Jus Corpus Law Journal
Open Access Law Journal – Copyright © 2022 – ISSN 2582-7820
Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

Identity Theft: A method of Cybercrime

Ganesh Arora[a]

[a]Amity University, Lucknow, India

Received 22 June 2022; *Accepted* 08 July 2022; *Published* 14 July 2022

In the realm of social media, there has been enormous progress in a very short duration. Starting with modest instant messaging and blogging sites to complete social networking sites, websites have evolved. This is not to say that advancement has only occurred in optimistic changes. On the other side, social media has helped fugitives find new and creative ways to commit their crimes. They have taken conventional frauds to a different level. Furthermore, criminals are increasingly showing off their crimes on social networking sites. Identity theft is one offence that has seen a significant increase in levels[1]*. This study aims to shed light on the evolution of identity theft on social media platforms, as well as how this repository of private data has become a target for criminals.*

Keywords: *social media, cybercrime, identity theft, conventional fraud.*

INTRODUCTION

Identity theft is an offence in which a criminal acquires susceptible data from a sufferer through delusion and then utilizes that data to act in the sufferer's name. Commonly, such offenders are encouraged by monetary gain themselves. Identity thieves frequently get and use private information such as passwords, bank details, and security numbers to conduct

[1] Katie Farina, 'Cyber Crime: Identity Theft' (*Research Gate,* December 2015) <https://www.researchgate.net/publication/304188885_Cyber_Crime_Identity_Theft> accessed 20 June 2022

fraud in the victim's name. These confidential details can be used for a variety of nefarious purposes, including obtaining loans, making online purchases, and gaining access to the victim's medical and financial records. Phishing is routinely used to attain susceptible information from victims, and they are closely associated with identity theft. Delinquents can use public profiles on social media sites as a source of data to imitate their targets. When identity thieves procure this information, they can utilize it to place orders, gain access to the victims' online accounts, or file legitimate actions in their names. Individuals who have been affected may suffer financial losses in the short term as a result of unauthorised transactions made in their names. Victims may suffer legal charges, changes in their credit status, and defects to their good names in the medium term if they are deemed culpable for the criminals' actions and are assessed by law enforcement agencies. If you're going to utilise your private information online, be sure you're using a secure connection, such as a home or office network or cellular data. Prevent using public Wi-Fi without a password if at all feasible. If there is no further option, use a VPN, which will encrypt all the communications and therefore save you from eavesdropping burglars. Use a strong, multi-layered, and up-to-date security solution to protect your laptop, tablet, or smartphone from malicious software and attackers.

LAWS THAT GOVERN ID THEFT IN INDIA

Identity theft also referred to as ID fraud, is a severe issue that affects people all over the world. Technology has had a rapid impact on people's mindsets as a result of the technological revolution, as well as globalisation and digital flexibility currently prevailing throughout numerous industries. The significance of information technology has attained new peaks, with both favourable and adverse repercussions. Identity theft has become a major problem in India in current years as a result of the country's rapid growth and revolution in information technology.

WHAT IS “ID THEFT”?

"Identity Theft" pertains to crimes in which an individual obtains and utilizes another person's data without consent. One example is the fraudulent or deceptive use of a person's name, date

of birth, and other personal information. This can technically be done for financial gain to get any form of product or service. This information could potentially be used by criminals to collect fake ID cards, bank accounts, birth certificates, and other important documents. Fingerprints, for example, can be used to steal someone's identity. A breach of personal data can occur if a phoney biometric device obtains a big amount of personal data. If a person's fingerprints end up in the nasty hands, thieves may be able to benefit from the former's name.

Furthermore, the majority of victims are unaware that a data breach has occurred, and by the time they do, it may be too late to recover. Identity theft recovery is a time-consuming process that might take months or years, with a poor success rate[2].

