IJRAR.ORG E-ISSN: 2348-1269, P-ISSN: 2349-5138

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS (IJRAR) | IJRAR.ORG

An International Open Access, Peer-reviewed, Refereed Journal

IDENTITY THEFT IN CONSUMER PROTECTION

K.M. Surraj, Harshitha Jayakumar

B.com. LLB. (hons.), BBA. LLB. (hons.)

School of Law, SASTRA University, Thanjavur, India

ABSTRACT:

In this article the author tries to outline about what identity theft is and discusses in detail about the types of identity theft. The author also talks about how to overcome those types of identity theft. The author mainly covers how identity theft prevails in India and how identity theft has emerged to be one of the heinous white collar crimes in India during the pandemic. The author has listed cases to support the complete analysis of identity theft and concludes by saying identity theft not only affects individuals but also has adverse effect on economy and business.

Index terms
Identity Theft, Overcome, Technology, Pandemic.

I. INTRODUCTION:

Technology advancements have made it possible to perform business transactions more quickly and easily. Particularly with regard to online transactions, it is frequently necessary for customers, companies, governmental organizations, and financial institutions to transmit personal data. However, the availability of personal information in the market enables outsiders to obtain personally identifying data from clients or organizations, frequently without their knowledge.

Information technology's significance has gradually increased, with both beneficial and negative consequences. Due to the growth and revolution of information technology in India, identity theft has become a significant worry in recent years. Almost everyone has heard of this idea at some point in their lives. But it seems as though we will never be the ones. But what if you were the victim?

Identity theft is one of the fastest growing crimes in society, and is becoming a major public policy concern for consumers and legislators. New protective measures are being introduced to protect ordinary consumers, both as legislative reforms and technological innovations.[1]

[1] Kamaal Zaidi, Identity Theft and Consumer Protection: Finding Sensible Approaches to Safeguard Personal Data in the United States and Canada, 19 LCLR, 99, 99, 2006.

In this article, the author tries to analyze what Identity theft is, the various forms of ID theft in India and the present legal framework that exists to combat and counter them.

II. TYPES AND HOW TO OVERCOME:

2.1 Financial identity theft:

When someone utilizes another person's information for financial benefit, this is the most prevalent type of identity theft. For instance, a fraudster might use your Social Security information to obtain a new credit card or your bank account or credit card number to steal money or make transactions.

2.1.1 What you can do:

Regularly review your statements, accounts, and invoices. Review the statements carefully because some crooks may start by making tiny credit or debit charges in the hopes that you won't detect them. Contact your bank or credit card company if you find a charge you're not familiar with.

You might not get a bill or statement for new accounts opened in your name. Your credit reports can be placed with a security freeze or a one-year initial fraud alert to assist stop access to open new accounts.

Another option is to sign up for a credit monitoring service, which will alert you to significant alterations to your credit reports.

2.2 Tax identity theft:

In this type of identity theft, criminals gain access to your personal data and use it to file a tax return and receive a refund, which is actually the consumer's refund.

2.2.1What you can do:

Watch out for phone Internal Revenue Service emails, messages, and phone calls. The IRS won't get in touch with consumers via these channels or issue a warning. Never respond to a telemarketing call, email, social media message, or text with personal information.[2]

Contact the IRS if you discover that your tax return has been denied because someone else has already filed a return under your name. It's possible that you'll need to submit a fraud claim and get a PIN for use on upcoming tax returns. Furthermore, if someone has submitted a tax return in your name, they already have access to at least some of your personal data.

2.3 Medical identity theft:

A fraudster who commits medical identity theft will exploit your personal information to obtain medical treatment in your place.

2.3.1 What you can do:

Look over any Explanation of Benefits statements you get from your health insurance to make sure there aren't any errors or strange charges on there. Inform your insurance provider if you come across any. To be sure your medical records are accurate, speak with your doctor. Call the provider and raise a complaint if you start receiving bills for medical treatments you didn't obtain.

The same care should be used with your medical identity as you would with any other sensitive information. Additionally, watch out for con artists who may approach you about a "recent breach" in an effort to obtain your personal information.

2.4 Employment identity theft:

Your information might be used by identity thieves to pass a background check or apply for a job.

[2] Equifax, https://www.equifax.com/personal/education/identity-theft/types-of-identity-theft/,(last visited June. 28, 2022)

2.4.1 What you can do:

Especially if they haven't conducted a background check on you yet, be suspicious of any prospective employers who request information about your credit or bank accounts. Additionally, be suspicious of any correspondence sent from a personal email address as opposed to a business one. You can view a list of all the employers who have reviewed your records on the E-Verify website run by the federal government to see if any of them are unfamiliar. More information about job identity theft and E-Verify is available from the Federal Trade Commission (FTC).

2.5 Child identity theft:

Since the majority of minors under the age of 16 don't have credit reports, a fraudster may open credit accounts in their name without being noticed. Some young victims of identity theft might not become aware of the crime until they seek for a job or school loan.

2.5.1 What you can do:

To find out if your child has a credit report, check with the three national credit bureaus. If this is the case, you can report the identity theft to the FTC and take additional steps, such freezing or locking your child's credit report.

2.6 Senior identity theft:

Because they could be more trusting and less able to spot a scam, senior citizens may be especially susceptible to identity theft. They could experience the same kinds of identity theft as everyone else, such as financial identity theft, tax identity theft, and medical identity theft.

