VOLUME 4 | ISSUE 2

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

IDENTITY THEFT- A CONTEMPORARY THREAT

- Harshit Choubey[1]

ABSTRACT

Identity theft has historically risen in frequency as information technology has advanced, and it has since been acknowledged as the world's fastest-growing crime. Identity theft is when someone else (usually a stranger) uses an individual's identity without their prior consent, permission, or knowledge. Such types of impressions are mainly committing fraud, which usually results in financial harm to the victim and illegal financial gain to the person who perpetrates it. However, the main issue with identity theft is that it is quite hard to detect and prevent. People who have used technology extensively, such as college students, children, and others, are also prone or can even fall prey to identity theft. It has been a major challenge for the societies of the digital age. Individual victims experience catastrophic psychological and financial losses, and the consequences to society as a whole are immense. The major topics on identity theft reviewed in this research are the definition and meaning of identity theft, statistics of identity theft, it's types and stages, recording and reporting of identity theft, law enforcement issues and response, effects, prevention, and defences of identity theft. The research further found that access to personal information about potential victims, as well as the anonymity provided by the internet, are significant facilitators of identity theft. In addition, the research has focused on the practices and operational environments of document-authenticating organizations that provide offenders with access to identification data. The researcher has followed the doctrinal and analytical method of research and at last, the inductive method which helped to arrive at a certain conclusion. Within the research, the first chapter is the Introductory part based on which whole research is created. The next two succeeding chapters consist of an Operational Introduction, and Law Enforcement Issues and Response which also includes an analysis of important international and national cases. The last chapter of the research

[1] Student at Maharashtra National Law University, Aurangabad.

consist of the Suggestions & Recommendations, and Conclusions. The Researcher has concluded that people must be informed that not only is it unlawful to exploit others' data, bit it is also illegal to obtain personal and sensitive information about others. Identity thieves must understand that peeping into someone's personal life is just as detrimental as peering into someone's restroom. Nothing in this world is more unsettling than someone professing to be someone they are not.

Keywords: Identity Theft, Information Technology, Fastest-growing crime, Unlawful exploitation, Impersonation, Illegal financial gain, Detection and Prevention, Technology users, Societies of the digital age, Doctrinal method. Etc.

"Identity is the qualities, beliefs, personality traits, appearance, and/or expressions that characterize a person or group."[2]

A person's quiddity is his or her identity which is a unique attribution of that person which creates a distinctive oneness from the other person, In the modern internet era identity means separate distinct characters, numbers, or digits. Any two individuals in the technological internet era shall hold a similar identity it's just like an approbation that is made by themselves. Legally, identification is just a formal consideration of an individual on Government papers and records such as Voter ID, Aadhar Card, Passport, and others.Identity theft which is also known as Identity Fraud is when the personal identity of an individual is used by someone else (commonly, a stranger) without prior consultation, permission, or knowledge of that individual. These types of impressions are mainly used to commit the crime of fraud which usually results in financial harm to the individual and unlawful financial gain to the offender.

In a study named "Personal Data Protection Law No. 9887 Dated 2008" published by UNCTD (United Nations Conference on Trade and Development), a series of semi-structured interviews were used as the main tool for data collection. Twelve undergraduate students (Six men and Six women) at Flinders Business School participated in this study. The interview was designed as a face-to-face interview. Research - The results of current research show that even students have less knowledge of the specific problems associated with identity theft. Researchers in the study found that students were unable to take

[2] Compare Collins Dictionary of Sociology, quoted in Covington, Peter (2008). "Culture and Identity". Success in Sociology. Dublin: Folens Limited. p. 12. ISBN 9781850082606. Retrieved 12 November 2020.

the necessary steps to reduce their risk of theft because of their limited knowledge or misconceptions about a topic students showed misconceptions about who criminals usually target when stealing personal information or who the thief is looking for. Authenticity/Value - Findings contribute to a better understanding of students' criminal knowledge. They can also help the government and other stakeholderssuch as financial institutions and educational providers, to educate individuals about the circumstances where they are potentially vulnerable to identity theft.[3]

