IDENTITY THEFT: A MAJOR CHALLENGE TO CYBER SECURITY IN INDIA

Dr.S. MADHURI PARADESI[1] and CHITRA SHUKLA[2]

1. ASSOCIATE PROFESSOR, HEAD & BOS, DEPARTMENT OF LAW, SRI PADMAVATI MAHILA VISVAVIDYALAYAM, TIRUPATI
2. LLM CONSTITUTIONAL LAW, SRI PADMAVATI MAHILA VISVAVIDYALAYAM, TIRUPATI

Abstract: *The development of technology in every sector of society has increased the problem of cyber threats in today's society. Identity theft is considered as a major challenge by various legal experts. It is very easy to do identity theft due to which data breach has become very common in India.*

In this paper the researchers will briefly analyze identity theft in India, which is widely spreading in our society. As cyber security is the most concerning issue of present society, it's very important that legal provisions on cyber crimes should be strengthened further by properly doing research on it. So, this paper widely studies the laws governing cyber crimes in India such as Bhartiya Nyaya Samhita, 2023, Digital Personal Data Protection Act, 2023 and Information and Technology Act, 2000 that deals with identity theft.

Through this article the researchers aim to analyze existing legal provisions in India on identity theft. The loopholes which exist in these provisions and the steps that can be taken to strengthen the existing laws so that strict action can be taken against people committing identity theft and data security of people can be done.

Key Words: *Identity theft, Cyber security, cyber crimes, Data protection*

INTRODUCTION

"If we don't act now to safeguard our privacy, we could all be victims of identity theft"

– Bill Nelson.

The above lines of Bill Nelson highlights the importance of laws on identity theft so that privacy of individuals can be safeguarded. Already the twenty-first century is known for its development in technology and now that all the data is digitized doing identity theft has become very easy. Identity theft is a type of cyber crime in which an attacker uses fraud or deception to obtain personal or sensitive information from a victim and misuses it to misrepresent himself as the person whose personal information he has taken. Identity theft is basically done for monetary gain by these perpetrators.

India is ranked first among researched countries worldwide by the number of identity theft cases with an estimated 27.2 million[1] adult and fraud victims, during the period. The United States followed, with approximately 13.5 million consumers having encountered an identity theft victim or fraud victim that year. Japan followed, with 3 million annual identity theft victims. Various developed countries have strict laws against identity theft and the people who actively commit such crimes are strictly punished.

Generally hacking of email id, credit card number, phishing, ATM skimming/carding, phishing are used as a tool to commit identity theft in India. The main problem occurs when innocent people have to pay for the frauds done by these identity thieves. People not only face financial losses but also suffer from mental stress due to the consequences of identity theft they are facing. Cyber security is becoming the priority of all the nation's so that justice can be done to identity theft victims and the

[1] "Identity theft victims by country 2022 | Statista" https://www.statista.com/statistics/1389318/identity-theft-victims-in-selected-countries/

people who actively commit such crimes can be severely punished.

Types of identity theft

India tops the list where most of the people suffer from the problem of identity theft. Lack of knowledge of legal provisions further increases this problem and in most of the cases there are delays in getting justice. There are four major types of identity theft through which a large number of people are affected they are:

- **Financial Identity Theft-** Financial identity theft occurs when someone uses another's identity to gain unauthorized access to credit cards of that person. The other monetary accounts can also be hacked due to which the original account holder suffers various financial losses. His account details can be used by hackers to take loans or do any other unauthorized transactions.

- **Criminal Identity Theft-** Criminal identity theft occurs when a person is arrested or cited for a criminal offense which is not committed by him. Such arrests can cause mental stress to the victims.

- **Medical Identity Theft-** Medical identity theft involves using another's identity to obtain healthcare benefits, such as prescription drugs or expensive medical procedures.

- **Social Security Identity Theft-** Social Security identity theft is when another's Social Security Number (SSN) is used to create a false identity. The false identity is then used to commit fraud, often to open a new line of credit or to get a loan. SSNs can be purchased on the dark web or found in personal documents incautiously thrown out.

