Czech University of Life Sciences Prague

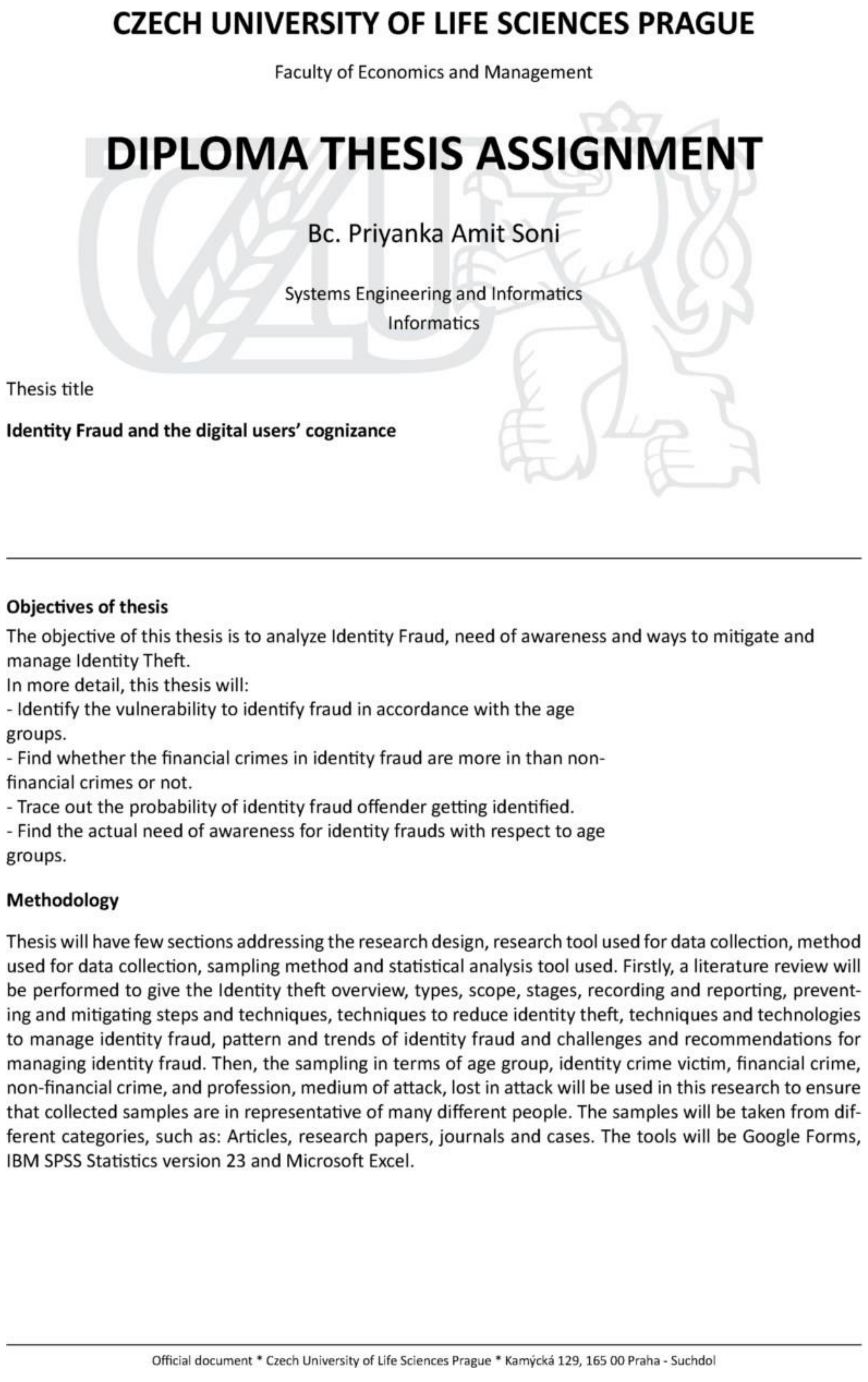
Faculty of Economics and Management

Department of Information Engineering

Diploma Thesis

Identity Fraud and Digital Gadget Users' Cognizance

Priyanka Amit Soni



CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Faculty of Economics and Management

DIPLOMA THESIS ASSIGNMENT

Bc. Priyanka Amit Soni

Systems Engineering and Informatics
Informatics

Thesis title

Identity Fraud and the digital users' cognizance

Objectives of thesis

The objective of this thesis is to analyze Identity Fraud, need of awareness and ways to mitigate and manage Identity Theft.
In more detail, this thesis will:
- Identify the vulnerability to identify fraud in accordance with the age groups.
- Find whether the financial crimes in identity fraud are more in than non-financial crimes or not.
- Trace out the probability of identity fraud offender getting identified.
- Find the actual need of awareness for identity frauds with respect to age groups.

Methodology

Thesis will have few sections addressing the research design, research tool used for data collection, method used for data collection, sampling method and statistical analysis tool used. Firstly, a literature review will be performed to give the Identity theft overview, types, scope, stages, recording and reporting, preventing and mitigating steps and techniques, techniques to reduce identity theft, techniques and technologies to manage identity fraud, pattern and trends of identity fraud and challenges and recommendations for managing identity fraud. Then, the sampling in terms of age group, identity crime victim, financial crime, non-financial crime, and profession, medium of attack, lost in attack will be used in this research to ensure that collected samples are in representative of many different people. The samples will be taken from different categories, such as: Articles, research papers, journals and cases. The tools will be Google Forms, IBM SPSS Statistics version 23 and Microsoft Excel.

The proposed extent of the thesis

60 – 100 pages

Keywords

Identity fraud, Identity Theft, Identity Theft Awareness, Cybercrime awareness

Recommended information sources

Clarke, R. V., & Eck, J. E. (2005). Crime Analysis for Problem Solvers in 60 Small Steps
Finklea, K. M. (2010). Identity Theft: Trends and Issues.
Gordon, D. R., & Willox, M. A. (2003). Identity Fraud: A Critical National and Global Threat.

Expected date of thesis defence

2020/21 WS – FEM (February 2021)

The Diploma Thesis Supervisor

doc. Ing. Vojtěch Merunka, Ph.D.

Supervising department

Department of Information Engineering

Electronic approval: 19. 11. 2020	Electronic approval: 19. 11. 2020
Ing. Martin Pelikán, Ph.D.	**Ing. Martin Pelikán, Ph.D.**
Head of department	Dean

Prague on 26. 11. 2020

Declaration

I declare that I have worked on my diploma thesis titled "Identity Fraud and Digital Gadget Users' Cognizance" by myself and I have used only the sources mentioned at the end of the thesis. As the author of the diploma thesis, I declare that the thesis does not break copyrights of any their person.

In Prague on date 30.11.2020

Signature: Priyanka Soni

Acknowledgement

This thesis would not have been possible without the contribution of the following:

Firstly, university has been a tremendous support system. The resource in terms of knowledge, exposure as well as the ambience gave me wonderful insight to devel into the topic.

I would like to express my deepest gratitude and thanks to my Thesis Supervisor doc. Ing. Vojtěch Merunka (Ph.D.), Head Of Department Ing. Martin Pelikán (Ph.D.) and Ing. Martin Pelikán (Ph.D.) for their wonderful encouragement and tremendous insights given which enriched my results. Their motivation, patience, immense knowledge and guidance have helped me during the entire research and writing of this thesis.

The largest and most effective contributor came in terms of the books available in library, which helped me quotes terms, issues, strategies, and case studies which were most apt to the relevant topic discussed. The internet, Google proved itself just next to god again. I thank my search engine to help me optimize research and study.

Last but not the least, I would like to thank my family who have always believed in me and have been always there for me.

Thank you all.

Identity Fraud and Digital Gadget Users’ Cognizance

Abstract

The present thesis aims at analyzing Identity Fraud and focuses on the aspects of awareness that the digital-devices users should have. Starting with the types of Identity Fraud, users of the various platforms on the Internet have been asked to share their experiences. Thereafter giving description of the types of offenders, scope and stages of identity theft and Recording and Reporting identity theft. The study sets out to explain how to prevent or mitigate identity crime and the challenges related to that. For this purpose, analysis has been done to target the correct people. Concerning the methodology, the study is based on a quantitative research. Therefore, a questionnaire was compiled and applied to a representative sample of

52 respondents from various backgrounds in terms of gender, age, length of their engagement with their company. In accordance with the obtained results, the conclusion to be drawn is that these days awareness related to identity fraud is very much essential and correct precautions and measures will lead to mitigate the identity fraud.

Keywords: Identity Fraud, Identity theft, Identity theft awareness, Cybercrime awareness, Types of identity theft, Digital attack, Internet crime, trends and pattern of Identity Fraud

Identifikace podvodů a povědomí uživatelů digitálních zařízeníz

Abstrakt:

Tato diplomová práce se zaměřuje na analýzu podvodů s identitou a zaměřuje se na aspekty povědomí, které by uživatelé digitálních zařízení měli mít. Počínaje typy Identity Fraud byli uživatelé různých platforem na internetu požádáni o sdílení svých zkušeností. Poté je uveden popis typů pachatelů, rozsahu a fází krádeže identity a záznamu a hlášení krádeží identity. Cílem studie je vysvětlit, jak předcházet trestné činnosti související s identitou a zmírňovat její problémy a problémy s ní spojené. Za tímto účelem byla provedena analýza zaměřená na správné lidi. Pokud jde o metodologii, je studie založena na kvantitativním výzkumu. Proto byl sestaven dotazník a aplikován na reprezentativní vzorek 52 respondentů z různých prostředí z hlediska pohlaví, věku, délky jejich spolupráce s jejich společností. V souladu se získanými výsledky je třeba učinit závěr, že v dnešní době je informovanost o podvodech s identitou velmi důležitá a správná opatření a opatření povedou ke zmírnění podvodů s identitou.

Klíčová slova: Identita Fraud, Krádež identity, Povědomí o krádeži identity, Povědomí o počítačové kriminalitě, Typy krádeží identity, Digitální útok, internetový zločin, trendy a vzorce podvodů s identitou

Table of Content

Table of Figures

List of Tables:

1. Introduction

The dawn of the Internet and computer technologies has had a substantial influence on modern societies. Information can now be obtained in a blink of an eye, and preserved on an exceptional large scale. For most professions such as businesses, academic institutions, and governments, computers are essential to do everyday tasks. Howbeit, those benefits come with challenges. New crimes have arisen, and existing ones aggravated. (Clarke R. , Information privacy on the Internet: Cyberspace invades personal space, 1998)

Many countries now struggle with the incidents of cyberspace identity theft, cyberspace identity fraud, hacking, sabotage, electronic money laundering among others. (Cradduck , 2007) For example, websites, as well as online services such as emails and chat rooms, enable cybercriminals to steal the personal data of naive users, defraud them, and lauder the proceeds.

In this age of the Internet, there has also been an intensification in the numbers and forms of computer crimes, particularly cyberspace identity fraud. This is because computers now possess telecommunication capabilities. Unlike previously when computer crimes were restricted to incidents such as trespass, and the destruction of data, identity theft can nowbe committed by re-routing web users from their intended destinations to fake websites, unbeknown to them. (Manap, Rahim, & Taji, 2015)

Over the past 35 years, cyberspace identity theft has developed and matured to carry on its own unremitting presence. Cyberspace identity theft is on the rise, according to studies, because hackers have discovered how convenient it is to conduct illegal business activities through new technologies that are applied on a daily basis. The methods used to commission cyberspace identity theft changed dramatically with the emergence of the Internet, the widespread use of credit cards, and the growing volume of e-commerce. (Schreft, 2007)

Criminals turned to new and sophisticated tactics that allowed them to function and scam thousands of people around the world; In other words, the Internet has changed the conventional essence of identity fraud to the point that the perpetrators will initiate their attacks and defraud a large group of people without physical contact with them.

There are substantial differences between the theft of identity in cyberspace and that of the real world. Another such distinction is that the methods are constantly evolving in the former case. This makes it difficult for law enforcement authorities to keep pace with them and therefore adopt appropriate procedures for investigation. Moreover, compared to its real-world counterpart, theft of identity in cyberspace can cause greater economic damage to the victim. (Newman & McNally, Identity Theft Literature Review, 2005)

Since, identity fraud is one of the major cybercrime which is usually ignored by many people around the world. Therefore, the aim of this thesis is to perform a research on a public survey to fulfill key objectives. Albeit, there are many research carried out on this topic, howbeit because of dynamic nature of identity crime only few countries such as the USA have proper yearly record of loss done by identity theft. Therefore, this research will try to get proper results of identity fraud in Czech Republic. Hence, the main focus of this research is to analyses the patterns and trends of victim and offenders, along with that, this research will also spread awareness about identity theft and how one can prevent themselves to become a victim.

1.1 Methods of Identity Frauds

The methods in which criminals start identity theft and related fraud growing and becoming more sophisticated day by day. The common methods of identity theft which are used by victimizers are listed.

- **Dumpster diving:** Looking through a target's garbage for "pre-approved" credit card offers, duplicates of old bills, loan applications, and official papers with the resident's SSN.

- **Shoulder surfing:** Eavesdropping a person give out personal information over a public telephone or cell phone, or eyeing over a person's shoulder as they fill out forms or use an ATM. To pay off employees to hand over personal customer information, and physically stealing confidential files or computer hard drives in which identity data is stored.

- S**kimming**: Attaching a data storage device to an ATM or a retail checkout terminal and stealing the credit card data or PIN numbers that was inserted.

- **Publicly available information:** Search in public and government databases and steal information about driver's licenses, real estate and other business communications, vehicle records, some types of official recognition, and licensing records. Newspaper classifieds and other private databases also provide information.

- **Mail theft:** Purling pre-approved credit card applications, insurance statements, tax information, or investment reports from person's mailboxes.

- **Changing address**: Diverting the victim's billing statements and other documents to a different location by making a change in address form.

- **Old-fashioned stealing:** Purling wallets and purses; mail, including bank statements and credit card, and new cheque or tax data. Delinquents steal personnel records or bribe employees who have access to misuse the information.

- **Retail theft:** Purling files or getting data from partner at retailers or service providers' offices by bribing them.

- **Pharming or Trojan-horse:** Many e-mails and websites have viruses attached with them. These viruses have programs that record keystrokes and obtain crucial information of victim.

- **Spoofing:** Sending a message to a computer from a fake source that pretends the message is receiving from a genuine computer's IP address. The spoofer could pretend as an ISP or even an "identity theft prevention" service provider.

- **Botnets:** A hacker can control a computer or a network of computers from an isolated location after inserting a control program into a naïve user's PC.

- **SQL Injection Attacks:** Generally recognizable information can be read and modified by SQL Injection Attack as it is the one of the most serious threats to the security of database-driven applications.

- **Pretexting:** Creating and using an invented scenario (the pretext) to engage a targeted victim in a manner that increases the chance the victim will divulge information or perform actions that would be unlikely in ordinary circumstances. It can be used to fool a business into disclosing customer information as well as by private investigators to obtain telephone records, utility records, banking records and other information directly from company service representatives. The information can then be used to establish even greater legitimacy under tougher questioning with a manager, e.g., to make account changes, get specific balances, etc.

- **Phishing:** Sending an email or a message to a victim, asking for the individual to access a web site that pretends to be a trusted body and then reveal private identity information. E-mails are sent to naive victims, asking for information and providing links to a fake website.

- **Wi-phishing:** Individuals sometimes unknowingly use wireless networks set up by hackers. This makes it easy for cybercriminals to steal passwords with other personal information.

- **Vishing:** This technique is called Vishing because it uses voice with phishing to conduct the fraud. The criminals will call, commonly with a pre-recorded message, instructing victim to call a number and give bank account or credit card information or the victim receives a typical e-mail, similar to any other traditional phishing scam. Then they asked to provide data over the phone instead of being directed to a website.

- **Smishing:** This method manipulates mobile phone operators' SMS by sending fake text messages to mobile users trying to trick them into succeeding a malicious mobile Internet link. These types of phishing traps are commonly known as Smishing. Cybercriminals are taking benefit of SMS technology by sending a messages and asking for a private bank or credit account information.

- **Typo Squatting:** They are websites with names related to genuine websites. When people make typing errors, they land on these fabricated websites. This gives cyber- criminals the chance to infect computers or to insert "bots" into them. (Tajpour, Ibrahim, & Zamani, 2013)

2. Objective and Methodology

2.1 Introduction

For any research, the methodology and objective should be sound. The objective of this thesis is to analyze Identity Fraud, need of awareness and ways to mitigate and manage Identity Theft. This chapter gives details about the research methodology for this research.

This chapter is having few sections addressing the research design, research tool used for data collection, method used for data collection, sampling method and statistical analysis tool used.

Firstly, a literature review will be performed to give the Identity theft overview, types, scope, stages, recording and reporting, preventing and mitigating steps and techniques, techniques to reduce identity theft, techniques and technologies to manage identity fraud, pattern and trends of identity fraud and challenges and recommendations for managing identity fraud.

The introduction chapter gives a brief about the Identity Crime & illustrates the methods of Identity Fraud because it is very much essential to understand the methods which is used to do it in order to prevent or mitigate the identity theft.

The sampling in terms of age group, identity crime victim, financial crime, non-financial crime, and profession, medium of attack, lost in attack will be used in this research to ensure that collected samples are in representative of many different people. The samples will be taken from all different categories. For this study research, a well-planned questionnaire was made. 52 respondents had a participation in giving their responds to the questionnaire.