While taking other Countries into Forethought there are 15% of countries where there is no legislation present on data protection, some other 5% of countries in the world which do not provide any data or record about the enactment or presence of proper legislation, around 71% of the countries are there which have provided the data of proper legislation enactment. While there is other 9% of countries that provide data of drafted legislation present for Data Protection. Proceeding further with the report provided by the UNCTD (United Nations Conference on Trade and Development), There are now 194 different countries in the world, with the UN (United Nations) reporting that only 128 possess some type of Data Privacy Legislation or Regulations. This leaves 66 countries with no Legislative Data Privacy Protection for their citizens. These include some of the major countries with fast-growing internet use as well as established commercial centres. Among those on the list of countries are Afghanistan, Bangladesh, the Central African Republic, Egypt, El Salvador, Botswana, and others.[4]

Statistics in Developed Countries

As per "The Identity Theft Research Centre (ITRC) Annual Data Breach Report, 2022"[5] report published by ITRC (Identity Theft Research Centre), the U.S.A had the Second-highest number of data breaches in a particular year which impacted around 442 million individuals. According to "Consumer Sentinel Network Data Book 2022"[6]by FTC (Federal Trade Commission) recorded over 5.1 million reports in the year 2022 where 46% of cases were of Fraud and 21% were of Identity Theft, in which

[3]Sda. (2014, September). Do they know, do they care? Researchgate.net. Retrieved May 18, 2023, from https://www.researchgate.net/publication/280158483_Identity_theft_and_university_students_Do_they_know_do_they_care
[4]Mash. (2020). Data Privacy Rankings. Privacyhq. Retrieved May 18, 2023, from https://privacyhq.com/news/world-data-privacy-rankings-countries/
[5] Data Breach Report. (2023, January). IdtheftCenter. Retrieved May 19, 2023, from https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf
[6] Consumer Sentinel Network Data Book 2022. (2023, February). ftc.gov. Retrieved May 19, 2023, from https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2022

credit card fraud accounted for 43.7% of Identity Theft. Also, in "Number of Digital Fraud Cases in Russia 2021"[7] published by SRD (Statista Research Department) on March 21, 2023, provided that in 2021, 249.2 thousand cases of internet fraud were reported in Russia. 117.7 thousand cases of the provided statistics were committed in the first half of the year in which nearly 150 billion Russian rubles were estimated to have been lost. According to research "Spam and Phishing[8]" by Kaspersky it was provided that France is the Sixth most prominent source of spam, it was responsible for 3.57 percent of spam in the world in 2021. Whereas, Russia was the largest source with a figure of 24.77 percent of all spam present in the world.

According to "Japan Cybersecurity Statistics"[9] in the last five years Japan has faced many notable cybersecurity cases, from the WannaCry ransomware assault in 2017 to the theft of cryptocurrency of Japan (Coincheck) in 2018, it was noticed that the country's digital security is impassive. In 2022 there were 429 cases of breach of the Japanese Act on prohibited computer access, where 235 offenders were arrested. In September 2021, 97.1% reported some sort of cybersecurity issues and adopted measures.

Developing Countries

According to the "Breach Level Study Index"[10] conducted by a digital security firm, Gemalto in 2017 which stated that approximately 3.24 million records were stolen, compromised, or lost in India. In that year, Identity Theft accounted for 58% of all data breaches instances. According to the report "Number of online identity theft offenses reported across India in 2021, by leading state"[11]published by Tanushree Basuroy on October 14, 2022, it was reported that in the year 2021, Karnataka (A Southern State in India) had the highest number of registered cases of Online Identity Theft, with several 1.7 thousand

[7] Number of Digital Fraud Cases in Russia 2021. (2023, March 21). Statista. Retrieved May 19, 2023, from https://www.statista.com/statistics/1196329/number-of-digital-fraud-cases-in-russia/#:~:text=In%202021%2C%20249.2%20thousand%20fraud,first%20half%20of%20the%20year.

[8] Kaspersky. (2021, February 15). Spam and Phishing. Securelist. Retrieved May 19, 2023, from https://securelist.com/spam-and-phishing-in-2020/100512/

[9] Maccart. (2022, December 29). Japan cybersecurity statistics. Comparitech. Retrieved May 21, 2023, from https://www.comparitech.com/blog/information-security/japan-cybersecurity-statistics/

[10] Gemalto. (2017). Breach Level Study Index. Legal Service India. Retrieved May 22, 2023, from https://www.legalserviceindia.com/legal/article-1780-identity-theft-a-threat-to-society.html

[11] Basuroy. (2022, October 22). Number of online identity theft offences reported across India in 2021, by leading state. Statista. Retrieved May 22, 2023, from https://www.statista.com/statistics/1097526/india-number-of-online-identity-theft-offences-registered-by-leading-state/

cases registered with the authorities. The same report also states that, in 2022, October the country recorded over Four thousand cases of Online Identity Theft.

