are careless in handling their information and end up exposing it to the wrong people. Regarding changes in resources, I believe the government and all other relevant institutions has put in place relevant policies and structures to help victims of identity them. As for the laws, the fines and penalties for the crime should be made more rigorous. The sentencing should also be hastened to ensure the criminals are penalized or end up in jail as soon as possible.

## References

Bilge, L., Strufe, T., Balzarotti, D., & Kirda, E. (2009, April). All your contacts are belong to us: automated identity theft attacks on social networks. In Proceedings of the 18th international conference on World wide web (pp. 551-560). ACM.

Cassim, F. (2015). Protecting personal information in the era of identity theft: just how safe is our personal information from identity thieves?. *Potchefstroom Electronic Law Journal/Potchefstroomse Elektroniese Regsblad*, *18*(2), 68. <http://dx.doi.org/10.4314/pelj.v18i2.02>

Elbirt, A. (2005). Who are you? how to protect against identity theft. *IEEE Technology And Society Magazine*, *24*(2), 5-8. http://dx.doi.org/10.1109/mtas.2005.1442375

OVC. (2017). *Expanding Services To Reach Victims of Identity Theft and Financial Fraud - Printer friendly version*. *Ovc.gov*. Retrieved 20 August 2017, from <https://www.ovc.gov/pubs/ID_theft/pfv.html>

Potter, W. (2014). *Media Literacy*. Thousand Oaks: SAGE Publications.

Romanosky, S., Telang, R., & Acquisti, A. (2011). Do data breach disclosure laws reduce identity theft?. Journal of Policy Analysis and Management, 30(2), 256-286.