2.2 Research Question:

Identity theft is very vast topic to research. There are many modern ways through identity crime can occur. Thus, the awareness on identity theft is required to control the numbers of crimes occurring every day. The motto is to reduce the vulnerability to identity theft because only awareness is the best possible way to prevent identity theft from occurring. Looking to all aspects of the identity fraud, certain questions were framed to get the optimized result of this research:

- Is there a higher probability of being attacked by Identity Fraud for Adults than Youth?
- Is identity crime majorly a financial crime or there are other non-financial targets also?
- Is there any chances of digital identity offender getting caught?
- How much is digital users' awareness required?

2.3 Data collection

Primary and secondary sources were used to collect data. Articles, research papers, journals and cases were used to collect secondary data related to identity theft. Questionnaire has helped to collect the quantitative primary data in order to get the public opinions broadly.

The google form was made and used to circulate the questionnaire to the general public from age group 12 to above 45.

A good research requires effective communication and hence every respondents had been contacted for sharing their experiences & opinions more deeply.

Due to limited time and budget, data from each kind of users was not possible for current research. So, sampling technique is used. The sample is collected from the google form questionnaire made.

2.3 Research Objectives

These are the objectives which have been taken for the study:

i) To identify the vulnerability to identity fraud in accordance with the age groups.

ii) To find whether the financial crimes in identity fraud are more in than non- financial crimes or not.

iii) To trace out the probability of identity fraud offender getting identified.

iv) To find the actual need of awareness for identity frauds with respect to age groups.

2.4 Research Hypothesis

Hypothesis: 1

H0: Adults above age 21 are being Victim of Identity theft and the proportion of it is more than Young people.

H1: Young people from age 12 to 21 are easily being victim of Identity Crime.

Hypothesis: 2

H0: Financial crimes occur more than non-financial crimes through identity theft.

H1: Non-financial crime are more in proportion as compared to financial crime in terms of identity theft.

Hypothesis: 3

H0: There is high probability of successfully tracing the digital identity fraud offender. H1:

The offender cannot be mostly traced in cases of digital identity fraud.

Hypothesis: 4

H0: Youngsters under age 21 are required more awareness for identity fraud. H1:

Adults of age 21 or above require more identity fraud awareness.

2.5 Statistical data analysis tool used

IBM SPSS Statistics version 23 and Microsoft Excel is used wherever needed for the statistical data analysis of research objectives and hypothesis made.

2.6 Significance of the study

In today's era, everyone is using smartphone and computers. As the result of these over mass using the internet, the fraudulent are increasing because they can easily target the audience. As per current scenario, everyone is using digital media but only few are aware of the results of the being victim of identity crime. If we won't take any further step, it will be difficult to handle the dark outcomes of it. This study not only shows the research of identity fraud but it also illustrates the awareness required for digital users.

3. Literature Review

3.1 Identity theft

This section covers a comprehensive review of literature on identity theft and the awareness of digital users.

3.1.1 Definition

There is no commonly accepted definition of ‘identity theft’ or ‘identity fraud’, and it's not possible to check the real threat of this development, therefore, it is necessary to delineate precisely what's meant by these terms. ‘Identity theft’ and ‘identity fraud’ are hardly defined in a precise way. Rather, it is mostly providing descriptions or working definitions. it is defined as ‘knowingly transfers or uses, without lawful authority, of a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.’ In the US Identity theft and Assumption Deterrence Act (title 18, s. 1028 (a)(7) U.S.C). (Newman & McNally, Identity Theft Literature Review, 2005)

However, ‘identity fraud’ can be considered as a broader term than ‘identity theft’. In a study by the United Kingdom Cabinet Office, this delineates functionally: ‘ID fraud arises when someone takes over a totally fictitious name or adopts the name of another person with or without their consent.’ This defines as the fraud is just an act of assuming another identity, regardless of a consequent unlawful act. (Koops & Leenes, 2006)

Identity theft isn’t one crime, however it consists of the commission of a wide variety of different crimes, several if not all of which are crimes are known to us all. The crimes with which identity fraud is commonly associated are: cheque and card fraud, monetary crimes of assorted types, various telemarketing and Internet scams (Newman & Clarke, 2002), felony of cars and auto components power-assisted by fraudulent documentation (Maxfield & Clarke, 2004), thefts or robberies of assorted types where identification information is purloined either accidentally or intentionally, counterfeiting and forgery, trafficking in human beings and act of terrorism. (Newman & McNally, Identity Theft Literature Review, 2005)

3.2 Types of Offender

- **Exploiting Weakness in Specific Technologies and Information Systems:** This type of identity theft targets a particular technology and its different attributes (magnetic strip, hologram etc.) for instance, Credit card. Here, the fraudster, using various techniques, tampers or alters credit cards which were either stolen from victims or were totally fake, however they have applied to them and obtains all the identity information from a target's financial records. Some of this information can also be used by criminals to access bank accounts, obtain credit cards, open telephone or other utility accounts, and consequently convert the information they have taken into cash. The use of individual identities from such stolen databases is subjective and wide.

- **Facilitating Other Crimes:** Document fraud are common identity related crimes that aid the commission of other crimes. An experienced identity thief will obtain a couple of key pieces of a victim's identity: e.g., a birth date and a social security number, and use these to create additional documents. The careful use of this information either over the telephone, the Internet, face to face with a bank official, or even filling in an application for credit, may assist in gaining more information, such as bank account numbers, driver's license or visas and passports. The information may be used to create new documents such as fake credit cards which may have account numbers and names of real account holders, thus making them harder to recognize. New bank accounts may be opened; new credit cards can be obtained. This is the entire way of doing business and necessary transactions to carry out further crime of a different sort.

- **Avoiding Arrest:** The offender can use another's identity to avoid arrest or detention, specifically if the victimizer already has a felonious record or if there is an arrest warrant released. Committing crimes in another person's name means that the crime squad will be looking for that person, not the true criminal.

- **Repeat Victimization:** This type of identity fraud has been the most commonly publicized. It implies a consistent and repeated attempt by the offender to use the individual's identity over and over again until the identities becomes completely useless.

- **Organized Identity Theft:** All the above mentioned types of identity frauds may be committed either by individuals or in organization. Cybercriminals who are committed to their organization generally work in groups because the sustained completion of their frauds requires more man power. In order to commit credit card fraud on a board scale, considerable expertise, experience people are required, along with an organization to make publicizing of fake credit cards possible.

At a minimum, such a gang must accomplish at least the following:

- Search for an easy target,
- locate sources of personal information for that target,
- obtain the necessary documents (legal or counterfeit) to establish legitimacy
- choose how to use the identity to obtain money,
- convince officials that one is the person named in identity documents,
- anticipate how long one can exploit the identity before the victim discovers the losses,
- Find easy ways to convert stolen identities into cash.

(Newman & McNally, Identity Theft Literature Review, 2005).

3.3 Scope of Identity fraud

As of October 2018, there are about 4.8 billion people who actively use the Internet each day. This means that more than half of the world population is at the risk of identity fraud (statista, 2018). The offenders who commit these cybercrimes are not always stereotype people. They can be anyone who knows how to use social media and other open source sites on the Internet for their benefit. Daily tons of data are posted on social media accounts or perhaps found with a Google search can lead to a cybercriminal collecting enough data to commit identity fraud. For example, according to National Cyber Security Centre one of the most common passwords consists of an individual’s pet name or birthday. This information is mostly available on social media profile, which aids identity fraud. About 2.8 billion people worldwide use social media such as Instagram, Facebook, Twitter, LinkedIn, Snapchat, or perhaps dating applications such as Tinder or Bumble, and more (statista, 2018). Moreover, according to Statista, only forty-five percent people reported that all of their social media accounts are private; meaning the other fifty-five percent have some of their accounts ‘public’, permitting anyone to see posted information (statista, 2018). Open source websites or applications such as Spokeo, White Pages, and other sites allow a cybercriminal to look up information such as phone number, location, birthday and age. This data are easily available on public websites, which can also help a criminal to gather more data on his target.

These attacks are completed by deceiving a victim in to leaks some of their personal information; this can let a hacker to steal his target's identity for their own benefit, most probably, in the financial sense. Over the past few years with 92% percent of these attacks are happening through email. These attacks are more advanced than social media searching and a Google search. Since, they may also reveal more private information, such as credit card number or bank account number. The leak of this type of date has cost users a total of 18 billion dollars in 2013.

Furthermore, the major problem with identity theft cases is that they are not reported, with only one in ten cases reported to the police (Bureau of Justice Statistics, 2014). Of these cases, under a half of a percent are solved with the criminal being imprisoned.

However, police force are overwhelmed and usually only tackle cases in which over a million dollars are stolen. Besides being underreported and unsolved, it takes an average of three months for a victim to notice that the theft is committed. An astounding sixteen percent of victims do not find out for up to 3 years. (Good, 2019)

3.4 Stages of Identity fraud

Phase 1: The identity theft process commences with a person generating a new identity, often using false identifiers or by assuming another individual’s identity (identity theft). Fake identifiers allow the procurement of a fake breeder document, such as a passport, birth certificate, driver’s license, or a SSN (Social Security Number). Internet supports fraudulent documents or ones provided by a Cybercriminals, open the doors to bonafide breeder documents. A breeder document is a single fake obtained document, such as a driver’s license, which provides the basic information necessary to forge additional fraudulent documents. Unlike documents acquired through the use of identity theft, it is impossible for a victim to become aware of and report the stolen identity. These documents are simply acquired by accessing public websites, engaging corrupt officials, and/or accessing the false document underground. Offenders use the Internet to buy and sell fraudulent identifiers, untrue documents, and fake identities.

According to the Senate Permanent Subcommittee on Investigations concluded in a report, “Phony Identification and Credentials via the Internet,” in February 2002. That, their investigation found several websites that deals with fraudulent identification documents through numerous methods, including e-mail order purchase of such documents, or free computer software that can be used by many people many times to produce or create realistic, yet false, identification.

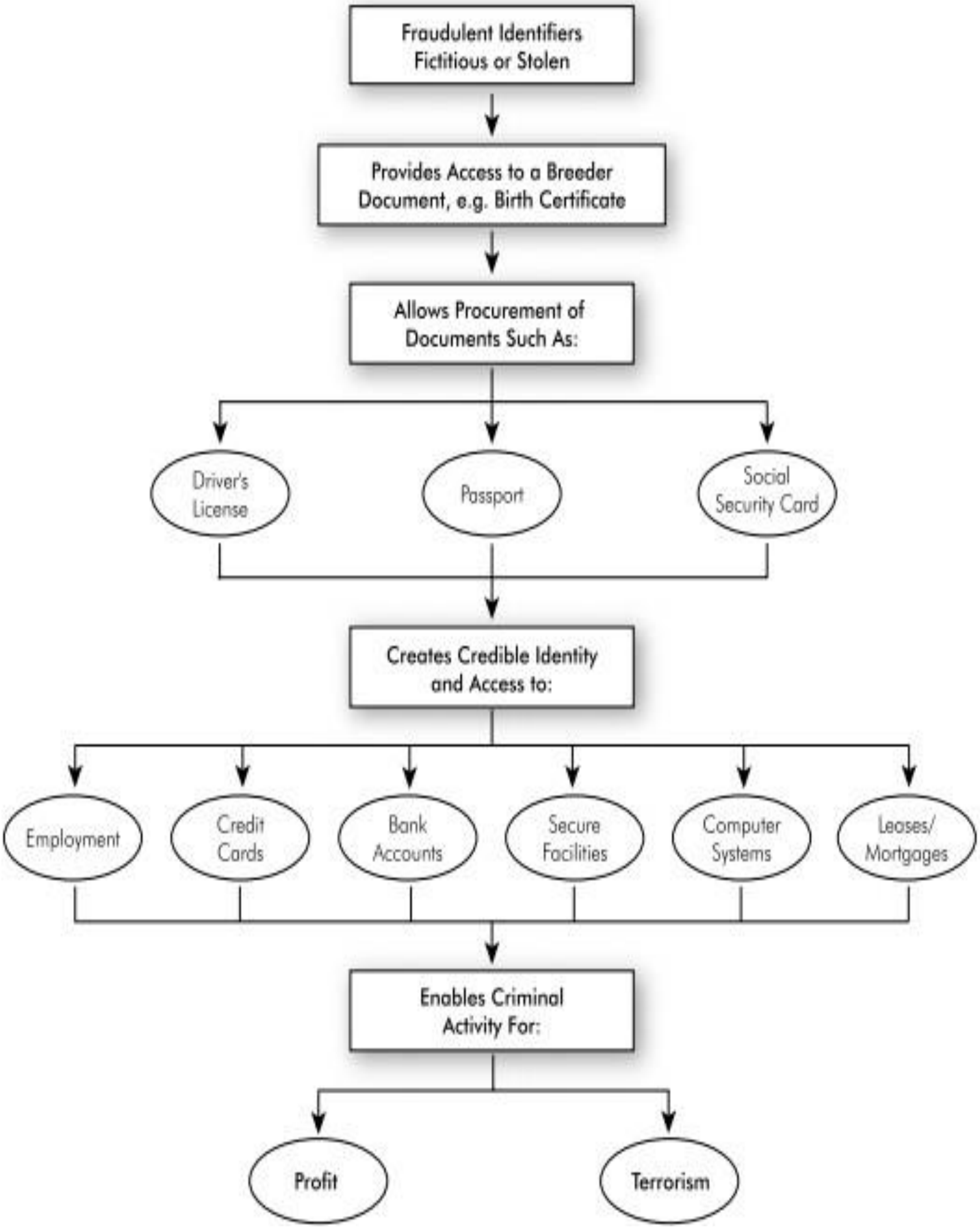

Fraudulent Identifiers Fictitious or Stolen
Provides Access to a Breeder Document, e.g. Birth Certificate
Allows Procurement of Documents Such As:
Driver's License
Passport
Social Security Card
Creates Credible Identity and Access to:
Employment
Credit Cards
Bank Accounts
Secure Facilities
Computer Systems
Leases/ Mortgages
Enables Criminal Activity For:
Profit
Terrorism

Figure 1 Identity fraud process chart [Source: Europol Annual Report, 2002]

Europol also found it true. As stated in its 2002 EU Organized Crime Report, Public Version, “There have also been significant developments in the area of computer and printer technology systems, increasing organized crime groups' capacity to produce counterfeit documentation of various types" (Europol Annual report, 2002).

- Procurement of Documents: Once an individual obtained fraudulent identifiers, they have the necessary identification to apply for fraudulent documents such as a Passport. Passport is prime verification tool all around the world for establishing age and residency, and as the quintessential photo identification. Such documents can also use to apply for a "replacement" birth certificate, Social Security card or other personal documents. Moreover, fake documents can be purchased on the "black market" by various criminals.

Phase II: Create Credible Identity and Gain Access:

Having a fake identity provides terrorists and criminals with access to numerous other elements of a credible identity – individual identifying documents, bank accounts, government titles, and many more. As these accrue, the criminals' genuine identity arduous to discern. Although they have been acquired with a bogus identity, but they seem to be real official documents. With a new identity, terrorists and criminals the can avoid detection by officials who are checking credentials, or fool systems used to detect fake documentation. At each succeeding stage of the process, the individuals build a more trustworthy identity as they collect more fraudulent documents and information is placed in a range of databases. Finally, the criminals or terrorists have obtained the documents essential to provide them access to money, secure facilities, transportation, and whatsoever is needed to commit criminal or terrorist acts for their profit or purpose such as:

- Access to Financial Institutions

- Access to Federal Entitlement Programs

- Access to Immigration Benefits Including Employment

- Access to Secure Facilities

Phase III: Using a Credible Identity to Facilitate Criminal Activity:

- Terrorism: According to the FBI's report, Terrorism in the United States 1999, terrorism is defined by the Code of Federal Regulations as "'the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives (28 C.F.R. Section 0.85)", the definition may differ, but a crucial factor in the acts of terrorism is the useof fraudulent identity to open many opportunities of infiltration and funding. In the case of the 9/11 terrorist attacks, some of the terrorists are alleged to have used fake official identification documents such as drivers' licenses, stolen credit cards, fabricated and/or provisional addresses, fake passports and other falsified travel documents, and fabricated Social Security Numbers.

- Money Laundering/Financial Crimes: Financial crimes are intent on taking money they have gained via illegal means and depositing it in a bank or other financial institution, or using it to obtaining insurance policies. When they extract the money, it seems to be coming from a genuine institution and, hence, presumed to be "clean." Once a bank account is opened with the help of fraudulent identifiers, deposits and withdrawals can easily be done. Insurance policies can be purchased and used as mutual funds. The criminals are then able to withdraw the bulk amount of the money they invested as "clean funds."

- **Drug Trafficking, Human Trafficking, and Weapons Smuggling:** Identity fraud is a vital element of human trafficking, narcotics trafficking, and weapons smuggling. According to INS, they have intercepted many fake documents, including border crossing cards or passports, alien registration cards, and many others. (Gordon & Willox, 2003)

3.5 Recording and Reporting Identity Theft:

According to Federal Trade Commission research, older persons and less educated people are expected to take long time to report identify frauds and sometime they do not even to report it at all. This research also suggests that the longer it takes to notice the crime and report it to the relevant authority, the greater will be the loss and suffering to the victim. However, to FTC's extensive database of customer complaints and victimization, the criminal justice system absences of any such data related to identity fraud. Criminal justice authorities, especially local police force, have been thwarted in recording and reporting identity theft crimes by three significant issues:

1. The difficulty of describing identity fraud because of its wide involvement in other crimes. Most police departments lack an established mechanism to record identity-fraud- related incidents as discrete crimes. This is make worse by the lack of training of police officers in recognizing and recording information regarding other crimes that also involve identity fraud.