In the report "Number of Internet violations reported in China March 2021"[12] published by Lai Lin Thomalaon February 23, 2023, there were around Five Thousand cases of cybersecurity (Identity Theft) and online gambling in China, Making up approximately 34 percent of all 11,594 internet infraction instances. In the report "China data breach likely to fuel identity fraud, smishing attacks"[13] by Eileen Yu published on July 5, 2022, it is stated that there is a spike in Smishing attacks and Identity Theft, same report stated that the personal data of One billion residents of the country has been put up for sale online. Offenders purporting to have access to databases holding the personal information and data that have been offered out for sale on an online platform that is specialized in trading stolen datasets. Personal information including Place of birth, National Identity Number, Cell phone Number, and was sold at 10 Bitcoins ($197,376) for 24TB of data.

Types of Identity Theft

Identity theftoccurs in several ways, that leave victims with harm to their credit, income, and reputation. Some common types of identity theft are as follows:

1. **Financial Identity Theft**

Financial theft occurs when a person obtains and uses the personal data of another person to obtain some unlawful financial gains. This is the most common form of identity theft. It may involve any account that an offender opens and uses without the consent of the victim, for which he/she will be financially liable. It could be a credit card account, a subscription, insurance, a loan, or some other type of account. Cybercriminals usually get this type of information through data breaches or purchase it from the dark web.

2. **Child Identity Theft**

[12] Lin Thomala. (2023, February). Number of internet violations reported in China March 2021. Statista. Retrieved May 22, 2023, from https://www.statista.com/statistics/1054173/china-report-number-on-online-violations/

[13] Yu. (2022, July). China data breach likely to fuel identity fraud. ZDnet. Retrieved May 22, 2023, from https://www.zdnet.com/article/china-data-breach-likely-to-fuel-identity-fraud-smishing-attacks/

Child Identity Theft occurs when an offender steals and utilizes a minor's personal information to commit fraud and obtain some unlawful gain. The imposter may be a family member, a friend, or even a stranger who targets children and use their personal information fraudulently. Children's social security numbers are desirable simply because they have no information associated with them, as generally offenders can exploit a child's identity to open new credit accounts, gain driving licenses, and even can purchase a property in their name. Since most youngsters do not realize the problem for years, this deception can continue unnoticed for years. This type of identity theft is quite rampant as studies suggested that it has become more prevalent in recent years.

3. Medical Identity Theft:

Medical Identity Theft occurs when an offender often poses as another person to obtain health care services. This entails obtaining prescriptions for drugs, accessing medical services, and obtaining medical devices and supplies under the victim's name by stealing personal information such as your health insurance or medical records. This type of identity theft results in the victim having bills for prescriptions, services, or devices that were not availed by the victim. An inaccurate medical record can make it harder for him/her to get the care needed in the future and even impact insurance coverage.[14]

4. Criminal Identity Theft:

Criminal Identity Theft occurs "when someone cited or arrested for a crime presents himself as another person, by using that person's name and identifying information".[15] In simple words when an offender poses as some other person during an arrest to avoid summons, prevent discovery of a warrant issued in their real name, or to avoid an arrest or conviction record. The offenders could be potentially adept to get away with charges and procedures by making a false identity or utilizing a stolen identity card, such as someone else's driving license, to show the cops. This form of identity theft is difficult to identify until the repercussions, such as receiving a court summons, a bench warrant issued for the arrest of the victim, or a background check is issued against the victim.

[14] McAfee. (n.d.). 5 common types of identity theft. Retrieved May 29, 2023, from https://www.mcafee.com/learn/5-common-types-of-identity-theft/

[15] Oswald. (2022, October 12). Types of Identity Theft. U.S. News. Com. Retrieved May 28, 2023, from https://www.usnews.com/360-reviews/privacy/types-of-identity-theft

5. **Tax Identity Theft:**

Tax Identity Theft is an aspect of financial identity theft that occurs when your tax returns and related information are compromised. The perpetrator uses your social security number and other information to submit a false tax return in the hopes of receiving a refund from the organization of income tax. Some perpetrators will also try to obtain a refund from the state in which the victim resides. The victim of this type of identity theft is often unaware of the fact until they file a tax return.