MODES OF IDENTITY THEFTS

Data theft and the theft of personal data from electronic devices can be performed in several ways. Hackers obtain unauthorised access to any computer system's data. "Anyone with the intention or intent to cause any loss, damage, destruction, deletion, or alteration of any information that resides in a public or any person's computer," according to Section 66. "Diminishing its utility, values, or adversely influencing it in any way" is what hacking is defined as. Hacking is an infringement of the Indian Constitution's basic right to privacy. It is a technique through which viruses such as malware, divert data from another computer system by decrypting it and transferring it to a hacker using or giving the information to others to do fraud with it. Phishing is when someone uses falsified email addresses or messages to send you to a virus-infected website. On these fraudulent websites, people are encouraged to enter private data such as login information. The origin of the falsified e-mail is different from where it originated from. SMS spoofing occurs when a criminal steals another person's identity in the form of a phone number and sends an SMS via the internet, with the recipient receiving the SMS from the victim's mobile phone number[3]. Cybercriminals use ATM debit and credit

[2] Debargha Chatterjee, 'Laws that govern ID theft in India' *(Ipleaders,* 22 August 2021*)* <https://blog.ipleaders.in/laws-that-govern-id-theft-in-india/> accessed 18 June 2022

[3] SS Rana & Co., 'Cyber Theft- A serious crime in India' (*Lexology,* 4 March 2019) <https://www.lexology.com/library/detail.aspx?g=4af6c044-dc77-4b1a-9288-986395eff8d1> accessed 18 June 2022

cards to make illegal withdrawals from a person's bank account. To deceive the victim into providing crucial information about their identity, the cyber-criminal poses as a bank representative or a contact centre employee. Pharming is a sort of online fraud in which fraudsters use harmful code and fake websites to install malicious malware on a computer system. These programmes automatically reroute users to fraudulent websites without their knowledge or consent. Because these websites appear to be real, users may not notice fraudulent behaviour when entering personal data and information, as well as financial data. Malware is a type of malicious software designed to harm or destroy computer systems and data to obtain unauthorised network access. Malevolent software kinds include viruses, ransomware, and malware. Malware is frequently sent as a link or a file in an email, requiring the recipient to click on the link or open the file to run it. The majority of victims aren't aware of the warning signs that they're being victimised by identity theft. Bank/service provider's warning/notice; unauthorized card purchases; obtaining one-time password (OTP) from unidentified websites at random intervals; bank or service provider verification calls; all indications are little amounts deducted from a bank account at frequent or regular periods. Cybercriminals utilise unsecure websites to earn access to a user's private and monetary information. Users are encouraged to visit these websites and disclose personal information, which cyber thieves or hackers subsequently acquire. Websites with the "HTTPS" domain are safe, whereas websites with the "HTTPS" domain are not.

IN MODERN ERA

In the present age of globalisation and the online world, our electronic gadgets collect a great deal of data on each individual and store it deep on the hard drive. Sensitive information is stored in files such as cache, browser history, and other interim internet files. A hacker can get unauthorised access to data and share it with others, or even install harmful software on a computer or electronic device to extract sensitive and secret information, using such sensitive information. In our digital age, identity theft is a major issue that affects everyone. It's a huge crime that's fast-spreading and wreaking havoc on customers, well-known institutions, retail shops, and the economy as a whole. Since electronic identity fraud has taken on new

dimensions, the truth is more ambiguous. Such theft doesn't need to have only monetary implications; it could also result in significant reputational damage, time spent dealing with incorrect information, and exclusion from specific services due to the misuse of the stolen name. It's past time to acknowledge that electronic networks facilitate identity theft by allowing criminals to gather information online to act offline and then use that information to commit theft or other online harm. The most recent and most horrible of a series of heinous white-collar crimes, identity theft, has become the crime of the century. The headlines are loaded with more and more data fraud occurrences by the end of the day, putting everyone in danger. Data fraud and identity theft cases have risen rapidly in developing nations such as India. Although the Indian government refuses to release information on the number of recent occurrences of identity theft, it is feasible to conclude from regular newspaper headlines how dangerous and common these identity thefts are in our daily lives.