2. The cross-jurisdictional characteristic of identity fraud, which may extent to numerous geographically distant jurisdictions. This has led to jurisdictional dilemma as to who is responsible for recording the crime.

3. Depending on the kind of identity fraud, victims probable report it to their bank, credit card distributing agency, or another financial agency rather than the police. Therefore, a genuine issue arises as to the extent to which police are the appropriate agency to deal with this type of victimization, when many financial agencies are in a better position to attend to the victim's problems and even to investigate the crimes. For this reason, police agencies have strong motivation to avoid taking on the added responsibility for dealing with these crimes. (Newman & McNally, Identity Theft - A Research Review, 2007)

3.6 Preventing or Mitigating Identity Theft from Arising

3.6.1 Simple steps to reduce vulnerability to identify theft (SCAM):

a.) Users should be stingy about revealing personal data to others except they have a reason to trust them. Adopt a need-to-know basis for revealing personal information. Keep personal documents or information printed on personal bank cheques to least possible. If someone contacts you on the internet or over telephone and offers a prize but asks for personal information, ask them to e-mail a form, and check the corporation with the

Better Business Bureau. When traveling, have e-mail held at the local post Identity fraud: the latest digital attack Volume VIII, No. 2, 2007 298 Issues in Information Systems office or have a reliable person collect the e-mail. Be careful while disposing documents that contain personal information.

b.) Check financial data as frequent as one can for irregular activity and review statements for any changes or transactions that should not be there. Bank statements and credit card accounts should arrive monthly.

c.) Request a copy of an updated credit report occasionally and review it to confirm that no anonymous accounts have been opened.

d.) Maintain careful records. Always keep monthly statements and invalid cheques or their copies for at least a year. These can be useful if you need to dispute them. (Forcht, Kieschnick, Thomas, & Shorter, 2007)

3.6.2 Prevention techniques for individuals

a.) Since criminals are able to steal personal data via the Internet, fax, regular e-mail, or telephone, one should never disclose personal data when they are not fully sure.

b.) It is suggested to carry entire identities document only when is required; otherwise should be kept in a safe place.

c.) Ask for frequent credit check reports from banks, creditors, or other financial institutions and report any anomalies to the credit bureaus.

d.) It is suggested that individuals do not let others such as cashiers to swipe their credit and debit cards.

e.) Personal identification number when using a PIN pad or an ATM should be enclosed.

f.) It is better to remember all personal ID numbers such as debit cards, and telephone calling cards and never write them on the rough papers.

g.) It is better that individuals be familiar with their credit and debit cards billing cycle and monitor them cautiously.

h.) Document shredding before disposal in trash bins is strongly recommended because garbage and trash bins are a goldmine for cybercriminals.

i.) The post office and other related financial institutions should be informed about any address modification.

Among all of these, all mail should be removed quickly from mailbox and a holiday hold when people travel is recommended (Paget, 2007). It also is suggested to review financial account balances and check into any mysterious withdraw or charges. (Hedayati, 2012)

3.6.3 The Identity Theft Red Flags Rule, issued in 2007, wants creditors and financial institutions to implement identity fraud prevention programs. It is executed pursuant to the Fair and Accurate Credit Transactions (FACT) Act of 2003 (P.L. 108-159). The FACT Act corrected the Fair Credit Reporting Act (FCRA) by directing the FTC, together with the federal banking agencies and the National Credit Union Administration, to develop Red Flags rules. These guidelines require creditors and financial institutions with covered accounts to develop and institute written identity fraud prevention programs. According to the FTC, the identity fraud prevention programs rules must provide for:

- Recognizing patterns, practices, or precise activities-known as “red flags”-that could indicate identity theft and then integrating those red flags into the identity fraud prevention program;

- Detecting those red flags that have been incorporated into the identity fraud prevention program;

- Reacting to the detection of red flags; and

- Updating the identity fraud prevention program sometimes to replicate any changes in identity fraud risks.

Possible “red flags” could include:

- Alerts, notifications, or warnings from a consumer agency;

- Doubtful documents;

- Suspicious personally identifiable information, such as a fake address;

- Rare use of-or suspicious activity relating to-a covered account; and

Notices from customers, sufferers of identity theft, law enforcement authorities, or other businesses about possible identity fraud in connection with enclosed accounts. (Finklea, 2010)

3.7 Techniques to Reduce Identity Theft

3.7.1 Increase the Effort

Target harden

- Alter proof credit cards
- Firewalls
- Alter proof ID documents
- Properly Shred utility bills etc.

3.7.2 Control access to facilities

- Proper lock mail boxes
- Card/password access to ID databases
- ID for mail forwarding

- Prohibit remote access to databases
- Limit the number of persons with access to ID databases Deflect offenders
- Require several forms of ID to obtain new ID or replacement.

Control tools/ weapons

- Control sale of ID making equipment (such as card readers, stripers, printers)
- Use tracing ID tags to track location of use and who uses machine

3.7.3 Increase the Risks

Extend protection

- Close inspection, background checks of employees with access to ID databases

Assist natural surveillance

- ATMs in well-lit spaces
- Prohibit employees to take work home
- Support whistleblowers

Reduce unrecognizability

- Photo, thumb print on ID documents, credit cards
- Require supplementary ID for on-line purchases
- Train clerks, police, officials in document verification procedures

Utilize place managers

- Reward vigilance for supervisors of employee/customer records

Strengthen formal surveillance

- Keep backup files of computer usage
- Track keystrokes of PC users
- Monitor all use of ID databases
- Cameras on ATMs, at check-out counters, shipping and mailing services, ID permitting agencies
- Background checks of employees

3.7.4 Reduce the Rewards

Cover targets

- No social security numbers(SSN) on health, school cards
- No credit card numbers on receipts
- Place ATMs so keystrokes cannot be detected or recorded

- Properly shred utility bills

Remove victim's

- Pre-paid cards for pay phones
- Smart cards that contain personal ID information
- Do not leave wallets or personal files in cars

Identify property

- Guaranteed ID authentication services (e.g. Microsoft Passport)
- Vehicle ID licensing and parts marking

Deny benefits

- Rapid notification of stolen credit card

3.7.5 Reduce Provocations

Avoid disputes

- Maintain confident management-employee relations

Reduce arousal and temptation

- Avoid public exposure of security holes and patches in software
- Do not boast of security features in software

3.7.6 Remove Excuses

Set rules

- Responsible computer use policy Post

instructions in college dorms, workplace

- Respect Privacy
- Protect our customer privacy

Alert conscience

- Hacking hurts people

Assist compliance

- Provide shredders to employees

(Clarke & Eck, 2005)

Tertiary online crime prevention

The capability of volunteer police services, as capable custodians, to punish criminals 'on the spot' demonstrates how tertiary crime prevention has developed within simulated worlds. This method of order-maintenance policing prevents reoffending by endowing cybernetic police services with extra powers. Further, computer-generated police services perform a related function to support policing in disconnected communities – a visible virtual patrol assures and secures citizen confidence, changing perception of safety (Lister & Crawford, 2004). However, these efforts to validate social control are only slightly effective at reducing instances of in-world eccentricity. While the virtual police services may be effective at reducing ordered forms of different activity and associated citizen anxieties, more regular acts of deviance remain prevalent. Groups of connected deviants are easier to identify reactivity, given their collective identity and their essential embeddedness within connected social networks. However, random acts of mischief by individuals are more problematic to detect.

Primary online crime prevention

Techniques of griefing, spoofing, and online deliberate destruction are directed by criminals' level of their technical knowledge. Hackers and cybercriminals look for vulnerable spots or loopholes in computer program that they use to gain access to protected areas, similar to Wall's (2001) categorization of Cyber trespassing. It follows that an alteration in the architecture of a simulated world to make it further complex and protected would have the advantageous result of plummeting the skills for hackers to gain access to secure areas. In most simulated worlds the architecture is updated and redrafted many times a year. While this procedure is not a straight response to the need to decrease general connected deviance, it does create a diffusion of assistance in routine and an organized way. Developments in system technology can be measured as a form of chief crime prevention. This major type of virtual world crime prevention allows for an organized eradication of deviance regardless of the level of administration. (Jewkes & Yar, 2010)

In addition, the following prevention techniques are recommended to organizations by (Paget, 2007)**, Senior Virus Research Engineer in McAfee to avoid ID theft:**

a) To engage an individual to be responsible for association security system.

b) To reduce the uncertain behavior such as sending and receiving e-mail without discretion and downloading programs through training, listing persons' responsibilities, and documenting the rules of the data system and networks.

c) To build a protected network and install secured software and hardware.

d) To accept manageable solutions for employees who are in charge to support the system.

e) To cope the institute network by documenting all activities, such as installing, testing, troubleshooting, and restoring.

f) To formalize the usage of the company's network, such as adding or deleting users.

g) To use prevention security systems to detect, block, identify, and report doubtful online activities.

h) To install trustworthy security systems, such as anti-Trojan, anti-virus, and anti- spyware on all workstations that connect to company network.

i) To update all security software frequently.

j) To modernize, reconfigure, assess, and administer corporate security system.

k) To ignore any free security system audits.

l) To protect every data backup device in organization.

m) To avoid carrying vital data and information into portable device.

n) To analyze, monitor, and control the corporation wireless network and devices.

o) To protect company's information system by limiting 10 J. Law Conflict. Resolute. Physical access to the computers.

p) To diminish the risks of replication or stealing of important data by supervising employees turnover and job flexibility.

q) To regulate information flow outside of the corporation electronic network such as presentations in conferences, interviews, responses to any questionnaires, and information exchanges in private or public. (Hedayati, 2012)

3.8 Techniques and Technologies to Manage Identity Fraud

It is obvious that focusing solely on identity fraud is inadequate, because the phenomenon is part of a much bigger and complex discussion. The identity theft problem quickly changes into several areas that impact on how organizations and persons conduct business or accomplish their mission. However gathering and matching personal identifying information presents a risk, it is key to providing customer services, maintaining a good status, ensuring trusted communications, protecting against fake applications, avoiding terrorism, and tracing sexual predators. Because personal identifier information is required to confirm or validate identity, it is precious and absolutely indispensable. Its market value makes it gradually more vulnerable to crime. It can be stolen and used for instant financial gain or as part of a consignment of identities available for sale via online websites. The challenge is to develop trusted and secure information-sharing environments that maximize the societal benefits of using this type of information and minimize the risks associated with it. (Gordon & Willox, The Ongoing Critical Threats Created by Identity Fraud: An Action Plan, 2006).

Employees with responsibilities for data content must be aware of the administration's risk, their responsibilities for keeping observance to it. Administration's risk management and assessment involve a number of technologies, including records management, business process management, enterprise ,documents management, web content management, workflow, business process management, identity management, content authentication, online record posting ,enterprise and digital rights management, and contextual information filtering. Using a combination of these technologies to develop a dynamic data access key which requires the development of enterprise policies, procedures and disciplines. These should be followed by management, together with a plan of action for when, not just if, a data break or fraud occurs. (Norm Archer, Sproule, Yuan, Guo, & Xiang, 2012)

PROFILING

As Hildebrandt and Backhouse stated in their paper that profiling is an influential, critical and worrying technology because it is possibly the only way in which great volumes of data about individual and group behavior can be extracted, whether for selfish or benign purposes" (Hildebrandt & Backhouse, 2005); profiling has prevention effects from good intelligence to detect criminal identity crime innovations; and to combat identity theft by limiting its spread or in a observing role (De, 2004). In addition, profiling is a powerful method to summarize information to be able to manage identity frauds from manydisparate IS (Information Systems) or knowledge management systems (KMS) online or offline through information sharing.

Profiling comes in various forms and interacts with information systems environments (Clarke R. , Profiling: A Hidden Challenge to the Regulation of Data Surveillance., 1993) when looking for to mitigate abuse (Straub & Nance, 1990) and other felonious acts online or offline (Casey, 2000), including identity frauds such as identity deception, identity theft, and identity fraud (Le Lievre & Jamieson, 2005). Examples of profiling in an IS context, include: social profiling (Egger, 1999); geographical profiling; user profiling (Fawcett & Provost, 1997); network profiling and intrusion detection (Dickerson & Dickerson, 2000); customer profiling (Wiedmann, K-P, Buxel, & Walsh, 2002); transactions profiling, applications profiling (Urgaonkar, Shenoy, & Roscoe, 2002); identity theft profiling (De, 2004) (Le Lievre & Jamieson, 2005); and identity fraud related criminalities, such as, terrorist profiling (Ballard, Hornik, & McKenzie, 2002), drug trafficking profiling (Batton & Kadleck, 2004) and Human trafficking profiling. Profiling methods have a large IS component from both crime and business categories in information and digital image storage for later retrieval and analysis through data sharing, data matching and data mining techniques. However, sometimes data is collected without permission or knowledge of the user e.g., CCTV, cookies, etc.

Profiling may be scientific or non-scientific (Hicks & Sales, 2006), singular or aggregative (Marx & Reichman, 1984), and proactive or reactive (Fredrickson & Siljander, 2002). Crime profiling of the offender or criminal follows the methodology of structured (above average traits e.g., intelligent quotient (IQ), competent) or random i.e., below average IQ, inadequate (Petherick, 2006). Profiling techniques can also be aided by machine learning programs, can be classified as supervised or unsupervised. Scientific modeling of profiling should distinguish itself from non-scientific models of profiling as per “scientific standards: development of a theory about profiling (e.g., criminal); hypothesis generation; operationalization approaches used in profiling; and empirical authentication, including a consideration of both disconfirming indication and the limitations of the subsidiary research” (Hicks & Sales, 2006)

As a technical method according to Gallo, “profiling can be seen as pattern recognition through analytically collecting, organizing and analyzing information composed by observation or measurement, drawing conclusions in evaluating criminal suspicion, and sharing information with other people where there are no privacy boundaries or other legal impediments. The procedure used in this method should be objective or free from personal and emotion bias. Which will increase its objectivity and allows a expert to check the data, as required” (Gallo, 2003). However, according to Turvey “a criminal profile is more of a sophisticated surmise or a non-scientific opinion” (Turvey, 2000). When detectives use profiling to try and solve crimes that have already occurred they are being reactive. Active profiling involves attempts to hinder and stop crime even before it happens, and has been defined as, "to make decisions about another, relative to similar criminal activity, based on a number of obvious and subtle factors which may or may not include things such as a person's manner of dress, race, and grooming, social characteristics, geographical characteristics the observation is complete, the conditions under which the observation is made, and relative to information the law enforcement may already possess"
(Rodger, Donald, Greg, & Stephen, 2008)

3.9 Pattern and Trends of Identity Fraud

The objective of this BJA-funded project is to identify trends and patterns in identity theft so that departments of public law enforcement and private sector security will have additional knowledge to apply to a proactive means of countering this nefarious crime. Although reports and anecdotes on identity theft victims exist, less research has been done on the trends and patterns of crime, the profiles of perpetrators, and the tactics used by individual suspects, as well as on organized crime. Societal perceptions of identity crimes are based on a combination of well-known cases, broadcast vignettes depicting the victims ' unfortunate experiences of the victims, press commercials warn against actions that could precipitate victimization and, quite often, word-of-mouth. Such research can have a powerful impact on how evidence is synthesized by the general public and draws conclusions about the real level of danger that the crime presents to them. In other words, hypotheses become reality.

While "identity fraud" was apt to be met with curiosity and some confusion no less than a decade ago, it has become one of the 21st century's most recognizable terms of crime. Nevertheless, questions remain as to what it really represents, what type of person is most likely to commit this crime, what criminal techniques are most commonly employed (and successfully) and who is most at risk of being victimized. Such questions must be resolved through an "empirical" approach, rooted in a comprehensive analysis of the data of the criminal justice system, in order to contain and deter identity theft. (Gordon, Rebovich, Choo, & Gordon, 2007).

For all payment clients, money theft is costly and has economic costs that impact all members of society. The theft of identification also occurs in payment theft, which is made possible because a counterfeit transaction is not detected by the authorizing process. Until closely examining how payment smart cards can improve payment authorization protection, it is useful to consider some basic issues such as, what are the consequences and distribution of payment fraud? How is data theft-related fraud payments? And what is the intention of approving payment and how does it work?

The costs of payments fraud

It is difficult to pin down the precise costs of transaction theft because the expense data is not consistently reliable. However, according to a study of Kansas City in 2008 37 data from the 36 Federal Reserve Bank helps show the extent of the situation and who bears the costs. Apparently, other members of society cover the risks. Banks, retailers, and customers are responsible for damages from payment theft. Bank losses total approximately $2.89 billion annually (Table 1, panel A).

1.) The largest proportion of bank losses is on credit cards, followed by losses on checks, debit cards, and ACH payments. Fraud losses for retail retailers average about $15.6 billion per year, with most damages due to bad checks.

2.) Reflecting the growing popularity of internet retailing, credit card fraud losses on websites are now higher than those at brick-and-mortar sites.3 ultimately, in 2007, out-of-pocket costs for identity theft users are reported at $5.6 billion.

