PREVENTION OF IDENTITY THEFT IN POST INTERNET ERA

DISSERTATION

Submitted in the Partial Fulfilment for the Degree of

MASTER OF LAW'S (LL.M.)

SESSION: 2019-20

UNDER SUPERVISION OF:

Mrs. Sarita Singh Sikarwar
Assistant Professor,
School of Legal Studies
Babu Banarasi Das University

SUBMITTED BY:

Aditya Maurya
ROLL No.:1190997004
Criminal and Security Laws
LL.M.(Second Semester)

DECLARATION

Title of Project Report PREVENTION OF IDENTITY THEFT IN POST INTERNET ERA

I understand what plagiarism is and am aware of the University's policy in this regard.

ADITYA MAURYA

I declare that

(a) The work submitted by me in partial fulfilment of the requirement for the award of degree **LLM** Assessment in this **DISSERTATION** is my own, it has not previously been presented for another assessment.

(b) I declare that this **DISSERTATION** is my original work. Wherever work from other source has been used, all debts (for words, data, arguments and ideas) have been appropriately acknowledged.

(c) I have not used this work previously produced by another student or any other person to submit it as my own.

(d) I have not permitted, and will not permit, anybody to copy my work with the purpose of passing it off as his or her own work.

(e) The work conforms to the guidelines for layout, content and style as set out in the Regulations and Guidelines.

Date : ………………

ADITYA MAURYA

Roll no.-1190997004

LL.M. (2019-20)

CERTIFICATE

This is to certify that the research work entitled "PREVENTION OF IDENTITY THEFT IN POST INTERNET ERA" is the work done by a student of Babu Banarasi Das University Lucknow, under my guidance and supervision for the partial fulfillment of the requirement for the Degree of (LL.M.) in Babu Banarasi Das University Lucknow, Uttar Pradesh. According to the best of my knowledge, he/she has fulfilled all the necessary requirements prescribed under the University Guideline with regard to the submission of this dissertation.

I wish him/her success in life.

Date – Mrs. Sarita Singh Sikarwar

(Assistant Professor)

Place- ……………….................., BABU BANARASI DAS UNIVERSITY LUCKNOW

ACKNOWLEDGEMENT

I acknowledge the heartfelt thanks to the Institute of legal Studies, Babu Banarasi Das University Lucknow, for providing me the opportunity to complete my dissertation for the Partial Fulfillment of the Degree in (LLM).

I am thankful to my Supervisor Mrs. Sarita Singh Sikarwar (Assistant Professor), for not only helping me to choose the dissertation topic but also for her valuable suggestions and cooperation till the completion of my dissertation. She provided me every possible opportunity and guidance and being a support in completing my work.

I also thank to all the respondents without whom this study would have never been completed.

I also like to thank my friend Saurabhi Pathak for her constant support in completion of this dissertation.

I am thankful to everyone from core of my heart.

Aditya Maurya

Roll No. 1190997004

(LLM)

Babu Banarasi Das University

Lucknow

Contents

LIST OF ABBREVIATIONS

- IPC- Indian Penal Code
- IT- Information and Technology
- ATM- Automated Teller Machine
- PC- Personal Computer
- Etc. - Et cetera
- CEO- Chief Executive Officer
- E-mail- Electronic Mail
- E.g.- Example
- IS- Information System
- i.e.- That Is
- E-commerce- Electronic Commerce
- ID- Identity Document
- T.V- Television
- DNA- Deoxyribonucleic Acid
- PIN- Personal Identification Number
- HTTP- Hyper Text Transfer protocol
- HTTPS- Hypertext Transfer Protocol over Secure Socket Layer
- PPP- Public private partnership
- UID- Unique identifier

LIST OF CASES

- *Pune Citibank MphasiS Call Centre Fraud*
- *Sony Sambandh Case*
- *The Bank NSP Case*
- *Andhra Pradesh Tax Case*
- *SMC Pneumatics Pvt. Ltd. vs. Jogesh Kwatra*
- *Bazee.com Case*
- *State of Tamil Nadu vs. Suhas Katti*
- *Nasscom vs. Ajay Sood & Others*
- *Cyber Attack on Cosmos Bank*
- *BSNL, Unauthorized Access*

CHAPTER 1- INTRODUCTION

CHAPTER 1-INTRODUCTION

In technologically developed society human beings started facing another major crisis, which is threatening to society at large, is identity theft or in other words known as high tech cyber-crime. With so much technological involvement in everyday lives of humans can make any one of us its victim and contrary to the popular misapprehension that just the personal information of rich are in danger. People with very modest background may fall victim to identity theft. So, what was common in most of the cases was a good credit score, which was used by identity thieves to appropriate thousands of rupees in the name of the victim. And no particular age group is free from its grasp but in reality, due to higher interest in internet which is a primary source of most of the identity theft crimes younger people may be victimized more often than any other group. The cyber-crime is one of the main problems faced by the world these days. It includes unauthorized access of information and break security like privacy, password, etc. of any person with the use of internet. Cyber theft is a part of cybercrime which means theft carried out by means of computers or the Internet.[1] The most common type of the cyber crimes are password theft, stealing of personal information, identity theft, internet time theft, etc.

Identity has been coined as the ‘central organizing principle’ of this information technological age. And quite unquestionably, identity symbolizes prevalence in modern and developed societies and as well as also for the developing countries and it also acts as a doorway to additional economic expansion. As dated back to 1997, Peter G. Neumann wrote that for such rise in identity theft access to computer is not essential, he also identified that ‘possibly anonymous access whether remote or global greatly increases such risks. Dr Collins who is also former director of the Michigan State University for Identity Theft, Partnership in Prevention program and the Identity Theft Crime Research Lab stated that the identity theft will be the crime of the near future and not

[1] Cyber theft - A serious concern in India https://www.lexology.com/library/detail.aspx?g=4af6c044-dc77-4b1a-9288-986395eff8d1, ACCESSED ON 10/3/2020.

the terrorism. Bruce Schneier who is the CEO and founder of Counterpane Internet Security Inc said that the identity theft will be the new crime of the information age.' However, despite a lot of misbelieve identity theft does not only targets online actions but because of the growing importance of identity in the delivery of communal services or of border control procedures it also draws attention of those waiting for chance to exploit vulnerabilities as their own criminal endeavor. There are different types of offline identity theft which includes forgery of administrative documents, passport forgery, and official documents and other information related to identity from 'dumpster diving'. But even with the increase of interest of media and concerns of the experts there is still broad discrepancy as to what identity theft actually is. What made it worse is that the complexity to understanding that identity is not a property which cannot be stolen as such and because the use of data related to someone's identity by a person does not usually take away from the others its use, so it leaves the metaphor of identity 'theft' misleading and inappropriate. Some even argue that identify theft should not be considered as a distinct crime in itself, and but should be primarily be dealt with in its relation ad dependency to other crimes or unlawful activities which may be resulted by it. They even argue that identity theft should be seen as the part of identity fraud or other identity-related abuses. Others assert that the ubiquity of technology when coupled with globalization led to the very appearance of illegal identity network with criminals committing thefts. Many also argued that identity theft should also have independent definition as a crime in order to efficiently dealt with. Others still contend that the collection and/or sale of identities without lawful justification is already a crime in its own right, since it constitutes a violation of European data protection rules, and that the problem lies mainly in the effective enforcement of these rules.

So, what identity theft actually means? It pertains to illegally acquiring someone else personal information for their own financial benefit. Identity theft is one of the most common forms of cyber theft and can happen to anyone whether dead or alive. Most of the time people complain that they first they come upon identity theft was through hacking/misappropriation of their email id with a spam message by using any name of famous people or some business association. That theft is of concern because most of the online population has yet to recognize that email addresses are readily forged and thus assume that the owner of a stolen address has either authorized the message or has failed to maintain effective anti-virus protection and thereby allowed a spammer to propagate messages from a 'zombie' machine.[2] Why this stealing of email address or online name/Id is to be worried about because most of the time it leads to blockage of genuine communication from the owner himself and also result in him forcefully changing his name and acquire a new identity. And most of the online spam filters are simply capable of blocking names on the basis of complaint and without any proper investigation. And misuse of someone's name is not only limited to email addresses but in several countries it has been complained that their game name/gaming id and social media ids has been compromised.

RESEARCH QUESTION

- How the identity theft and identity fraud are similar and different at the same time?
- How to recover from the clutches of the crime so rapidly evolving?
- Whether and to what extent are the Indian laws pertaining to identity theft sufficient to cater to the present requirement and whether the implementation mechanism of the laws is in synchrony with the legislations?
- What can be done to have a normal life again by the victim without taking a lot of time?

HYPOTHESIS

There is less awareness about identity theft among the people, most of the time identity theft and identity frauds are understood as one and the same but in reality both have different standing this might be due lack of proper understanding as to what constitute identity crime. Improper implementation of the existing rules and insufficiency in the infrastructure required in implementing the laws plays another role for such growth in identity related crime. With time and due to technological advancement, new forms of encryption technology are used by the cyber criminals, which is difficult to decipher owing to the limited resources of the authorities. Much or less it is required to come up with a proper framework and that too one that is in consonance with laws around the world.

[2] Economic Impact of Identity Theft in India: Lessons from Western Countries, 2011 http://www.ipedr.com/vol12/42-C106.pdf, Last accessed on 10/3/2020

LITERATURE REVIEW

The literature on the subject of identity theft and the related area of computer privacy is extensive and cuts across many disciplines and data sources. These include issues from the online and computer environment to legislation and governmental policy, as well as to the burgeoning field of the study of security and online commerce. The latter area of study has in recent years received close attention in the literature due to the increase of online fraud and security breaches.

However, at the same time many pundits point out that while there has been a surge of studies, reports and theses in the last few years on identity theft and computers, there is as yet no definitive or established body of research or documentation on identity theft. This important point is raised in an article from the Journal of Consumer Affairs entitled How Well Do Consumers Protect Themselves from Identity Theft? by George R. Milne (2003) Milne clearly illustrates the status of research in this area.

The literature addressing the issue of identity theft is sparse. Law review articles have provided a general overview of the problem (e.g., Hoar 2001), while others have evaluated the effectiveness of the courts and existing statutes to provide a remedy to the victims of identity theft (e.g., Alwin 2002; Saunders and Zucker 1999). In the marketing and public policy literature, identity theft is not directly addressed. (Milne, 2003. p. 388)

The above article also serves as an excellent overview of the central issues and problems involved in the research on identity theft. 3 Security and Identity Theft On the other hand it should also be noted that since the date of publication of this article (2003) there has also been a resurgence of articles and studies on this subject, which has become more germane to the growing field of ecommerce and individual online usage. In this regard there has been an increase in the number of comprehensive and valid online sites and database sources which provide a vast array of documentation and that deal with the fight against this type of crime, with a growing number of references and up-to-date information.

There are numerous studies and reports as well as surveys that provide a general and useful overview of the problem of identity theft. For example, an article entitled, Internet Commerce Grows 88 Percent by Dollar Volume and 39 Percent by Transaction Volume: Fraud Remains a

Concern, provides a comprehensive overview of the problem. The article deals not only with the extent of identity theft but also focuses on the important aspect of the way that security issues like ID theft are perceived and understood by the general public. As will be discussed in the various sections of this study, the awareness and the requisite knowledge about identity theft is one of the most important factors in dealing with and fighting this insidious crime.

The above article provides some insightful and relatively contemporary statistics on the extent of ID theft. For example, the author notes that in recent years the "…. United States remained the top source country for security events generated with an overwhelming 79 percent, followed by Canada (5.7 percent), Taiwan (2.6 percent), Korea (2.5 percent) and the U.K. (2.4 percent)." (Internet Commerce Grows 88 Percent by Dollar Volume and 39 Percent by Transaction Volume: Fraud Remains a Concern)

Another online source that provides a wealth of relevant and contemporary data on these issues is (https://nudatasecurity.com/resources/blog/the-impact-of-identity-theft-its-not-just-about-the-money/Security). This is one of the better online resources and the Identity Theft section of this site is constantly updated with some of the latest information and data and provides a wealth of information on ID theft practices such a phishing, as well as possible solutions to these problems. An article that was particularly useful with regard to ascertaining the effects of identity theft and fraud on the corporate and banking security was Debit's Growing Popularity by Lauren Bielski (2006). This article explores the extensive impact of identity theft and fraud on various sectors and some alarming statistics. "Looked at as a group these incidents suggest a security flame-out and the perception that electronic information housed in computers is vulnerable. They also suggest that fraud seems to be mutating at a rate…"(Bielski, 2006).

How Well Do Consumers Protect Themselves from Identity Theft? by Milne, (2013) is an article that not only exposes the various ramifications of the effects of identity theft on the consumer, but also takes an in-depth look at measures that can be used to counter this intrusive crime. Like many similar studies, the extent of the problem is reiterated in this article;" The Economist (2001) reports that identity theft, defined as the appropriation of someone else's identity to commit fraud or theft, continues to be one of the fastest growing white-collar crimes in the United States." (Milne, 2003, p. 388) The article explores in detail the impact of this form of crime and the invasion of privacy on individual and business concerns.

It should also be noted that there are numerous studies, report and surveys that repeat figures and statistics which emphasize the increasing rate and incidence of identity theft in the electronic and digital environment. While many of these studies will be referred to in the course of the present study, this aspect will not be repeated. Security and Identity Theft and only some of the latest and most cogent data reflecting this factor will be referred to. There are also many other general overviews and studies of the ramifications of identity theft that will be cited in this thesis.

While there are many general studies that cover a wide and diverse range of information in this field, one locus that can be used as a baseline as it were in the literature is the impact of identity theft on the emerging ecommerce processes and markets. The reason for this is that it is in this area that contemporary research on identity theft is focused due to the consumer popularity and the increased importance of online commerce and shopping for all shades and styles of entrepreneurship and business. There has therefore been more research focus on this area than any other.

In this regard a work by Miyazaki and Fernandez, Consumer Perceptions of Privacy and Security Risks for Online Shopping (2011) is notable. The article provides some of the most significant information on this subject area. The authors discuss the issue of online shopping and the way that identity theft has influenced buying perceptions and views. One of the aspects of this article is the clear and concise outline of identity theft and the negative impact that it has on ecommerce.

In terms of online shopping and ID theft one should also bear in mind the plethora of information from reliable and validated sources on the Internet. It is to be expected that this topic should be of particular concern to online pundits and those involved in ecommerce. One study that should be mentioned in this regard is Online Privacy and Security: The Fear Factor (2006) from the well respected e-marketer Web site. This particular site also provides extensive and up-to-date statistics and views for specialists in this area.

Another useful resource is, OFT launches fact-finding market study of internet shopping. This article from the UK Government site ‘Office of Fair Trading’ is a “… new fact-finding study into online shopping is launched today by the Office of Fair Trading.” (OFT launches fact-finding market study of internet shopping) The site provides a wealth of data on the factors affecting ecommerce and the impact of identity theft. Reports by research companies such as Gartner also proved to be a reliable and invaluable contribution to the research into this topic.

There are also numerous studies which indicate that the importance of security, specifically in terms of online purchases and methods of ensuring transaction privacy, has become a central concern of ecommerce. There is an increasing realization that attention has to be given to security issues in order to build consumer confidence and to reduce the perception of risk in online sales, so that ecommerce can reach its true potential. It is also deemed to be important that the efforts made by business in this regard are seen by the public and that there is a reduction of any underlying doubt and suspicion relating to online transactions. There is the fear that if this is not achieved then media reports and other sources may increase security fears and reduce online purchasing.

Financial Fraud by Arjan Reurink explores the phenomenon of fraud in the context of financial market activities. Increasingly, it appears, financial fraud has moved from the fringes of financial market activity to become a widespread type of behavior throughout the industry. The aftermath of the financial crisis of 2007–2008 revealed a great number of scandals in which financial market participants infected the markets with fraudulent information to gain personal advantage. Despite the clear observability of this trend in the news media and the significant empirical implications accompanying it, mainstream academic research on financial markets has so far largely failed to account properly for this trend.

Perceptions of online fraud and the impact on the countermeasures for the control of online fraud By Faisal Alanzei this paper talks about the influence of identity theft on the environmental context. Combatting online fraud is facilitated when the public is fully educated and is aware of its types and of the prevention methods available. People are reliant on the Internet; the possibility of being breached by hackers and fraudsters is growing, especially as socialising, online shopping and banking are carried out through personal computers or mobile devices. Online fraud has been described as an epidemic that has spread to most online activities. Its prevalence has been noted to be in regions where there is high adoption of e-commerce, and, along with it, large online financial transactions. The argument is therefore the measures taken are either are inadequate or have failed to effectively address all the issues because of the organizational and environmental context of the country.