THE PANDEMIC EFFECT OF IDENTITY THEFT IN INDIA

The pandemic-induced remote working is being blamed as a major factor in India's alarmingly high rate of identity theft. According to polls, approximately 70% of Indian adults have been harmed by various cybercriminals and hackers as an outcome of remote working, which the victims had to adjust to owing to the circumstances. Despite the dangers of remote working, studies show that just 36% of adults have acquired security software after having their account or device accessed illegally.

LEGALEXPLORATION OF IDENTITY THEFT IN INDIA

"Identity" refers to proof of one's existence, while "theft" refers to illegal possession without the permission or ownership of a rightful owner. As a result, personal information theft occurs when one person owns the existence of another without that person's consent or property. Simply, if one individual accidentally imitates or replicates another, his or her identity is stolen. Theft of personal information is defined by the Black Law Dictionary as the unauthorised collection and use of another's identity. Personal information theft is a broad word that encompasses a wide range of crimes, from forgery to misrepresentation, yet some

are considered traditional crimes, such as ATM skimming and phishing. This refers to the larger scope of the heist. The theft of personal information is a criminal violation in India, according to two laws: the Indian Penal Code (IPC) 1860 and the IT Act 2000. Under the revised Information Technology Law, theft of personal information is now considered a criminal act. The Indian Criminal Code was enacted in the year 2000. These new regulations are largely concerned with electronic records. Electronic recordings are defined as "data, recordings, or generated data, images, sounds, transmissions or receptions in any electronic format" under the IPC of 1860, which is similar to the definition of "data, recordings, or generated data, images, sounds, transmissions or receptions in any electronic format" under the IT Act of 2000. As well as. In terms of the rules relating to personal information theft offences, section 378[4] of the IPC of 1860 states that "theft" only refers to tangible assets or movables and does not encompass cyberspace, making personal information theft illegal. Possibly not applicable. Although sections 463, 464, 465, 469, and 474[5] of the Indian Penal Code of 1860 do not address "personal information theft," they do offer provisions to punish counterfeiting. We gave personal information after the IPC was revised in 1860. Theft is also covered by these clauses. The theft of personal information is considered fraud under IPC sections 419 and 420[6] and is punished in the same way as spoofing fraud. The theft of personal information was classified as a crime in the Indian Criminal Code of 1860, and it was included as an extension of forgery and fraud. After a 2008 modification, the term "personal information theft" was added to the Information Technology Act 2000. It took some time for the necessity for a criminal legislation to safeguard fraudsters and the misuse of personal identification to be recognised under Section 66C[7] of the 2000 IT Act. Another key challenge for the judiciary is the execution of these statutes. In India, there is no manpower to handle the ever-changing cybercrime. In addition, a lack of knowledge of these significant cybercrimes leads to an increase in occurrences of personal data theft. The National Cyber Security Policy (NCSP) of 2013 concentrates on the establishment of nationwide node agencies as well as adequate and stringent authentication procedures, however, it falls short in several areas. Because the IT

[4] Indian Penal Code, 1860, s 378
[5] Indian Penal Code, 1860, ss 463, 464, 465, 469, and 474
[6] Indian Penal Code, 1860, ss 419 and 420
[7] Information Technology Act, 2000, s 66C

2000 Act currently only allows for one form of authentication policy, ISO027001 ISMS certification, which does not meet the legal requirements for such authentication, NCSP has no intentions to implement additional authentication policies. NCSP, 2013, also promotes open standards and public key infrastructure compliance without offering the main description[8]. Over the following five years, the policy plans to establish a team of personnel worth roughly 50,000 rupees, which is insufficient. Overall, the National Cyber Security Policy of 2013 was a flimsy blueprint that was distant from reality. While these regulations appear to be adequate in combating identity theft, the rising number of reported cyber breakouts raises some concerns about existing laws.