Ways of doing identity theft

There are various ways by which identity theft is committed in India such as:

Hacking - It is a method by which the virus is inserted in the computer system of another person and all his data is hacked. Hacking in cyber security refers to the misuse of devices like computers, smartphones, tablets, and networks to cause damage to or corrupt systems, gather information on users, steal data and documents, or disrupt data related activity. As per Section 66 of IT Act when a person with the intention to cause or with the knowledge that he will cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in computer resource or diminishes it value or utility or affects its injuriously by any means commits hacking.

Phishing - Phishing is a type of online scam used frequently to obtain sensitive data from the users such as passwords, credit card numbers and other personal information that can be misused. Identity theft of this information mainly impacts the mental health of people. The attackers mislead the users to obtain their sensitive information. After obtaining the information fake credit cards can be created and by doing unauthorized purchases using these cards victims are harassed. Earlier before it was declared unconstitutional Section 66A of Information and Technology Act, 2000 covered the crime of phishing. 2014 Sony phishing incident[2] is the best example of phishing. It was a high-profile cyberattack case where hackers infiltrated Sony Pictures Entertainment's network, resulting in a massive data breach. The attackers sent spear-phishing emails to Sony employees, tricking them into clicking on malicious links that installed malware on the company's systems. The breach led to the theft of a vast amount of sensitive information, including unreleased films, employee data, internal emails, and executive salaries. The hackers, who identified themselves as the

[2]https://en.m.wikipedia.org/wiki/2014_Sony_Pictures_hack

"Guardians of Peace," leaked the stolen data publicly, causing significant embarrassment and financial damage to Sony.

Pharming- It is a cyberattack technique used to redirect a website's traffic to a fake website without the user's knowledge. Unlike phishing, which relies on tricking individuals into clicking on malicious links, pharming manipulates the resolution of domain names to direct users to fraudulent sites, even if they enter the correct web address.

Vishing: In this, the fraudster calls the victim by posing to be a bank representative or a call center employee, thereby tricking the victim to disclose crucial information about the identity.

ATM skimming- It is a type of fraud in which criminals use a device to steal credit or debit card information from ATM users. Skimming devices are typically placed on or near the card slot of an ATM and are designed to look like legitimate parts of the machine. When a user inserts their card into the ATM, the skimming device reads the magnetic stripe and stores the information. Once they have the card information and the PIN, they can use this information to create a cloned card and make fraudulent purchases or withdrawals.

Malware - Malware is a type of malicious software that is intentionally designed to harm a computer system and network of the users. A keylogger is a type of malware which captures everything a user types on their keyboard, including passwords and other confidential information by which identity theft can be done easily.

There have been various cases of identity theft in India.

CBI v. Arif Azim (Sony Sambandh case)[3]

A website called www.sony-sambandh.com enabled NRIs to send Sony products to their Indian friends and relatives after online payment for the same. In May 2002, someone logged into the website under the name of Barbara Campa and ordered a Sony Colour TV set along with a cordless telephone for one Arif Azim in Noida. She paid through her credit card and the said order was delivered to Arif Azim. However, the credit card agency informed the company that it was an unauthorized payment as the real owner denied any such purchase.

A complaint was therefore lodged with CBI and further, a case under Sections 418, 419, and 420 of the Indian Penal Code, 1860 was registered. The investigations concluded that Arif Azim while working at a call center in Noida, got access to the credit card details of Barbara Campa which he misused. The Court convicted Arif Azim but being a young boy and a first-time convict, the Court's approach was lenient towards him. The Court released the convicted person on probation for 1 year.

Vidyawanti Joshi v State Bank of India[4]

In this case after a failed transaction at the ATM the complainant submitted a revision petition to the National Consumer Disputes Redressal Commission, New Delhi. He also wrote a complaint to State Bank of Patiala seeking refund of Rs. 40,000 wrongfully withdrawn from account. However, the respondent failed to oblige. So, he filed a consumer complaint.

The Court held that the ATM machine was manipulated by the third party resulting in unauthorized transactions. Since the money had been wrongfully withdrawn from the account of the complainant, the body corporate involved in such banking business, earned a profit out of it and was liable to pay compensation to the aggrieved party.

National Association of Software v Ajay Sood & Ors.[5]

In this case plaintiff has filed inter alia injunction praying for a decree of permanent injunction restraining the defendants or any person acting under their authority from circulating fraudulent Emails originating from the plaintiff of using the trademark "NASSCOM" or any other mark confusingly similar in relation to goods or services. They prayed for rendition of accounts as well as compensation for damages suffered by the plaintiff.