The huge cost of preventing payment fraud and meeting regulatory and network security standards is similar to the estimates of actual fraud-related losses (Table 1, panel B). Banks invested an additional $3.1 billion in 2006 to stop theft in transactions, while consumer investment may have exceeded $5.0 billion. Various card services (Visa, MasterCard, Discover, American Express, and JCB) have recently formalized and revised their security standards for merchants and service providers that accept or handle payment card payments. Such guidelines, known as the Data Security Guidelines of the Payment Card Industry (PCI DSS), began a staggered implementation process in 2005. There have been significant costs for retailers to follow PCI DSS requirements, with estimates ranging from $2.6 billion to
$5.5 billion in 2006.

Indirect money fraud risks include local and national law enforcement costs, obstacles to online trade and its advantages, barriers to electronic payment acceptance and its efficiencies, and possible loss of trust in payments. For example, many shoppers are wary about sharing personal information and prefer not to shop on the Internet. Another estimate indicates that if shoppers were not afraid of sharing personal or credit card information, the share of customers shopping on the Internet, currently estimated at 66 percent, would grow to 73 percent. Likewise, because of privacy and security issues, many users shun electronic payments. Unless customers had less worry about electronic payment reliability, the ongoing transition away from less effective check payments would be smoother.

Therefore, direct payment fraud costs are spread across banks, merchants, consumers, and others, while additional costs, such as failure to get the full benefits of internet retailing and electronic transaction, affect the economy as a whole. But money theft is not recent and over time society has sought to reduce costs. (Sullivan, 2008)

iDefense research has detected a different type of phishing attack; one that does not redirect the user to complicated website mock-ups like most phishing schemes produced to date. Rather, this new technique helps the attacker to explicitly insert HTML into the client of the victim through a form of Trojan phishing horse. These attackers threaten customers of different European banks, create web pages designed to look just like the website of a real bank, and insert HTML code for extracting login credentials such as username and password directly from the browser of the victim. When active, the perpetrator logs into the official banking site of the victim using the compromised login credentials and moves money from the account and into other bank accounts of third parties. Then, naive "money mules" accomplice steal the cash for payment, possibly to the cyber criminals who unleash the assaults. (da Silva, de Oliveira Nascimento, & Alves Nascimento, 2008)

3.10 Challenges and recommendations for managing identity fraud

When companies are rapidly expanding their services and data through departmental, corporate, and even jurisdictional boundaries they must be assured that they can recognize and validate the clients, enterprises, staff, and third parties that use them. Current identity protection methods, such as documents are clearly not working in the virtual world, yet there is no passport or photo-id counterpart online to date. Rather than, each corporation and sometimes even individual programs within organizations have developed a variety of content management practices, such as passwords or questions of "shared secret."

Even so, as data and services integration progresses, IT managers are struggling with more holistic and standardized identity and authentication approaches that could optimize access to various services and allow organizations to collaborate and cooperate to deliver services across global organizational boundaries. In fact, as all companies have to deal with identity theft and fraud, administrators are constantly challenged to enforce policies to keep identity information safe and confidential. (Smith & McKeen, 2011)

It is necessary to explore and assess the revolving, repetitive, non-sequential relationships between all the phases of the Fraud Management Lifecycle in order to establish an understanding of how the components of the lifecycle affect each other. In an evolving world, the direction of innovation within fraud detection is towards increased complexity and speed of transition. The challenge for professional fraud management is to effectively manage the evolution. Fundamental systemic changes are needed to sustain a fraud detection system that can adjust fraud prevention, consumer effect, capital demands, and IT budgets rapidly and efficiently. The interaction of the stages in the Fraud Prevention Lifecycle demonstrates the network design's stability and adaptability. (Wilhelm, 2004)

Likewise, there are ample of practical barriers to apprehending criminals to prosecute them even if laws are in place to prosecute them. Those involved in identity theft have highly sophisticated technological ways to obscure their actual identities and avoid detection, especially if they live in a different jurisdiction. Documentation is often difficult to obtain and collate, and financial considerations can potentially make it impossible to continue the inquiry. This will be compounded if an individual has to be extradited from another country. This is not only expensive, it is also difficult to obtain support from foreign authorities. If the extradition is effective, the legal issue is to decide the legislation is relevant in a case. Even if these challenges are resolved, the difficulty is to deliver highly complex and technological facts to juries of lay people who may have limited understanding of information technology and how it is used to perpetrate the sophisticated offenses under investigation. Judges presiding over the trials also need to understand the technology involved. (Sampford, Dixon, & Giskes, 2005)

3.10.1 Challenges to Managing Identity Fraud

Easy Access to False Identifiers

The unlimited abundance of blogs, guides, websites, and mail-order businesses that allow individuals and organizations to build or steal identities. Many of the rules and regulations enacted focused on restricting access to information and criminalizing such behavior. The results of these measures were difficult to measure, but as a result, the issue of identity fraud does not seem to have subsided. While the public was made more aware of the risk of stolen their identities and thus began to take steps against it, identity fraud is not the same.

Limited Data Analysis and Research

The general capacity to address incisive questions about the pervasiveness of identity fraud in the society is severely impaired by the absence of a credible, structured and equitable reporting system that accurately reflects all identity fraud identified and observed, cutting through enforcement agencies at each government level. Such a system would allow access to information for government agencies and private firms to identify trends such as the use of identity fraud as a cause for other crimes. While parts of the puzzle from a variety of such organizations have been assembled, it remains divided and inconsistent. Federal agencies, private organizations, and corporations use different identity fraud metrics and do not work together to present a common image, while state and local authorities do not typically compile and/or disclose the identity fraud cases they have worked with. Without reliable, correct, and shared knowledge on identity fraud cases, it will continue to impede the creation of a systemic mechanism that allows more research in this area.

Limitations on Information Sharing

Data on identity information can be accessed from different sources, including business, residential, governmental and international equivalents. Commercial data includes credit reports that can be purchased for use. Companies like LexisNexis and Acxiom, which provide government and business database tools, also have commercially available records. Private information data includes documents kept by businesses and mortgages and credit cards that are not commercially available and are protected by laws and regulations. Government information includes public records such as certificates of birth and death and business records, which is available for a minimal fee and often without restriction.

For most of the part, these sources do not share with each other their data or use the data of each other to create a composite or full picture of a personal or business record. Even within sectors such as insurance companies, credit card companies, and the similar, information sharing is restricted due to competition, legal and regulatory prohibitions, and the lack of a secure system to encourage communication. There must be greater sharing between these entities in order to control criminal and terrorist activities. To this purpose, legislation, laws and regulations need to be clearly formulated, structured, and controlled in order to ensure enforcement. Moreover, a methodology and technology that would allow each unit to grant information requests from the others without provide an entire data set would inspire these groups to cooperate.

Privacy and Information Security

Government or commercial use of an evidence-based authentication system to mitigate the possibility of identity fraud involves consideration of the privacy rights of the individual whose information is being used. This is not a recent concern as confirmation in legislation such as the 1974 Privacy Act and the Equal Credit Reporting Act, which was first enacted in 1975. Recently, the GrammLeach Bliley Act and the Health Insurance Portability and Accountability Act regulations outline how important social and economic interests, such as fraud prevention and law enforcement, can be balanced with the interests of personal privacy, even when personal information is very sensitive.

Domestic and Global Policy

As mentioned previously, the main focus of U.S.A and international law on identity theft and identity fraud has been criminalizing identity misuse and imposing stricter privacy and security standards on the use of personally identifiable information. Even when specific legislation has supported identity verification, it has been biometric and credential-based, thus failing to recognize the need for information-based identity authentication approaches, with limited exceptions such as Section 326 of the USA PATRIOT ACT.

As the Federal Trade Commission's recent report "Review of the Identity Theft System" shows sadly, it is clear that the issue of identity theft and the problem of identity fraud persist practically unabated by natural extension. To quote Assistant Treasury Secretary Wayne Abernathy, we need to bring more knowledge into the hands of those agencies that need it about the names of the people who are seeking to do business with an agency than an identity thief would have (Speech delivered to the 2003 Banking Institute of University of North Carolina School of Law’s Center for Banking and Finance, 2003). This is definitely the case when the person is new to the organization and no biometric or token-based solutions are available or effective for authenticating the person. The new or original interaction process is often referred to as "registration."

Dedicated Resources

Identity fraud was not a high priority of government or the private sector until the events of 9/11. As the issue continues to grow and the awareness of its insidious nature has been raised, a higher emphasis has been given to finding solutions to it and more efforts have been made to reduce it. Successfully solving this issue would require substantial monetary investment to fund research to quantify and understand the problem, build a structured identity fraud reporting system, create a trustworthy information sharing atmosphere, promote the research and development needed to create a trusted identity fraud authentication system, buy and implement this innovative technology, hire new personnel, and train the staff.

Leadership

There have been a number of decent efforts being made to reduce the impact of identity theft, but they need to be brought together. This is inhibited by a lack of strong central leadership. Fraud of identity has become a national and global problem. The government must play a key role in providing guidance to help solve it once an issue has grown to that level. The need for a common platform through which problems can be addressed is implicit in that leadership.

3.10.2 Recommendations

Proposing a comprehensive national and international strategy to combat identity fraud in order to meet these challenges. The guidelines given are meant to provide the basis forsuch a strategy to be created. Governance and support at the high level of the federal government are necessary for this plan. In order to implement the plan, the federal government must make a commitment of both leadership and finances. The elements of the program would work together to provide the evidence, statistical analysis, a trusting environment, laws and regulations, and research and development needed to manage identity fraud by making fake documentation useless and facilitating reliable identity evaluation while improving privacy protection.

Comprehensive recommendations for national and global strategies

a) Gain a commitment from the federal government's highest levels to implement and finance a nationwide strategy to fight identity fraud.

b) Establish a central incident identity fraud database of information.

c) Establish a research agenda for national identity theft.

d) Establish more complex networks for the exchange of domestic and global intelligence.

e) To establish best practices to counter identity fraud, conduct a study of current domestic and global policies, rules, and regulations.

f) Improve the security of personal privacy and possession of records.

g) Develop mechanisms for sharing information that develop identities verification solutions while protecting confidentiality.

(Gordon G. R., Willox, Rebovich, Regan, & Gordon, 2004)

4. Practical Part

4.1 Introduction

Primary and Secondary data is used to conduct this study. Secondary data was collected from the Evaluation report on the 7th round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating cybercrime", a report on the Czech Republic by council of the European Union. Moreover, primary data was collected through the online questionnaire form and it was then analyzed using the help of IBM SPSS statistics version 23 for different tests. And, excel software is widely used to generate tables and graphs for interpretation.

4.2 Objective-1

To identify the vulnerability to identity fraud in accordance with the age groups.

This objective answers the research question “Is there a higher probability of being attacked by Identity Fraud for Adults than Youth?” It is related to question 1 and question 8 in the questionnaire which was presented by Charts and GGraph in figure 2, figure 3 and figure 4.

According to figure 2**,** research question 1 examined the age of the respondents for the Identity Theft survey. The age group of 21 and below is considered as young age. And the age group above 21 is considered as Adult age. In figure 2, the conclusion can be drawn that the majority respondents are adults.

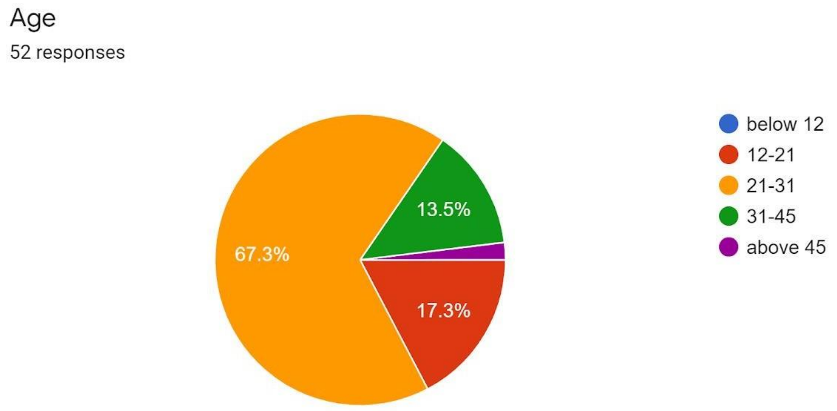


Figure 2 Age group of the respondents [Source: Primary Data collected by the author of this thesis]

As question 8 in the questionnaire is Yes or No choice question, there are 15.7% Identity crime victims found whose account had been misused or attempted to misuse at least once.
84.3 percent of the respondents never ever felt being attacked by Identity crime offenders. This proportion is illustrated in figure 3.

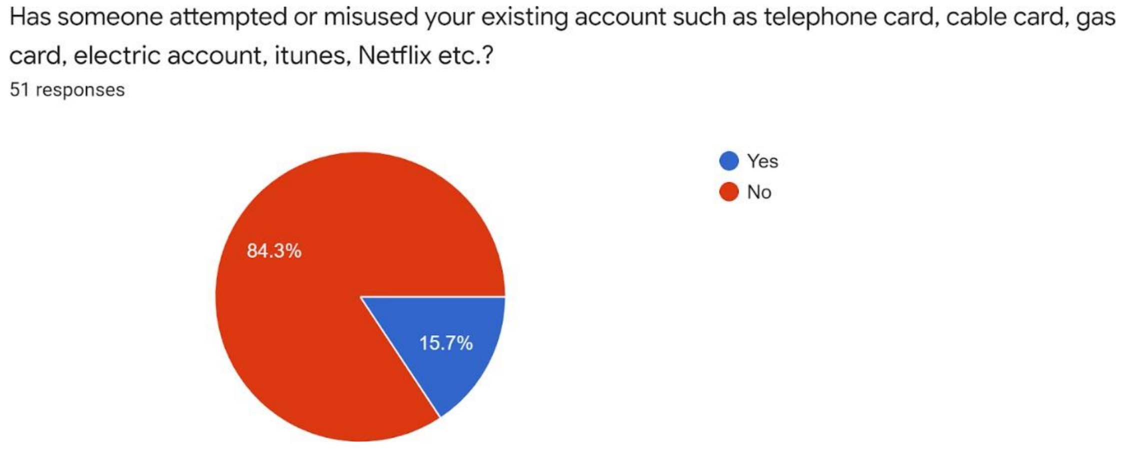


Figure 3 Proportion of identity fraud victim in the cases of offender attempted or misused existing account [Source: Primary data collected by the author of this thesis]

Hypothesis: 1

H0**:** Adults above age 21 are being Victim of Identity theft and the proportion of it is more than Young people.

H1**:** Young people from age 12 to 21 are easily being victim of Identity Crime.

SPSS Data testing:

In the following part, there are test results of how vulnerable the Identity Theft victims are, according to their age. The GGraph on figure 4 demonstrates the graphical representation of Identity crime victims according to their age groups. Where vertical dimension "0" means that they had never experienced or faced identity fraud and "1" means that they have at least once faced or experienced identity fraud.

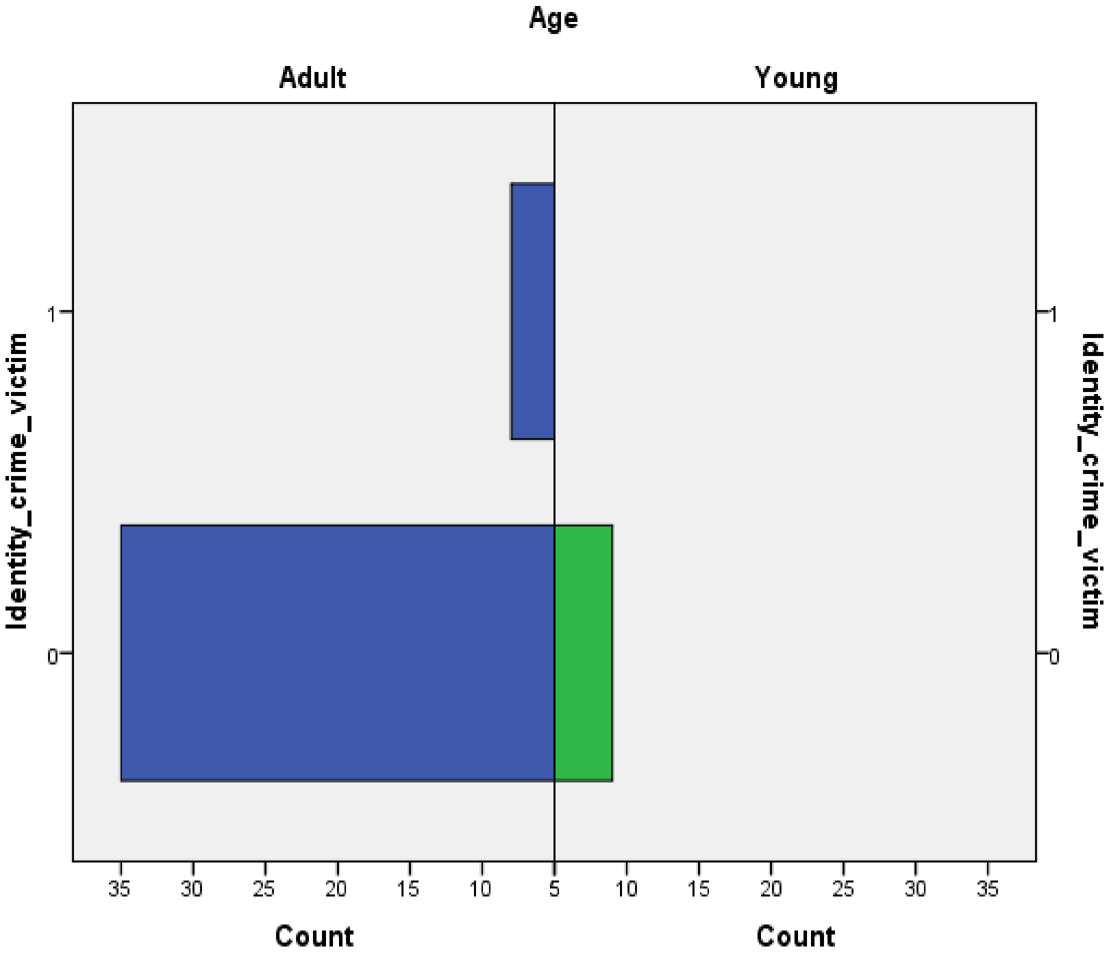


Figure 4 GGraph of the identity crime victim with respect to their age group [Source: SPSS GGraph derived by the author of this thesis from the Primary Data

		B	S.E.	Wald	df	Sig.	Exp(B)
Step 1[a]	Identity_crime_victim	-19.845	14210.361	.000	1	.999	.000
	Constant	-1.358	.374	13.205	1	.000	.257

Table 1 Significance of identity crime victim over age groups [Source: SPSS - table of Significance value derived by the author of this thesis from the Primary Data using regression test]

Interpretation: As per the table 1**,** it was revealed that the significance level is greater than 0.05, hence the null hypothesis was found to be accepted and hence alternative hypothesis was rejected. Thus, it was interpreted that adults of age more than 21 are having higher probability of being attacked by Identity fraud offenders than young fraternity. That means adults should be targeted more for Identity Theft awareness.