6. **Identity Cloning:**

Identity Cloning is such type of identity theft where the imposter continues to exploit someone else's personal information to develop their new identity and conceal their own true identity over the long term. The perpetrators often commit this type of identity theft to avoid scrutiny over their past criminal convictions or bankruptcy. It is among the most difficult types of identity theft to track down since the offender gets the impression to be living a normal, law-abiding life.

Stages of Identity Theft:

What?

Identity theft occurs when someone obtains personal or financial information from another person to use their identity to commit fraud or other criminal activities, such as making unauthorized transactions or purchases. True identity theft occurs when the perpetrator steals information about a person's identity, such as their name, address, phone number, date of birth, Social Insurance Number (SIN), driving license number, or health card number, and then impersonates the victim, effectively stealing their identity.

Where?

Identity theft is a crime that may occur in a virtual or even is a physical form, as the instances of identity theft are evolving as technologies advance and thieves get more creative. Although users are storing more and more information online, reports revealed that a stolen wallet or pocketbook is still one of the

leading causes of identity theft. An average person's wallet includes a plethora of sensitive personal information, such as credit cards, driver's licenses, and, in certain cases, Social Security Numbers, through which fraudsters may establish new credit lines, rent or purchase a property, use to charge purchases or apply for loans. Of course, a wallet is just one of the physical resources an identity thief can leverage, but considering other sources like digital devices (mobile, laptop, tablets, etc), mail, trash, insecure online data, unsafe connections, insecure websites, password security (easy-to-guess passwords), phishing, doxing and many more.[16]

When?

The phrase "identity theft" is a modern term for a centuries-old phenomenon. This crime has evolved and so have the methods to commit it. The history of identity theft extends backward to the first times that some form of verification of identity was used. Since this type of crime certainly dates back to ancient times, the sorts of identity theft seen back then were most likely the most rudimentary, simple impersonation and lying. But as more contemporary varieties of identity theft are thought to have started with the introduction of credit cards and the increasing number of identity verification processes in government. Identity theft has become more prevalent as there are fewer chances for identity verification.[17]

Why?

Identity theft is an intentional exploitation of another person's identity to acquire monetary advantages or get credit and other benefits and inflict loss on another person. Identity theft occurs for many causes such as opening new credit cards or other lines of credit using someone else's identity information, making unauthorized purchases by using existing credit or debit cards of another person, filing a tax return using someone else's Social Security Number to claim the refund, to get medical care by using

[16] True Identity part of Trans Union. (2023). How does identity theft happen? True Identity. Retrieved May 29, 2023, from https://www.trueidentity.com/identity-theft-resource/how-it-happens

[17] Fraud Laws. (2019, December 23). All you need to know about identity theft. fraud.laws.com. Retrieved May 29, 2023, from https://fraud.laws.com/identity-theft/history-identity-theft

someone else's health insurance, to pass an employment background check or to rent or purchase a property on someone else's name and financial standing.[18]

How?

Fraudsters are always looking for new ways to commit identity theft to obtain some unlawful gain. Some of the common ways in which identity theft happens are as follows:

1. **Phishing:**

Phishing refers to the practice of gathering personal information and data through the use of fraudulent email messages sent to the target, where the receiver is persuaded in such a way that the email was sent by an authorized and legitimate source or that it is the one required by the recipient. For instance, a bank or a corporation where the receiver works.[19]

2. **Pharming:**

Pharming is a type of online fraud similar to phishing, in which the traffic on a website is controlled and personal information is stolen. It is essentially the unlawful practice of creating fake websites and then diverting users to them. The attacker employs desktop redirection or popups to present the phishing website in a camouflaged link. In short, it is a practice of presenting fake, fraudulent, and data-grabbing websites as legitimate and trusted ones.

