PDFCYL - Expert Report

Theft of one's identity is a serious problem that affects people all around the world. Throughout the technological transition, and with globally and digitally adaptability now reigning across many industries, technology has had a fast impact on people's mindsets. Information Technology's importance has risen to unprecedented levels, with both beneficial and harmful consequences. Due to the growth and transformation of IT in India, identity fraud has been a significant worry in past years (Tungekar, 2021a).

Chatterjee (2021) mentioned that in growing countries like India, information piracy and identity fraud crimes have increased dramatically. Even though the Indian government is unwilling to share statistics on the number of incidents of identity fraud that have occurred within those past years, it is possible to infer from daily media stories how hazardous and common such identification crimes are in our daily activities.

As stated by the Norton Cyber Safety Insights Report for 2021, the cyber security company polled over ten thousand adults in ten countries for the outcomes, with one thousand adults from India responding. According to the survey, 36 percent of Indian grown-ups identified illegal login to a profile or computer in the last 3 years, out of a total of one thousand participant in the nation (Das, 2021).

Moreover, Das (2021) stated that identity theft affected two out of every five Indians. According to the data, 14 percent of the respondents were affected in the previous year, implying that nearly 27,000,000 Indian grown-ups were perpetrators of identity fraud in the previous year. According to the surveys, about 60 percent of the elderly community, particularly the senior citizens, is concerned about their identification being robbed.

Similarly, nearly 65 percent of inhabitants believe they are adequately shielded opposing the identity fraud, but many others have no clue what to do in the

circumstance of identity fraud. The majority of people who are uninformed of the reality surrounding identity fraud want additional data so that they can brace properly.

But the distant operating induced by the outbreak is seen as a crucial explanation for the recurrent and startlingly large climb in occurrences of identity fraud in India. According to surveys, nearly seven out of ten Indian grownups have been harmed by numerous cyber - criminals and hackers as a result of the working remotely characteristic that the individuals had to adjust to related to the situations. And regardless of the risk of working remotely, surveys show that just 36 percent of individuals have installed or upgraded their security features after being hacked into their profile or computer.

Identity is the evidence of somebody's extant, while *theft* is the unauthorized holding of property outside the approval of the rightful individual. As a result, identity theft happens if a person takes possession of someone else's identity outside their permission or proprietorship. In simplistic terms, identity theft happens when an individual duplicates or impersonates someone he is not.

Hence, the Indian Penal Code (IPC) of 1860 and the Information Technology Act (IT Act) of 2000 both regard identity fraud to be criminal offenses. Identity fraud became a crime following the Information Technology Act of 2000, which amended the Indian Penal Code. To be more explicit, these newly modified regulations pertain to digital data. According to the IPC, 1860, a digital data is information, document, or details created, picture, or audio delivered or collected in any digital mode, which is comparable to the description given in the IT Act, 2000 (Indian Penal Code, 1860, n.d.a).

Based on the laws relating to the crime of identity fraud, the term *theft* as defined in Section 378 of the Indian Penal Code, 1860, may not cover identity theft because it only refers to moveable, physical assets and excludes the Internet. Although no explicit section of the Indian Penal Code, 1860, specifies *identification theft*, Sections 463, 464, 465, 469, and 474 of the IPC, 1860, have measures for punishing falsification, and identity theft has now been added to the

ambit of these sections following the modification of the IPC, 1860. Identity theft is defined as having cheated under sections 419 and 420 of the IPC, and it is correspondingly punished because it involves cheating through deception.

Accordingly, the Indian Penal Code, 1860, roams around the issue of identity fraud by classifying it as a form of prolonged falsification or deception. After being amended in 2008, the word *identity theft* was introduced to the Information Technology Act of 2000. It required significant times to grasp the importance of disrespect intended legislation, such as Section 66C of the Information Technology Act of 2000, which prevents the illegal and unethical exploitation of any individual's identity characteristic.

As a result, under section 66C of the IT Act, 2000, anybody who uses another individual's digital identification, passcode, or other distinctive authentication characteristic illegally or deceitfully is subject to jail of either kind for a term up to 3 years, as well as a penalty up to £1755. Another major issue that law faces is the implementation and execution of these laws. In India, there is no officials to deal with the continuously evolving cyber-attacks. Another contributing to the surge in the frequency of occurrences of identity fraud is an unawareness of these cyber-attacks.

Conversely, in terms of legal protection against identity fraud, or a person's or company's information, Indian laws lag behind, abandoning a lot of room for development in terms of legislation, regulations, and procedures. The shortage of particular rules has resulted in a slew of deceptive offenses that have exploded in recent years, prior to the previous two years. A robust system with an effective structure of law is required to guarantee appropriate application of current legislation and to equitably assess the reality.