4.3 Objective-2

To find whether the financial crimes in identity fraud are more in proportion than non-financial crimes or not.

This objective answers the research question "Is identity crime majorly a financial crime or there are other non-financial targets also?" It was related to question 4, question 5, question 6, question 7, question 8 and question 9 from the questionnaire.

According to the graph of question 4 in the questionnaire which is a Yes or No choice question, 92.3% of individual have their own debit or credit card. Hence, it can be seen that majority of persons have their personal card. A graphical representation of it is illustrated in figure 5.

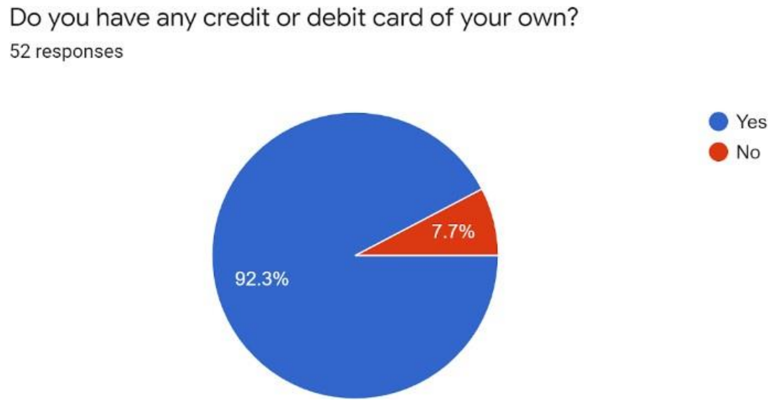


Figure 5 Proportion of credit or debit card owners [Source: Primary Data collected by the author of this thesis]

From question 5 pie chart in figure 6, it is vividly seen that, out of 51 respondents 84.3% of the respondents found that someone misused or attempted to misuse their existing card. Thus, it concludes that the financial Identity crime is more prevalent.

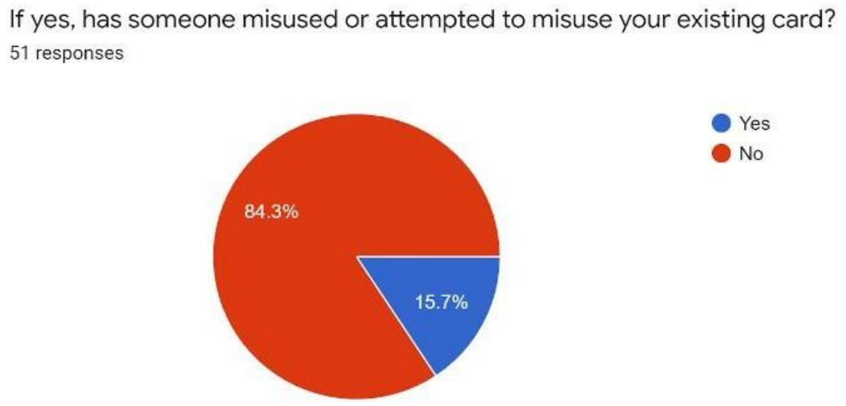
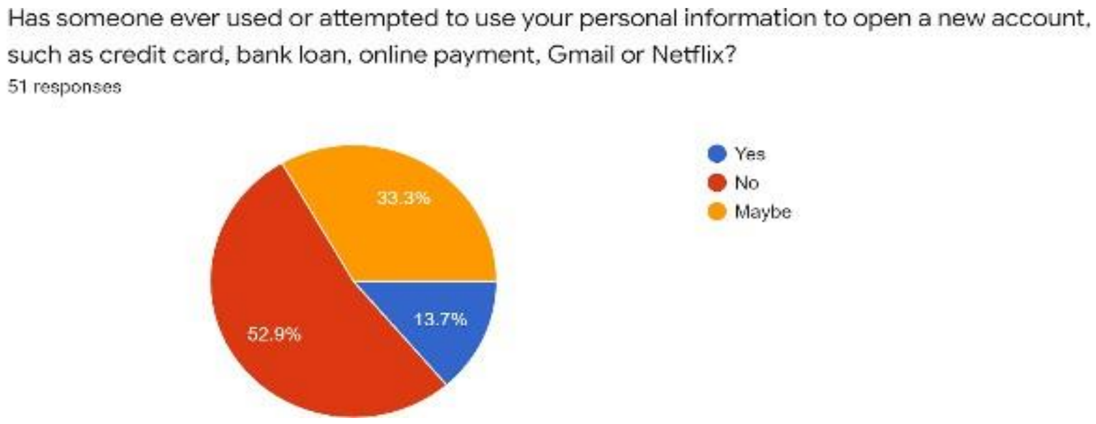


Figure 6 Proportion of victims of credit or debit card frauds [Source: Primary Data collected by the author of this thesis]

From question number 6 of questionnaire, a pie chart was made from the data. From that chart in figure 7, it can be observed that only 13.7% of responded has reported that someone used of attempted to use their personal information to open a new bank account or social media account or tried to obtain credit or debit card and made some kind of online payment. However, more than half of individuals did not experience something like this. Although, one-third of responded are in dilemma whether it is happened to them or not.



Has someone ever used or attempted to use your personal information to open a new account, such as credit card, bank loan, online payment, Gmail or Netflix?

51 responses

Figure 7 Proportion of identity fraud victim in the cases of offender attempted or misused personal information to open a new account [Source: Primary Data collected by the author of this thesis]

From question 7 pie chart in figure 8, it is clearly seen that, out of 22 respondents Majority of the individuals reported that their personal information has been used to open fake accounts, seemingly 36.4% for social media, 31.8% for Gmail and 9.1% for Netflix and Amazon Prime accounts. This type of identity crime come under non-financial crime. However, there are some respondents who reported credit card, Bank loan and online payment crime which are financial crime.

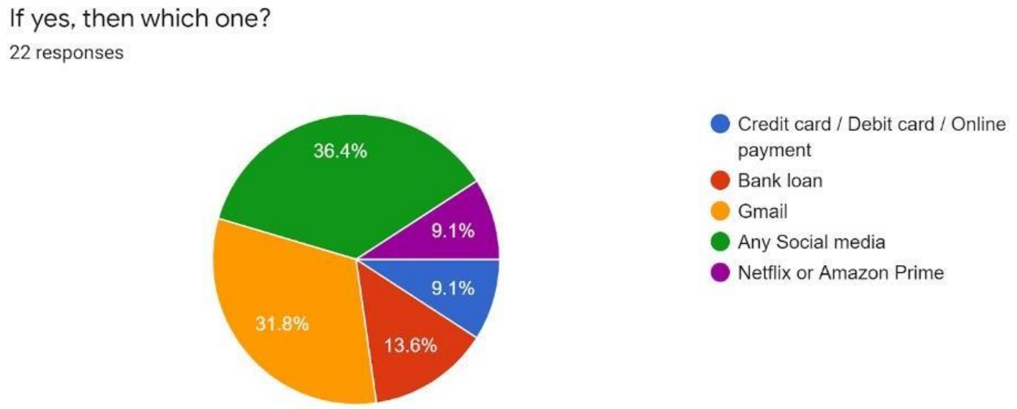


Figure 8 Platform from which victim experienced identity fraud to create a new account [Source: Primary Data collected by the author of this thesis]

Hypothesis: 2

H0 – Financial crimes occur more than non-financial crimes through identity theft.

H1 – Non-financial crime are more in proportion as compared to financial crime in terms of identity theft.

Data Analysis:

As per the certain data of if someone has used or attempted to use the personal information for opening new account, a table was made which is illustrated in table 2.

Personal Information used for	Financial crime
Any Social media	No
Credit card / Debit card / Online payment	Yes
Gmail	No
Gmail	No
Bank loan	Yes
Bank loan	Yes
Bank loan	Yes

Table 2 Table of identification of financial crime or non-financial crime from the certain data of victims of personal information being misused or attempted to misuse for opening new account
[Source: Primary Data collected and interpreted by the author of this thesis]

By further interpreting this table, following information & bar graph was achieved shown in table 3 & figure 9.

Financial crime	Count of Financial crime
No	3
Yes	4

Table 3 Table of Count of financial crime and non-financial crime by opening new account [Source: Primary data analyzed by the author of this thesis]

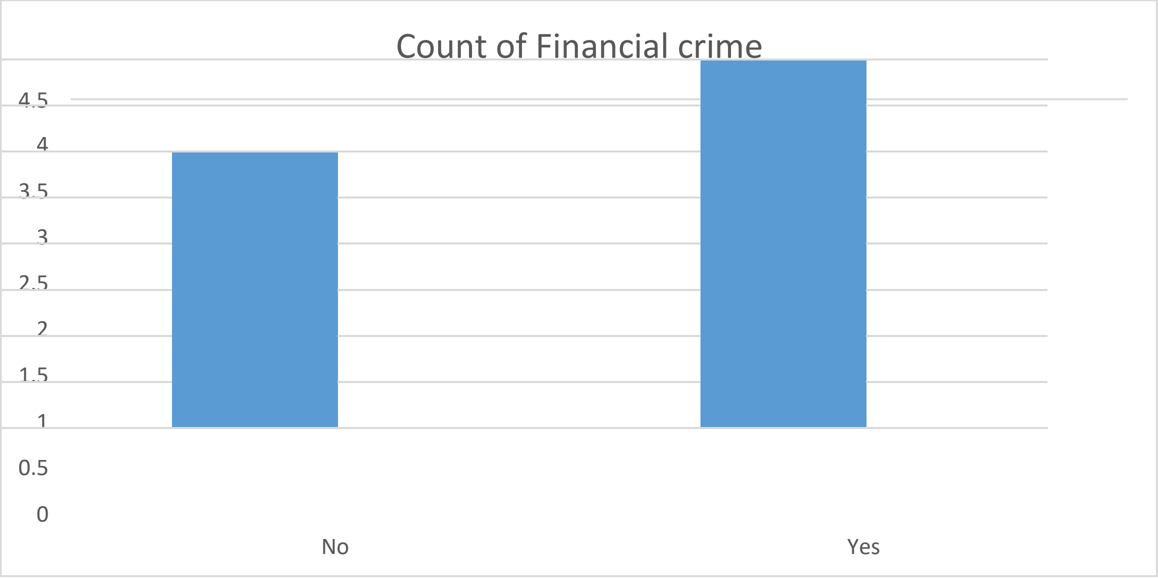


Figure 9 Graphical representation of Count of financial crime and non-financial crime by opening new account [Source: Primary Data analyzed by the author of this thesis]

As per above table 3 & figure 9, it is concluded that personal information used to create new account for financial crime is higher than personal information used for non-financial crime.

Similarly, taking out the information of the account being misused or being attempted to misuse, the following information was get illustrated in the table 4

Misused existing account of	Financial crime
Netflix/Amazon Prime/iTunes	No
Netflix/Amazon Prime/iTunes	No
Online Payment/Credit card/Debit Card	Yes
Netflix/Amazon Prime/iTunes	No
Online Payment/Credit card/Debit Card	Yes
Online Payment/Credit card/Debit Card	Yes
Online Payment/Credit card/Debit Card	Yes
Netflix/Amazon Prime/iTunes	No

Table 4 Table of identification of financial crime or non-financial crime from the certain data of victims of personal information being misused or attempted to misuse of existing account [Source: Primary Data collected and interpreted by the author of this thesis]

Further interpretation of this table is shown in the table 5 & figure 10 below.

Financial crime	Count of Financial crime
No	4
Yes	4

Table 5 Table of Count of financial crime and non-financial crime by misusing existing account [Source: Primary data analyzed by the author of this thesis]

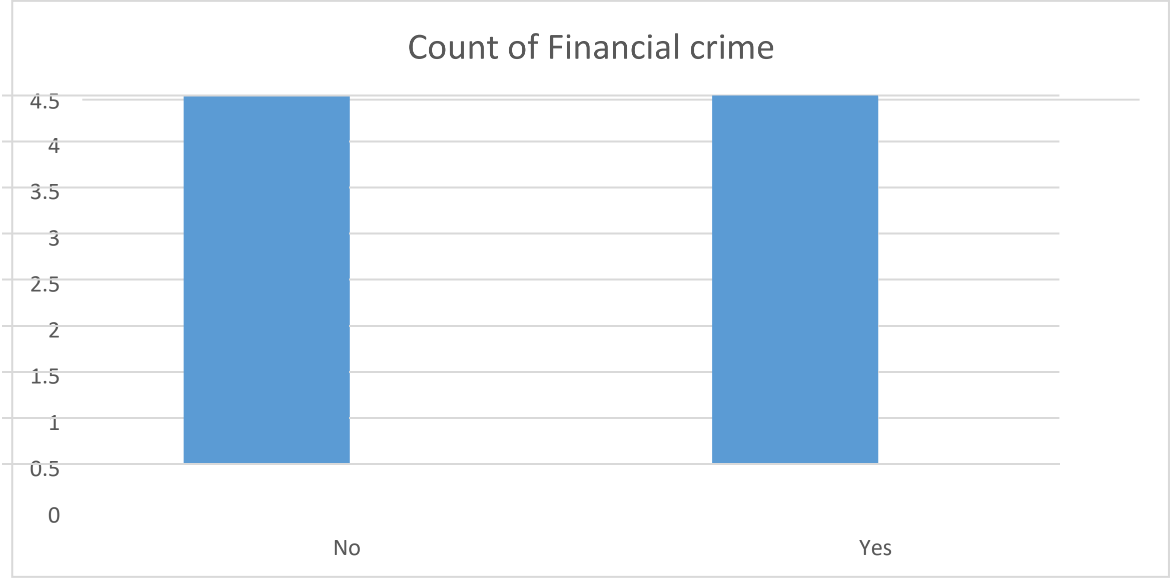


Figure 10 Graphical representation of Count of financial crime and non-financial crime by misusing existing account [Source: Primary data analyzed by the author of this thesis]

As per above table 5 & figure 10, it is concluded that personal information used to misuse existing account for financial crime and non-financial crime are same in proportion.

Interpretation: As per table 4 and table 5 it was revealed that the count of financial crime is higher than non-financial crime, hence the null hypothesis was found to be accepted and hence alternative hypothesis was rejected. Thus, it was interpreted that proportion of financial crime over non-financial crime is higher. That means one should be more aware about their personal information while dealing with digital process which includes financial transaction or information.

However, there is not much difference between the numbers of financial crimes and non- financial crimes. So, focus on both the possibilities should be encouraged equally.

4.4 Objective-3

To analyze about the probability of identity fraud offender getting identified or caught.

This objective answers the research question "Is there any chances of digital identity offender getting caught?" and it was related to question 10, question 11, question 12 and question 13 in the questionnaire.

According to the pie chart of question number 10, 72.4% of respondent's experience identity theft once in two years whereas, 24.1% have experience multiple identity theft in past 2 years. The chart is represented in figure 11.