ATM SKIMMING

The concept of "cash anywhere, anytime" fueled the development of ATMs that made it simple for authorised account holders to withdraw cash. Automated Teller Machines (ATMs) have become the major and important mechanism through which banks provide services to their consumers, sooner or later. Over the years, ATM fraud has taken numerous forms, including the use of keyboard overlays, breaking into booth cameras, and embedding cameras in the machines themselves. It has become a more familiar and connected form of monetary fraud as a result of all of this. Identity theft is the starting point since it leads to other types of crime, and the complete chain of events can result in financial loss. ATM skimming is defined as a criminal exercise that comprises the installation of a gadget that is typically unnoticed by the ATM user and confidentially stores data. When a user puts in a specific ATM card, data from their bank account is displayed machine. Criminals can encrypt stolen data from an empty bank card and use it to loot monies from the bank account using such a complete way. When looking into the scale of a crime like skimming an ATM, the adequacy of the law and liability for such a serious high-profile crime is an angle that needs to be addressed, such a blunder. The IT Act of 2000 and 2008, were the only pieces of legislation that could deal with ATM skimming in any way (as amended)[9]. ATMs come under the ambit of cyber penal law,

[8] Debargha Chatterjee (n 2)
[9] Debargha Chatterjee (n 2)

according to the court in ***Commissioner of Income Tax-III v M/S NCR Corporation Pvt. Ltd.,***[10] because any computer system is a crucial part of an ATM and relies on the data processed by the machine system. The automatic function of cash dispensing deposit is conducted in the related ATM. As a result, under the Information Technology Act of 2000, an ATM can be considered a computer.

PHISHING

The fraudulent activity of sending e-mails disguised as reputable firms encourages users to divulge crucial private data such as passwords and card details, according to the Oxford Dictionary. Phishing is a type of identity theft in which criminals attempt to acquire sensitive information from consumers such as banking passwords, card numbers, and other similar details. It is defined as a type of activity that involves duping people into giving up their financial identities, such as bank details, pan card numbers, passwords, and other susceptible data, via e-mail, or other online means, and then utilizing that data for fraudulent purposes to loot money from them. In the case of the National Association of Software and Service Companies v/s. Ajay Sood, the Indian judiciary system defined "phishing." The court determined that 'phishing' is a type of online fraud. In the case of phishing, a person poses as an authentic organisation, such as a bank, insurance company, etc, to retrieve personal data from a user, such as passwords which he then uses for his objective, and distorts the individuality of the valid party. In general, phishing scams involve individuals posing as representatives of banks and siphoning funds from e-banking accounts after duping customers into providing personal banking information. Though phishing is not a recent threat, the steady improvement in attack quality makes it more unexpected. The intro of new distribution lanes poses newer threats and makes phishing detection even tougher. Vishing, also known as 'voice phishing,' is the most recent development in this field. Vishing attacks are carried out over the phone. Similarly, 'Smishing' is a new technique for phishing through SMS. As a result, 'Pharming' is the most contemporary form of phishing in which the detractor redirects the

[10] *Commissioner of Income Tax-III v M/S NCR Corporation Pvt. Ltd.,* (2020) I.T.A. No. 242/2011

victim to a vicious website of their choice. This is achieved by converting an alphabetical URL into a numerical IP address to discover and send visitors to the website.

CASE REFERENCES OF IDENTITY THEFT

There are several historical issues related to the various sections of the Information Technology Act of 2000. Mphasis BPO Scam In 2005, four call centre agents operating at Mphasis Outsourcing in India collected PIN codes from four customers of the Mphasis Citi Group. These suspicious employees cannot obtain these PINs. Employees, along with others, opened new accounts in Indian banks with fake IDs. For two months, they used PINs and other account information that they obtained while working for Mphasis to transfer money from a relevant Citigroup customer's bank account to a newly created bank account at an Indian bank. . In April 2005, Indian police reported a bank scam in the United States and quickly identified those involved. The defendants were arrested for trying to withdraw money from a fake account. About $ 426,000 was stolen. The recoverable amount was $ 230,000. The court found that section 43 (a)[11] applies here because of the nature of unauthorized access to such transactions. Syed Asifuddin Zhane Ors. On/on. In Andhra Pradesh, an employee of Tata Indicom was arrested on charges of violating a 32-bit electronic number called ESN, which was only programmed for mobile phones stolen from the Reliance Infocomm franchise. The court found that the violation of the source code violated section 65[12] of the Information Technology Act 2000. The suspect was identified as Kumar. Whiteley gained unauthorized access to the Joint Academic Network (JANET) and was removed to prevent unauthorized users from accessing the organization, additional files were added and passwords were changed. According to the investigation, the suspect, Kumar, stated that he "modified the computerized database of subscribers' broadband internet accounts" by accessing the BSNL broadband internet connection as a real authorized user. The CBI has launched an investigation into cybercrime against Kumar following a complaint from the Chennai media office. Subscribers also lost rupees. 38 248 / - Consequently, according to the complaint. According to the media, "infringing" sites have been detected in Bangalore, Chennai, and other