The Prevention of Internal Identity Theft-Related Crimes: A Case Study Researchby Romanus Izuchukwu Okeke This research set out three aims to answer the two questions. First, it provides understanding of causes, methods of carrying out and prevention of internal identity theft related crimes. Second, it extends a role-based framework (RBF) for the prevention of internal identity theft related crimes. Third, it evaluates the extent the RBF can be applied in the prevention of internal identity theft related crimes in online retail companies. It talks about how the rapid growth in the use of credit and debit cards in e-commerce, the online retail has been a key target for the internal identity theft related crimes perpetrators. Internal identity theft related crimes involve the misuse of information systems (IS) by the dishonest employees to steal victims' personal identifiable data. The crimes pose significant socio-economic impact and data security risks. In the context of online retail, relatively little research has been done to prevent internal identity theft related crimes.

RESEARCH METHODOLOGY

The research methodology adopted by the researcher is a doctrinal research. However the researcher with a view to compliment and substantiate his research paper corroborated his study with other forms of legal research such as comparative legal research, case studies and also critical analysis. It also throws light on the list of study materials and data and their sources, procured by the researcher as the instrument to conduct the research. Comparative legal research enabled the researcher to critically appreciate and compare the legal interpretations of various courts.

CHAPER 2-OVERVIEW OF IDENTITY THEFT

CHAPERT 2- OVERVIEW OF IDENTITY THEFT

2.1 What is Identity?

When we think of identity we perceive it as a physical attribute of a person. In ancient time, the only basis to recognize a human being was by means of his superfluous visual feature and by confirming whether it matches with some image stored in the past and if it was satisfactorily close, the person was accepted as the actual person concerned, or else, was to be considered an impostor.

While other living creature use other ways to identify each other i.e., smell. Human being also expanded their method of identifying each other as their mode of communication developed: so, sound became a means to identify. And as the society grew more complex new means were introduced to identify another human.

And as the human being evolved more intellectually the focus more shifted toward the wellbeing/interest of human being and in order to precisely identify a human being for security or financial purpose, ways of imitating a person and identifying him became more advanced. So the Identity characteristic may be measured into three types[3]

- Physical Attributes which is classified by way of Appearance i.e., Face, Stature, Gender or by means of Behavioral or Personality traits of a person or by Biology of a person i.e., biometric information (Voice recognition, DNA, Fingerprints, Retina or retinal patterns) and lastly by augmentation.
- Assigned Attributes i.e., Name, Address, Identifying number, Aadhar card no. etc. Financial credentials like Credit cards, Bank account, electronic information.
- Abstract Attributes What a person knows (Mother’s maiden name, Company of First T.V set, Refrigerator). Virtually all of the above-mentioned attributes are used at some point in order to recognize a person, with exclusion of attributes which are more tedious to draw out such as DNA or iris, retina forms. The “assigned attributes” needs related proofs (Birth

[3] IDENTITY THEFT; SOCIAL ENGINEERING AND CYBER CRIMES, https://shodhganga.inflibnet.ac.in/bitstream/10603/209150/12/12_chapter%202.pdf. Last accessed on 10/3/2020

Certificate, Passport, Credit cards, Identity Card). The assigned attributes can more easily be transported to another person than the physical attributes. Due to this Identity theft becomes an easier task for criminals.

So generally identity of an individual is to be understood as an assortment of unique and secure characteristics connected with the individual which differentiate them from others. Each such person, even two look-alikes will have a unique identity.

In legal perspective, identity includes the identification facet of a human being as per the government data through birth registration, voter ID, driving license, etc. It comprises the name, address, citizenship, physically unique feature (a scar or mole), photograph, and blood group information. This also helps the authorities to maintain a track of the individuals living in or visiting the region. Identity for the purpose of Identity theft crimes can range from Social Security Numbers to details of credit card account. It comprises of any such information which can be used by the criminal to take over the victim's identity to do countless offense. Section 66 C of the Information Technology (Amendment) Act, 2008 includes electronic signatures and password into the meaning of identity.[4]

Identity theft is alleged by various people to be a new occurrence. But truth be told it is accepted that the imitation and abuse of identity credentials has existed for a long time.

The issue related to the misuse of information related to identity was reported during the 1980s. Identity thieves used methods like pick-pocketing and stealing information related identity from mail boxes of people to get hold of and abuse people's credit and identification papers. The advancement of information technology and the rapid growth of digitalization is said to have changed the target and technique of such criminals. And it indeed technological advancement has provided identity thieves speed and the readily available personal information have provided identity thieves innovative ways to do offenses. Identity theft is a violation of the security which is necessary to the Internet and e-commerce transactions. With the increase in the use of latest communication technologies it has resulted in seen consequential increase in the act of identity

[4] DENTITY THEFT- A CRITICAL AND COMPARATIVE ANALYSIS OF VARIOUS LAWS IN INDIA Aishwarya Josh, http://jcil.lsyndicate.com/wp-content/uploads/2016/08/Aishwariya-Joshi.pdf. last accessed on 10/3/2020

theft as vulnerabilities in electronic networks are open to security flaws and hence breached. Identity theft disrupts the lives of thousands of people each year.

Defining what constitute identity in the present era, where a seemingly endless amount of data is available online or is held electronically, has been summarized by Joint Research Centre of European Commission as: Each person has a unique identity, but in the digital age, many pseudo identities exist, and these may be artifacts of a person or elements of a piece of hardware or software or even an organization. Other qualities, including the actions of persons, can be attached or linked to their identity, and people do not need to divulge their identity for all transactions.[5]

2.2 Is Identity Theft Part of Identity Fraud?

In 1994, Roger Clark said that: Human beings' identity is a fragile notion that needs deliberation at the various levels of psychology and philosophy. Identifying human beings, then again, is a realistic matter. In a diversity of circumstances in order to carry out a conversation or transact business every one of us needs to identify other human being[6]. On the basis of this very difference between the unclear and complex concept of 'identity' in comparison to the more practical dilemma of 'identification', the use of the term 'identity' in combination with 'fraud', 'theft', and 'crime' or other similar terms has undergone a lot of criticism[7]. However, there is a conceptual need to define the term identity and to coin more correct meaning and use of term 'identification' so that it isn't confused with the term 'identity', so the net probable line of direction would be the definition of 'identity fraud', 'identity theft', and 'identity crime'. Now the more feasible term that should be used is 'identity crime' or 'identity-related crime' which might be terminology-wise more appropriate. Because it is difficult to link the legal definition of 'theft' to a data-centric concept of 'identity' since even when a person loses his identity he doesn't get dispossessed of it because of the informational characteristics of identity. So, it renders the transfer of the status of property meaning thereby theft complex. It does not necessarily end up falling into the categorical definition of the theft just because one person is wrongly using the identity of some other person

[5] Definition by WordNet Search 3.0. As of 25 January 2011, available at: http://wordnetweb.princeton.edu/perl/webwn
[6] Clark (1994)
[7] Sproule & Archer (2007)

does not automatically mean that the victim is dispossessed of his identity. So, the use of legal definitions of theft or fraud may result in having a confusing impact if consider both of its definition and then definition which would be understood if we use the term ‘identity theft’ or ‘identity fraud’. As defined under the Indian Penal Code (and it also applies to many other criminal laws in the world) theft entails the loss of possession of corporeal goods; as a result the application of the notion of theft with respect to identity might be restricted. Use of the term of ‘theft’ may also weaken the actuality that there can be not only a criminal aspect to identity theft/fraud but also a civil which may bring in a tort liability for damages.[8] A broad definition of ‘identity crime’ will cover any crime which involves the deceitful use of information related to identity, even if that information relates to a living or deceased or natural person, to any legal person or to fictitious person. Mistreating identity related information would in turn require stealing it, falsifying it, or accessing it illegally by other means.

Now the general understood difference between identity theft and identity fraud is as below:

Identity Theft happens when someone has access to personal information of an individual, such as their social security number, credit card information, their driving license number, and other important data to be able to impersonate them, is committing of identity theft. Once he has all this information, the thief usually opens up new credit account, buy a cell-phone, and other things in the name of the victim. The thief can also use victim’s information to gain access to his existing accounts to commit crime.

- **Identity Fraud**. Identity fraud refers to a crime where a thief creates a made up person and also fabricates personal information. Instead of stealing an individual’s identity, the thief takes up a easier step which is making up an identity from their imagination. A person committing identity fraud typically does "true accounts identity theft" he also opens new accounts of credit in the name of that fictitious person.

It can be easily seen there are some underlying distinctions between these two classes of crimes. Identity theft requires involvement of the individual, whose personal information is stolen. While the victim of identity fraud will include the credit card companies, lenders, merchants, or other organizations, but it will not be the fictitious person.

[8] FIDIS (2006)

2.3 What is new?

As the above discussion already demonstrate that the bulk of identity fraud cases will fall in the domain of the conventional idea of fraud. It also means that if we adhere to a strict legal perspective there is no requirement to pay heed to identity-related fraud because most of it will not even fall into the category of fraud as we understand now. Then we are faced with a new question why should we handle identity related fraud as a distinct category of crime? Even though it will not be an inevitable conclusion that identity related fraud is a fundamental category in its own, but for several reasons it also merits special treatment. Essentially, fraud happens in different forms and on an unknown scale and because of the new function of identity management in the information culture in person business has increased which had paved the way to on-line service-provision and e-commerce, and the information world is based on even more intricate web of communications in intricately entwined relationships. This entails that identifiers such as names of persons and numbers and figures associated to them have become more important as indispensable entry points for social connections and without having ID, nothing happens. And with the new position of identity in information world, identity fraud is coming out as an inevitable outcome. The new scale and forms of identity management creates more opportunities for criminals. Phishing (fishing for personal information online to utilize it in economic services) can be taken as a prime instance of such new phenomenon, which has been growing from last few years. To fight with these new types of fraud efficiently not only it should be studied that whether present legal provision must be extended or not, but also more importantly, plans should be developed specific to the crime of identity fraud. This also requires sufficient insight and perception of the vulnerabilities of identification management, forming a reasonable mix of technical, legal, and socio-economic measures. A major part of any identity related fraud combating policy is raising awareness and this is also a reason to treat identity related fraud as a particular category. Opportunities for identity related fraud thrives only if people build up and use identity managing technologies without paying attention to its potential for misuse. It can only happen when people are educated about the risks of identity related fraud, that’s how even the weakest of the links in identification related vulnerabilities can be strengthened. Another reason why we should look at identity related fraud as a distinct category is the perspective of the victim. Illegal identity invasion i.e., identity theft differs from conventional fraud in two primary ways. First, it might take a while to the victim to perceive the crime, which may be after a long the identity theft has occurred. Second, the victimization may continue even after the crime has been committed a long time ago, since, opposing to most conventional cases of fraud, a characteristic of identity invasion is that the individual is blacklisted and has trouble in repossess their credit history and the trustworthy image. This complexity is one more characteristic of present identification management. It is for that reason is so important to study the particulars of identity related fraud in order to support the victims efficiently.

2.4 Types of Identity Theft

The offense of identity theft comprises of two steps that may or may not be done by the same individual, which is namely:

1). Wrongful collection or obtaining of personal information of any person.

2). By using such information wrongfully with purpose of causing lawful harm to that person.

The first step of deceitfully acquiring of someone's personal identification information can be done in several ways. It can be done by the stealing such information and then deceitfully using such information or by buying the stolen identity from someone in such illicit trade[9].

Criminal Identity theft

Criminal Identity theft occurs when someone is arrested for impersonating another person to commit a crime presents by using that individuals' details and personal information for example When someone have knowledge about personal information of some other individual such as his name, date of birth, address, or driver's license, etc, they can give that information to authorities when being arrested or getting caught doing something illegal. Which results in the creating criminal record of the victim who have no knowledge of the crime committed or and he might not know about such crime until it's

[9] THE EVOLUTIONAL VIEW OF THE TYPES OF IDENTITY TH EFTS AND ONLINE FRAUDS IN THE ERA OF THE INTERNET, Internet Journal of Criminology © (2011), available at www.internetjournalofcriminology.com/wang_huang_the_evolutional_view_of_the_types_of_identity_theft s_and_online_frauds_in_the_era_of_internet_ijc_oct_2011.pdf

too late or unless summoned for it. It becomes difficult for the victim to clear their records as the jurisdiction for every crime is different and it becomes more difficult to find the true criminal.

Financial Identity theft

Financial Identity theft is taking over of the individual's account by the criminal by thieving that individual's personal information. In such identity theft the main goal is to obtain the credit card information of the victim or to withdraw the money from the account of the victim.

Synthetic Identity theft

Synthetic Identity theft refers to forging someone's identity completely or partly and is the most common identity theft i.e., legitimate Social Security number with fake personal information, such as birth date, name, and address. It is most commonly used by the offenders by merging the genuine personal information of the injured party and some fake credentials in order to create a false document. Then this fake document is used by the criminal for the purpose of application of a loan, obtain a duplicate license, apply for credit, etc.

Identity cloning and concealment

Identity concealment and cloning happens when someone's identity is used as someone else in order to hide his true identity. It is mainly used by migrants. An individual may opt for the visa or other document by using false information and thus, covering up the actual identity. Terrorists always use this to impersonate someone else.

Medical Identity theft

Medical Identity theft commonly happens when the offender or someone uses the information of any individual such as your name, Social Security number, Medial care number, or health insurance benefit or other information to get recommended drugs or to get appointment with the doctor or to claim the benefit of the insurance. Which results in the medical history of the criminal being added to that of the victims.

Child Identity theft

This theft is children focused, especially those minors, who have no credit history. Criminals see this as "blank slate" an opportunity which in results makes children a prime target to being victims of identity theft. When a child's identity is stolen by some person to gain some illegal benefit is known as child identity theft. In this case the imposter can be anyone an unknown but most of the time a friend or even a family member who targets the child.

2.5 Methods of Identity Theft

Phishing

Phishing refers to the collecting sensitive information of a person by sending him deceiving emails. That person is then made to think that the email is sent by some official source or the one which is required by the person receiving such email. For Example, a bank or a firm in which that person works. The swindler sends an e-mail with a link with attached fake web address which resembles authentic link where information as to personal details and account will be asked. The reasons shown for asking such information from the customer to keep his information up to date so that better services can be provided by the bank, or claiming that if the customer fails to provide such information then it will amount to suspension of his account[10].

Smishing:

Smishing' is a hybrid version of *'Phishing'*. In Smishing, instead of sending the mail to the person the criminals use text messages to obtain the personal information of that person. Now these cyber-criminals more often use social engineering methods to attract victims to obtain personal information of the victim. These cyber-criminals generally direct the victims to open any link or to make a phone call on a specific number.

[10] Neeraj Aarora, Identity Theft or Identity Fraud | A Platform to discuss & analyse Financial and Cyber ForensicsA Platform to discuss & analyse Financial and Cyber Forensics Neerajaarora.com (2009), available at www.neerajaarora.com/identity-theft-or-identity-fraud

They do it by requesting that an instant action is required to avoid loss or to avail any advantage of the offer and thus finally stealing the personal information.

Vishing

Vishing is the amalgamation of two words “Voice” and “Phishing”. In Vishing the cyber-criminals use normal phone calls or Voice over Internet Protocol (VOIP) to obtain the personal information of the person. They often create fake Caller IDs or profiles in order to be seen as legitimate source. In vishing the impostor calls the person by pretending to be a firm or bank representative or a call center employee, thereby tricking the person in disclosing some sensitive information about his identity.

Pharming

Pharming refers to the cheating by installing any malicious code or program on the personal computer or server by a cyber-criminal hence misdirecting the users to a sham website without their knowledge or consent. Pharming is often done by disguising all the fake, fraud and data grabbing websites as genuine and trusted ones. It is very similar to Phishing but here when clicking on the valid link given of the bank website instead of entering the legitimate/real internet address user would be redirected to a false site. Since, it is usually done by installing a malicious code in the personal computer of user or in a server which makes it easy to target various users at the same time. It happens without the consent or knowledge of the victim and is often called “Phishing without a lure”.[11]

Credit Card Skimming

The person suffering from of credit card skimming finds fake withdrawal of money and charges on their account and all this happens while the victim has the possession of his credit card.

Most often it is done by installing a small device to steal the information from the credit card which such as the number on the credit card, expiry date on the card, name of the cardholder, etc. All of

[11] SearchSecurity, What is pharming? - Definition from WhatIs.com (2007), available at http://searchsecurity.techtarget.com/definition/pharming

this data of the credit card is stolen by the help of a device called a “skimmer”, and it is done when credit card is swiped on the skimmer all the data which is stored in the magnetic strip of the card is obtained by the skimmer. Once all the information is gained, a cloned credit card is made to make numbers of transaction in the name of the victim. Victims of such skimming are often oblivious of the theft. Such credit card skimming can also take place by hiding camera to steal the PIN of the ATM card.