Additionally, it is vital to limit power clashing and engage sufficient compassionate people. Finally, the authorities must raise user understanding about how to secure confidential data and use the web safely. They must also be taught on their responsibilities and the restitution processes accessible to them in the event of identity fraud. Therefore, users should also maintain record of their bank

statement and sensitive information when it is utilized, and request for reasons of why such personal information is necessary and how trustworthy it is, to reduce the impact and immediate discovery of identity fraud (Tungekar, 2021b).

As previously mentioned, identity theft occurs when a criminal obtains confidential details such as your username, location, bank card or bank account numbers or credentials and utilizes this for financial benefit. The steps you must take, the duration it will end up taking to recuperate, and the implications of having your private details taken will all be determined by the type of identity fraud you have suffered. Several individuals have invested over six months settling credit and financial concerns related to identity fraud in exceptional circumstances.

Moreover, Sehgal's (2019) article demonstrated the financial implications of identity fraud are common, however there can also be additional effects, such as an emotional impact. For instance, when a fraudster breaks a law and gives the officers your identity, this is known as criminal identity fraud, and the police detain you as a consequence, you can envision the pressure and interruption to your lifestyle until the problem is resolved. The following are the four most prevalent impacted aspects of a victim of identity fraud:

1. Physical
2. Economical
3. Social
4. Mental

Physical aspect

It is a distressing scenario if an individual is utilising your identity to commit offences and police officers pursue you. And even if you redeem your record, your criminal history may still show up in future assessments, affecting anything from your career to your accommodation facilities. For example, if your credit and bills are compromised, you may lose your house. If your business is harmed, you may forfeit your employment, and you may also lose out on start-up possibilities.

Likewise, fraudsters with your personal details can acquire your health insurance and even manipulate your health records (Sehgal, 2019a). When you are under a doctor's treatment or in a crisis, and doctors do not have proper health data or you no more have health plans to support you, this might have serious consequences.

Economical aspect

The economic challenges that identity fraud may create might persist for long, following your sensitive data has been exposed. The difficulties that individuals confront are determined by the sort of data that crooks acquire.

- Dispute the activities of an unauthorized user in your bank statements and attempt to repair your exceptional money.
- Organize and close account numbers, as well as establish new ones.
- Username and passcode are changing.

Basically, fraudsters can seize control of your assets and other investment securities by profile control, which can have serious consequences for your pension, property, and children's schooling.

Furthermore, identity fraud is not one that you should take lightly, particularly if it concerns critical information about individuals such as your personal details. Fraudsters may wait years longer to utilize your details, hoping that you would be less aware of the danger. On the internet, hackers may also trade confidential information. You may have to be vigilant and on the lookout for risk factors permanently. Actually, several offenders seek government assistance while recuperating from identity fraud, demonstrating the extent of the problem (Sehgal, 2019b).

Social aspect

In India's computer crimes world, the Internet is another way for identity fraudsters to gain exposure to private confidential material like email or social media authentication tokens. Regardless you utilize social platforms for work or to keep in touch with relatives and friends, attackers can harm your reputation or endanger

your career by exploiting your present user credentials or creating additional, fraudulent profiles on which they can publish offensive remarks while posing as you.

On a far more basic level, recovering from identity fraud may disrupt social relationships as you deal with all of these pressures, as well as if you ask relatives and co-workers for help and monetary assistance when you get up on your own. Identity fraud has a long-term harmful impact on its users. One of the finest actions you can do is respond quickly to reduce its consequences and seek assistance (Sehgal, 2019c).

Mental aspect

The mental aspect that may result from having your hacked identification is perhaps a lower evident effect. Identity fraud is typically an anonymous offense that can elicit a wide range of emotions. Hatred is often the initial emotion that sufferers experience. However, from the first trauma, more difficult and lengthy impacts might emerge. Somebody who steals your individuality, as instance, might commit atrocities in your identity, causing immediate damage to your reputation and making it difficult to prove. If you apply for an employment and your character inspection reveals a lawbreaker past, this might endanger not just your career as well as your consciousness. Never the less, but illegal identity fraud may result in your imprisonment till you can resolve the issue (Sehgal, 2019d).

Since identity fraud is often nameless, individuals might seem helpless. Sehgal (2019) added that the incidence of identity theft-related mental distress was shown in a 2016 study of identity fraud victims conducted by the Identity Theft Resource Centre as:

- 8 said they were suicidal
- 74% of the participants said they were frustrated
- 60% said they were anxious
- 69% said they were worried about their own personal finances
- 42% said they were worried about their family's economic stability

However, even there is a fixing up of the jumbled path of fraud and identity theft, mental pressure may disrupt your health and food, as well as contribute to melancholy and solitude. Additionally, once a person incurs bankruptcy on your behalf, proving that the obligation is not yours might be difficult. You must also adopt efforts to ensure that the latter is no longer reported as yours by enterprises and credit bureaus.