[11] Information Technology Act, 2000, s 43(a)
[12] Information Technology Act, 2000, s 65

cities. Defendant NG Arun Kumar, an engineer from Bangalore, was sentenced to one year in prison and a fine of Rs. 5,000/- 420 CPI (fraud) and additional capital according to section 66[13] of the IT Act Master, Egmore, Chennai. A crook set up a fraud profile in the name of Mrs. Pratibha Devi Patil, India's then-Hon'ble President. The Additional Controller, the President Household, and the Secretariat filed a Facebook complaint about 4fraud profiles forged in the name of the then-Hon'ble President. The President's House, according to the complaint, had nothing to do with Facebook, and the fake profile misled the common public. An FIR was filed under Section 469[14] IPC and Section 66A[15] of the IT Act, 2000, based on which the Economic Offences Wing police station, the special wing of Delhi Police specialises in the investigation of financial crimes, including cyber offences. A representative of a company that traded and distributed petrochemicals in India and abroad lodged a complaint against 9 people in the case of ***Sandeep Varghese v State of Kerala***[16], alleging violations of various sections of the IT Act, 2000, as well as the Sections of 419 and 420[17] of the IPC. The company's website was www.jaypolychem.com. Another website, called "www.jayplychem.org", is a social platform by another defendant, Preeti, and Charanjeet Singh, in collaboration with Sam's sister and sister, respectively, defendant Samdeep Varghese, also known as Sam (dismissed from the company). It was opened above in law. This website contains a damaging and defaming statement about the company and its directors. Cochin resident Sam's accused sister and her brother-in-law co-founded the company and acted in collusion with known and unknown people who committed counterfeiting, and other crimes. Two other defendants, Amardeep Singh and Rahul, travelled frequently to Delhi and Cochin. To disparage the names and reputations of the company and its directors, the first defendants and others sent emails from fake email IDs from many customers, suppliers, banks, etc. All of the Smear Campaigns by the above people have caused enormous damage to the company's name and reputation. As a consequence, the company lost tens of millions of rupees from producers, suppliers, and

[13] Information Technology Act, 2000, s 66
[14] Indian Penal Code, 1860, s 469
[15] Information Technology Act, 2000, s 66A
[16] Lionel Faleiro, 'IT Act 2000 – Penalties, Offences With Case Studies' (*Network Intelligence*, 24 June 2014) <https://niiconsulting.com/checkmate/2014/06/it-act-2000-penalties-offences-with-case-studies/> accessed 18 June 2022
[17] Indian Penal Code, 1860, ss 419 and 420