Hacking

Hacking is done through installing malware in computer like viruses or software which are used to redirect information to the hackers who then decrypt such information and either use it for themselves or sell it to some other person who may then commit fraud using acquired information. Attacking a computer in such way can happen by disguising infected links or by offering free software download or by signing in through social media account or when computer is not protected by proper firewall protection or lack of strong password to protect the networks and computers. Cyber-criminals most often hack the computer of any person and then control the actions of that person. [12]

Unsecured websites

People should make sure that the website that they are trying to access or accessing is secure before doing any transaction. An unsecured website leads to the stealing of sensitive personal information of that person. He should also ensure that the website is using “https” and not “http”, “s” means that the website is secure. This reduces the chances that the personal ID and password of the user will be compromised.

Weak passwords

People who often use weak passwords for their social media account and ATMs PIN are often vulnerable to the cyber-crime. This makes it easier for hackers to guess such passwords and steal the personal information of that person. So, it is always recommended

[12] Privacymatters.com, Computer Hacking and Identity Theft | PrivacyMatters.com, available at www.privacymatters.com/identity-theft-information/identity-theft-computer-hacking.aspx

to use a longer and strong password with a combination of alphabets, special characters and numbers and not to share them with anyone.

By targeting children online

Children are easy prey on the internet and they easily share their passwords without even knowing its consequences. Therefore, the parents must remain vigilant and instruct their children to not share the password with anyone. Some other type of methods consist of online frauds like business transaction fraud and advertisement click fraud which involves online payment by any unsecured gateway[13]

So, after the very first step of unlawful collection or stealing of personal identity information is complete, next step is to achieve economic enrichment by criminal like taking out of money from the account of the victim or applying for bank loans in his behalf, credits cards, taking advantage from any government proposal in the name of the victim whose identity is stolen. This design of new ways of identification by means of an already existing identity of the victim is known as breeder identification. The criminal might not have been capable to take advantage of such amenities if he had applied for it in his real name.[14]

[13] Dazeinfo, Internet Users In India: 354M, 60% Access From Mobile [REPORT] - Dazeinfo (2015), available at http://dazeinfo.com/2015/09/05/internet-users-in-india-number-mobile-iamai/

[14] ibid

CHAPTER 3-IDENTITY THEFT IN CYBERSPACE

CHAPTER 3 - IDENTITY THEFT IN CYBERSPACE

The explanation for the significance of identity theft in the current times is because of the growing importance of identity-related data in the e-governance, economy and in social interaction. In the past only having “good name/reputation” and good personal relations with others dominated business and all the daily transaction. With the change to electronic trade, face-to-face identification of a person and relying on his good reputation became hardly possible, and, as a result to that the identity-related data in doing business became more relevant for the interactions in socio-economic transactions. For the ease of transaction the non- physical method of identification is suitable to norm for e-commerce businesses or e-governance. For example, while buying any item online, when the buyer enters his card information that just not only identifies the buyer, but also verifies legitimacy of the payment from the identified buyer. This is for the easiness of carrying out business, but lack of proper cyber knowledge, education and lapses in the cyber security leads to cybercrime of identity theft which results in the stealing of identity of the unaware victim or by authorised access to victim’s account.

Cybercrimes generally means “crimes that are done against persons or groups of individuals with a criminal intention or motive to harm the reputation/name of the person or to cause him physical or mental loss directly or indirectly with the use of modern telecommunication networks such as Internet, social media accounts, chat rooms, emails, etc, and through mobile phones by sending SMS or MMS)”[15] . It is offense of modern times which includes unlawful activities in cyber space, where any e-communication tool or information system, or internet can be used as a device or target and maybe both. Cyberspace is a virtual space where contact over computer network happens so; it is a place with no geographical location and it is accessible to any person, from any place in the world who have access to internet.[16] In the recent times with the rising reliance on internet, computer and advanced technology and with the digitalization of diverse services,

[15] Halder and Jaishankar, Cyber Crime and Victimization of Women: Laws, rights and Regulations, 2011, ISBN no. 978-1-60960-830-9

[16] Dr SR Myneni, Information technology law (cyber laws), 1 st Edition, Asia law house, Page no. 33

cybercrime is also on rise and it is becoming a threat which needs to be immediately contained. Like other technologies, internet and similarly linked technology also have positive and negative sides coupled with them. Although there are indisputably many advantages of internet but at the very same time it has also provided ease to the criminals for commission of some crimes. And one of such crime is identity theft happening in cyberspace. Identity theft is a cybercrime where the identity of any individual is stolen to obtain any illegal financial benefit or to mislead others and it may also in some cases causes threat to that individuals personal safety. Whenever the identity theft is done over the cyberspace, it is known as online identity theft or identity theft in the cyberspace. While the name of this crime is a little deceptive because when anything is stolen from the victim he gets dispossessed but in the case of identity theft if someone's identity is stolen, he doesn't lose his identity. Basically what constitutes an identity of any person whether he is alive or dead? It means and includes personal information such as his name, date of birth, e-mail ID, information relating to bank details, IT return forms, medical insurance, etc. The terms Identity theft and identity fraud are commonly interchangeable and it refers to and covers all types of offences where someone wrongfully gains and uses someones personal information in any way that includes scam or deception, usually for financial gain". There are many ways through which such offences are committed such as hacking accounts, phishing, denying of services, spear phishing, distributed denial of service, data theft, installation of spyware, cookies, e-mail/SMS spoofing, etc.

The reporting of this crime and the matter of determination of Jurisdiction, investigating authority and trial of these crimes are not similar to the conventional crimes. The law enforcement agencies in such cases are required to have a detailed knowledge and expertise in the computer and internet to undertake such crimes to enable speedy trial and just punishment o the criminals. The occurrence of such crimes are increasing rapidly and causing considerable financial loss to private sector as well as to the government in India and around the world. According to National Crime Record Bureau, India recorded 9622, 1192, 12317 and 21796 cybercrimes in the years 2014, 2015, 2016 and 2017 respectively[17]. And according to the same bureau, the year 2018 recorded 27248 cybercrimes out of which, 55.2% (15,051 out of 27248) were registered for the motive of fraud.

[17] https://www.livemint.com/companies/news/cyber-crime-cases-in-india-almost-doubled-in-2017-11571735243602.html

According to the Norton Cyber Security Insights Report 2016, 49% of India's online population, or more than 115 million Indians, are affected by cybercrime at some point which makes the country's ranking second in terms of highest number of victims. And with the rising use of cloud computing that provides numerous accesses to files which make the stored data far more susceptible to such threats of cybercrimes. These developments in it are proof of lack of proper law and which in turn demands that an efficacious and robust Legal Redressal machination and a preventive measure should be devised to prevent this crime. And to achieve this goal everyone must be educated about the risk associated with using internet and awareness as to its safe usage.

There are different cases through which we can understand Cyber Crime in India.

1. Pune Citibank MphasiS Call Centre Fraud[18]

In present case, one of the ex-employees of the company MphasiS Ltd cheated US customers of Citibank. It was done by getting unauthorized access to the personal information available in the Electronic Account Space of the customers.

It was held by the court that that the above crime falls under the Information Technology Act, 2000 where use of any electronic documents is a crime when such document is used through 'breach of trust', 'cheating', 'and conspiracy', etc. So this was considered as offense under the Section 66 and 43 of the Information Technology Act, 2000 and they were sentenced to be liable for imprisonment with fine.

2. Sony Sambandh Case[19]

In present case, a complaint was filed against Non-Resident Indians by Sony India Private Ltd. The website Sony Sambandh helped them to send Sony products to their friends and family in India after paying online. Someone gifted a Colour Television and wireless headphones to Arif Azim. The payment was made through a credit card, after payment the product was delivered to

[18] Pune Citibank Mphasis Call Center Fraud - leading case, on: July 30, 2013, https://www.legalserviceindia.com/lawforum/cyber-laws/17/pune-citibank-mphasis-call-center-fraud-leading-case/2236/

[19] Sony.Sambandh.Com Case - India saw its first cybercrime conviction on: July 30, 2013, http://www.legalserviceindia.com/lawforum/cyber-laws/17/sony-sambandh-com-case-india-saw-its-first-cybercrime-conviction/2242/

Arif Azim. Later the company was informed that the real owner of the card has declined doing any such transaction and the transaction was claimed to be unauthorized.

The company then filed a complaint to the Central Bureau of Investigation under Sections 418, 419 and 420 of the Indian Penal Code. After the investigation, Arif Azim was detained and he was questioned where he told that through his job at call center he somehow gained access to that credit card number and he then misused it.

This was India's first cybercrime conviction in 2013 and CBI recovered the headsets and colour television. The CBI established the case with evidence and the offender admitted his crime. The Court sentenced Arif Azim under Sections 418, 419 and 420 of the IPC.

3. The Bank NSP Case[20]

This is one of the most important cybercrime case in this case one management trainee of bank broke up with his girlfriend to whom he was promised to married. Later, that girl created a fake email id and started to send emails to the foreign clients of the trainee from the bank's server. Which resulted in the loss of the clients to the company which then dragged the bank to court and but then it was found out that it was not bank's fault but bank was also a victim of cybercrime.

4. Andhra Pradesh Tax Case[21]

In Andhra Pradesh one of the government officers exposed a businessman. Who was the proprietor of a plastics compamy and after he got arrested by the Vigilance Department around Rs. 22 crore cash was recovered from his house.

[20] A Critical Analysis of Cyber Phishing and its Impact on Banking Sector, https://acadpubl.eu/hub/2018-119-17/2/128.pdf

[21] Case study cyber law - Andhra Pradesh Tax Case, Monday, July 27, 2009 http://cyber-law-web.blogspot.com/2009/07/case-study-cyber-law-andhra-pradesh-tax.html

The accused used to present fake vouchers to prove the legality of his business, but vigilance department searched his personal computer and found out that he was running around five businesses under the cover of one company.

5. SMC Pneumatics Pvt. Ltd. vs. Jogesh Kwatra[22]

This is India's first ever case of cyber defamation, the offender Jogesh Kwatra used to work in plaintiff's firm and but he started sending insulting, demeaning, derogatory, obscene and offensive emails to other workers and owner and to some other firms those were also related to his company just to injure the reputation of the company as well his Managing Director Mr. R. K. Malhotra.

The plaintiff then filed suit against the defendant in the Court. The court held that the emails which were sent by the accused to the people were extremely slanderous, obscene and offensive in nature. The learned counsel of the plaintiff added that the offender wanted to tear down the reputation of the plaintiff. So, he should be restricted from sending such types of mails and anyone else who coddle in such type of actions will also be fired.

The Court finally after hearing the both parties passed an ex-parte injunction in favor of the plaintiff to stop those emails from being send.

6. Bazee.com Case[23]

In December 2004, the CEO of bazee.com was under arrest because his website solds a CD with dubious content. But the same CD was also accessible in few areas in Delhi. Leading question in this case was who should be made liable here, the Content Provider the or Internet Service Provider? Finally the CEO was released on the bail to prove that as he was only the Service

[22] India: Cyber Defamation In Corporate World by Pradhumna Didwania,31 January 2013. https://www.mondaq.com/india/social-media/218890/cyber-defamation-in-corporate-world

[23] India: The Bazee.Com Saga Unravelled: Supreme Court Clarifies Intermediary Liabilities For Hosting Obscene Content, 28 February 2017, https://www.mondaq.com/india/it-and-internet/572042/the-bazeecom-saga-unravelled-supreme-court-clarifies-intermediary-liabilities-for-hosting-obscene-content

Provider his liabilities were not as extensive as that of the Content Provider. This case raised basic questions on handling of cybercrime cases.

7. State of Tamil Nadu vs. Suhas Katti[24]

This is one of the important cases in the cyber law for its speedy justice. In the present case, a man who was a family friend of the victim was posting obscene, slanderous and humiliating messages about the victim. The accused was sending mails to the other women to collect information through a sham account he made in the name of the women. The accused sought after the lady rather for marriage but she married someone else which afterward resulted in a divorce. He contacted her again after the divorce but again she rejected him. Due to which the accused started harassing her through the internet. Because of that victim started getting a lot of phone calls asking why she was collecting such information or if she was soliciting the same. So, in February 2004, the victim filed a complaint and the accused was found he got arrested by the police within few days..

He was accused under Section 67 of the Informational Technology Act, 2000 and Section 469 and 509 of the IPC. The Court finally held that the man was guilty and charged him with both imprisonment and fine. This was the first ever case where conviction was under Section 67 of the Information Technology Act, 2000.

8. Nasscom vs. Ajay Sood & Others[25]

This is one of the landmark judgments in cyber crimes as this case deals with the definition of ‘phishing’ on the internet. It defines it as an unlawful act entitled for recovery of damages and an injunction. The plaintiff in the present was the National Association of Software and Service Companies (Nasscom) which is India’s leading software organization. The offenders were the placement group which was hired by Nasscom to recruitment and headhunt.

[24] State of Tamil Nadu Vs Suhas Katti - Cyber law case in India, https://www.legalserviceindia.com/lawforum/cyber-laws/17/state-of-tamil-nadu-vs-suhas-katti-cyber-law-case-in-india/2238/

[25] Case study cyber law - Nasscom vs. Ajay Sood & Others, http://cyber-law-web.blogspot.com/2009/07/case-study-cyber-law-nasscom-vs-ajay.html

The accused started sending emails to third parties in the name of plaintiff to obtain confidential information which they used in headhunting. Hence they were accused of phishing which is an internet scam where an individual pretends to be an organization to gain personal data from customers such as access codes or passwords, etc.

The Court then appointed a committee to search the offender’s premises, where they found two hard drives through which the mails were sent to customers by the accused. The offensive mails were downloaded and presented as evidence. The offenders used different fabricated identities to evade identification and legal action.

The arties later settled the dispute through compromise and the accused to paid Rs. 1.6 million to the defendants for the violation and damages of their trademark rights.

9. Cyber Attack on Cosmos Bank[26]

In August 2018, Pune branch of Cosmos Bank was target of a cyber-attack in the which it was drained of Rs. 94 crores. The assailant hacked into main server of the bank and transferred the money to account in a bank in Hong

The hackers somehow found a link between the centralized system and the payment gateway that’s how they was able to compromise the system, which means that both bank and account holders had no idea that the money was being transferred.

This attack was massive and one of its kind of malware which somehow attacked and ended all the communication link between the bank and payment gateway. This attack caused a lot of pecuniary injury as to there were around 14,000 transactions across more than 28 countries by using 450 cards and among them were 2,800 transactions in which 400 cards in India were used.

[26] Cosmos Bank's server hacked; Rs 94 crore siphoned off in 2 days https://economictimes.indiatimes.com/industry/banking/finance/banking/cosmos-banks-server-hacked-rs-94-crore-siphoned-off-in-2-days/articleshow/65399477.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

10. BSNL, Unauthorized Access[27]

In the present case, JANET (the Joint Academic Network) was hacked which constrained the access of authorized users by changing the passwords and adding/deleting records saved in their account.

The company had to file a cyber-crime case and CBI investigated this case and found that the broadband internet of the company was being used by someone without the permission. The accused used different VPN's to piggyback into the server of the company from different sources.

The accused was then sent to prison and was fined to pay Rs. 5,000 under Section 66 of the Information Technology Act, 2000 and was also charged under Section 420 IPC.

[27] BSNL, ISRO cases show India not a country for ethical hackers, https://economictimes.indiatimes.com/tech/internet/bsnl-isro-cases-show-india-not-a-country-for-ethical-hackers/articleshow/63278882.cms?from=mdr

CHAPTER 4-THREAT OF IDENTITY CRIME AND ITS ASSESSMENT

CHAPTER 4- THREAT OF IDENTITY CRIME AND ITS ASSESSMENT

Mainly, identity violations are crime already in the work." This is principally in light of the fact that in the current PC age, individual data is more open than any time in recent memory and the quantity of hoodlums searching out this data is consistently on the ascent. This section tends to two unique parts of character wrongdoing:

1) threat agents, and

2) the impact of identity crime.

Threat agents are those components or individuals that make identity theft conceivable or more probable. The chance that one can address ahead of time the threat agents that is, the variables that may prompt, or the individuals who may carry out, a character wrongdoing, at that point it is conceivable that the identity theft won't be submitted. In any case, disposing of identity theft altogether is unimaginable in reality, so it is helpful to look at in the second piece of this section the effect that character violations have upon people and associations that are deceived by such wrongdoings.