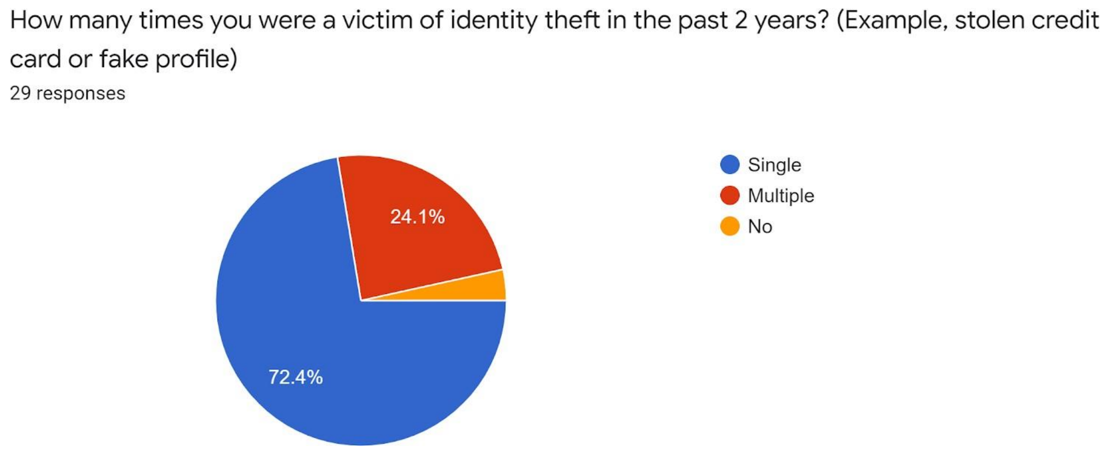

How many times you were a victim of identity theft in the past 2 years? (Example, stolen credit card or fake profile)
29 responses

Figure 11 Pie chart of how many times a victim faced identity fraud [Source: Primary Data collected by the author of this thesis]

The realization of identity fraud is very important and according to question number 11 from questionnaire 48.1% of participants find out that someone misused their card or personal information by others. Whereas, 51.9% out of 27 respondents found it by themselves. The pie chart of it is shown in figure 12.

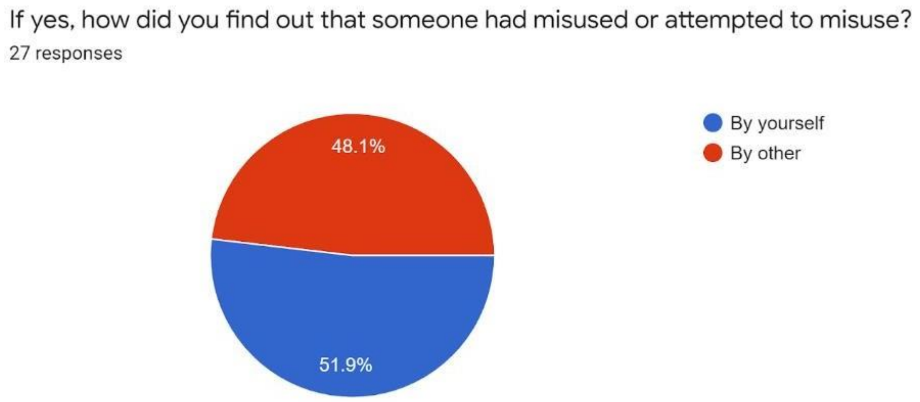

If yes, how did you find out that someone had misused or attempted to misuse?
27 responses

Figure 12 a pie-chart of identity fraud victim found out of being a victim by own self or by other [Source: Primary Data collected by the author of this thesis]

As the data from question 12 shows that, in most of the identity fraud cases victim discovered within a week that their personal information has been misused by cyber criminals. Whereas, in worst case scenario in 19.2% cases victim was unable to discover that his personal information has been misused for more than a year. The below figure 13 depicts the pie chart of it.

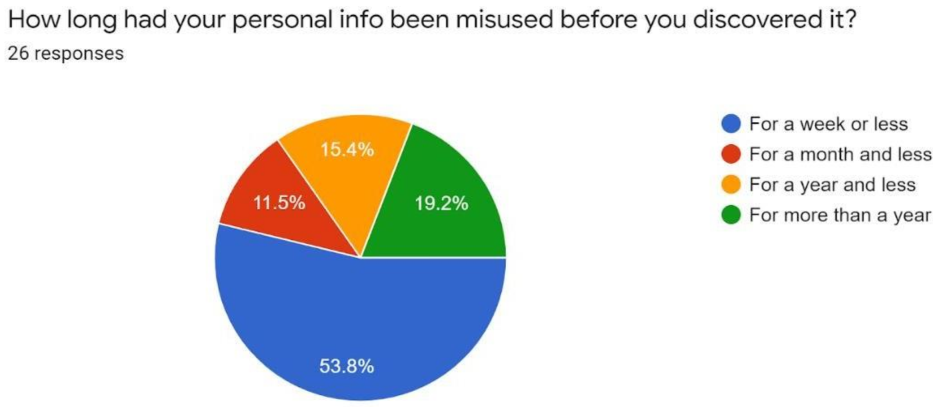
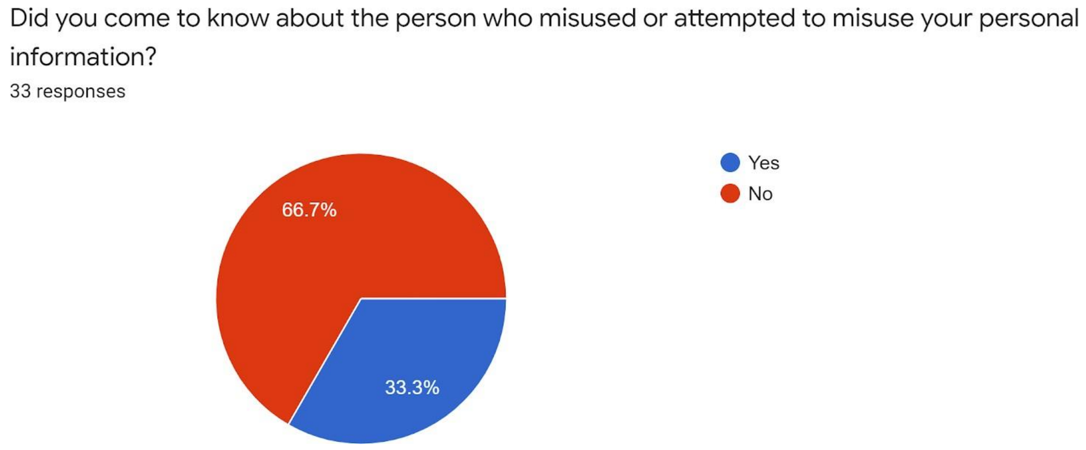


Figure 13 A representation of the time duration of personal information been misused
[Source: Primary Data collected by the author of this thesis]

As per the data of question 13, only 33.3 percent of the victims came to know about the person who misused or attempted to misuse the personal information. Rest 66.7 percent victims were unable to find the offender. It is represented in a form of pie chart shown below in figure 14.


Did you come to know about the person who misused or attempted to misuse your personal information?

33 responses

Figure 14 Proportion of the victims found out the offenders [Source: Primary Data collected by the author of this thesis]

Hypothesis: 3

H0**:** There is high probability of successfully finding out the digital identity fraud offender. H1**:** The offender cannot mostly be found out in cases of digital identity fraud.

The table 6 was made by the certain primary data. It displays the count of respondents who faced identity fraud with respect to the platform where they faced identity fraud.

Experienced fraud with	Count of Experienced fraud with
Any Social media	5
Gmail	5
Netflix or Amazon Prime	1
Netflix/Amazon Prime/iTunes	4
Online Payment/Credit card/Debit Card	7
other/unrevealed	11

Table 6 table of count of identity fraud experienced [Source: Primary Data collected and interpreted by the author of this thesis]

The graphical representation of count of respondents faced identity fraud with respect to the media where they faced of Table 6 is represented in Figure 15.

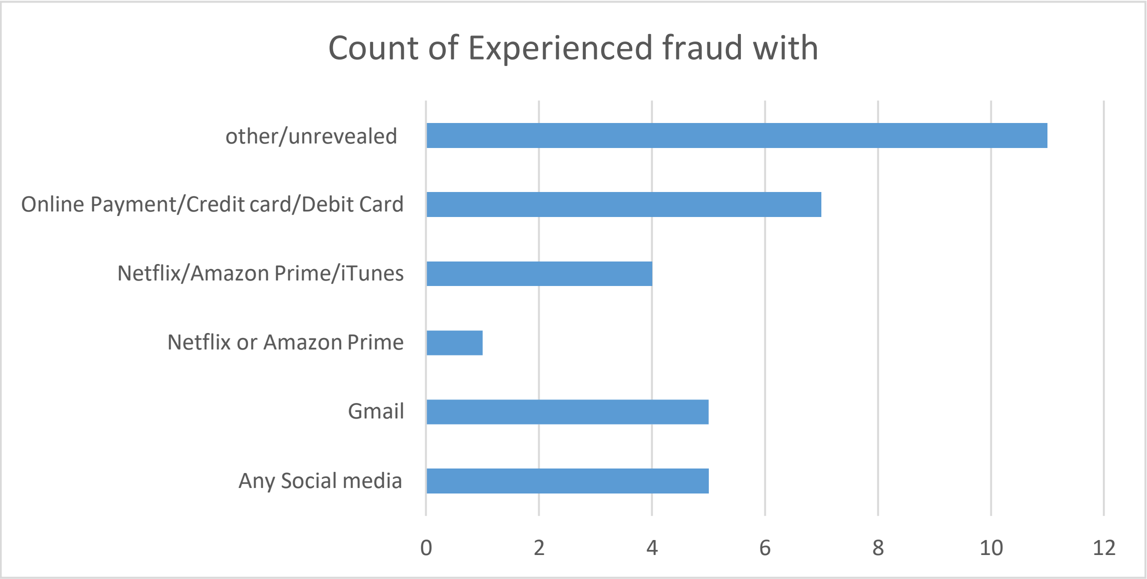


Figure 15 Graphical representation of count of experienced identity fraud [Source: Primary Data collected and interpreted by the author of this thesis]

Those victims were asked if they found out the offender. That primary data were then analyzed and encapsulated in the Table 7.

Offender Found	Count of Offender Found
No	22
Yes	11

Table 7 Table of count of offenders found [Source: Primary data analyzed by the author of this thesis]

The analyzed data of Table 7 were then instantiated in Figure 16 in the form of bar graph. It shows that out of 33 offenders, 11 were got caught. Rest 22 were never got identified.

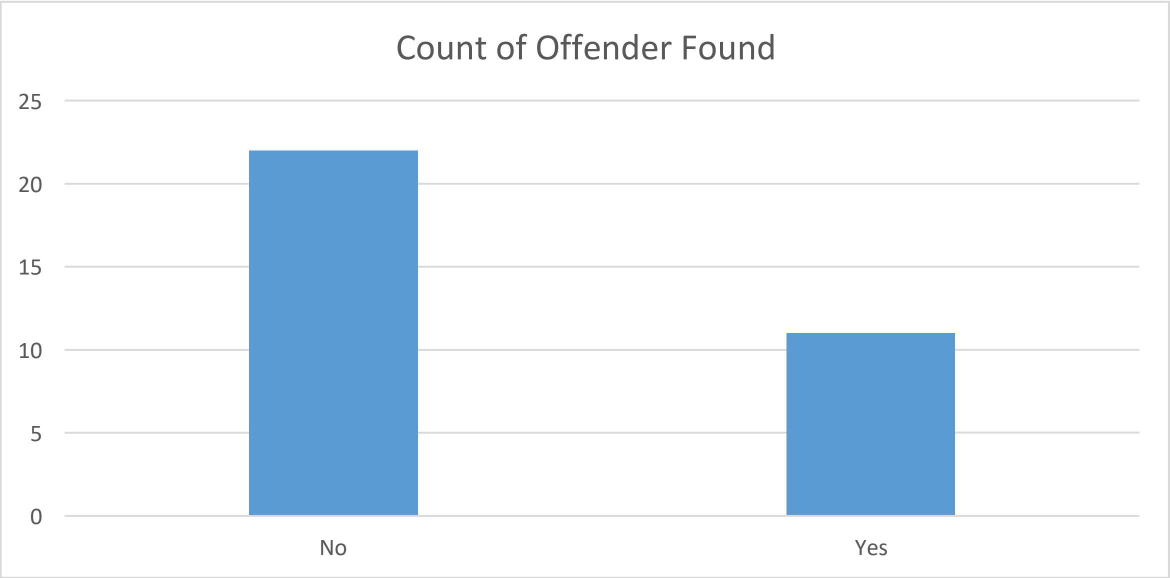


Figure 16 Graphical representation of Count of offenders found [Source: Primary data analyzed by the author of this thesis]

Interpretation: It was interpreted from this analysis that offenders were being found out or getting caught in 1/3 of the cases. Hence, it is certain that 2/3 of the offenders were not getting caught or being found out. So, alternative hypothesis was found to be accepted and null hypothesis was found to be rejected.

It indicated that a future study should be done finding the techniques and processes to catch the offenders and implementation of it.

4.5 Objective-4

To find the actual need of awareness for identity frauds with respect to age groups.

The research question **"**How much is digital users' awareness required?" is getting satisfied in this objective 4. It was related to question 16, question 17 and question 19 in the questionnaire.

From data collection and pie chart of question16, It can be concluded that majority of individual come across fake ID's. Whereas 38.6% said that they haven't come across any fake profiles.

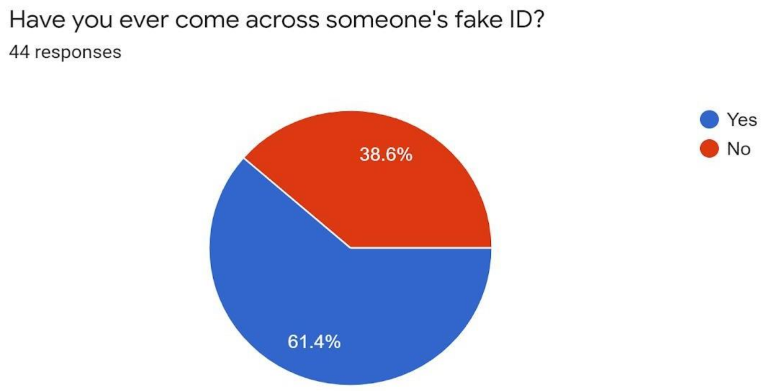


Figure 17 Pie-chart of if a respondent came across someone's fake ID [Source: Primary Data collected by the author of this thesis]

As question 17 in the questionnaire is a Yes or No choice question, and 73.3% of the respondent feel insecure about their digital Identity while, 26.7 percent do not feel that way.

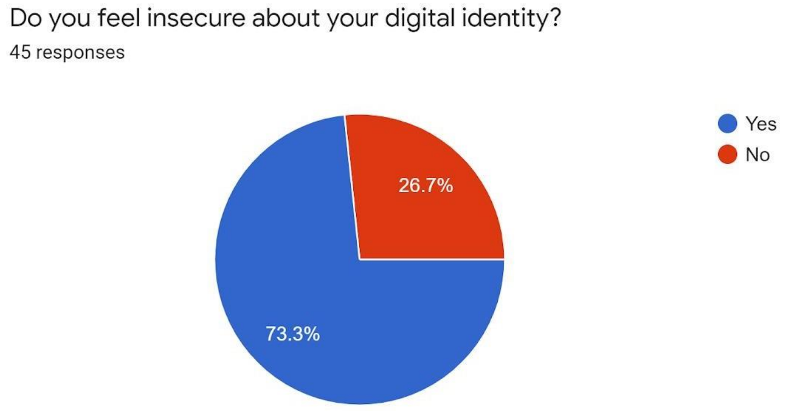


Figure 18 Proportion of respondents who feel insecure about the digital identity [Source: Primary Data collected by the author of this thesis]

According to question 18 in the questionnaire, it can be concluded that, almost everyone feels that awareness is required for cyber-crime and Identity fraud as many people still didn't know the scope and the damage which can be caused by the identity frauds. However, a petite amount of 3.1 people thinks that awareness is not required.

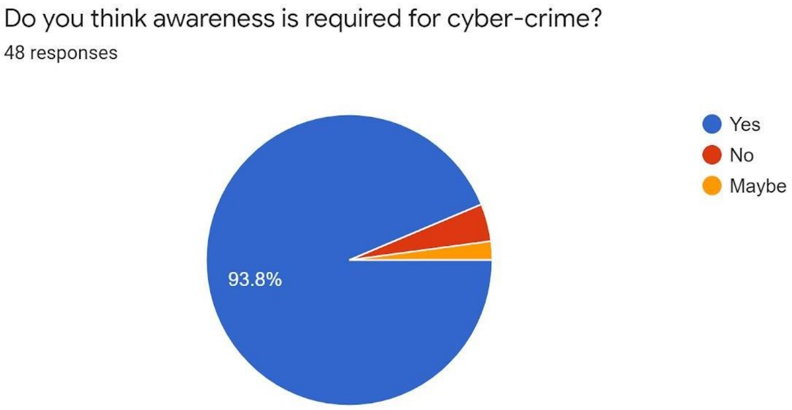


Figure 19 Proportion of respondents who think awareness regarding cyber-crime is required [Source: Primary Data collected by the author of this thesis]

Hypothesis-4

H0: Youngsters under age 21 are required more awareness for identity fraud. H1:
Adults of age 21 or above require more identity fraud awareness.

The Table-8 was made by the interpretation of the primary data. It shows the count of respondents as per their age group. It shows that there are 43 respondents who were of age 21 or above. And, 9 respondents were of below 21 age.

Age	Count of Age
21 or above	43
below 21	9

Table 8 Table of Age group of the respondents [Source: Primary Data collected and interpreted by the author of this thesis]

The graphical representation of the Table 8 is displayed in the Figure 20. It is represented as bar graph.