3. **Skimming**

Skimming, also known as Credit Card Theft, occurs when small devices, also known as skimmers, are illegally installed on ATMs (Automated Teller Machines), POS (Point of Sale) terminals, or fuel pumps

[18] Norton. (2013, August 8). Identity theft: what is it and how to avoid it. Retrieved May 29, 2023, from https://us.norton.com/blog/id-theft/what-is-identity-theft

[19] Grover. (2019, September 3). All you need to know about identity theft in cyberspace. Ipleaders. Retrieved May 29, 2023, from https://blog.ipleaders.in/all-you-need-to-know-about-identity-theft-in-cyberspace-in-india/#How_to_Report_Identity_Theft_to_the_Police

to capture data or record cardholders' PINs (Personal Identification Number). These collected data are often used by fraudsters to create fake debit and credit cards and then steal from victims' accounts.[20]

4. Data Breaches:

Data breaches may lead to exposing your passwords or sensitive data, it occurs when offender often hackers break into services that you are availing of and might steal your stored information. This could include your name, email, address, passwords, credit and debit card numbers, and even your social security number. To commit this type of fraud hackers often deploy sophisticated technical attacks or simply trick an employee of an organization into clicking on a link that creates an attack opening to be exploited. Regardless of how it happens, a data breach can, in one fell swoop, expose the PII (Personal Identification Information) of millions of unwitting victims.[21]

5. Lost or Stolen Wallets, Phones, or Digital Devices

Lost or stolen wallets (or purses) are often a good source of personal information for fraudsters, and it is a general practice that people carry their credentials like a credit card, identity card, or driver's license in their wallet or purse, that is enough for a criminal to steal and utilize victim's identity. Also, lost or stolen phones or other digital devices are a golden ticket for identity thieves, as with access to victims' phones cybercriminals could make unauthorized payments and purchases by using their credit line or might break into personal data like photos, videos, or sensitive information stored in the device.[22]

Recording and Reporting Identity Theft

Cybercrimes are at an all-high in India at present days, since demonetization boosted online transactions, these crimes escalated. The rise in these crimes prompted the creation of the "Cyber and Information Security Division (C&IS), which deals with cyber security, cybercrime, National Information Security

[20] Federal Bureau of Investigation. (2023). How We Can Help You. FBI.gov. Retrieved May 30, 2023, from https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/skimming
[21] Norton, & Johansen. (2017, October 7). 7 Ways Identity Theft Can Happen to You. Norton. Retrieved May 29, 2023, from https://lifelock.norton.com/learn/identity-theft-resources/ways-identity-theft-happen-can-happen
[22] Ravichandran (CEO of AURA). (2023, January 6). How Does Identity Theft Happen? Aura. Retrieved May 30, 2023, from https://www.aura.com/learn/how-does-identity-theft-happen#2.-Lost-or-stolen-wallets

Policy and Guidelines (NISPG), and the implementation of NISPG among other things. Under, C&IS a department of 'Crime and Criminal Tracking Network and Systems' (CCTNS) was established in 2009 which was approved by Cabinet Committee to create a nationwide networking infrastructure for an IT (Information Technology)-enabled criminal tracking and crime detention system.[23]

Laws enacted in India that are related to identity theft are as follows:

1) Indian Penal Code, 1860

Identity theft is not simply a cybercrime; it may also be committed physically, such as when someone steals another person's wallet (or purse), which may include documents consisting of PII (Personal Identification Information) that can be readily utilized to perpetrate identity theft. As a result, it may be determined that identity theft incorporates both theft and forgery and so the provision in the Indian Penal Code, 1860 for forgery can be used to prosecute identity theft. The following provisions under the Indian Penal Code, of 1860 govern such practices:

a) Section 416: Cheating by personation
b) Section 463: Forgery
c) Section 464: Making a false document
d) Section 469: Forgery for purpose of harming reputation
e) Section 471: Using as genuine a forged document or electronic record

2) **Information Technology (Amendment) Act, 2008:**

The Information Technology (Amendment) Act, 2008 is the primary governing legislation for cybercrimes in India. However, its primary goal was to recognize e-commerce in India, it did not define cybercrime. In Section 3A the Act defines 'electronic signature' which"mandates a technologically neutralthreshold of 'reliability' that must be met for the Central Government to notify a new type of electronic signature under Schedule II. The following sections of the Information Technology (Amendment) Act, 2008 governs such practices:

[23] Grover. (2019, September 3). All you need to know about identity theft in cyberspace. Ipleaders. Retrieved May 29, 2023, from https://blog.ipleaders.in/all-you-need-to-know-about-identity-theft-in-cyberspace-in-india/#How_to_Report_Identity_Theft_to_the_Police

a) Section 66: Computer-related offense
b) Section 66C: Punishment for identity theft
c) Section 66D: Punishment for cheating by personation by using computer resource
d) Section 74: Publication for fraudulent purpose

However, the Act ensures to protect personal and private data from infringement, it is not as effective as one might think. The statute also specifies particular challenges and standards that must address the scope of identity theft and may necessitate immediate amendment. The Act does not define what constitutes an identifiable characteristic, which is at the heart of "identity theft". However, the "Information Technology Rules, 2011" has stated a definition of "Sensitive Personal Information". Each of these terms sounds similar, but they are not interchangeable and cannot have the same meaning. Therefore, it is the desecration of the court by using interpretation statutes to determine what exactly it is.