4.1 Identity Crime Threat Assessment Model and Threat Agent Identification and Analysis

The Bike Analogy Suppose you have a bike. One day, someone steals it. How do you handle it? Do you get another bike, or do you give up biking altogether because of the threat of theft? Perhaps you'll try to mitigate the threat agents," those things that make a bike theft more or less likely. You could get a better lock. You could avoid riding in neighborhoods you perceive as places where theft is more likely to occur. You could bring your bike inside at night, since thieves are more likely to operate under the cover of darkness. In most cases, you will not stop riding your bike. You will take the steps necessary to reduce the risk of it being stolen. You become more aware of the risks, the things that make theft more likely and you continue to enjoy your bike.

Just as it is with the bike analogy, so it is with identity crime. At the point when you know the dangers and dangers that make identity crime which is bound to happen, you can find a way to mitigate their effect. You don't surrender your Mastercard or quit utilizing the Web since they speak to dangers to your identity. You find out pretty much all the threats that apply to identity violations and make a move to keep away from it totally or decrease the harm as well as misfortunes that may emerge from them.

There is a propensity for governments, organizations, and different authorities to concentrate on only a couple of danger operators when devising a counteraction systems and remedies for loss caused for character wrongdoings. Be that as it may, it is essential to think about all the threat agents and how they collaborate with one another to develop a complete identity crime moderation approach.

4.2 Threat versus Risk

A threat can be viewed as a component of a threat agent's inspiration, capacity, opportunity, and the effect a wrongdoing may have on the individual or association against whom it was done. As indicated by Webster's Word reference, threat " indicate something impending while dangers" represents to a possibility of a physical issue or misfortune. The Oxford Word references characterize threat' as the statement of an intention to exact agony, injury, harm, or other antagonistic activity on somebody in requital for something not done or done; someone or something prone to cause harm or risk. So it can be seen that with identity crime risk, chances of the likelihood that a danger will be effective, along with the degree of the potential misfortune caused.

Threat assessment has normally been a part of or can be used is analyzed by managers to decide the expenses and advantages of taking any specific action. Risk analyses are quantitative, depending on the figuring of numerical probabilities, or subjective to sorting expenses and advantages as far as low/medium/ high potential. Most threats challenge any sort of likelihood, in probability analysis in all case. But the existence of new threats, for example, those introduced by identity crime in the internet age, has made most existing threat assessment models insufficient. Since the ideas of risk and threat are unique, they should be dealt with in a different way.

4.3 Threat Assessment

Threat assessment offers to characterize, investigate, and comprehend the dangers that apply to their specific exercises. For instance, as to identity crimes a threat assessment can reveal the vulnerabilities in a credit card processing framework that take into account its misuse by criminals. An effective appraisal will prompt the formation of countermeasures to shield vulnerable areas from such misuse."

Threat assessment includes an assurance of dangers identified with vulnerabilities of identity crime casualties and the abilities of criminal threat agents. It ought to likewise think about the cost/advantage components of any methodology intended to control identity crime. In the event that the expense of a program planned for decreasing the danger of a wrongdoing is high, however the specific variable focused on has an exceptionally low pace of event or an minimum loss impact, the program will not be as helpful or effective in diminishing actual crime percentages as one that tends to cause a high-loss variable and it often happens. What's more, if potential loss is identified with a specific threat agent are low while the cost is high, it may not be advantageous for associations to make any move to decrease or forestall the danger.

The effect of identity theft is identified with the increase or advantage acquired by the wrongdoer after perpetrating the crime, joined with the victim’s loss. Organizations ought to create danger investigation models that address each sort of identity crime so as to make avoidance or relief methodologies that are proper to the risk in question. For instance, the effect of an identity crime submitted concerning migration status is high when the danger of expanded international mobility for terrorists is considered.

There are two significant measurements to risks: likelihood and effect. Likelihood alludes to the way that an event may happen, while impact means to the different money related and non-monetary expenses related with the risk that occurs If a risk has a low likelihood and a low effect, it is usually overlooked, while high-impact/high-likelihood dangers are tended with much attention.

4.4 Threat Agents.

Threat agent" is a term that typically used for an individual or gathering that has the apparent capacity to undermine another individual or gathering. As some author expressly said,

"It is the threat agent that deal with the dangers, and not the security officials. A threat agent may likewise, in any case, be some other factor or power, for example, a power outage, tornado or other similar tragic unforeseen occasion that can make devastation for an individual if the occasion harms or modifies the individual's PC records, ledgers, or other individual data. Recognizing threat agents is a continuous procedure that must adjust as conditions and technological advances takes place, and threat agent may acquire new abilities after some time.

Threat agents can be seen in corporate settings as PC viruses or other malware, representatives and additionally subcontracting upkeep staff and security watchmen, psychological oppressors or terrorists and other ideologically spurred people.

As far as identity crime is concerned, a threat agent might be a profoundly prepared and well-funded proficient employable from an opposing government playing on fear based oppression, or an individual from a psychological militant gathering with its own political plan. Sorted out crime groups are keen on purchasing and selling taken personality and monetary record data, including financial balance numbers, Visas, or other information and archives that can be changed over to cash or influence to carry out different violations. Vandals, composed wrongdoing gangs, and even natural catastrophic events like flames or quakes are threat agents.

.

4.5 Identity Crime Threat Agent Assessment.

A threat agent's evaluation is valuable for adjustment, anticipation and deterrence purpose. It is intended to find out the exercises and procedures that can limit or potentially decrease identity crimes most adequately. It has additionally been created to help in making a savvy anticipation technique for personality violations and to limit the effect of such violations on singular crime and society overall. By getting an inside and out comprehension of every danger specialist, it is conceivable to recognize the variables that expansion or reduction the likelihood of a personality identity crime from happening.

A subjective threat assessment accentuates the requirement for a more in-depth investigation of the particular factors related with identity crime threat agents. The rundown of factors distinguished here by no means extensive or exhaustive, yet it represents the beginning stage for associations organizations thinking of making relief projects to address identity crimes.

Identity Crime Threat Agent is a component of the accompanying factors:

1. Capability
2. Commitment
3. Effort
4. Gain to the offender
5. Potential loss to the victim
6. Motivation
7. Neutralization
8. Opportunity
9. Probability of loss occurring
10. Probability of arrest
11. Repercussions of arrest
12. Reason for motivation
13. 13 Exposure to crime or victim vulnerability

Governments, law enforcement officials, and business authorities can focus their efforts to impact seven variables

1. Potential loss to victims or magnitude of the potential loss (Impact)
2. Gain to the offender

3. Effort required to commit the crime
4. Repercussions of arrest
5. Probability of loss occurring
6. Neutralization
7. Exposure to crime

Moreover when experience to offense decreases, the threat of identity crime decreases, so if the gain to the criminal is lower than the threat rate is lower. When the endeavor to do the crime rises, the threat risk lowers. The elements that control the result in a lower identity crime threat are:

1. Reduced exposure to crime.
2. Lower gain/benefit to the offender.
3. Increased effort to commit the crime.
4. Increase in repercussions of arrest for the crime.
5. Increase in probability of arrest for the crime.
6. Reduced neutralization or justification for the crime.

Decrease in circumstance of gain and opportunity decreases the responsibility and additionally the capability expected of a wrongdoer to carry out a identity crime. With an expansion in Ability or potential commitment the opportunity may increase too.

On the off chance if the potential loss is low, it may not be lucrative to make any move to lessen or keep threat agents from showing. When managing risk, 'an enormous potential of misfortune and a low likelihood of it happening is regularly treated differently in contrast to one with a low potential misfortune and a high probability of happening

A crime always relies upon the assets accessible to the guilty party. The criminal must have the ability to carry out the crime. Various kinds of violations require various degrees of capacity. Some require explicit specialized ability, for example, falsifying identity records. Others require insignificant capacity, for example, utilizing a companion's name when addressed by police or while speaking to oneself on the web.

Most identity criminals get individual data by buying it from others, taking it from post boxes, or discovering it in the junk. Indeed, even these basic strategies require a specific capacity which the criminal must use so as to carry out the crime. After some time successful identity criminals, create explicit abilities that empower them to carry out their crimes. Notwithstanding mechanical aptitudes, identity thieves may have certain mental capacities, for example, instinct and social abilities that upgrade their capacity to pull off a crime.

On the off chance that a identity criminal has the capacity to carry out a wrongdoing, it implies that the individual in question has the information and apparatuses required to do as such, just as the capacity to use them adequately. Notwithstanding tools, abilities, and information, the capability to perpetrate a wrongdoing may incorporate relationship with others who may give help and backing to the guilty party. Some identity wrongdoings require more asset abilities than others.

For instance, identity wrongdoings that depend on the utilization of PCs require a specific degree of information. The utilization of malware implies that lawbreakers need to realize how to compose or actualize malevolent code that will introduce a shortcoming in a PC network. Or on the other hand, if the criminal doesn't have the PC abilities required to create malware, the person needs to have the monetary assets to purchase a specialist to actualize it. At any rate, an identity criminal who needs to utilize innovation to acquire identity related data ofsomeone must know how and where to discover the ability necessary to carry out the wrongdoing. Another case of ability to carry out a wrongdoing includes having the correct equipments. On the off chance that an identity criminal needs to acquire account numbers from Mastercard holders or from ATM card clients, a 'skimmer" is required. A "skimmer" is a specific gadget that can duplicate the data remembered for the magnetic strip of a Mastercard. At that point, to utilize that data, the identity cheat either needs the hardware for copying the card as well as other details.

Whenever the chance to perpetrate a identity related crime diminishes, or if there is a decreased gain to the offending party, a higher level of commitment or potential ability is required. As capacity builds, the opportunities themselves presents to the criminal and in turn his will in general will increase too.

If a criminal's dedication expands, the person in question may find extra chances to make that crime to occur, consequently improving the probability that the crimes will be perpetrated. Committing of a criminal offence is anything but an aloof procedure, however it emerges from the manner in which a criminal deciphers the dangers/prizes and exertion required to effectively take that activities.

There are a few different ways that a criminal's view of exertion and risk can be routed to reduce the potential of remuneration. Initially, the apparent danger of being caught can be upgraded. Next, the apparent danger of being recognized can be raised. The measure of exertion required to arrive at the prize objective can be increased, lastly, the apparent or desired gain can be decreased.

Criminals originate from an assortment of sections, having altogether different age groups, social class, occupation or criminal accounts. They utilize numerous strategies to get identity related data and to change over it to money and additionally other significant merchandise, for example, new credit card records or credits.

Identity violations may likewise be sorted as " white-collar" since they are often carried out over the span of ordinary employment obligations, or as a result of the conviction that the crimes does normally not include physical damage to the person in question. And keeping in mind that identity criminals are as often as possible accepted to be talented PC programmers with well organized networking system, actually identity criminals normally work on a mundane level without refined PC innovation. They are bound to burrow through the junk or pay insiders to get individual data than they are to play out a complex PC activity."

Identified with the variable of Commitment, the exertion required to carry out a specific identity crimes reacts to the transaction of risk and prize. In the event that the guilty party's impression of risk as well as effort is expanded, all things considered, the crimes won't be committed so easily."

Raising the view of risk and the measure of exertion required, while recucing impression of potential award simultaneously can be accomplished by the authorities if they increase the wrongdoer's apparent danger of being gotten. Offenders are additionally more averse to put forth an attempt to commit an offense in the event that they know that their chance to gain something will be low. As rational creatures, offender won't be motivated to commit the crime by low degrees of profit.

Identity thieves are normally inspired by monetary benefit; however some have ideological inspirations or social motivations to perpetrate a crime. A fear based oppressor might need to make harm to an apparent enemy, or an individual might need to conceal their actual identity for reasons unknown and will in this way take somebody else's. Now and again, the loss to a survivor of identity crime might be a lot of lower than the gain for the lawbreaker.

The criminal will consistently gauge the degree of gain against different variables affecting the commission of a wrongdoing; the criminal will consistently ask whether it is "justified, despite all the trouble. Guilty parties may get a lot higher wages from unlawful undertakings than they could earn through real work, yet they try to balance this with the chance of being getting caught and sent to jail. For this situation, the expense of going to prison can’t be estimated in fiscal terms, however in the estimation of limitations imposed and loss of freedom.

Governments and different organizations liable for paying for prevention of crimes, its recognition, and finally punishment also tries to balance the effect of the crime with the expenses of tending to these issues. Each addition by a criminal speaks of a loss to an individual who falls prey to identity related crime and to society at large too. Gain by a criminal additionally represents the kind of forced exchange of money. For instance, somebody who utilizes a taken or phony personality to enter a nation wrongfully as a last resort means that an expense will have to be bear by the nation regarding social administrations, tutoring employments, medicinal services, benefits, and different elements.

Most of the time, it takes a very long time to recuperate from an identity crime. People experience issues getting any assistance from financial foundations. They normally have issues managing the credit managing organizations to get incorrect data expelled from their records. Victims might be hassled by collection organizations for obligations they didn't cause; they may be confronted with claims, garnishment of wages, or loss of their homes. The normal measure of time it takes for identity crimes victims to clear up the wreckage made by the criminal can be as not be surely deduced.

Identity crimes victims may feel irate and defenseless and are regularly genuinely scarred forever. A most dire outcome imaginable happens when a identity thief commits a crimes in the victim's name. The entire weight for demonstrating the crimes was submitted by another individual falls on the person in question and it can take up to years and huge measures of cash to clear up all this.

Survivors of identity violations endure similar encounters, paying little heed to the sort of crimes related with their loss. At the point when they report the crimes, they frequently get no assistance from the specialists answerable for at first giving the identity data, for example, the offices that issue birth endorsements, charge cards, or driver's licenses. Law enforcement seldom explores identity crimes as a result of the sheer number of fraud cases they should deal with.

CHAPTER 5-LAW GOVERNING IDENTITY THEFT IN INDIA

CHAPTER 5-LAWS GOVERNING IDENTITY THEFT IN INDIA

Indian law doesn’t have any specific legislation for identity theft but when problem related to identity theft arises a few provisions of Indian Penal Code 1860 together with Information Technology (Amendment) Act, 2008 are used to deal with this crime. And as we know that the identity theft has characteristics of both theft and fraud, cheating by impersonation, fraud, and, the basic requirements of forgery etc as given in the IPC, so, these provisions are quite frequently invoked along with those of the IT Act.

5.1 Whether identity theft is theft within the meaning of IPC,1860?

Despite the fact that by its name, identity theft is a sort of theft of explicit kind which includes stealing of client/individuals information, it isn't represented by Section 378 (which defines theft) of the IPC[28]. This is on the grounds that, it obliges just mobile property or such property which is equipped for being cut off from the earth, and is corporeal in nature (defined under Section 22 of IPC). Electricity has been incorporated inside the ambit of theft however on the account of the case law of Avtar Singh v. Province of Punjab[29], the Supreme Court said that electricity falls under the ambit of the Section 39 of the Electricity Act so, stealing of it would also be part of and dealt with the same law and there was no goal of extending the extent of Section 378 of the IPC. Subsequently, despite the fact that identity related data is as parallel information signs of zeros and ones, administered by surges of electronic waves like power, Section 378 can't be perused to incorporate information or identity fraud.[30]

5.2 Provisions of the IPC that can be used for identity theft.

Certain laws in the IPC, similar to fraud and forgery, which prior represented wrongdoings concerning false documents, was amended by the Information Technology Act, 2000 to incorporate electronic record. Consequently, the ambit of such wrongdoings was extended to incorporate electronic information related violations also. Consequently forgery (Section 464), making false documents (Section 465), impersonation for cheating (Section 468), forgery for purpose of harming reputation(Section 469), using as genuine a forged document (Section 471) and possession of a document known to be forged and intending to use it as genuine (Section 474) can be combined with those in the IT Act. For example, Section 468 and Section 471 can be invoked when an individual manufactures a site in nature of electronic record so as to bait the victims into revealing their personal data with the goal to swindle them. Further, Section 419 can

[28] Padala Rama Reddy, Indian Penal Code, 1860 196 (16 ed. 2014).

[29] Avtar Singh v. State of Punjab AIR 1965 SC 666

[30]Robin George, Data Theft in Cyber Space Legalserviceindia.com (2008), available at www.legalserviceindia.com/article/l267-Data-Theft-in-Cyber-Space.html

be utilized in situations where the offender has utilized the personal data of the person in question and imitates to be such person to cheat or commit fraud. Section 420 can be utilized on the off chance that "anything capable of being converted into a valuable security” which incorporates the importance of the unique identification information of a person (Privacymatters.com) Further, the Expert Committee on Amendments to the IT Act, 2000 had prescribed certain revisions in the IPC to incorporate Section 417 A which would give as long as up to three years of punishment for swindling utilizing any personal information of someone else. It additionally made cheating by impersonation by method of a system or PC asset punishable with as long as five years detainment and a fine, under Section 419 A[31]. These suggestions may have not been included into the IPC so far; however, it would have given more inclusive and extensive law on data theft.