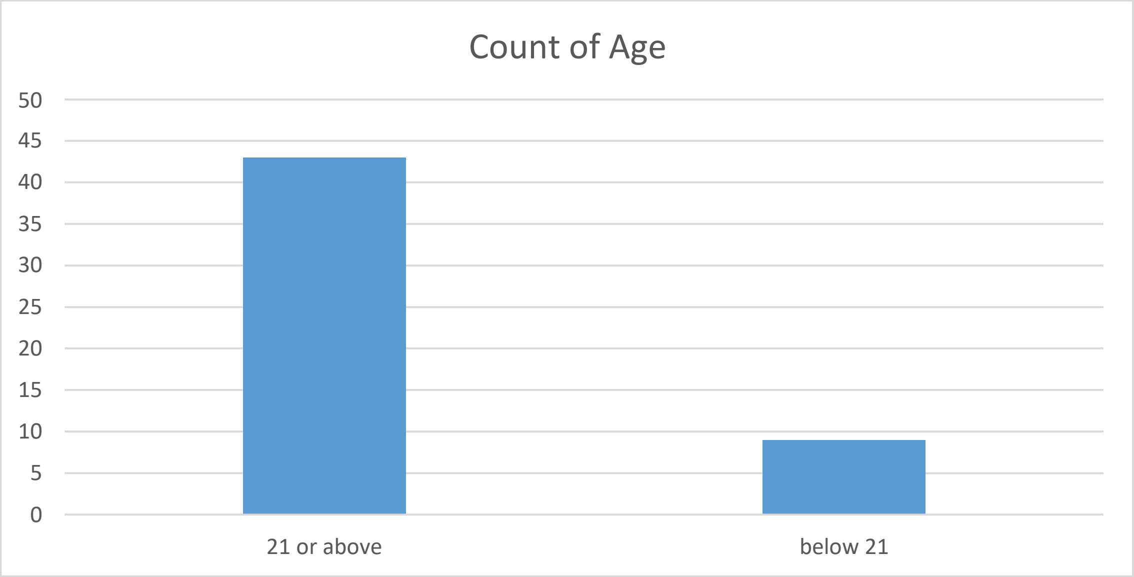


Figure 20 Graphical representation of Age group of respondents [Source: Primary Data collected and interpreted by the author of this thesis]

Through the Primary data collected, respondents in the questionnaire were asked if they are aware about identity theft or not. Through the interpretation of that data, a Table 9 was made which shows proportion of respondents aware about identity theft.

Aware about Identity Theft	Count of Aware about Identity Theft
No	16
Yes	36

Table 9 Table of Proportion of respondents aware about identity theft [Source: Primary Data collected and interpreted by the author of this thesis]

The Figure 21 is a simple illustration of the data interpreted from the Table 9. It is represented in the form of bar graph.

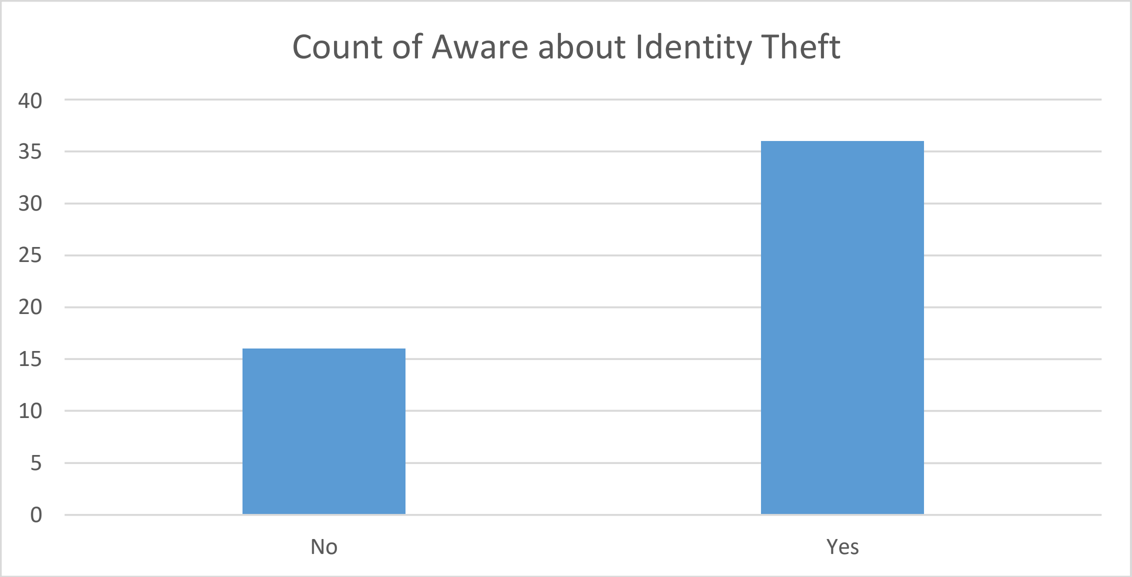


Figure 21 Graphical representation of Proportion of respondents aware about identity theft [Source: Primary Data collected and interpreted by the author of this thesis]

The further analysis were done from the primary data related to the interpretation of Table 9. According to that, it was divided as per the age group and then analyzed. It shows that out of 43 respondents of age group 21 or above, 30 were aware about identity theft and rest 13 were not knowing what it is. Hence, 30.23 percent of them were fount not to be aware about identity crimes. The analysis is encapsulated in Table 10.

Age group of 21 or above aware about Identity Theft	Count of Age group of 21 or above aware about Identity Theft	Percentage
No	13	30.23%
Yes	30	69.77%

Table 10 Analysis of the age group of 21 or above aware about identity theft [Source: Primary data analyzed by the author of this thesis]

The Table 10 was further transformed into bar graph which is demonstrated in Figure 22.

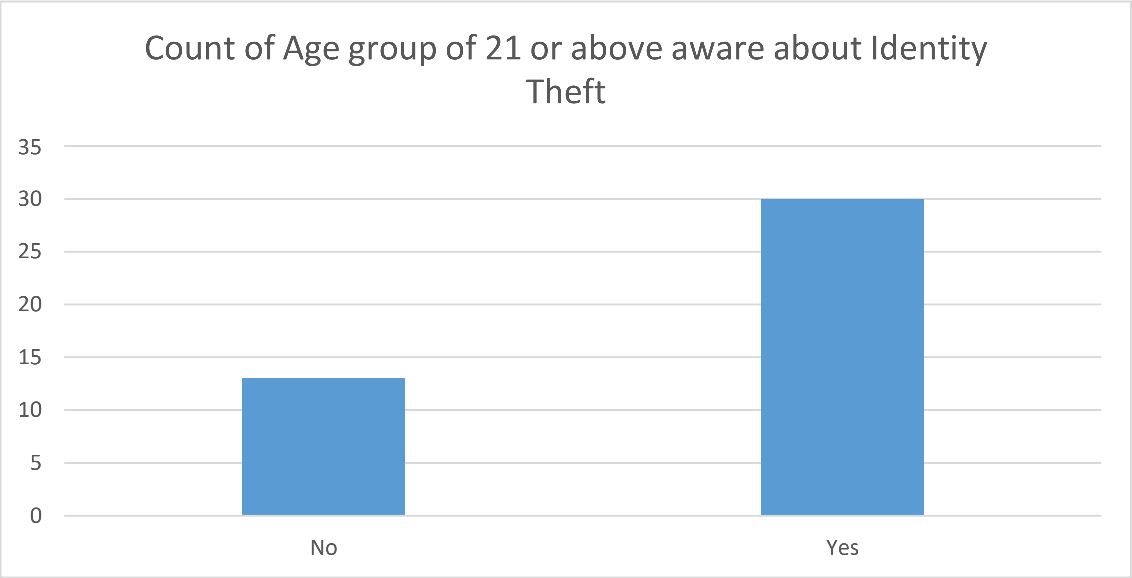


Figure 22 Bar-graph of Analysis of the age group of 21 or above aware about identity theft [Source: Primary data analyzed by the author of this thesis]

Similarly, the primary data was analyzed for the age group below 21 to identify how much proportion from it was aware about identity fraud. It was analyzed that 6 out of 9 from the age group below 21 are aware about identity theft and rest 3 are not at all knowing what it is. This analysis is encapsulated in Table 11.

Age group below 21 aware about Identity Theft	Count of Age group below 21 aware about Identity Theft	Percentage
No	3	33.33%
Yes	6	66.67%

Table 11 Analysis of the age group of below 21 aware about identity theft [Source: Primary data analyzed by the author of this thesis]

The bar representation of the Analysis of the Age group of below aware about identity theft is demonstrated in Figure 23.

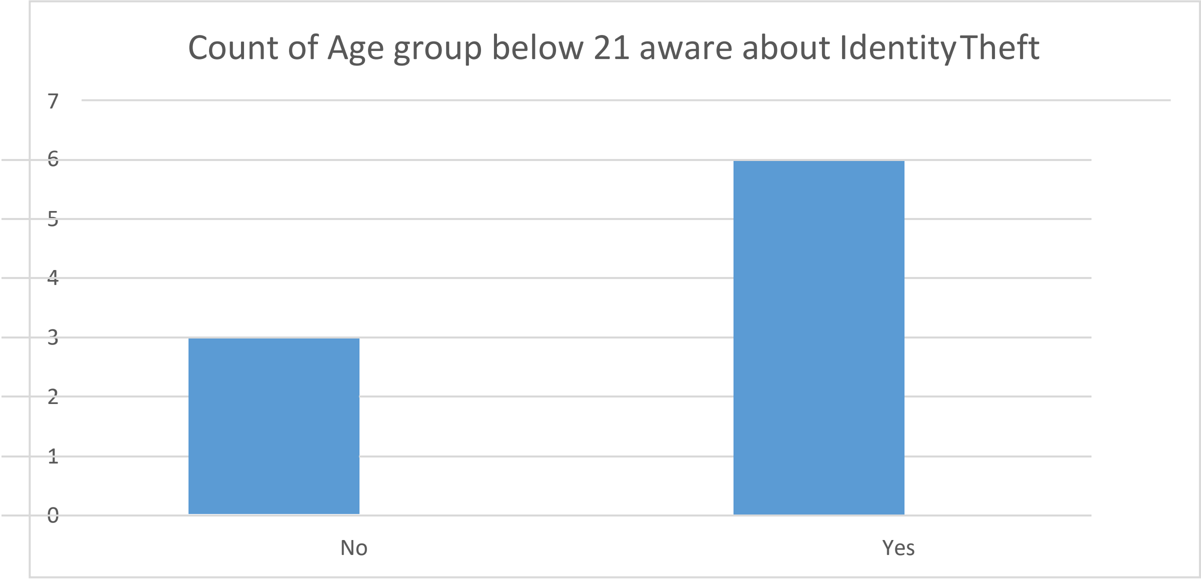


Figure 23 Bar-graph of Analysis of the age group of below 21 aware about identity theft [Source: Primary data analyzed by the author of this thesis]

Interpretation: From the analysis done, it was interpreted that the null hypothesis and alternative hypothesis, both were to be accepted as there is no significance difference between both the age groups. From the age group of 21 or above, 30.23 percentage of the respondents were not aware about identity fraud. And similarly, from the age group of below 21, 33.33 percent of the respondents were not aware about identity fraud. Hence, both the age groups have no much visible difference in terms of awareness.

Through this analysis, it can be stated that awareness of identity crimes were independent of the age groups. So, digital users' cognizance programs should be conducted irrespective of the age groups.

4.6 Data of Cybercrimes from a report on Czech Republic

According to the secondary data of 2014 identity theft in Czech Republic, the majority of the crimes are identity frauds whereas, extortion and forgery seems uncommon. The figure 24 depicts the pie chart of it.

To embark on, more than half of identity theft crimes are related to identity fraud (57%) which includes misuse of credit card or personal information of victim by the offender. After frauds most common identity crime is damage and abuse of media records (12%) where victimizer alter the media records for their own benefits. Seemingly, vice crimes which includes immoral or sinful act and infringements to copyright to databases are about 6%.

Moreover, there are 2% cases of unlawful possession of payment means such as electricity bills or any other kind of bill in which all essential information of an individual is mentioned. Furthermore, dangerous pursuing and threatening to a victim is also recorded to 2%.

Furthermore, Extremist manifestation where one can extremely exploit someone identity and forgery and changes to official documents reported least of about 1%. There are also some of miscellaneous criminal activity which covers 13% of the pie chart.

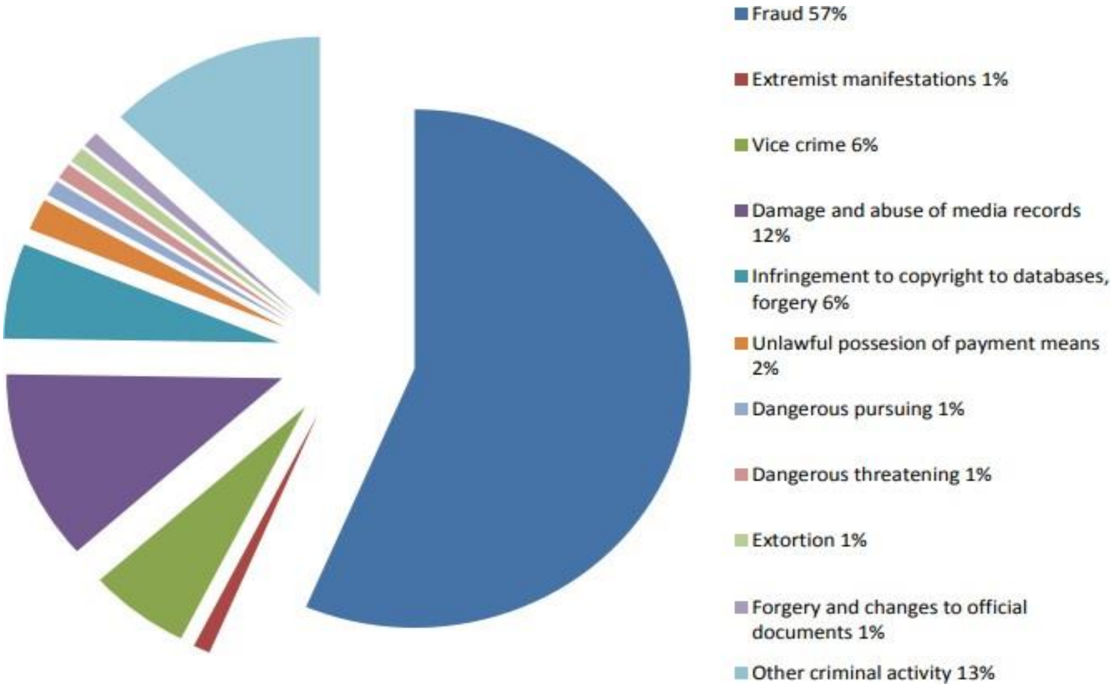


Figure 24 Cybercrime offences in 2014 [Source: Evaluation report on the 7th round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating cybercrime", a report on Czech Republic by council of the European Union]

The multi-bar graph chart in the figure 25 shows the cases related to identity theft reported to Czech Republic government. Three bars represent individual year; 2012, 2013 and 2014 respectively, moreover, 16 different categories are compared in this chart.

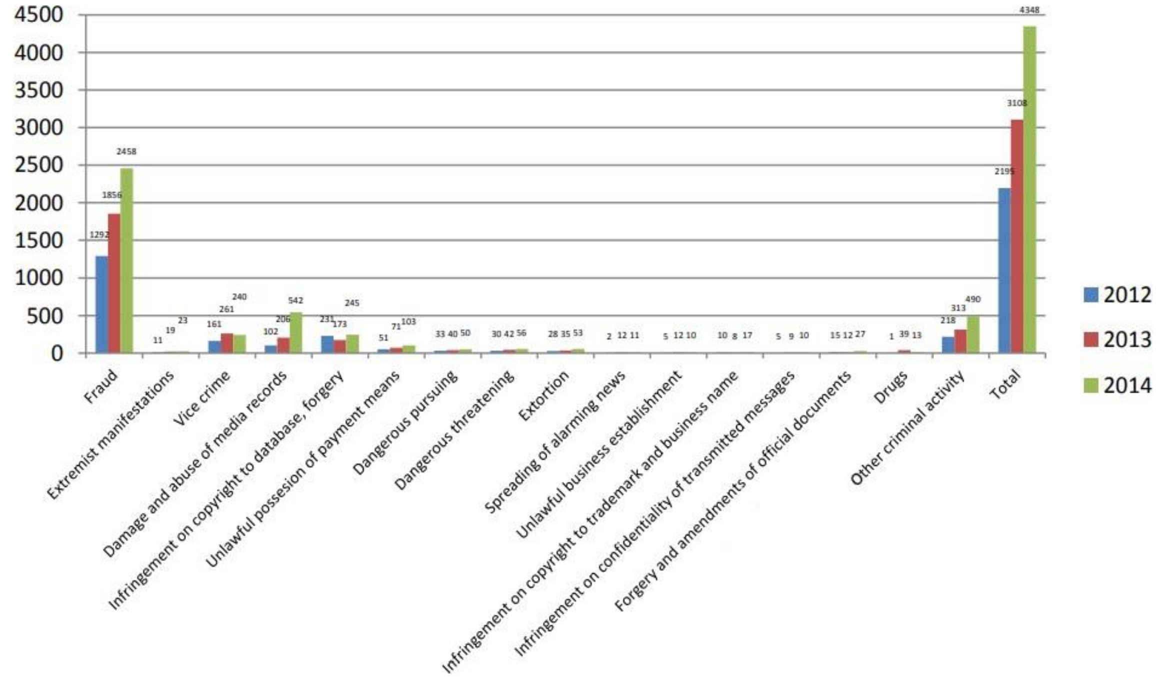


Figure 25 Cybercrime offences in 2012, 2013 and 2014 [Source: Evaluation report on the 7th round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating cybercrime", a report on Czech Republic by council of the European Union]

In most of the cases, it is ostensible that cases of identity theft have increased with respect to time and major raise can be seen in Frauds, damage and abuse of media records and dangerous pursuing and threatening.