Considerably, as identity fraud is now on the rise and represents a danger to communities, the Indian government has committed to take steps to safeguard individuals from cyber-criminals together while ensuring that residents' confidentiality is not compromised (Rai, 2020). Furthermore, there are two approaches that identity fraud can occur, as per the authorities:

1. Unlawful gathering and theft of a user's personal identification.

2. Misuse of a user's confidential data in such a way of incurring lawful detriment.

Identity fraud is an offense that encompasses combined fraud and theft, so the laws of the Indian Penal Code, 1860 (IPC), as well as the Information and Technology Act, 2000, are frequently applied. Accordingly, some of parts of the Indian Penal Code such as Forgery under Section 464 of IPC, Making False Documents under Section 465 of IPC and Reputation under Section 469 of IPC can be combined with the Information Technology Act. Consequently, the Information and Technology Act, 2000 governs cyber-attacks legislation in India governing cybercrimes. The following are sections concerned with cybercrimes:

- **Section 43** – Retribution in the form of a fine and reimbursement for system destruction
- **Section 66** – Crime involving computers.
- **Section 66B** – Penalties for getting a hacked computer system or communication tool in an unethical manner.
- **Section 66C** – Penalising identity theft.

- **Section 66D** – Penalizing someone for violating by using a computer system to impersonate someone else.

Indeed, the Indian Penal Code, 1860, has been amended by the government to include two additional sections, namely:

- **Section 147A**– Concerns with deception by utilizing another person's distinct identity aspect shall be penalized by detention for a duration of up to three years, a penalty, or both.
- **Section 419A-** Concerns with deceiving by impersonating another individual through a communications system or desktop asset shall be penalized by detention for a duration of up to five years, a penalty, or both.

(Indian Penal Code, 1860, n.d.b)

Correspondingly, when such case of identity fraud is referred to the headquarters for inquiry, information must be gathered to assess how data breaches has happened, if the sufferer requires urgent specific assistance, and also what assistance, whether any, may be offered. To get at this conclusion, the underlying ethical difficulties must be minimized or even eliminated in coping with such offenses. The following are some of the most prevalent ethical concerns to examine and what should be executed:

Ethical Issues	***Expectations***
Honesty	Employees have to: • perform their own work • refrain from accessing unauthorised information • provide authentic results of program outputs.
Protecting confidential information	Employees should not: • try up network access ports with multiple logins • send useless emails and computer files to others • introduce computer viruses into networks • give unauthorised users access to private computer systems
Acceptable use	Computer systems in workplaces should automatically convey unrestricted use of them. That is, employees are forbidden to download microcomputer software for personal applications or use of free mainframe time for personal gain.
Rights of privacy	Head offices should not have the right to read the personal e-mail of their employees. While employees should not use their business email for personal use.

(Hugel, n.d.)

To summarize, this report focuses on how the Indian government expresses worry about emerging cyber-attacks, particularly identity theft. As a result of the different situations involving innocent people, revisions to the legislation book have been made. However, because the crime remains anonymous at times, the existing legislation fails to punish the perpetrators, and victims continue to encounter challenges. As an expert, I would advise the Indian government to focus its efforts on an identity theft prevention campaign that teaches people how to protect their data in the first place.

References:

Chatterjee, D., 2021. *Analyze the various forms of ID theft in India*. LawSikho: ipleaders.

Das, S., 2021. *Identity Theft the Biggest Cyber Security Threat in India, 2.7 Crore Affected in 2020: Norton*. [online] News18. Available at: <https://www.news18.com/news/tech/identity-theft-the-biggest-cyber-security-threat-in-india-2-7-crore-affected-in-2020-norton-3656822.html>.

Hugel, B., n.d. *Core Concepts of accounting information system*.

Indiacode.nic.in. n.d. *Indian Penal Code, 1860*. [online] Available at: <https://www.indiacode.nic.in/handle/123456789/2263?locale=en>.

Rai, D., 2020. How is Identity Theft a Growing Threat to Families. [Blog] *ipleaders*, Available at: <https://blog.ipleaders.in/identity-theft-growing-threat-families/>.

Sehgal, D., 2019. All You Need to Know About Identity Theft in Cyberspace in India. [Blog] *ipleaders*, Available at: <https://blog.ipleaders.in/all-you-need-to-know-about-identity-theft-in-cyberspace-in-india/>.

Tungekar, B., 2021. Laws that govern ID theft in India. [Blog] *ipleaders*, Available at: <https://blog.ipleaders.in/laws-that-govern-id-theft-in-india/>.