[3] https://www.indiancybersecurity.com/case_study_sony_sambandh_case.php

[4] "Vidyawati Joshi vs State Bank Of India on 27 October, 2020" https://indiankanoon.org/doc/34477875/

[5] [119 (2005) DLT 596]

The Court in this case stressed on the need for strict laws on phishing which is a form of internet fraud to defraud individuals and companies. It has further acknowledged those defendants whose employees were involved in doing illegal action which is violative of plaintiffs right. It has awarded a sum of Rs. 16,00,000 to plaintiffs.

Pune Citibank Mphasis Call Center Fraud[6]

According to the case in the year 2005, US $ 3,50,000 were dishonestly transferred from the Citibank accounts of four US customers through the internet to a few bogus accounts. The employees gained the confidence of the customer and obtained their PINs under the impression that they would be a helping hand to those customers to deal with difficult situations. They were not decoding encrypted software or breathing through firewalls, instead, they identified loopholes in the MphasiS system.

The Court observed that the accused in this case are the ex-employees of the MphasiS call center. The employees there are checked whenever they enter or exit. Therefore, it is clear that the employees must have memorized the numbers. The service that was used to transfer the funds was SWIFT i.e. society for worldwide interbank financial telecommunication. The crime was committed using unauthorized access to the electronic accounts of the customers. Therefore this case falls within the domain of 'cyber crimes". The IT Act is broad enough to accommodate these aspects of crimes and any offense under the IPC with the use of electronic documents can be put at the same level as the crimes with written documents. Further the court held that section 43(a) of the IT Act, 2000 is applicable because of the presence of the nature of unauthorized access that is involved to commit transactions. The accused were also charged under section 66 of the IT Act, 2000 and section 420 i.e. cheating, 465, 467 and 471 of The Indian Penal Code, 1860.

Legal provisions in India on identity theft

Section 66 B of Information and Technology Act, 2000 pertains to dishonestly receiving any stolen computer resource. Section 66 D of Information and Technology Act, 2000 on the other hand was inserted to punish cheating by impersonation using computer resources. The Section 66C of Information and Technology Act, 2000 mentions the punishment for identity theft. Whoever, fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh. [7] Identity theft is currently a cognizable, bailable, and compoundable offenses under the IT Act.Section 77A states that an offense committed under section 66C is a compoundable offense. [8] Women and children have also been provided protection under Section 67 A and 67 B of the Information and Technology Act.

Further, stronger laws have been formulated with respect to protection of "sensitive personal data" in the hands of the intermediaries and service providers (body corporate) thereby ensuring data protection and privacy. Only exceptional cases where such data can be revealed is to an agency authorized by the State or Central government for surveillance, monitoring or interception, under Section 69 of the IT Act. The ambit of sensitive personal data is defined by the IT Rules, 2011 to mean password, financial information, physical physiological and mental health condition, sexual orientation, medical record and history, and biometric information.[9]

In Bhartiya Nyaya Samhita there are various sections which mention forgery and frauds which are a result of identity theft.[10]

[6] https://bnwjournal.com/2020/07/17/pune-citibank-mphasis-call-center-fraud/

[7] Section 66C of Information Technology Act, 2000

[8] Section 77A of Information Technology Act, 2000

[9] Amber Gupta, Data Privacy in India and data theft Slideshare.net (2013), available at www.slideshare.net/AmberGupta6/data-privacy-in-india-and-data-theft

[10] Section 335, 336, 340 and 344 of Bhartiya Nyaya Samhita, 2023

- **Section 335 - Making a false document**. A person is said to make a false document or false electronic record— (A) Who dishonestly or fraudulently—

  (i) makes, signs, seals or executes a document or part of a document;

  (ii) makes or transmits any electronic record or part of any electronic record;

  (iii) affixes any electronic signature on any electronic record;

  (iv) makes any mark denoting the execution of a document or the authenticity of the electronic signature, with the intention of causing it to be believed that such document or part of document, electronic record or electronic signature was made, signed, sealed, executed, transmitted or affixed by or by the authority of a person by whom or by whose authority he knows that it was not made, signed, sealed, executed or affixed; or

  (B) Who without lawful authority, dishonestly or fraudulently, by cancellation or otherwise, alters a document or an electronic record in any material part thereof, after it has been made, executed or affixed with electronic signature either by himself or by any other person, whether such person be living or dead at the time of such alteration; or

  (C) Who dishonestly or fraudulently causes any person to sign, seal, execute or alter a document or an electronic record or to affix his electronic signature on any electronic record knowing that such person by reason of unsoundness of mind or intoxication cannot, or that by reason of deception practiced upon him, he does not know the contents of the document or electronic record or the nature of the alteration.