5.3 Provisions in the Information Technology Act, 2000

The IT Act, 2000 is the principle enactment in India administering cyber-crimes. In spite of the, fact, that, its whole point was to give recognition to web-based business/e-commerce in India it hasn’t define cybercrimes[32]. Prior to its amendment in 2008, Section 43 of the Act could be utilized to force civil liability by method of remuneration not surpassing one Crore for unapproved access to a PC framework or system (Subsection ‘a’) and for giving help to encourage such unlawful act (Subsection ‘g’) [33]. The IT Act Amendment, 2008 has embedded section 66-C to the IT Act, 2000, which characterizes and endorses punishment for the offense of data theft as follows: 'Whoever, fraudulently or dishonestly make use of the electronic signature[34], password or any other unique identification feature of any other person shall be punished with imprisonment of either description for a detainment of either for a term which may reach out to three years and will likewise be at risk to fine which may stretch out to rupees one lakh.' The offense under this segment is cognizable and bailable and triable by the magistrate of First Class.

[31] Privacymatters.com, Computer Hacking and Identity Theft | PrivacyMatters.com, available at www.privacymatters.com/identity-theft-information/identity-theft-computer-hacking.aspx

[32] Sanjay Pandey, Curbing Cyber Crime: A Critique of Information technology Act 2000 and IT Act Amendment 2008

[33] ibid

[34] Defined under section 2(1) (ta) of the IT ACT, 2000 as "electronic signature" means authentication of any electronic record by a subscriber by means of the electronic technique specified in the Second Schedule and includes digital signature

The terms fraudulently and dishonestly are characterized under provisions 25 and 24 of the IPC,1860. A consolidated perusing of over three sections proposes that data fraud is a crime whereby an individual or a gathering of individuals purposefully make use by downloading, duplicating or extracting any of the electronic mark, secret word or some other unique identification proof of that individual to cause loss to him/her. An electronic mark is a strategy for verifying an electronic record by attaching e-signature. Another section of the previously mentioned act which provides punishment for cheating by impersonation is section 66-D[35] which characterizes the offense and endorses it as follows: 'Whoever, by means for any communication device or computer resource cheats by personating, shall be punished with detainment of either for a term which may stretch out to three years and will likewise be at risk to fine which may reach out to one lakh rupees.' The offense under this area is cognizable, bailable and triable by the court of the Magistrate of the First Class.

Section 66 of the Act just related to cybercrime of hacking wherein some deletion, alteration destruction or decrease in the estimation of PC asset will attract the punishment under this section. In the event that an individual got personal data from the PC covertly without causing any adjustments in it at all, this section can't be invoked. The term data theft itself was first used without precedent in the amended IT Act in 2008. Section 66 condemns any deceitful and exploitation for Section 43 of a similar Act[36]. Section 66 (A) which is currently held to be unconstitutional, secured the crime of Phishing. Section 66 B relates to dishonestly getting possession of any PC asset. Section 66 C explicitly provides the punishment for identity theft and is the main section where it has been defined. Section 66 D provides for the punishment for cheating by impersonation utilizing PC assets. Further, more laws have been inserted in the Act concerning insurance of "safety of individual information" in the hands of the intermediaries and specialist organizations (body corporate) in this manner guaranteeing information security and protection. Only in some situations where such information can be revealed is to an organization approved by the State or Central government for observation, checking or block attempt, under Section 69 of the IT Act. The ambit of sensitive individual information is given under the IT Rules, 2011 to mean financial information, password, mental health condition, physiological, physical and sexual orientation,

[35] Information Technology Amendment Act, 2008

[36] MINISTRY OF LAW, JUSTICE AND COMPANY AFFAIRS (Legislative Department), the Information Technology (Amendment) Act, 2008

medical record and history, and biometric information, money related data, psychological and physical well-being, sexual direction. Henceforth, contingent on the technique with the help of which identity theft has been done, the previously mentioned laws can be applied.

The occurrences where cloned sites are made and utilized for cheating clueless individuals falls within the meaning of the above mentioned sections. Different instances of fake emails, production of phony profiles on the internet sites or application form to cheat, email phonies, stealing of information, breach of privacy by unapproved access and other such cases are culpable under this section. On account of Sandeep Varghese v, State of Kerala,[37] an objection recorded by the delegate of a Company, which was occupied with the matter of exchanging and appropriation of petrochemicals in India and abroad, a wrongdoing was enlisted against nine people, asserting offenses under Sections 65, 66, 66-A, 66-C and 66-D of the Information Technology Act, 2000 alongside Sections 419 and 420 of the IPC. The said organization had a site 'www.jaypolychem.com' however another site with the name 'www.jayolychem.org' was made by the offender Samdeep @ Sam who sacked was from the organization with other accused. Abusive and malignant issues were distributed in the site. The principal accused and others would send messages from counterfeit email records to clients, chiefs of organization, providers, manage an account with the aim to slander the name of the organization. The principal accused alongside other co-accused plotted to swindle the organization and submitted different demonstrations of fraud, pantomime and slander which brought about monetary loss of a few crores of rupees to the organization.

5.4 Instances of identity theft and the loss caused to the victims – with a focus on cases that occurred in India

Identity theft cases are on an ascent world over. In U.S. alone, around 15 Million occupants have their identities has been utilized deceitfully consistently, with absolute loss of about $50 Billion. Around 100 Million extra Americans have their own information in danger when records kept up in Government and corporate database is lost or taken. So also, in India, according to the findings of an organization, one out of four is a casualty of fraud and such cases have ascended by a 13% since 2015. According to the Microsoft's Annual Computing Safer Index, at any rate 20% of

[37] I.L.R. 2010 (3) Kerala

Indians have fallen prey to phishing assaults and identity theft has caused loss of around Rs. 7500 on a normal. The numbers appeared in this Survey is very huge that known web clients in India are around 19.9% of the whole populace.[38]

5.5 Some famous cases of identity theft across the world

Because of their popularity and active social life, getting personal data of celebrities is quite simple. This is on the grounds that, much about the life of famous people is public knowledge rest of the information which is not is its safety is ensured by a password which can be changed effectively by answering to the security question. Consequently, they are an obvious target of Identity theft. First in this rundown is Michael Bloomberg, the renowned American Businessman and proprietor of the Bloomberg LP Company. A criminal utilized his data to pull back a four figure sum from his financial balance through an online exchange and another criminal utilized a produced check in Bloomberg's name to move $ 190,000 into his own record. Likewise, a cybercriminal hacked into the Social Security number, date of birth and charge card data of golf player Tiger Woods and attempted an online exchange worth $ 17,000.[39] Similar kind of identity theft was faced by entertainer Will Smith and artist Whitney Houston. In India, it was the administration's Income Tax Portal which turned into the target. In two particular cases, a programmer from Hyderabad, hacked into industrialist Anil Ambani's personal assessment forms account while another from Noida got to Shah Rukh Khan,

Mahendra Singh Dhoni and Sachin Tendulkar's personal assessment subtleties. A few other huge scale identity crimes occurred in India incorporating the RBI Phishing Scam, ICC World Cup, 2011 trick and the password phishing trick focusing on Google email account holders[40]. As phishing tricks have become normal methods of submitting data fraud in India, the Delhi High Court, in the milestone instance of NASSCOM v. Ajay Sood and Ors[41], announced phishing on the web as an illicit demonstration against which harms could be guaranteed. This case was

[38] Internetlivestats.com, India Internet Users - Internet Live Stats (2015), available at www.internetlivestats.com/internet-users/india/

[39] Reagan Gavin Rasquinha, From Will Smith to Tiger Woods: Famous folk who were victims of identity theft, The Times of India, 2015, http://timesofindia.indiatimes.com/entertainment/english/hollywood/news/FromWill-Smith-to-Tiger-Woods-Famous-folk-who-were-victims-of-identity-theft/articleshow/48915181.cms

[40] ibid

[41] NASSCOM v. Ajay Sood and Ors. 119 (2005) DLT 596

pronounced in 2005 when there were no particular laws regarding phishing. The court set priority and called phishing as deception in course of exchange, prompting disarray as to source of inception of email and making harm to the expected individual as well as discoloring the picture of the individual whose character is abused.

CHAPTER 6- LACUNAE IN THE INDIAN LAWS ON IDENTITY THEFT AND ITS IMPLEMENTATION

CHAPTER 6 LACUNAE IN THE INDIAN LAWS ON IDENTITY THEFT AND ITS IMPLEMENTATION

The IT Act, 2000 resulting to its alteration in 2008 has gone far in ensuring the protection of the information and individual data of a person from being abused. All things considered, there are sure some parts of the enactment and laws on identity fraud that require clearness or modification. Right off the bat, Section 66 C of the altered Act secures "unique identification feature", the importance of which has not been determined anywhere in the whole Act. The Information Technology Rules, 2011 has characterized "sensitive personal information" which should be secured by the intermediaries. However, it would be too outlandish to even think about deciphering unique ID features to mean sensitive individual data except if it were to be deciphered by the legal executive or explicitly given by an enactment.

Furthermore, despite the fact that the IT Act applies to any person who is associated with identity fraud including any PC asset situated in India, the jurisdictional issues despite everything can't be acquiescent. At the point when the accusation is of a non-Indian resident, the nation of his citizenship has different laws relating to identity fraud and might not have extradition arrangement with India, so arresting of such offender can't be attempted.[42]

Thirdly, bearing in mind the pay granted to the person in question, the Act is lacking. Under Section 43 of the IT Act, the pay granted has a maximum restriction of 1 Crore and if loss of information is brought about by corporate body, the maximum limit is 5 Crores. An individual may endure bigger loss than this sum, yet that perspective is dismissed. Further, according to Section 47 of the Act, the Adjudicating Officer investigating the situations where cases are underneath 5 Crore needs to think about just into corporeal/proven loss happened to the person in question while granting remuneration. As examined before in the paper, there is immense measure of mental injury and hardship that the victim has to face as an outcome of the subsequent wrongdoing to which the unique identification data is put to utilize. It requires some investment and assets to recapture the lost notoriety or to get the credit report amended, which ought to likewise be represented while awarding the grant.

Fourthly, the fine accommodated for identity theft under Section 66 C of the Act is up to I Lakh rupees. Identity fraud is a bigger ambit under which violations of various crimes can be executed. A identity stealing criminal can make loss of property of a solitary individual worth exactly thousand rupees or to a huge population where misfortune may add up to millions. In both the cases, a negligible token fine not surpassing one lakh would be nothing compared to actual loss. Further, different Sections of the Indian Penal Code alongside which Section 66 C of the IT Act might be clubbed, still id don't specify the breaking point (lower or upper) of fine or the way in

[42] Prashant Mali et al., Data Theft and The IT Act, 2000 of India | Daily Host News Dailyhostnews.com (2013), available at www.dailyhostnews.com/data-theft-and-the-it-act-2000-of-india

which it ought to be calculated, in this manner leaving it to the judgement of the appointed authority.

In conclusion, laws are intended to fill a double need of avoidance of a wrongdoing and how to provide deterrence[43]. Pre-emption and along these lines anticipation of data fraud is impossible. The deterrence impact can be made if there should be rise in specific measure of deliberation or pre thought before the occurrence of this wrongdoing. This should be possible by forcing stricter discipline or potentially strict fines. At present, the IT Act makes data fraud a cognizable, bailable and compoundable offense. Section 77A accommodates offenses submitted under Section 66 C to be compoundable. Further, a detainment term of 3 years is small and won't fulfill the purpose of causing prevention of the crime. By allowing the bail, it may give a chance to the offender who may meddle with the examination for the offence by the digital cell by messing with his digital footprints and proof of his wrongdoing.

6.1 Problems in implementation of the laws

In spite of the fact that the event of cyber-crimes is blossoming quite a lot year with the time, the conviction rate in India is grimly low. Considerably after heaps of complaints just not many of the criminals get caught. This may be because of inappropriate execution of the current laws or an inadequacy in the framework required in actualizing the laws. First of all, there is a deficiency of police staff having some expertise in managing cyber-crime cases. With time, because of innovative headway, new types of encryption innovation are utilized by the digital criminals, which is hard to translate due to the constrained assets provided to the authority. This defers the whole procedure, once in a while prompting discharging the blamed because of need for confirmation. In U.S. some judicial pronouncements have enabled to the police to ask the cybercriminal to unscramble the digital evidence in exchange of some detainment concessions, however it has not been done so regularly. Additionally, the quantity of digital labs in India is eight till date, which are overburdened because of the various cybercrime cases. Finally, one reason for low pace of conviction or announcing might be a result of non-enlistment of cybercrime registration by the police. This issue ought to likewise be investigated. These deficiencies can be

[43] The purpose of Criminal Punishment, (1 ed. 2004), http://www.sagepub.com/sites/default/files/upmbinaries/5144_Banks_II_Proof_Chapter_5.pdf

overwhelmed by expanding the number of opening for talented cops by the administration and conveying more assets to update the system with to the most recent innovation which can help in the current day necessity of standing up to a cybercriminal.

CHAPTER 7-IMPACT OF IDENTITY CRIME

CHAPTER 7-IMPACT OF IDENTITY CRIME

Having analyzed Identity crime threat agents and their various factors, we will now analyze the effect of crime related to identity. This analysis is planned to offer a structure by which countries around the globe may comprehend the genuine expenses of identity crime and utilize this comprehension to make fair reactions to the issue. Until this point, no countries other than the United States and Canada have actualized laws legitimately focusing on identity violation despite the fact that the United Kingdom and Australia have designs in progress to do as such.

By gathering information about the real effect of identity crime by examining its expense and playing out a cost-effective examination of the issue a successful enactment/law and policy target to lessen identity crime can be made. This analysis will examine two significant themes: the effect on and cost to the survivors of identity theft and a general perspective on the effect and expenses of identity crime to society

The effect will change with each sort of identity crime, as indicated by its motivation or use. The complete expense occurred is diverse depending on how the personality related data was utilized. For instance, the effect of an identity crime carried out for business related purposes will contrast from that of an offence related to identity involving a credit card. The expense to citizens and the legislature from business related identity crime is not quite the same as a credit card related offence. This methodology sets the identity crime cost examination separated from evaluations of the expenses of different sorts of offence.

Analysis of effect is a significant yet more often disregarded component in the identity offence lifecycle, and the way that there are various individuals affected by this crime yet the situation is seldom given much needed consideration. For instance, consider the person whose identity has been taken and afterward utilized by an identity thief to get credit accounts and advances. In the event that the person in question, at some point of time attempts to loan his home to get crisis reserves, he is precluded the loaning it on the grounds that there are adverse affecting data has been reported to his credit. Plainly the person for this situation feels the immediate effect of the identity offence, however different affected persons in this situation incorporate the credit card and credit organizations and indirect impacts are felt by society on the loose.

In the event that there is no investigation of the effect and additional expenses of identity offence on its different victims, it is difficult to organize issues related with the different kinds of identity violations or to create proper prevention and reaction measures. Deciding the effect/cost of identity offence is a complex undertaking that requires thought of the methodologies taken in various nations around the globe. It reaches out past financial issues. For instance, it is important to consider which exercises in a specific jurisdiction have been condemned under the law, since meanings of criminal offenses are not normalized or general far and wide.

Also, there are significant mental/physical expenses related with identity offences that affect people and social orders. For instance, an expanded dread of identity offence in a inhabitants may bring about loss of trust in a business or government organization, prompting more straightforward repercussions, for example, less incessant utilization of credit cards or diminished purchasing conduct. The expenses of identity offence can be considered from the perspective of legal thinkers talking about the idea of the state or by deciding the advantages of offence counteraction programs in which effective intercession to diminish offence in one territory just results in uprooting the crime in another zone.

It has been noticed that there are troubles related with isolating the effect and misfortunes related with identity offenses from those emerging from different violations like misrepresentation that are executed by means of stolen and false identity. A few agencies that give general loss figures did as such by accumulating the loss caused from essential offenses identified with identity offense. Evaluation of loss in certain cases, for example, those connected to harmed reputation, stays hard, nonetheless. A few governments accept that subjective appraisals of loss resulting because of identity offense can be resolved.

These misfortunes would include:[44]

- Victim's monetary and non-budgetary misfortunes.
- Time and exertion expected of casualties to fix harmed notoriety.
- Budgetary and non-money related misfortunes emerging from different wrongdoings submitted
- Public and private costs of prevention, investigation, and prosecution(prevention, response, recovery).
- Loss of efficiencies due to security measures.
- Costs linked to loss of consumer confidence in business.