customers and was unable to do business. In the ***Jawaharlal Nehru University MMS Scandal***[18], a pornographic MMS clip was constructed on campus and distributed outside the university, stunning the prestigious and prominent Jawaharlal Nehru University. According to some media reports, the two accused students planned to extort money from the girl in the video at first. After that failed, the accused distributed the video via mobile phones and the internet and even retailed it as a CD in the blue film market. When a threat email was sent to the BSE and NSE, the Mumbai police registered a case of 'cyber terrorism,' one of the first in the state since the Information Technology (Amendment) Act of 2008. The MRA Marg police and the Cyber Crime Investigation Cell are both looking into the case. The suspect, in this case, had been apprehended.According to police, Shahab Md., using the email address "sh.itaiyeb125@yahoo.in," delivered an email to the BSE's administrative email address "corp.relations@bseindia.com" challenging security agencies to prevent a terror attack. The sender's IP address was traced, and the email was discovered to have originated in a village near Patna, Bihar. The ISP was Sify. It was quickly discovered that the email ID had been created only a few minutes before the email was delivered. When creating the email ID, the sender included two mobile phone numbers in the personal details column to prevent the police from tracking down the accused. Following an investigation, it was discovered that both numbers belonged to a photo frame manufacturer in Patna. As a result, under the IT Act of 2008, the MRA Marg police registered forgery cases for fraud, criminal intimidation, and cyber-terrorism. In ***Suhas Katti's case***, the posting of obscene, derogatory, and disturbing messages about a divorced lady in a message group on Yahoo was the subject. The accused delivered emails to the victim for information using a fake email account opened in the victim's name. The lady received vexing phone calls as a result of these postings. Based on the lady's complaint, the police tracked down and arrested the accused. An investigation revealed that he was a family friend of the victim who wanted to marry her. However, she was married to another person, and after their divorce, the accused began contacting her. After she turned down his marriage proposal, he began harassing her on social media. The accused was found

[18] Lionel Faleiro (n 16)

guilty of violating Sections 469, and 509[19] of the Indian Penal Code, 1860, and Section 67[20] of the IT Act, 2000. The accused was sentenced further for the offence. He was sentenced to two years in prison and a fine of Rs.500/- under Section 469 of the Indian Penal Code, 1860. He was sentenced to one year in simple imprisonment and a fine of Rs.500/- under Section 509 of the Indian Penal Code, 1860. He was sentenced to two years in prison and a fine of Rs.4000/- under Section 67 of the Information Technology Act, 2000. Each of the preceding verdicts had to run simultaneously. The accused yielded the fine and was lodged at Chennai's Central Prison. This was the primary case in India where the accused was found guilty under Section 67 of the IT Act, 2000. In ***Janhit Manch and Ors. v Union of India***[21]**,** public interest litigation was filed, wherein, the plea aimed a ban on porn websites. The NGO had asserted that websites exhibiting such sexual content, particularly those that comprise children, had a negative effect and impact, steering the youngsters on a criminal path.

PROTECTION FROM IDENTITY THEFT

To defend yourself from the rising number of identity theft cases, use a strong password and security PIN; change passwords regularly; avoid suspicious websites and links; never provide personal information to anyone else; have an authorised security firewall to protect against being hacked into devices, and limit the exposure of credit cards and other personal information cards. It is critical to reaching the local police station instantly, followed by a complaint at the area's Cyber Cell Police Station if someone has been a sufferer of identity theft.

CONCLUSION

Theft of personal information is a large-scale intrusion of personal privacy that has emotional and social consequences for victims. On the other hand, the theft of personal information has a non-personal effect. It also poses a threat to organizations and businesses. From a legal, policy, and regulatory standpoint, Indian law lags behind the theft of personal information and

[19] Indian Penal Code, 1860, ss 469 and 509
[20] Information Technology Act, 2000, s 67
[21] *Janhit Manch and Ors. v Union of India & Anr.,* (2022) Public Interest Litigation No. 24/2004

protection from personal or organizational data, and there is plenty of room for improvement. The lack of clear law has led to an increase in operational crimes in recent years compared to the last two decades. Proper application of existing legislation and equal monitoring of the situation requires a robust system with an effective hierarchy of responsibilities[22]. It is also important to limit duplication of power and involve a sufficient number of compassionate people. Finally, governments need to educate consumers on how to protect personal information and use the Internet safely. You also need to be aware of your rights and remedies if your personal information is stolen. Individuals also trace credit reports where private information is used and seek reasons for why such information is desired and its security to reduce the impact and early detection of personal information theft is needed.

[22] Debargha Chatterjee (n 2)