- **Section 336. Forgery -** (1) Whoever makes any false document or false electronic record or part of a document or electronic record, with intent to cause damage or injury, to the public or to any person, or to support any claim or title, or to cause any person to part with property, or to enter into any express or implied contract, or with intent to commit fraud or that fraud may be committed, commits forgery.

  (2) Whoever commits forgery shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both.

  (3) Whoever commits forgery, intending that the document or electronic record forged shall be used for the purpose of cheating, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine.

  (4) Whoever commits forgery, intending that the document or electronic record forged shall harm the reputation of any party, or knowing that it is likely to be used for that purpose, shall be punished with imprisonment of either description for a term which may extend to three years, and shall also be liable to fine.

- **Section 340. Forged document or electronic record and using it as genuine -** (1) A false document or electronic record made wholly or in part by forgery is designated a forged document or electronic record.

(2) Whoever fraudulently or dishonestly uses as genuine any document or electronic record which he knows or has reason to believe to be a forged document or electronic record, shall be punished in the same manner as if he had forged such document or electronic record.

- **Section 344. Falsification of accounts-** Whoever, being a clerk, officer or servant, or employed or acting in the capacity of a clerk, officer or servant, wilfully, and with intent to defraud, destroys, alters, mutilates or falsifies any book, electronic record, paper, writing, valuable security or account which belongs to or is in the possession of his employer, or has been received by him for or on behalf of his employer, or wilfully, and with intent to defraud, makes or abets the making of any false entry in, or omits or alters or abets the omission or alteration of any material particular from or in, any such book, electronic record, paper, writing, valuable security or account, shall be punished with imprisonment of either description for a term which may extend to seven years, or with fine, or with both.

Recently, the Digital Personal Data Protection Act, 2023 was passed by the Indian Government which came into effect on September 1, 2023. This Act also aims to protect personal data of Indian Citizens. The Act proposed penalties for data privacy breach such as[11]:

A. The major penalties include the Data Protection Board has the power to issue penalties up to INR 250 crore.

B. Data fiduciaries are liable to pay a penalty up to INR 250 crore for breach in observing the obligation of a data fiduciary to take reasonable security safeguards to prevent personal data breach.

C. Penalty on data principal includes breach in observance of the duties of data principal Non-compliance shall lead to a penalty of INR 10,000.

D. Breach in observing the obligation to give the board or affected data principal notice of a personal data breach. Non-compliance in this case shall lead to a penalty of INR 200 crore.

E. Breach in observance of additional obligations in relation to children. Non-compliance shall lead to a penalty of INR 200 crore.

F. Breach in the observance of the additional obligations of a significant data fiduciary Non-compliance shall lead to a penalty of INR 150 crore.

Challenges for law enforcement agencies

Though there are various laws in India but lack of specific laws on the serious cyber crimes such as data breach, identity theft, cyber bullying etc. can cause serious consequences on a normal person's life. This problem has been raised several times but still lack of strict action in controlling them, creates major legal challenges in the law implementation.

Lack of common law in two countries sometimes creates major challenges to law enforcement agencies. No extradition treaties between two countries further delays the legal procedure among two countries. This has a major contribution in the increase of identity theft crimes.

There is also lack of knowledge on significant changes adopted by perpetrators in committing identity theft which is further increasing challenges

[11] Section 33 of Digital Personal Data Protection Act, 2023

for law enforcement agencies to punish these people who are actively involved in doing these crimes.

More people use the electronic devices but lack of awareness among them on the ways in which identity theft is committed victimizes them. This is also a major challenge as people could not identify that their account has been hacked. No proper and effective solutions to control these crimes further help the perpetrators to commit these crimes.