The expenses of identity violations are ascending in numerous nations. The growth have been `credited to the growing accessibility of the methods for fast transmission of data, more prominently globalization, expanded use of remote interchanges to conduct business in comparison to direct exchanges and face to face co-operations, the simplicity with which identity data can be fabricated with accessible cutting edge methods, and the undeniably the faster

[44] U.N. Secretary-General, U.N. Commission on Crime Prevention and Criminal Justice, Results of the Second Meeting of the Intergovernmental Expert Group to Prepare a Study on Fraud and the Criminal Misuse and Falsification of Identity, U.N. Doc. E/CN.15/2007/ 8/Add.3, at 62-63 (Jan. 31, 2009) [hereinafter "U.N. Commission, Second Meeting, Study on Fraud"), available at http://www.unodc.org/documents/organized-crime/E_CN_15_ 2007_8_Add_3.pdf.

gathering assembling and spread of data about people by private and public sector. Since such a great amount of data about individual people is open on the web, individuals have gotten increasingly worried about unapproved access and abuse of their own information.

A identity crime forces a few distinct expenses on the people in question, which might be on the people, organizations or associations, and governments and citizens. Every identity crime will have at least one victim that will endure the vast majority of the effect, which can sometimes more than one. Truth be told, there are four particular ways that an identity crime forces costs on its casualties.

- There are costs related with endeavors to forestall the crime, (Prevention Cost)
- costs emerging from its results, (Consequential Cost)
- costs connected to reactions to the crime, (Response Cost)
- expenses identifying with endeavors to recuperate from the impacts of having been a survivor of an identity crime. (Recovery Cost)

Prevention cost

Counteraction of identity crime additionally includes the immediate expenses to a business for guaranteeing that client records are put away and dealt with as safely as could be expected under the circumstances. It is hard to guess the expenses related with the dread of turning into a victim of identity crime, and significantly subsequent to taking precaution, the dread of being a potential victim frequently stays sufficiently enough to affect the conduct of that individual. For instance, an individual utilizing an ATM may choose one area over another as indicated by its security highlights, regardless of whether this area is out of the way and no secured in reality. The way that individuals and organizations are eager to pay for these opportunities provided by the fears implies that there is an incentive to the fear that might be in need to be measured.

One of the unintended expenses of identity offence anticipation endeavors is deterrence, or a situation where plans and strategies intended to ensure identity may repress desired exercises. On account of email, for instance, the programmed identification proof of mail senders, which is intended to diminish the dangers of identity offence and different other problems related with spam messages, really constrains the activities of genuine mail senders. Some Internet specialists have recommended some solutions, for example, programmed ID really urge spammers to hack into PC frameworks and steal records to send harming messages; at the end of the day, spammers depend much more vigorously on taken identities than before the anti-spam measures were put in place. In this way, any estimates that are intended to shield potential casualties from happening due to identity theft are bound to restrict the exercises of individuals as well as organizations, while giving lawbreakers the motivating force to change their conduct and adjust to another system[45]

Money sent in anticipation of prevention of the crime of violations of identity related information includes various opportunity costs. For property thief, for instance, these expenses incorporate the time it might take for a person to bolt the doors of their home or to set off an alarm, or taking a longer way when strolling to destination so as to stay away from regions of known risk. For an identity related offence, opportunity costs incorporate the time it takes to check a month to month bank explanation or service bill.

National security, public safety and wellbeing of citizens which is threatened by the illegal migrants having potential to harm privacy that is guaranteed by Indian Constitution for that purpose legislators by means of preventive endeavors called for national identity proof cards (i.e. Aadhar Card) or biometric ID measures, and the expenses of formulating and actualizing these measures.

Consequences Cost

The outcomes of identity crime are numerous and incorporate both money related and non-budgetary effects. Whether or not a survivor of identity crime really loses any wages because of time away from a vocation to manage the results of the theft, time away from work speaks of lost in efficiency, and somebody will pay for that misfortune, ordinarily the business owner or the legislature.

Moreover, the intangible expenses and outcomes of torment and distress experienced by a victim of identity crime, and maybe even a diminished life quality coming about because of the mental effect of the crime, probably represent the greatest issue for a casualty and must be considered in the ambit of cost.

[45] Adam Shostack & Paul Syverson, What Price Privacy? (And Why Identity Theft Is About Neither Identity Nor Theft), 12 ECON. OF INFO. SEC. 129, 137 (2004), available at www. nrl.navy.mil/chacs/pubs/04-1221.1-1128.pdf.

The expenses to society because of identity crime are inclusive of those spent on law implementation and national security. Since most identity violations are carried out with the expectation to utilize the procured data to carry out different crimes, for example, burglary of assets or getting credit or government benefits deceitfully, the weight on law implementation is generously expanded. Also, there is a developing pattern among composed crime groups to perpetrate identity violations so as to facilitate the carrying or dealing in trafficking of individuals or medications. Terrorist may likewise utilize fake identity records to land positions in different nations to conceal their real motive and maintain a strategic distance from law implementation agency.[46] It is hard to guess the non-financial and intangible expenses that identity crimes have on society at large.

Expenses for loss of privacy and security reduction are additionally also an expense incurred by the society. Surveys have once in a while asked how much protection individuals would trade for expanded security. Nonetheless, it is accepted instead of contended that diminishing privacy means better security. Just the inverse might be valid. Lawful authority has utilized unknown tips for a considerable length of time with the acknowledgment that a great part of the data assembled would not be given without a conceivable desire for anonymity.

So also, the Witness Protection Program depends on the capacity to allot individuals another identity. In a situation where all business and public activities by people are observed, this chance becomes far less conceivable.

Casualties of identity crime as a rule endure direct monetary misfortunes. For instance, they may lose their reserve funds or be required to take care of utility tabs as well as credit installments on accounts that were made without their insight. Indirect misfortunes to identity crime casualties incorporate harm evaluation of their credit ratings. There is no simple route for a casualty to beware of whether they have become the subject of a criminal record, since there is no organization or method like a credit-report check to make this assurance. Being exposed to a criminal record for the activities of another may have a noteworthy financial effect on identity crime casualties through loss of work, property, or status.

[46] LAW COMMISSION, REVIEW OF THE PRIVACY ACT 1993 STAGE 4, at 448 (Mar. 2010), available at http://www.lawcom.govt.nz/sites/default/files/publications/2010/03/ Publication_129_460_Whole%20Document.pdf.

There is additionally a mental effect that is related with identity crime. The stealing of a person's identity is an ambush on the individual's security and feeling of distinction, Victims experience the ill effects of pressure and are frequently less inclined to participate in the public eye after a identity crime. They no longer have a sense of security after criminals have gotten to their own data; the knowledge that an offender has an individual's place of residence is sufficient to cause that individual to feel uncertain and stressed over the potential for extra offenses on their protection, at least, or even the danger of physical mischief.

One of the most noteworthy impacts of identity offence on casualties is the harm done to their status. This harm has both money related and emotional expenses. At times, casualties may even be indicted for violations they didn't submit. Generally what affects most is as it may be the negative data that is attached to their credit reports because of offender utilizing their records to add to enormous bills with no aim of paying them. This regularly implies, later on, survivors of identity offence will be denied housing or based loans on this pessimistic credit data until the credit report is fixed.

People who are survivors of identity offence are often subjected to financial, emotional, and other non-economic harm. While economic establishments don't consider casualties responsible or subject them for the obligations deceitfully caused with their taken data, casualties must invest significant measures of energy and cash endeavoring to resolve the issues that emerge from identity offence. These incorporate dismissal or closing of the credit card applications, badgering from debt collectors, denial of advances, etc.

7.1 Long-Term and Short-Term Effects of Identity Crime

There is a differentiation to be made between costs that depend on frequency and those dependent on predominance, Costs dependent on occurrence are about individual scenes of identity offence, deciding all the expenses related with that solitary incident. A person who encounters the theft of their identity may need to confront the effect of that offence and its ramifications for a considerable length of time after the initial event. Incident based expenses are those that represent both the present and future expenses of a rate of identity offence in the year where the offence happened. Costs dependent on commonness are those that represent hurt done to a casualty of identity offence at whatever year, paying little mind to the date of the underlying offence

When one talks of identity related offences exploitation one must consider the underlying mischief and the mental effect of the offense over time. The genuine identity related offense might be viewed as the primary injuring while the second injury occurs when an individual is treated negatively by the general population and private organizations when trying to remedying and reporting the circumstance for purpose of prosecuting the crime. It also inclusive of the effect on the victim of a damaged credit score by the activities of the identity thief or the result of having a criminal history reported against him whenever a background search id done for verification purposes.

Recovering from Identity offense an individual must put forth significant attempts to determine issues, both related to money and non-monetary, that resulted from the offense. As they try to do as such, their encounters with recovery exercises and the agencies they contact to remedy the circumstance in which they were left because of the offense often result in creating more issue and dissatisfaction.

Emotional impact on many survivors of identity violations results in encountering worry in their family life and sentiments of outrage or double-crossing. Different feelings referenced by victims incorporate dread with respect to individual funds, the inclination that law requirement can't secure them, melancholy, trouble confiding in individuals, powerlessness and the longing to surrender and quit fighting the system. Some even feel that the identity criminal has taken "everything from them and even have self-destructive thoughts because of the identity offense.

Since relatives are at times associated with the stealing of identity and individual information from different individuals, the effect on the family can be critical and require a lot of exertion to recuperate from. Some relatives will betray the identity crime victim if that victim decides to accuse the cheat, they may pressurize the victim to drop the case. Survivors of identity violations are regularly reluctant to document a police report about the offense when a relative is included.

CHAPTER 8-PREVENTION OF INDENTITY CRIMES

CHAPTER 8-PREVENTION OF INDENTITY CRIMES

The number of identity-related offences and crimes continue to be on a rise, but on the flip side there are also various techniques and strategies available to prevent identity theft. Almost everyone has a stake in preventing identity crime; The Governments, businesses, and consumers. This chapter emphasizes on the role of business organizations and what they can do to avert identity crimes. However, to deal with the issue of identity crime on a larger scale, a number of steps and variety of initiatives need to be taken up by various bodies of the government.

First, a standard definition of the phrase "identity crime" is required to be established. A number of international bodies have already glanced upon this problem, but agreement between different nations on a standard definition has seen very little progress. Apart from the definition there also needs to be standardized international language to be used to explain and prosecute for identity crimes. The need for a standard language is imperative for cooperation between the prosecutors and final prosecution of identity related crimes.

Second, it is imperative that the five essential components of identity crime are reflected in the standards that are adopted by all the nations. These five essential ingredients include- acquisition, transfer, use, possession and production. It is necessary to criminalize each one of these components. It is important to understand, evaluate solutions and develop various methods to not only prevent and prosecute identity crimes, but also recover from them.

Third, identity crime impact assessments must be conducted by not only the government bodies but also by businesses. An identity crime centric and specific approach needs to be followed. This helps them in reaching upon the correct decisions and making right strategies to prevent identity crime. They also need to engage in threat assessment and analysis to better determine how and where resources should be invested to handle the problem of identity theft in the best manner.

The objective of this chapter is to discuss and suggest the several ways in which identity theft can be prevented effectively and efficiently. Identification tools and documents must be developed in a way which allows authentication and verification of the identity of the person and his documents in real-time. A mode of identification needs to be developed which can be used for fraud proof identification both offline and online sources. Better protection, strict laws and high prosecution rates can help in preventing identity crimes to a larger extent.

But these methods, while commendable, do not provide for a definite strategy to fight identity crimes and are highly uncoordinated. Therefore, a far more better and appropriate way is to develop a broader framework or structure that can be further used to evaluate several prevention techniques.

8.1 Proposed Approaches to Identity Crime Prevention

Out of the various crime prevention approaches and models present, some are more suitable than other with regard to prevention of identity related crimes. Advances like the situational prevention approach, the crime prevention through environment design, and the victim-centric prevention approach have been given substantial attention by specialists in the criminal justice field.

The intention here is to introduce crime prevention and impact minimization theories that are exclusively meant for application to crimes related to identity. The most fundamental approach is the Identity Crime Model Approach (IDCMA).

In the present time, there is no exact structure for developing a methodological approach to preventing and minimizing the impact of identity associated crime. Several suggestions and recommendations have been made in this regard by government bodies, NGO's, for-profit and non-profit organizations, academics, and law enforcement agencies but the issue with these proposals is that they are not based on preventive approaches targeted towards specific elements of identity-based crimes.

Most of these recommendations are pretty constricted in their extent, focusing majorly on the victim of the crime. The predicament with this form of approach is that a single identity crime may affect numerous stakeholders and victims. By a fraudulent use of an individual's credit card, not only he is impacted but the issuer of the card is impacted as well.

An additional dilemma is that the victim of an identity-related crime may be repetitively affected; personal documents and information acquired by identity offenders may be used to commit the same form of offense over and over again. Criminals may also use the same information for different and various identity related crimes or they may even offer the information or the documentation for sale to other criminals or offenders who will exploit it in committing several additional identity crimes.

The techniques mentioned here can be utilized to develop a consistent and cohesive plan for identity crime prevention and impact minimization approaches. Distinct from elsewhere recommended approaches, the approaches discussed here focus on the consequent methods that should be encouraged to prevent and avoid the use of personal information or documents acquired during the initial crime. This approach is the crime-centric approach which focuses on the actual commission of the crime or offence and the perceptions e=which the criminal may have in regard to commission if the crime.

8.2 Approach based on the Identity Crime Model (IDCMA)

This approach is founded on the main five components of crime: Acquire, Produce, Transfer, Possess, and Use. These factors are used to extend a prevention and impact minimization strategy. The principal goal of this method is to focus on building a plan that will deter the acquisition of personal identity related information or documents, and if the criminals or offenders do succeed in getting hold of that information, to stop the documents or information from being transferred, trafficked, manipulated, or used for financial gain of any other kind. It gives less motivation to identity thieves and criminal to commit the same crime again if they cannot use the stolen information or documents.

8.3 Utilizing the Identity Crime Threat Agent Assessment

As a part of prevention and minimization strategy, apart from following the IDCMA mentioned above, in performing a general risk assessment, the performer can also sometimes identify the risk agents. This method will be successful if all the risk agents are comprehended and if an overall strategy to diminish these threats is formed. Threats or risks are warning of potential danger, and to deal with such risks, the probable victim of the crime has a responsibility to take future actions that may deter the crime. The organizations and individuals have a way to analyze, understand and define the potential risks to their specific activities by way of a threat assessment.

For instance, a threat or risk assessment can expose the vulnerabilities and threats in a credit card processing system that let the identity criminals exploit it. An efficient and successful evaluation will lead to the formation of countermeasures to guard susceptible areas from being exposed and exploited.

A crucial element in considering while forming this strategy is that the various threat or risk agent variables are reliant upon each other.

8.4 Developing an International Identity Crime Treaty

Governments of every nation around the world are struggling at every level to deal with the inadequacy of identity related laws to efficiently prosecute criminals and the lack of coordination in identity related crimes between different jurisdictions. This in turn makes it complicated to work with law enforcement in that jurisdiction, in a cooperative and efficient manner, though both the jurisdictions may be affected by the same crime.

Nonetheless, it was recommended that these improvements fall short of the necessity for the larger international community to develop and expand strategies and guidelines that will generalize techniques of dealing with identity crime. Consequently there is a want of an international treaty that presents universal rules, regulations and guidelines to deal with identity crime.

8.5 Developing Identity Information and Documents with Real Time Authentication and Verification

One approach to trim down identity crime is to make it more complex for criminals to exploit and abuse the data or documents they acquire illegally. Consider, for instance, that systems can be put in place to determine if a person using a document or information is in fact the real holder of that document. The rationale of such a system would be to verify and validate the person seeking to use the information. When the information is sensitive the controlling access to it is critical. Mechanized systems carry out an extensive variety of crucial functions, and it is vital to acknowledge their vulnerabilities and restrictions so that steps may be taken to execute apt defensive policies and actions.[47]

Most companies use single-factor verification, which means that a client requires only a solitary password to access online information. By using two factor verification, the defense of sensitive information is enhanced, and the threat to such information is narrowed. Banks have already begun to use multi-factor authentication with consumers who access their accounts through online mode.

The purpose of the multi-factor authentication is to make it harder for a person not authorized to use the information to pose as the real account holder. A simple example of this is a debit card, which not only necessitates a user to have the authentic corporeal card and the personal identification number (PIN) in order to get access to the account.[48] Also, in online banking, multi-layered authentication necessitates numerous login names, passwords, or other knowledge to attain

[47] International Review of Criminal Policy, United Nations Manual on the Prevention and Control of Computer Related Crime, UNITED NATIONS CRIME AND JUSTICE INFORMATION NETWORK, http://www.uncjin.org/Documents/Eighth Congress.html (last visited April. 14, 2020).