Effects of Identity Theft

Identity theft is much worse than anyone could assume, everyday new news reports explaining new techniques of how fraudsters have stolen someone's personal information, as well as warnings about big data breaches that make the sensitive information available to hackers on the dark web are seen.

On an Individual:

The negative effects of identity theft are often financial, but there can also be emotional repercussions one could face. For instance, if an offender commits a crime under your name and police identify you as the offender, which is known as criminal identity theft, you can depict the stress and disruption to your life until the matter is addressed. The effects of identity theft that can be faced by an individual are:

- Financial damage
- Emotional damage
- Social Damage

On a Business:

Business identity theft occurs when someone impersonates an organization rather than an individual to execute malicious schemes. This can illustrate itself in a variety of ways, including Acquiring company-related data via stealing business ID documents/credentials, filing false business paperwork to get refundable business credits or to begin personal identity theft, or sending fraudulent messages/emails in the name of the firm to get under wrapped personal or business information.[24]

On Society:

Identity theft is an emerging criminal offense that has serious ramifications in our society. Its victims lose their identity in a matter of seconds, irrevocably altering one's future. The established nature of modern electronic payment methods simplifies crime. In today's global economy, sellers of commodities and services are driven to offer their goods and services in exchange for money. The crime is both harrowing and traumatic as it has long-term consequences for individuals, governments, and the economy. The consequences also affect business, the government, and society as a whole.

Preventions for Identity Theft

Identity theft may take years to become apparent and much longer to clean your reputation and credit rating, so prevention is paramount. Some steps to protect yourself from identity theft:

1. Use Strong passwords and PINs:

People commonly use their birthdate, phone number, or physical address as their passwords and pin codes. This information is significantly vulnerable to being used for identity theft. If your friend or near ones can guess your pins, a hacker can, too. It is advisable to look for a password generator to generate a random password, or get a creative and strong password (using a combination of letters, numbers, and symbols).[25]

2. Be Defensive with Sensitive Information:

[24] Ramezani. (2022, July 7). How Your Business is Impacted by Identity Theft. Constellaintelligence. Retrieved June 3, 2023, from https://constellaintelligence.com/how-your-business-is-impacted-by-identity-theft/
[25] Burdova. (2020, December 18). How to Protect Yourself from Identity Theft. Avast. Retrieved June 5, 2023, from https://www.avast.com/c-prevent-identity-theft

Submitting sensitive information by email, social media, or text message is not an ideal approach. These procedures might not be secure as any hacker can obtain them by illegally entering your account. One should look for warning signs that a website is safe and legitimate before entering your sensitive information, it is preferable to make sure the site URL (Uniform Resource Locator) begins with https (Hypertext Transfer Protocol) here, "s" stands for secure and displays a locked padlock. Monitor Bank Statements

3. Boost your Computer's Security:

In usual practice, hackers are unable to acquire your computer or mobile devices if you use antivirus software. According to Federal Trade Commission (FTC), you might be a victim of malware, which includes viruses, spyware, and other unwanted software. Because criminals can more easily hack outdated software, you should keep all software (including your Web browser) current with automatic updating. You should never turn off the firewall protection of your computer.

4. It's just not Digital:

Keeping in mind that tangible papers are still widely exploited in identity theft, given the prevalence of phishing scams and internet breaches, dumpster diving may appear to be an archaic method of collecting personal information, yet thieves persist to use it. It is preferable that you should shred or burn documents containing personal information before disposing of them and should store copies of important documents.