To begin with, in 2012, total of 2195 of identity theft cases reported and within 2 years this number increased with twofold. The main contributor of the cases are Frauds with cases of 1292, 1856, and 2458 in year 2012, 2013, and 2014 respectively. Also, a significant raise can be observed in damage and abuse of media record where cases increased from 102 in 2012 from 542 in 2014. While in vice crime cases decreased form 261 in 2013 to 240 in 2014. Whereas, almost in all other categories cases are increased with respect to time with same numbers (dangerous pursing and threatening, Extortion, Spreading of alarming news, forgery and amendments of official documents, drugs). Furthermore, there are also miscellaneous activities related to identity crime which is also rise two times from 2012 to 2014.

5. Results and Recommendations

As per research data collected and various tools and techniques applied, the data has been analyzed. The primary data was randomly collected from various people of various age groups. Secondary data was collected from the Evaluation report on the 7th round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating cybercrime", a report on the Czech Republic by council of the European Union.

5.1 Observations and Evaluations:

Based on the research done, there were many observations and evaluations made which are pointed below:

- There are many ways for preventing or mitigating identity theft from arising which were described in literature review chapter. If we implement those or if people be aware about those, then identity frauds can easily get reduced.

- Adults of age more than 21 should be more focused for awareness because they are having high probability of being attacked by identity fraud offenders. It is analyzed and interpreted in the Objective-1.

- According to research Objective-2, it was interpreted that financial crime occur more than non-financial crimes in identity fraud. So, the target for awareness on digital safety in financial transaction or information should be majorly focused. However, there is not much difference in numbers of financial and non-financial crimes. Hence, awareness and further study ought to be focusing on both the possibilities.

- It was interpreted in the third Objective that only 1/3 of identity fraud offenders can be found out or caught. Rest 2/3 of the offenders were not getting caught. So, a further research or study should be done in finding offenders techniques and processes to be followed after being a victim of identity frauds.

- The fourth Objective focuses on whether young age group were more aware of identity fraud or adults were more aware about identity fraud. It was believed that the new generation is more aware about identity crimes. But the interpretation research objective 4 proved that there was no significant difference between the older and new generation in terms of identity crimes awareness. Hence, a further study and actions should be done irrespective of the ages of the digital gadget users.

5.2 Comments and Recommendations:

There are many recommendations from this research to prevent or mitigate identity crimes. Opinions of the respondents were also been asked in primary data where few respondents gave their feedbacks. From that, the valid comments had been carried out and elaborated as per the research done.

- Protect your digital identity as best as possible. For example, use strong passwords; use multi factor authentication (MFA) and smart notifications for your online accounts.

- Cybercrime should be taken seriously and the governments should do something strict about the increasing levels of identity frauds in our society. Government and education system should implement awareness programs for identity fraud awareness.

- There should be awareness programs and posts on Social media as it is the new tool which is widely. The online platforms should have easiness of use so that end user can use it easily and not being the victim of identity frauds in the chaos of messy and confusing online platforms.

- Measures should be taken by the government frequently and security of online surfing should be enhanced.

- A person should report the frauds and leaks of their personal data instead of taking it easy and not taking any steps to report it.

- Android and IOS applications and Computer software access to the system should be limited by restricting unnecessary access of any software or application.

- Freeze or lock your credit card or debit card in case of lost or not using.

- Limit the information you are sharing with unknown person.

- Do not open any unauthenticated link or website. (Md Shahrear Iqbal, 2018)

6. Conclusion

Identity frauds are very highly occurring crime in a contemporary world. This research was done using the resources which are valid in current situation. There are many future scopes of this research also. Due to limited time and budget, the study could not be done for all or large sample size. Identity fraud is almost similar everywhere in the world hence a global level study of it can help more than the study of particular region as it is a broad domain.

The stages of identity fraud was described with process chart in figure 1 in literature review chapter. There is a scope of detailed research for each stages of identity fraud so that it can be understand from the roots of it. That way it will be easy to control the frauds also.

The issues of reporting and recording identity theft were discussed in 3.5 section of literature review chapter. Those issues can deeply get studied and another research can be carried out so that recording and reporting of identity frauds can be done with ease.

The challenges and recommendations for managing identity theft was mentioned in detail. However, there are more challenges than we think. It needs a deep study of it to identify those and so, more recommendations can be carried out. For example, it is a common perception that younger people are having higher knowledge of modern technologies and they are more aware about the frauds related to it. Howbeit, the results from this study challenges that view as it is the same among all age groups and so, awareness should be conducted independent of the age groups.

Finally, it is concluded that identity fraud is very vast topic to do research. There were many research done and many more still remained to carry out. It is good as we do more and more deep research on it and those will help reach us more people for awareness programs and the methods of awareness will be optimized. This research can be useful for many further researches and implementation or use of the data.

7. Bibliography

(2014). Retrieved from Bureau of Justice Statistics: https://www.bjs.gov/index.cfm?ty=pbdetail&iid=5408

(2018). Retrieved from statista: https://www.statista.com/

Ballard, D., Hornik, J., & McKenzie, D. (2002). Technological Facilitation of Terrorism: Definitional, Legal, and Policy Issues. *American Behavioural Scientist*, 982-1016.

Batton, C., & Kadleck, C. (2004, March). Theoretical and Methodological Issues in Racial Profiling Research. *Police Quarterly*, 30-64.

Casey, E. (2000). *Criminal Profiling, Computers, and the Internet. Journal of Behavioural Profiling.*

Clarke, R. (1993, December). Profiling: A Hidden Challenge to the Regulation of Data Surveillance. *Journal of Law and Information Science*, 1-12.

Clarke, R. (1998). Information privacy on the Internet: Cyberspace invades personal space. *Telecommunications Journal of Australia*, 48.

Clarke, R. V., & Eck, J. E. (2005). *Crime Analysis for Problem Solvers in 60 Small Steps.* United States of America: NCJRS. Retrieved from https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=232576

Cradduck , L. e. (2007). Identifying the identity thief: Is it time for a (smart) Australian card? *International Journal of Law and Information Technology*, 140.

da Silva, P. Q., de Oliveira Nascimento, F., & Alves Nascimento, A. (2008). *The International Journal of FORENSIC COMPUTER SCIENCE.* The International Journal of Forensic Computer Science (IJoFCS). Retrieved from http://ijofcs.org/V03N1-FULL.pdf

De, K. (2004). *The Role of Profiling in the Detection and Prevention of Identity Fraud.* Unpublished Dissertation. University of New South Wales.

Dickerson, J., & Dickerson, J. A. (2000). Fuzzy Network Profiling for Intrusion Detection. *Electrical and Computer Engineering Department Iowa State University*, 1-6.

Egger, S. (1999). Psychological Profiling: Past, Present and Future. *Journal of Contemporary Criminal Justice*, 242-261.

(2002). *Europol Annual report.* Retrieved from https://www.europol.europa.eu/sites/default/files/documents/europol_annual_report_2002.pdf

Fawcett, T., & Provost, F. (1997). Adaptive Fraud Detection. *Data Mining and Knowledge Discovery*, 290-316.

Finklea, K. M. (2010). *Identity Theft: Trends and Issues.* Congressional Research Service. Retrieved from https://books.google.co.in/books?hl=en&lr=&id=eM7xRWjJoEUC&oi=fnd&pg=PA1&dq=identity+theft+prevention&ots=Gyyegpcqvm&sig=pRo-GLci-8HFSoH90EV1EIAk4kU&redir_esc=y#v=onepage&q&f=false

Forcht, K. A., Kieschnick, E., Thomas, D. S., & Shorter, J. D. (2007). *IDENTITY THEFT: THE NEWEST DIGITAL ATTACK.* Retrieved from http://iacis.org/iis/2007/Forcht_Shorter_Thomas.pdf

Fredrickson, D., & Siljander, R. (2002). Racial Profiling: Eliminating the Confusion between Racial and Criminal Profiling. *Springfield, IL: Charles C. Thomas*.

Gallo, F. (2003). Profiling vs. Racial Profiling Making Sense of it All. *Trainer Magazine*, 15-21.

Good, V. R. (2019). *IDENTITY THEFT AND THE INTERNET.* ProQuest LLC. Retrieved from https://search.proquest.com/openview/f376ecce6c043045bf5b5a205ab22c6b/1?pq-origsite=gscholar&cbl=18750&diss=y

Gordon, D. R., & Willox, M. A. (2003). *Identity Fraud: A Critical National and Global Threat.* Retrieved from http://veracity.lexis-nexis.com/presscenter/hottopics/ECIReportFINAL.pdf

Gordon, G. R., & Willox, N. A. (2006). The Ongoing Critical Threats Created by Identity Fraud: An Action Plan. *The Ongoing Critical Threats Created by Identity Fraud: An Action Plan*. Retrieved from http://www.shephardsoftware.com/government/insights/whitepapers/Identity_Fraud_Plan.pdf

Gordon, G. R., Rebovich, D. J., Choo, K.-S., & Gordon, J. B. (2007). *Identity Fraud Trends and Patterns: Building a Data-Based Foundation for Proactive Enforcement.* Utica College, Center for Identity Management and Information Protection. CIMIP. Retrieved from https://core.ac.uk/download/pdf/21748215.pdf

Gordon, G. R., Willox, N. A., Rebovich, D. J., Regan, T. M., & Gordon, J. B. (2004, Winter). Identity Fraud: A Critical National and Global Threat. *Journal of Economic Crime Management,* *2*(1). Retrieved from https://www.politieacademie.nl/kennisenonderzoek/kennis/mediatheek/PDF/8245.p df

Hedayati, A. (2012, January). An analysis of identity theft: Motives, related frauds, techniques and prevention. *Journal of Law and Conflict Resolution* . doi:10.5897/JLCR11.044

Hicks, S., & Sales, B. (2006). Criminal Profiling: Developing an Effective Science and Practice. *American Psychological Association, Washington, DC.* .

Hildebrandt, M., & Backhouse, J. (2005). *Descriptive analysis and inventory of profiling. Future of Identity in the Information Society (FIDIS).*

Jewkes, Y., & Yar, M. (2010). *Handbook of Internet Crime.* New York: Willan Publishing. Retrieved from https://books.google.co.in/books?hl=en&lr=&id=_2TIMDlOWU4C&oi=fnd&pg=PA273&dq=identity+theft+prevention&ots=rdHrwym2ew&sig=qDImolsI2JWEWtEunBua2IHeQeQ&redir_esc=y#v=onepage&q&f=false

Koops, B.-J., & Leenes, R. (2006). Identity theft, identity fraud and/or identity-related crime. *Identity theft, identity fraud and/or identity-related crime,* 553-556. doi:10.1007/s11623-006-0141-2

Le Lievre, E., & Jamieson, R. (2005). An Investigation of Identity Fraud in Australian Organisations. *Collaborative Electronic Commerce Technology and Research (CollECTeR)*, 1-10.

Lister, S., & Crawford, A. (2004). *The patchwork shape of reassurance policing in England and Wales: Integrated local security quilts or frayed, fragmented and fragile tangled webs?* Emerald Group Publishing Limited. Retrieved from https://www.emerald.com/insight/content/doi/10.1108/13639510410553149/full/ht ml

Manap, N. A., Rahim, A. A., & Taji, H. (2015). Cyberspace Identity Theft: An Overview. *Mediterranean Journal of Social Sciences* , 299. Retrieved from https://www.researchgate.net/publication/282465632_Cyberspace_Identity_Theft_An_Overview/link/568e034008aeaa1481ae80e6/download

Marx, G., & Reichman, N. (1984, March). Routinising the Discovery of Secrets: Computer as Informants. *American Behavioural Scientist*, 420-452.

Maxfield, M. G., & Clarke, R. V. (2004). *UNDERSTANDING AND PREVENTING CAR THEFT.* Willan Publishing. Retrieved from https://pdfs.semanticscholar.org/32a5/c87fe4d50280d7eab171782e800759737f99.p df

Md Shahrear Iqbal, M. Z. (2018). Protecting Internet users from becoming victimized attackers of click-fraud. *Journal of Software: Evalution and process*.

Newman, G. R., & McNally, M. M. (2005). *Identity Theft Literature Review.* NCJRS. Retrieved from https://www.ncjrs.gov/pdffiles1/nij/grants/210459.pdf

Newman, G. R., & McNally, M. M. (2007, July). *Identity Theft - A Research Review*. Retrieved from ncjrs.gov: https://www.ncjrs.gov/pdffiles1/nij/218778.pdf

Newman, G., & Clarke, R. V. (2002). ETAILING: NEW OPPORTUNITIES FOR CRIME, NEW OPPORTUNITIES FOR PREVENTION. Department of Trade and Industry (DTI) Office of Science and Technology (Foresight Directorate).

Norm Archer, Sproule, S., Yuan, Y., Guo, K., & Xiang, J. (2012). *Identity Theft and Fraud - Evaluating and Managing Risk.* University of Ottawa Press. Retrieved from https://books.google.co.in/books?hl=en&lr=&id=zZljAwAAQBAJ&oi=fnd&pg=PP1&dq=managing+identity+fraud&ots=rsyRBWHB-m&sig=tauHw5Ym0EyUZAV61novnTWa-0s&redir_esc=y#v=onepage&q=managing%20identity%20fraud&f=false

P. F. (2007). *Identity Theft [Internet].* Santa Clara: McAfee.

Paget, F. (2007). *How many Bot-Infected Machines on the Internet?* McAfee. Retrieved from blogs.mcafee.com/mcafee-labs

Petherick, W. (2006). Serial Crime: Theoretical and Practical Issues in Behavioral Profiling. *Elsevier Inc., London, Great Britain.* .

Rodger, J., Donald, W., Greg, S., & Stephen, S. (2008). *DEVELOPING A CONCEPTUAL FRAMEWORK FOR IDENTITY FRAUD PROFILING.* Researchgate. Retrieved from https://www.researchgate.net/profile/Stephen_Smith47/publication/221407796_Developing_a_Conceptual_Framework_for_Identity_Fraud_Profiling/links/53e70c490cf25d674ea57e20/Developing-a-Conceptual-Framework-for-Identity-Fraud-Profiling.pdf

Sampford, K., Dixon, N., & Giskes, R. (2005). *Identity Fraud.* Queensland Parliamentary Library. Retrieved from https://www.parliament.qld.gov.au/documents/explore/ResearchPublications/ResearchBriefs/2005/200503.pdf

Schreft, S. L. (2007). *Risks of identity theft: Can the market protect the payment system?* Kansas City: Economic Review - Federal Reserve Bank of Kansas City.

Smith, H. A., & McKeen, J. D. (2011). *The Identity Management Challenge* (Vol. 28). doi:10.17705/1CAIS.02811

Speech delivered to the 2003 Banking Institute of University of North Carolina School of Law's Center for Banking and Finance, C. N. (Performer). (2003, Arpil 10). *The many ugly faces of identity theft.* Retrieved from https://home.treasury.gov/

Straub, D., & Nance, W. (1990, March). Discovering and Disciplining Computer Abuse in Organisations: A Field Study. *MIS Quarterly*, 45-60.

Sullivan, R. J. (2008). Economic Review • Third quarter 2008 . *Can Smart Cards Reduce Payments Fraud and Identity Theft?*, pp. 35-55. Retrieved from https://www.kansascityfed.org/Publicat/Econrev/PDF/3q08Sullivan.pdf

Tajpour, A., Ibrahim, S., & Zamani, M. (2013). Identity Theft Methods and Fraud Types. Retrieved from https://www.researchgate.net/profile/Atefeh_Tajpour/publication/273259976_Identity_Theft_and_Fraud_Type/links/5527c9fa0cf2e089a3a1d3b3.pdf

Turvey, B. (2000). Criminal Profiling and the Problem of Forensic Individuation. *Journal of Behavioral Profiling*, 1-26. Retrieved from http://www.profiling.org

Urgaonkar, B., Shenoy, P., & Roscoe, T. (2002). Resource Overbooking and Application Profiling in Shared Hosting Platforms. *ACM SIGOPS Operating Systems Review*, 240-254.

Wiedmann, K-P, Buxel, H., & Walsh, G. (2002). Customer Profiling in E-Commerce: Methodological Aspects and Challenges. *The Journal of Database Marketing*, 169- 184.

Wilhelm, W. K. (2004, Spring). The Fraud Management Lifecycle Theory: A Holistic Approach to Fraud Management. *Journal of Economic Crime Management*. Retrieved from https://www.utica.edu/academic/institutes/ecii/publications/articles/BA309CD2-01B6-DA6B-5F1DD7850BF6EE22.pdf