Lack of technological advancement to identify the manners in which identity theft is committed is also a major challenge for lack enforcement agencies. India, being a developing country, still needs a lot of advancement in the technical field so that the crime of identity theft can be identified at the right time and these perpetrators can be punished.

Delay in identifying and reporting of identity theft cases also create challenges for the investigating agencies in carrying on their investigating procedures. This has also delayed in doing justice to the victims. This is also the main reason for the increase of various cyber crimes including identity theft.

Suggestions

The people should be made aware of identity theft and the steps such as monitoring their accounts, changing passwords of their credit cards, and reporting the authorized agencies such as banks and police about online frauds if it happens with them should be done so that to some extent identity theft can be controlled.

The Government should regularly monitor their cyber laws so that if any amendment is required it can be done immediately. This is very important so that the Government and its agencies regularly keep a check on the effectiveness of present cyber laws so that data protection can be promoted.

For making laws, the Government should discuss problems of identity theft and other cyber crime with technical cyber experts. Proper discussion of these problems will bring out new solutions to these legal challenges. This is very important so that time to time interaction on various cyber problems can be carried out between Government authorities and cyber experts. This will strengthen cyber security in our country.

Report the bank and other legal authorities such as police officers in case of illegal transactions happening from your bank account. By doing early reporting of the cyber fraud can help in blocking such hacked accounts. This will one side help the victim whose account has been hacked to save his remaining money and on the other side it will help police and other investigating authorities to take strict action against these hackers and other people committing identity theft.

Appointing more vigilant officers to deal with the increase of cybercrime in our country. This is very important as there will be more officers than large numbers of cases that can be investigated thoroughly. As delay in investigation procedure also causes delay in getting justice to the victims.

People should be educated about methods of online security which includes using strong and distinctive passwords to prevent identity theft done by malware software. Media and other cyber crime experts should take this as their responsibility towards society. By doing This, not only identity theft but various other cyber crimes can also be controlled.

Next, Bank officials should also be properly trained so that they can identify financial frauds of customer accounts. This is very important so that bank officials can identify the problems that arise due to cyber crimes and take strict action against perpetrators. On one side this will help the people who are victims of these cyber crimes and on the other side in future financial frauds can be controlled.

Various international conferences should be organized where the methods to tackle these online identity theft and other cyber crimes should be discussed so that developing countries which lack

technology to identify these cyber crimes can seek help from developed countries where technologies are very much advanced. By doing this, at global level everyone can combinedly fight against identity theft and other cyber crimes. These efforts will help all the countries and their law enforcement agencies.

Conclusion

From the above discussion on the problem of identity theft and issues concerning threat to cyber security we can conclude that identity theft and other cyber crimes is increasing every day and many people are becoming victims of these problems. Finding effective solutions to these problems is the need of the time and our major responsibility to contribute in spreading awareness on cyber crimes.

To achieve the goals of data protection various legal provisions have been introduced recently. By enactment and enforcement of various Acts the Government is trying its level best. Further, we can conclude that the Government is taking various efforts to resolve the problem of identity theft and other cyber crimes, but still due to lack of technical advancement, public awareness of these crimes, lack of knowledge on changing techniques of doing these crimes and various other factors are involved in creating challenges to law enforcement agencies. These investigating agencies face a lot of problems in order to meet the present needs of the society.

So, there is a need for collective efforts from the Government and all other responsible technical experts. People can definitely bring change and resolve the problem of identity theft effectively. Hence, all of us should be ready to take steps to be aware of the ways identity theft is committed and take the responsibility to spread awareness among other peoples on the issues of identity theft and what steps can be taken by us to secure our data from identity thieves.

References

Margaret C. Jasper, Identity Theft and How to Protect Yourself (Legal Almanac Series), Second edition, (2007), Oceana Publications.

Jon Erickson, Hacking: The Art of Exploitation, Second edition, (2008), Starch Press Publications.

Wenliang Du, Internet Security: A Hands on Approach, Third edition, (2022), Wenliang Du publications.

MINISTRY OF LAW, JUSTICE AND COMPANY AFFAIRS (Legislative Department), THE INFORMATION TECHNOLOGY ACT, 2000 (No. 21 OF 2000).

https://secureprivacy.ai/blog/india-digital-personal-data-protection-act-2023-guide-protected-data

https://blog.ipleaders.in/laws-that-govern-id-theft-in-india/