Case Laws on Identity Theft

- In Re Zappos.com, Inc, Theresa Stevens and Others appeal against Zappos.com, Inc (2018)[26]

In this appeal, the plaintiff alleged an "imminent" risk of identity theft or fraud from the Zappos data breaches. They defined identity theft and identity fraud based on definitions provided by the USGAO (United States Government Accountability Office) as encompassing various types of criminal activities, such as when PII (Personal Identification Information) is used to commit fraud or other crimes,

[26] Re Zappos.com, Inc, Theresa Stevens and Others v. Zappos.com, Inc, 2018 SCC Online US CA 9C 104. Retrieved June 6, 2023, from https://www.scconline.com/Members/SearchResult.aspx

including credit card fraud, phone or utility fraud, bank fraud, and government fraud. Plaintiffs allege that the information obtained in the Zappos breach can be used to conduct identity theft, particularly by increasing their vulnerability to "phishing" and "pharming" which are the methods for hackers to leverage the information they already have to get even more PII (Personal Identification Information). Plaintiffs also claim that their credit card details were among the data stolen in the breach. It was held, that the Zappos data breaches contained the information that can be used to commit identity theft and identity fraud so the United States Courts of Appeals for the Ninth Circuit, reversed the district court's judgment as to plaintiffs' standing and remand.

- President Balochistan High Court Bar Association against Federation of Pakistan & Others (2012)[27]

In this case, a group of 8 people was alleged of committing kidnapping for ransom and activating unregistered SIM cards by stealing the personal information of others by committing Identity theft.

It was held that implementing the directive dated May 21, 2012, regarding the issuing of 5 SIMs per citizen solely for the Province of Balochistan would not serve the objective of reducing the illegal use of mobile phones in crimes. A person who desires to use mobile phones in any criminal activity can obtain SIM cards from another province that can be utilized throughout the country. In a case of kidnapping for ransom of Doctor Saeed, the Quetta of police, in coordination with the Bahawalpur police, apprehended a group of three people involved in illegally activating unregistered SIMs through identity theft using data taken from voter's lists.

- In Steven Bassett's appeal against AMB Parking Services, Inc. and others, (2018)[28]

When Steven Bassett used his credit card at an AMB parking garage, he received a receipt that included the full expiration date of the card-a breach of the rule that companies redact some credit card information from printed receipts, which is a common warning sign of identity theft. The question that

[27]President Balochistan High Court Bar Association v. Federation of Pakistan & Others, 2012 SCC Online Pak SC 25. Retrieved June 6, 2023, from https://www.scconline.com/Members/SearchResult.aspx

[28] Steven Bassett v. AMB Parking Services, Inc. and Others, 2018 SCC Online US CA 9C 113.Retrieved June 6, 2023, from https://www.scconline.com/Members/SearchResult.aspx

arrived before the McKeown, Circuit Judge was: "Is receiving an overly revealing credit card receipt-unseen by others and unused by identity thieves—a sufficient injury to confer Article III standing?

- In the State of Tamil Nadu's appeal against Suhas Katti (2004)[29]

The Suhas Katti case is the first in India to set a precedent in the field of cyber-harassment. A lady filed the complaint after receiving filthy texts about her. The case involves online stalking and harassment of a lady. It was filed in February of 2004, and the Chennai cybercrime unit concluded the process of conviction[30].This case involved a complex identity theft and impersonation scheme where the accused created fake social media profiles and impersonated the victim to defame her. The court ruled that impersonation with the intent to harm someone's reputation constitutes an offense under the Information Technology Act, of 2000.

- In Sanjay Jha against State of Chhattisgarh (2014)[31]

In this case, the second bail application was filed by the petitioner as the first application was dismissed on merits as the co-accused was released on bail by the Hon'ble Supreme Court of India on grounds that she was a young girl of 21 years and was pursuing her first-year studies in law, accused persons allegedly generated fake documents from the internet, used fake letterhead of Railway Minister, appended forged signature of Railway Minister, made arrangement for mock medical examination, prepared forged medical report and obtained payment of Rs 20 Lakhs from the complainant. The petitioner was denied bail by the Hon'ble High Court.

Suggestions and Recommendations

After the study, the researcher humbly submitted some recommendations regarding Identity Theft- A Contemporary Threat to law and policymakers. As only stating problems and not recommending solutions for them, defeats the purpose of the research.