[48] CC PACE, RISK ASSESSMENT EXECUTIVE OVERVIEW 6 (2009), available at http://www. ccpace.com/Resources/documents/RiskAssessmentExecOverview.pdf..

access to high-risk transactions and susceptible records. This method may ask over numerous additional security questions or added passwords as transactions amplify in risk.[49] Specialists advise that businesses use only multi-factor authentication with employees or clientele who may access their information tenuously.[50]

In 2007, 94 percent of U.S. banks were acquiescent with the multi-factor authentication directive, and online fraud and scams diminished by 30-40% between 2006 and 2007 as a result of following the stated guiding principle on verification.[51]

The benefits of using multi-layered authentication system have been seen in online transactions by financial firms as well. In a review of fiscal organizations and brokerages, stronger log-in validation that used measures further than usernames and passwords, was established to be a "very important" security and safety trait of the company for 95% of the respondents.[52]

8.6 Employee Policy

Organizations can create system to address the danger of identity related offence with the workers.

Around 33 percent of identity offenders utilize their business to perpetrate their offences. They may work in government organizations or organizations that have access to unique identification numbers or credit card. The employer can make it quite hard for criminals to take this data if they implement a strict data access by authentication methods for instance, banks may require passwords each time an individual need to take out cash, even if it’s a face to face transaction.

A clear set of rules and security obligations on the workers and the assigning security duties among the workers can help control the danger of identity offence being committed by the employees.

By running careful background verifications of the employees, restricting the access of the access to information related to personality to a limited number of employees, and by making a positive and constructive workplace that reduces the employees’ motive to commit offences like theft

[49] Id.

[50]U.S. G.O.A., INFORMATION SECURITY: PROTECTING PERSONALLY IDENTIFIABLE INFORMATION GAO-08-343, at 2-3 Jan. 2009), available at www.gao.gov/new.items/ do8343pdf.

[51]DIGITAL RESOLVE, HOW SECURITIES AND BROKERAGE FIRMS FIGHT ONLINE FRAUD AND IDENTITY THEFT 3 (n.d.).

[52] Id. at 4

against the company, the employer can decrease the occurrence of identity related crime. Providing data to workers about the genuine outcomes of identity related offences on the individual is frequently helpful in discouraging potential criminals from executing their plans.

A practical approach with respect to identity crimes inside an association with the help a group of interior partners for that very purpose is required. These representatives ought to be selected from security, client support, data innovation, activities, and risk managing departments.[53].

8.7 Risk Management Policy.

To have a successful risk managing system the organizations need to have an approach as to what kinds of data will need to meet government rules and regulation and which data should fall outside is ambit and to make plans and procedures to that effect with regard to introduction of data frameworks which will meet up that standard[54]. Organizations should likewise make procedures to distinguish security dangers, execute communication controls to guarantee the security of computer equipment and programming, and unmistakably restricted access to the information. Communications dangers can be addressed by utilizing electronic screening system, updating encryption, etc. The complex idea of communication frameworks implies that each framework's security must be considered to dependent upon the situation and facts of each case.

Another component of an efficient risk strategy includes the creation and testing of a disaster recovery plan, and keep analyzing and testing the plan and assessing of how viable the data safety measures truly are.

Some of the time exceptionally common activities have a solid effect. For instance, organizations can create more secure procedures for changing e-mail addresses or diverting e-mails to a backup address. By taking up such measures would result in significant reduction in identity crime is fundamentally[55]. Observing and examining the use of exchanges relating with identity may assist

[53] Proactive Approach to Fraud Prevention, brochure (pdf), http://www.philadelphiafed.org/ pec/consumer/index.html (accessed Feb. 14, 2012) (on file with author).

[54] Id.

[55] U.N. Secretary-General, Comm'n on Crime Prevention and Criminal Justice, International Cooperation in the Prevention, Investigation, Prosecution, and Punishment of Fraud, the Criminal Misuse and Falsification of Identity and Related Crimes (Draft Short Version), 48, U.N. Doc. E/CN.15/2007/8 (2007)m (hereinafter "U.N. Draft Short Version"), available at https://www.unodc.org/unodc/en/organized-crime/identity-related-crime.html.).

with recognizing suspicious activities by users. There ought to likewise a system must be set up to distinguish, report, and react to breaches of security.

Money related transactions are significant fragment of online action. Dealers need to improve their request order rates while decreasing identity related offence and online fraud without paying enormous expenses for requesting confirmation and charge backs. As indicated by a survey on online transaction that online dealers when use IP address and its geo-area abilities they found it to be one of the best devices for escaping online fraud. Geo-area technology can consequently give the geographic area of the network from which a request for products was placed or orders was set, offering extra data that can be utilized with other information to help in determining the danger of related with the particular exchange.

8.8 Risk Management in Identity Determination

The task of deciding an individual's identity is a simple matter of just matching his driving license and a credit card to check if the name and address on the these two are the similar. It has gotten very simple for identity criminal to get such records over the Internet, from offenders who fake them, or by making a deceitful report to gain a driver's permit or credit card in a fake name. In this manner, different methods must be applied to decide a genuine identity.[56]

Validation is the initial phase in data-based identification confirmation, and keeping in mind that it requires the most minimal degree of risk management, it determines whether the identifying information introduced by an individual is genuine and that it follows the established procedure[57].

The second step in data based identity validation is verification, which decides whether the information given by an individual are correct. This includes looking through various databases to

[56] GARY R. GORDON ET AL., IDENTITY FRAUD: A CRITICAL NATIONAL AND GLOBAL THREAT: A JOINT PROJECT OF THE ECONOMIC CRIME INSTITUTE AT UTICA COLLEGE AND LEXISNEXIS 30 (2003), available at http://www.utica.edu/academic/institutes/ecii/ publications/media/identity_fraud.pdf

[57] Id.

decide the accuracy of the data. In the event that there are inconsistencies found in the database search, extra examination is required. Utilizing complete databases has a greater expense, in any case, so risk must be offset with the cost[58].

Lastly, verification requires a third stage of the data-based personality validation process. In which the main component of verification is a "displaying and scoring" that helps in deciding the likelihood that a claimed identity is a genuine one. An identity decision engine decides the genuineness of a personality based on factors, for example:

A. Existing records for that personality (approval)

B. Consistency of interior codes (approval)

C. Given identifier mix across databases (confirmation)

But the confirmation procedure presents difficulties, since the data required to predict the credibility of an identity could undoubtedly include numerous databases, some of which may be accessible just from international sources which presents a critical issue for people who claims to be residents of other nations.[59]

8.9 Technical Solutions

Advances in electronic technology have beneficially affect on the identity related crime managing arrangements. Putting resources into technology and executing framework with wide guidelines to promote consistency in digital situations can assist organizations with preventing the theft of personal data. [60]

An educated purchaser is best defense against identity related wrongdoing, others accept that customers ought not to be the main line of defense" since identity crime doesn't start with an activity performed by the buyer. The best spot to stop identity related crime is in the business network. Researcher Gregory Kipper takes note of the availability of a program known as Graph Theoretic Anomaly Detection (GTAD). This program finds patterns based on identity information

[58] Id.
[59] Id.
[60] U.S. DEPT. OF JUSTICE, OFFICE OF COMMUNITY ORIENTED POLICING SERVICES, A NATIONAL STRATEGY TO COMBAT IDENTITY THEFT 44 (May 2006), available at www.cops.usdoj.gov/files/ric/Publications/eo3062303.pdf. Similar

elements that are recorded on an application. These components incorporate name, address, phone number, and ID. Some examples discovered are classified as "likely authentic" or "high-likelihood cheats." The fraudulent irregularities found by GTAD are utilized by organizations and the Identity Crime Resource Center to create explanatory scores that assess the danger of character wrongdoing.[61]

8.10 Vendors

Organizations must choose their merchants cautiously, especially when dealing with personal data. They should also check that all the merchants have suitable information security programs. Merchants targeted for assessment should include finance organizations, programming firms, etc. Cautious reviewing is basic since liabilities caused by these sellers could be passed to the organizations.

8.11 Consumer Education

Educating the consumer is a basic requirement of identity theft prevention. Furnishing potential victim of identity theft with data about fraud decreases the opportunity that they will be misled[62]. Customer training can appear as general intention to raise the public's awareness to the perils of identity violations, or it might concentrate on specific kinds of frauds and be found out by checking of the fake activities by experts in both private and public sectors.[63] Campaigns for raising public awareness can be intended to target specifically fragments of society, including youngsters and seniors. These campaigns could likewise teach people about procedures used to react to identity crime notwithstanding offering practical methods for counteraction.

[61] Id.

[62] U.N. Secretary-General, Comm'n on Crime Prevention and Criminal Justice, International Cooperation in the Prevention, Investigation, Prosecution, and Punishment of Fraud, the Criminal Misuse and Falsification of Identity and Related Crimes (Draft 1 Short Version], 21, U.N.Doc. E/CN.15/2007/8 (2007)m (hereinafter "U.N. Draft Short Version"), available at https://www.unodc.org/unodc/en/organized-crime/identity-related-crime.html.

[63] Id.

8.12 Consumer Actions

There are numerous ways through which buyers can abstain from turning out to be victims of identity criminals. One activity is the proper removal of financial reports, including month to month bank and credit records. Specialists suggest destroying these reports, since identity thieves regularly profit themselves from “dumpster diving” or really getting into garbage bin to discover and recognizing data that has been discarded. Utilizing a shredder is a generally reasonable approach to secure individual information.[64]

One more thing customer can do is ask for a copy of credit report in any case at least annually. These reports should be evaluated just to make sure that no illegal activity has because of the identity crime.[65]

Customers ought not to give individual data via telephone, through the mail, or over the Internet except when they are certain of who is getting it. Links in spontaneous messages should never be opened. But address given in the link should be typed instead. Firewalls, against spyware, and hostile to virus containing program in consistently be utilized to ensure the safety of the computer network. The software should also be updated regularly. When approached to make a secret password to get into, purchasers should never use obvious questions like birthdates or mother's original last name. Individual data need to be kept in a protected and secure spot, particularly if work is being done from the home.[66]

8.13 Foundation Documents

Governments issue IDs for their citizens and habitation that are known as "foundation documents." These records include the birth declaration, driver's permit, marriage endorsement, health card, passports and residency cards, etc. Notwithstanding their unique capacities, these records are as often as possible used to prove identity of a person, which makes them target for identity thieves. Thieves can take these records, or produce them, to commit fraud or to imitate someone else to get

[64] About Identity Theft, FTC, https://web.archive.org/web/20120503022415/http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity theft.html (last visited April 31, 2020).

[65] Id.

[66] Identity Theft Resources, FTC, http://www.ftc.gov/bcp/edu/microsites/idtheft2012) (last visited April 31, 2020).

benefits or to disguise themselves from the law. Since foundation documents are such high-esteem targets, governments need to come up with strategies to improve their security.

Different measures intended to shield foundation documents from identity criminals includes making a limitation periods for such documents during this time frame these are legitimate. Forcing new renewal necessities and utilizing technology to make identity records increasingly hard to alter is another method to prevent identity crime.

8.14 Information Sharing

To stop identity offense successfully, all parties must put forth an attempt to share what they know about the violations and the thieves that committed the crime. Law experts in private as well as public sectors locally and globally should share information while adhering to appropriate privacy and security provisions[67]. Data on identity related violations and thieves need to be accurately gathered so that a strong domestic identification program can be established effectively. Countries having special information and anti-cybercrime training material are also been asked to help the other nation in coming up with such programs.

This presents numerous difficulties, since the data is usually stored in a various distinct databases and there is no single standard structure for reporting identity crime protests. The constrained assets of law requirement agencies additionally prevent from sharing of data. The private area, especially financial services organizations and credit detailing organizations have enough access to give significant data to law authorization. These associations are in situations to detect early issues connected to identity theft. Various private organizations have created as of late to help and improve data sharing. But the best way to apply identity crime prevention methods is help on international level to create a common program to fight and to train against identity crime.

A portion of the suggestions made by law implementation and other identity offense experts incorporate the making of a standard organization for sharing knowledge, secure strategies for sharing information, improved correspondences among public and private divisions, and the dynamic support on the research on identity crime. A particularly encouraging area for analysis

[67] PHILIPPA LAWSON AND JOHN LAWFORD, "IDENTITY THEFT: THE NEED FOR BETTER CONSUMER PROTECTION 36 (2003), available at http://www.ic.gc.ca/app/oca/crd/dcmnt.do?id=1603&lang=eng,

about identity crimes is the examination of the socioeconomics of people and organizations that succumb to identity criminals and deciding the best way of intervention to stop identity offense.

8.15 Public-Private Partnerships (PPP)

In order to prevent identity crime, cooperation and knowledge sharing between public and private sector is very important. Sensitive personal information can be protected in a more efficient way if a private employer collaborates with government and service organizations, for example, unnecessary use of Social Security Numbers for the purpose of identification of any employee. For timely investigation victims of identity crime can work with private organizations along with law enforcement authorities as partners. To improve the security of customer credit card, bank usually works with credit card issuers such as VISA, Mastercard etc. and government authorities by exchanging the identity verification techniques.

A much better co-operation is required between the governments and Private sector organizations to develop identification systems that works together efficiently. Effective sharing of relevant information that is obtained after investigation of identity crimes can be facilitated by an inter-operable technology. For Example, measures should be taken to ensure that certain documents like credit cards and passports are made more difficult to alter or falsify for identification purposes by making them subject to more compatible and reliable information systems. Law enforcement agencies and private sector firms, both, at international as well as domestic level, should share the information about identity crimes so that data is likely to be timely and accurate. Information shared between law enforcement and private sector must include data from financial institutions, policies to counteract identity crime in the financial sector, and communications with credit reporting agencies about prevention of identity crime.

To prevent identity crime by use of drivers’ licenses, PPP can also be created among state motor vehicle administration and the businesses. Enhanced communications and cooperation between state and government agencies and the private sector could comprise warnings sent to the Internal Revenue Service, passport Office, or central medical database once an individual becomes a victim of identity crime, which makes it easier in determination of a new account that has been created in that person's name or if an existing account has been taken over by anyone else. Such cooperation is required to know if a criminal has applied for a driver's license or passport, or applied for medical benefits under a false name in another state.

Human error can be effectively eliminated by the us of various methods i.e. Fingerprint identification an retinal scan identification technology. The integrity of individual identity can be protected in a more efficient manner by using these bio-verification measures before the occurrence of any cash or credit transaction. As it will help in the eliminating the dependence of social security or credit card numbers in upcoming years. For example, identity criminals will not be able to commit identity related crimes without access to Social security numbers, bank account numbers, and driver's licenses if a single unique retinal scan would provide for a secure identity verification of such numbers.

8.16 Fingerprint Identification Technology

For quite some time, fingerprints have been used by forensic scientists as unique identifier (UID). Every individual has unique distinctive patterns on the skin of their finger tips like arches, loops and whorls which never change and such patterns are relied upon by the technology. This technology of fingerprinting identification makes it easier to use in criminal cases as it has, vastly, been computerized.

8.17 Retinal Scan Identification Technology

The retinal scan in a biometric technique that uses unique patterns on a person's retina blood vessel. It is a highly dependable technology as it is highly accurate and difficult to spoof in terms of identification. It may be because of such reason this technology is very expensive and is limited to use at high security government and military facilities.

8.18 Bio verification Systems

Genetic make-up of an individual is used to verify his or her identity in bio verification systems. US Congress, because of this reason, has suggested the encouragement of the adoption of bio verification systems. General use of this technology has been objected in most countries by Privacy advocates for the purpose of identification. The main reason for their objection is the potential misuse of private information which is held in a centrally controlled large database. While the supporters rebut such concern and argue that there would be no central storage as such data would be highly encrypted and placed on a card which will in turn function as a “lock” which can only be accessed by a person by matching the stored fingerprint and retinal scan. As no other person can access such biometric information the chance of its misuse is highly improbable.

8.19 Biometric Passports and National Identification Cards

Creation of two documents i.e. the biometric passport and the national identification card has been proposed by the supporters of biometric technology. But creation of such documents have been highly criticized on the point that if such National ID cards has been obtained by fraud it will be very difficult to challenge and the victim of such fraud will face unascertained amount of difficulty for the damage caused to him and also for the damage incurred to him in such a case. An identity crime expert in the United Kingdom suggested that once "more reliable" fake identification documents become available there would be no way in which false information could be brought into question.