[29] State of Tamil Nadu v. Suhas Katti, C. No. 4680 of 2004, Retrieved June 6, 2023, from https://www.scconline.com/Members/SearchResult.aspx

[30] S. (2021, January 1). Suhas Katti v. State of Tamil Nadu. Indian Law Portal. Retrieved June 7, 2023, from https://indianlawportal.co.in/suhas-katti-v-state-of-tamil-nadu/

[31] Sanjay Jha v. State of Chhattisgarh, (2014) 3 SCC 202, Retrieved June 6, 2023, from https://www.scconline.com/Members/SearchResult.aspx

- While several countries can prosecute certain components of identity theft-related offenses under standard rules such as fraud or forgery, only a handful have established explicit legislation criminalizing identity theft as a separate offense. This suggests that the need for such solutions is not universally recognized.
- Governments might encourage awareness camps, seminars, capacity-building programs, or dedicated cybersecurity subjects in schools, colleges, and undergraduate programs to educate students about such threats and how to prevent them.
- Currently, there is a need for some technologies that would provide a new "Three-step Authentication and Protection" (similar to parental control) for devices primarily used by children to prevent their vulnerability to data breaches or information theft, which would lead to cybercrimes such as identity theft.
- Firewalls with identity theft protection should be developed and installed in every device, which would immediately notify the offender's unauthorized access to the victim's devices and personal information.
- With a spike in the number of frauds and cyber-related crimes, the government should come up with stringent legislation to protect the public's interest and prevent mishaps on the internet. These laws should be enacted to safeguard "sensitive personal data" in the hands of intermediaries and service providers (corporations), thus assuring data protection and privacy.
- Shortfalls in the information in the Information Technology (Amendment) Act of 2008, although the Act helps to protect personal and private data from misuse, it is not as strong as one might think. The statute additionally lays out specific hazards and standards that must address the scope of identity theft and may necessitate immediate amendment. Section 66C, which protects an individual's "Unique Identity Feature" in digital space, has not been stated in the statute. The Act does not define what constitutes an Identifiable attribute, which is at the heart of "Identity Theft".
- Identity-related information is essential in social life. A particular method to criminalize identity theft should allow the legislator to respond to the rising relevance of identity-related information

by enacting a criminal law provision that will focus on this information as the object of legal protection. [32]

- The construction of legislative frameworks to criminalize identity theft is scheduled to take place only on a national scale. As of yet, no international organization dealing with criminal law concerns has established a unique identity theft legislation with criminalization measures for related offenses. Notwithstanding the lack of universally applicable criminal law norms, international and regional organizations have expanded their pursuits in this area.[33]

Conclusion

Identity theft is defined as a person portraying another person without their consent or knowledge to engage in illegal or personal advantage acts. It cannot be accepted like any other minor offense. A person might be forgiven for losing everything, but losing their identity is like losing themselves since any culpability that comes during identity theft lies on the individual who has been duped. Information and identity theft are less complicated and riskier than robbery and extortion. Regardless of the number of thefts, online identity theft must be penalized in much the same way as physical identity theft. Whether it is a once-only or a hundred-time infraction, the court of law must take serious measures since an offense is an offense.

The researcher has examined the topic "Identity Theft- A Contemporary Threat", its meaning, statistics, legal parameters, types, stages, recording and reporting, effects, preventive measures, and case laws in this study since it has grown into a widespread and increasing threat in recent years as technological advancement, as the number of victims grows, it is prudent to take precautions to avoid malicious actors using your personal information and wreaking your personal and financial life. This sort of crime may result in substantial and long-term ramifications for the victim, such as money losses, credit score deterioration, and the need to spend time and resources recovering their identity.

[32] Corruption and Economic Crime Branch of UNODC (Director). (2007, August 15). Handbook on Identity- related Crime. UNODC.org. Retrieved June 9, 2023, from https://www.unodc.org/documents/treaties/UNCAC/Publications/Handbook_on_ID_Crime/10-57802_ebooke.pdf

[33] Corruption and Economic Crime Branch of UNODC (Director). (2007, August 15). Handbook on Identity- related Crime. UNODC.org. Retrieved June 9, 2023, from https://www.unodc.org/documents/treaties/UNCAC/Publications/Handbook_on_ID_Crime/10-57802_ebooke.pdf

People must be informed that not only exploiting others' data is illegal, but also gathering personal and sensitive information about others is illegal. People will not even attempt to acquire access to the private information of others if they are aware of this. Identity thieves must realize that looking into someone's personal life is as detrimental as peering into someone's lavatory. Nothing is creepier in this world than someone claiming to be someone they are not.