For addressing identity crime appropriately in the developing countries a UN Study on identity crime training for investigators and prosecutors was made for the training and technical help in such countries. Such training would help the developing countries in addressing the already committed variety of economic identity fraud, the sophistication of identity criminals, the issue of transnationality, and the criminalization of identity crime. Multidisciplinary materials for investigators must also be includes in the training programs to make them well versed in the areas related to accounting and commercial financial systems. Information about forgery, impersonation, national identity infrastructure and systems which supports it must also be provided to the investigators.

A comprehensive domestic and international strategy is required to be implemented in order to address the problem of ever-growing threats which is associated with the identity crime.

CHAPTER 9- OBSERVATION

CHAPTER 9-OBSERVATION

If we attempt to classify crime related to identity, there will be n number of scope which will be significant, including: the very role of information technology in the committal of such activities; the machinery used to acquire or engineer fake identity information; the nature of identity related data and targeting stakeholder; and to what use that information related to identity is put up to like, character assassination or defamation or crimes against individuals, to infiltrate any organizations for surveillance, harm, terrorism, money laundering, illegal immigration, drug smuggling, etc. Moreover, misuse/crime related to identity can be further classified as per its purpose which can be related to or may be different depending upon consideration whether it will be fraud or a totally distinct form of crime. In most of the case the common intention for stealing identity related documents are financial benefits, which also include gaining and using credit, obtaining cash and sham loan applications.

When examining how countries attempt to address identity theft and identity-related crime from a policy perspective, the central conclusion of this study is that there exists a fair amount of difference. Only few countries, most obviously the U.S.A, have specific identity theft legislation but other countries such as India, Canada, etc. tackle the problem by dealing with antecedent activities with the help of criminal law. Even in India there is no specific legislation as a whole specific to identity theft or identity-related crime but we deal with such problem with the help of existing fraud or forgery legislation and amendment into some legislation. But this creates another problem as to how to intervene and when since the possibility of these types of misuse where identity theft and identity-related crimes are concerned as compared to organized crime. As discussed in Chapter I there is a need of general agreeable definition of identity theft amongst the experts and academicians. It may be seen that many of them are of the view that 'we know it when we see it', but this approach has its own limitations: while it may be adequate for police but the cross-border cases require a clear understanding to deal with the problem. Moreover the lack of a clear definition makes the gathering of statistics difficult. However, the studies show that that key priorities should be focusing on the sharing of best performance and improving the communication. The latter should be aptly applied to interactions between investigator and victim. Setting up portal or a system can be a key element to the solution, as it will allow the victims to more effortlessly inform identity crimes, and it will also act as the communications machinery to enable the investigators to update the victims about the status of the ongoing investigations. Such approach can be seen in the Stockholm Program, where it was suggested that the European Commission take measures to improve public-private partnerships.

A second pivotal point is the collaboration between a permanent cooperation body with user and victim organizations and the private sector. Which will in result at facilitating interactions at par to European level, which in terms would improve the efficiency of investigations and will also provide some additional advantages that can also be extended to other categories of crime related investigations. In conclusion, identity theft also faces the confrontation of policy precedence. This is not just about a matter of making a suitable legislation or addressing the current challenges but also a matter of prioritization as to which cases of identity theft should be worth prosecuting and investigating? The question is not inconsequential and especially when international cases are concerned in such cases investigations can be really complex and time consuming, and also very costly. There are too many reports identifying several occurrences where such cases were ignored just because of actual or alleged disparity between the harm undergone by the victim and the resources which were required to take action and the uncertainty of the outcome. This challenge mainly applies to categories of crime committed internationally, and those conducted through the Internet, where it is easier to hide traces by a skilled criminal. In such cases a common working ground is needed to be established at the international level, since differences in prosecution and investigation priorities between the countries will lead to investigations done by the weaker country being blocked. More importantly, the lack of universal criminalization rules is not the only problem in efficiently addressing identity related challenges, as any scrutinized occurrence of identity theft is feasibly covered by one or more likely the criminal.

In theory, the European data protection rules such as the criminal qualification of illegal processing of private data should act as a convenient safety net for all the incidents. However, the speculation that data protection rules can play a unifying role is only a theory and it also should be accordingly acknowledged that the reality will be much more different. Data protection regulations are rarely applied to cases of identity related crime in practice and it can be seen in the above discussed case laws. Enforcement of only data protection rules thus cannot be an effective strategy to tackle the current problem.

Identity theft, unless taken seriously and the emphasis lies on the enforcement of certain rules and better and significantly improved law dealing with such crimes. It is not shocking that a number of countries chose to introduce additional qualifications with to identity theft to see it as a crime i.e., it has to be of national preference or associated with some other giving it a higher priority. While with the lack of a common definition and understanding of the identity related crime it does becomes the primary barrier to making of effective laws to combat identity-related theft hence resulting in the lack of cooperation between the countries during investigations and reporting and sharing of follow-up of the cases in the issue. The studies also show that interactive online reporting machinery is not yet widespread, and that their functions whenever available are generally very limited. Even when victims are allowed to register complaints, the follow-up of the complaints are generally unclear, and investigations into some incidents are not treated as of high priority or easily closed when cost of investigation seem to exceed the alleged loss. Whether or not prioritization is needed in this matter is mostly a policy issue. However, it is clear that a more efficient response to identity related crime is required which can be broken down in two areas as a priority. Firstly, the cross-border investigations which should be rationalized and secondly, building of a strong legal framework which is agreed by most of the country agreeable. It will require a more efficient communication between national level investigative authorities, and also a consensus as to how to decide a case is of priority for investigation, in order to evade wastage of resources. Secondly, it is important that reporting mechanisms whenever available should be perceived as helpful by the victims, and it will only be possible when it clearly indicates how all the complaints ware to be processed, and most importantly that the victim will get follow-up notification telling them the status of their complaint. Finally, the use of such reporting machinery will also help in maintaining a systematic compilation of statistical data on identity related crime theft and identity-related crime, which in result will help in getting the categories of identity-related crime and identity theft, what are the consequences of such crimes on the victim, and may possibly help in the outcome of the investigations. Such statistics are at present largely not available at national level. So, the improvement in the availability of data will improve the awareness of identity-related crime risks and will facilitate the making of policy at the national level, if implemented in a sufficiently homogeneous way across the nation. On the basis of this approach, reporting of identity related incidents can be enhanced, as could the reports on the complaints and the efficiency of international investigations.

Nonetheless, there remains a number of hardship in respect of execution and explanation of existing laws in relation to identity theft, most importantly the applicability of present rules with varying authorization to identity related incidents, and the differences observed in non-legal reaction i.e. existence of and effectiveness of reporting system and lack of awareness campaigns which questionably are potentially more feasible routes to addressing the misuse.

Given the choice of probable definitions of identity theft might be possibly better to choose on the basis of relevant features so that a proper working definition can be provided. For example, a list of characteristics of identity theft should be provided so that we know how to make a conceptual framework to draft a definition so it can be comprehensive and adequately well prepared to cover, from a practical standpoint, all the sorts of misuse which can be imagined. A proper definition would be of description which will state what traits crime of identity theft must exhibit for example, conscious action; malicious intent; creation of a semblance; use of a third party's identity not belonging to the perpetrator; not mere possession of someone's identity; and lastly that identity theft should also involve non-existing and existing identities both. However, the adoption and use of any working definitions at any level will need a lot of cooperation which generally cannot be seen in the legal domain. Against the profusion of definitions and the blurred lines that divide each definition existing, identifying those which are used in other jurisdictions is necessary to start functional international cooperation.

CHAPTER 10- CONCLUSION AND RECOMMENDATIONS

CHAPTER 10- CONCLUSION AND RECOMMENDATIONS

Laws and mechanism for its implementation to prevent identity cheats ought to be dealt with by the lawmaking body. In any case, it is likewise significant that the information theft is precluded by executing stricter information protection laws. The significant sources from which personal identity data can be gotten to by digital criminals are the organizations which are fundamentally BPO and IT organizations having the individual database of individuals around the globe. Despite the fact that, the information assurance laws in India are not solid at present but the proposed Personal Data Protection Bill is a constructive advance towards actualizing stricter information security laws[68]

Following are the recommendations that can be implemented in India to make the laws regarding identity theft more effective.

- Making change to the current laws for forcing stricter discipline for aggravated types of crime related to identity. The laws can be made victim friendly with the end goal that he/she can

[68] The Personal Data Protection Bill, 2019 Ministry: Law and Justice, https://www.prsindia.org/billtrack/personal-data-protection-bill-2019

recoup from the misfortune caused and giving as much compensation as could reasonably be expected. India can follow the laws in U.S. which has consolidated the above thoughts into legislations. Therefore, the individuals must be given help, both for the quick misfortune brought about by Identity theft and for the repercussions of such wrongdoing[69].

- In India, different police offices have their own cybercrime units where cops are not very much prepared and find it hard to manage cybercrimes. Because of their absence of aptitude here, either the cybercrimes stay unreported or inclined to inappropriate examination. This issue has been brought to the Supreme Court's notification in a few PILs to form Special agencies free of the police or an alternate preparing foundation must be built up in India which can help the neighborhood police division to examine the cybercrime
- Cybercrime which occurs at a huge scale is commonly trans-national in nature. Different nations should co-work by utilizing multilateral arrangements so as to have fundamental consistency as far as sharing of cybercrime data is concerned.
- In order to stop or limit danger of data fraud, the biological part of character check (biometric) like unique finger impression, voiceprint, retinal scan and hand prints, etc, ought to be utilized any place there is an online financial exchanges or email account login. Such unique data can be gathered and stored when enrolling and joining any of the online web sites.
- Finally, the government should spread awareness among consumers in respect of the ways they can protect their personal information and have safe internet applications. Additionally they also need to educate the people about their rights and redressal system available to citizens in case of an offense of identity theft and make sure that individuals know it’s helpful in preventing identity theft when they keep a track of their credit report. To reduce the harm and to detect the identity theft at the early stage.

It is presented that a cautious scrutiny of the identity crimes practices and laws in India gives a feeling that by slight change, as proposed, to the current laws and its viable usage, examples of identity fraud can be controlled. The misfortune caused to the casualty can be alleviated quite far and by considering the intermediaries responsible for the information that they hold, information

[69] Key Global Takeaways From India's Revised Personal Data Protection Bill By Arindrajit Basu, Justin Sherman, https://www.lawfareblog.com/key-global-takeaways-indias-revised-personal-data-protection-bill

security can be maintained that the law and its execution doesn't appear to cover. The execution angle lags behind the enactments, because of which the genuine proficiency of the current laws isn't being accomplished

The offence of identity theft ought to be checked and measures should be provided before it becomes it gets profoundly established in the India. In contrast to different violations, this offence can be forestalled by following straightforward acts of digital hygiene. One of the ways is to occasionally check the safety of individual data put away in PCs or telephones and readily solving any errors, whenever found. Portable storing gadgets ought to be regularly managed, and a normal stock of their utilization should be kept. Another significant area wherein government need to make rules is guideline to be given as to who will have access as a worker and the quantity of people who can have information also needs to be observed with the allowing of access dependent on the work obligations of that individual. Another way to handle this offence is making of awareness campaign in schools, work environments and towns to teach individuals about the preclusion and redressal of this offence. A national database of loss identity programming ought to be created to act as the nodal point associated with all significant government workplaces, banks and such different spots to identify any unlawful utilization of those lost identity. Following these few measures would go far in checking the offence of data theft and spare time and pointless problem.

CHAPTER 11 BIBLIOGRAPHY

CHAPTER 11- BIBLIOGRAPHY

11.1 Primary Source

Bare Act

1. Indian Penal Code, 1860
2. Information and Technology Act, 2000

11.2 Secondary Sources

Web Sources

- Spamlaws.com, "The History of Identity Theft," 2017. [Online]. Available: http://www.spamlaws.com/id-thefthistory.html

- J. Velasco, January 2016. [Online]. Available: http://socialnomics.net/2016/01/13/4-case-studies-in-fraudsocial-media-and-identity-theft/
- Equifax, "A Lasting Impact:The Emotional Toll of Identity Theft," 2015
- McAfee, "What is Criminal Identity Theft?," October 2014. [Online]. Available: https://securingtomorrow.mcafee.com/consumer/identityprotection/criminal-identity-theft/.
- B. Singer, 2013. [Online]. Available: http://www.parents.com/kids/safety/tips/what-is-childidentity-theft/
- Mountain Alarm, June 2016. [Online]. Available: https://www.mountainalarm.com/blog/9-most-commontypes-of-identity-theft/
- The Data Protection Bill only weakens user rights, DECEMBER 27, 2019[ONLINE]. https://www.thehindu.com/opinion/lead/the-data-protection-bill-only-weakens-user-rights/article30405339.ece
- Key Global Takeaways From India's Revised Personal Data Protection Bill By Arindrajit Basu, Justin Sherman. January 23, 2020. [Online]https://www.lawfareblog.com/key-global-takeaways-indias-revised-personal-data-protection-bill
- The Personal Data Protection Bill, 2019 Ministry: Law and Justice.[Online] https://www.prsindia.org/billtrack/personal-data-protection-bill-2019
- The Personal Data Protection Bill, 2019: All you need to know by Anurag Vaishnav - December 23, 2019 [Online]. https://www.prsindia.org/theprsblog/personal-data-protection-bill-2019-all-you-need-know
- All You Need to Know About Identity Theft in Cyberspace in India By Diganth Raj Sehgal -September 3, 2019[Online] https://blog.ipleaders.in/all-you-need-to-know-about-identity-theft-in-cyberspace-in-india/
- Identity Theft Written by: Pulkit Tare[Online] http://www.legalserviceindia.com/article/l278-Identity-Theft.html
- Cyber theft - A serious concern in India, March 4 2019[Online] https://www.lexology.com/library/detail.aspx?g=4af6c044-dc77-4b1a-9288-986395eff8d1
- Economic Impact of Identity Theft in India: Lessons from Western Countries Dr.P.Arunachalam [online]. http://www.ipedr.com/vol12/42-C106.pdf

- Common Types of Identity Theft and How to Protect Yourself, [Online] https://www.discover.com/credit-cards/resources/common-types-of-identity-theft-and-how-to-protect-yourself/
- How Common Is Identity Theft? (Updated 2018) The Latest Stats, Written for NortonLifeLock[Online]https://www.lifelock.com/learn-identity-theft-resources-how-common-is-identity-theft.html
- Mitigating the Impact of Identity Theft on the Economy[Online] https://identity.utexas.edu/mitigating-the-impact-of-identity-theft-on-the-economy

REFERENCES

1. Baxter, B. (2009, January 22). Kroll Report: Fraud Will Rise as Economic Crisis Deepens. The AM Law Daily. Retrieved from http://amlawdaily.typepad.com/amlawdaily/2009/01/kroll-report-says-fraud-to-rise-as-economic-crisisdeepens.html
2. Ahmed Syed.R. (2020). Preventing Identity Crime: Identity Theft and Identity Fraud: An Identity Crime Model and Legislative Analysis with Recommendations for Preventing Identity Crime.
3. B Singh, Regulations and Guidelines for Effective Investigation of Cyber Crimes in India Centre of Excellence for Cyber Security Research and Development in India (CECSRDI) Perry4law.org (2013), available at http://perry4law.org/cecsrdi/?p=302
4. McCoy Erin L. , Hanel Rachael,(2018). Identity Theft: Private Battle or Public Crisis?
5. Collins Judith M. (2016). Preventing Identity Theft in Your Business: How to Protect Your Business, Customers and Employees.
6. Biegelman, M. (2009). Identity Theft Handbook: Detection, Prevention and Security. Hoboken, NJ: Wiley & Sons Incorporated.
7. Copes Heith , Vieraitis Lynne M.(2012). Identity Thieves: Motives and Methods
8. Martin, G. (unknown date). Identity Theft. The Phrase Finder. Retrieved from http://www.phrases.org.uk/meanings/identity-theft.html
9. Unknown author (2005). Working to Resolve Identity Theft. Identity Theft Resource Center. Retrieved from http://www.idtheftcenter.org/

10. Unknown author (n.d.). Punishment for Identity Theft. Identity Management Institute. Retrieved from http://www.identity-theft-awareness.com/punishment-for-identitytheft.html
11. Neeraj Aarora, GOONDA ACT- INEFFICACY OF POLICE TO CONQUER INTERNET CRIME | A Platform to discuss & analyse Financial and Cyber Forensics A Platform to discuss & analyse Financial and Cyber Forensics Neerajaarora.com (2014), available at www.neerajaarora.com/goonda-act-inefficacy-ofpolice-to-conquer-internet-crime