2.6.1 What you can do:

In particular, if they don't frequently need access to credit, encourage the senior citizens you know to lock or freeze their credit reports as a protective measure.

2.7 Estate identity theft:

This occurs when a fraudster uses the personal information of a deceased person to steal money or open accounts.

2.7.1 What you can do:

Make sure the three nationwide credit bureaus place a “death notice” on the person’s credit reports after someone’s death.[3]

2.8 Criminal identity theft:

Although all forms of identity theft are illegal, this particular one involves someone who is apprehended giving your information to the police. You wouldn't be able to tell until something bad happens, like when a judge issues a bench warrant for your arrest because you didn't pay a speeding ticket.

2.8.1 What you can do:

You never know who might access the personal information you disclose on social media, so you might want to minimize how much you do. Law enforcement should be contacted right once if you are a victim of criminal identity theft.

[3] *Id at 2.*

2.9 Synthetic identity theft:

Fraudsters can fabricate identities in synthetic identity theft by utilising either false or accurate information, or a combination of the two. An identity thief might, for instance, use a valid Social Security number but a name that isn't connected to that number. Since their Social Security numbers are often not used frequently, children and the deceased can be particularly vulnerable.

2.9.1 What you can do:

Check your credit reports frequently, as well as the reports of elders and, if appropriate, your children. Think about an identity monitoring service that searches the "black web" for potentially accessible Social Security numbers. Consider putting a security freeze on your credit reports as well.

Early identification of identity theft is essential to reducing harm in any case. One approach to notice any questionable activity and respond quickly is to check your credit reports, credit card records, and bank accounts.

III. IDENTITY THEFT IN THE MODERN ERA

Computers and other electronic gadgets in the present era of computerization, globalization, and the internet gather a lot of data about every human being and store it in files hidden deep on its hard drive. Using files like cache, browser history, and other temporary internet files, sensitive information is stored, including login IDs and passwords, names, addresses, and even credit card details.

The use of such sensitive information allows a hacker to get unauthorized access to the data, share it with others, or even install malicious software on a computer or other electronic device to obtain sensitive and secret information.

In this digital age, identity theft is a very important issue for everyone. It is a severe crime that is spreading quickly and harming customers financially as well as leading institutions, retail businesses, and the economy as a whole. Electronic identity fraud has increased the variety of forms, making the situation more complex. Such fraud may not only have a negative financial effect; it may also seriously harm one's reputation, require time to deal with misinformation, and result in exclusion from some services because the stolen name has been misused.

It is time to take into account that electronic networks can operate as a facilitator for identity theft, where the criminal seeks to obtain information online in order to commit the crime offline, as well as the foundation for theft or other harm that will be committed online.

Identity theft, the most recent and heinous of a string of horrifying white-collar crimes, has emerged as the crime of the century. With more and more data fraud instances making news by the end of the day, everyone is in danger.

Cases of identity theft and data fraud have rapidly increased throughout developing nations like India. Despite the Government of India's reluctance to provide information on the number of identity theft cases that have occurred in the recent past, it is possible to infer from the regular reporting in newspaper columns how risky and common these identity thefts are in the course of our daily lives.

IV. THE PANDEMIC EFFECT OF IDENTITY THEFT IN INDIA

The 2021 Norton Cyber Safety Insights Report states that the cyber safety specialist polled more than 10,000 adults in 10 countries for the findings, and that among those, 1000 adults from India provided their separate responses. According to the report, 36% of Indian people, out of the 1,000 respondents in the nation, discovered unauthorised access to a device or account within the previous 12 months. [4]

Identity theft happened to every second Indian person in five. According to the reports, 14% of the victims had their identities stolen in the previous year alone, which means that approximately 27 million Indian people were affected. According to estimates, about 60% of all adults, particularly those in the older generation, worry about having their identity stolen.

Nearly 65 percent of the adult population believes they are adequately protected from identity theft of any kind, yet many folks are unsure of what to do in such a situation. The majority of people who are ignorant of the facts surrounding identity theft want more information so they can be better prepared.

The frequent and startlingly rapid increase in identity theft incidents in India is attributed in large part to the pandemic's remote working trend. According to surveys, roughly 7 out of 10 Indian individuals have fallen victim to various cybercriminals and hackers as a result of the victims' adaptation to remote working due to their predicament.

Despite this vulnerability associated with remote working, estimates indicate that just 36% of all adults have upgraded their pre-existing security software or acquired new security software as a result of experiencing illegal access to their accounts or devices.[5]

V. CASES ON IDENTITY THEFT:

Syed Asifuddin and Ors. v/s. The State of Andhra Pradesh:

This case relates to the Tata Indicom employees who were arrested for the manipulation of the electronic 32-bit number, known as ESN, that is programmed into the cell phones which had been stolen exclusively franchised to the Reliance Infocomm. It was held by the Court that such tampering with the source code invoked Section 65 of the Information Technology Act, 2000.[6]

Mphasis BPO Fraud Case , 2005:

In this instance, four employees of a call centre at an outsourcing facility run by "Mphasis" in India collected PIN numbers from four clients of Mphasis' client, The Citi Group. These alleged employees lacked the authority to acquire such PIN codes. The staff opened fresh accounts at Indian banks jointly with others while posing as someone else.

Within two months, they transferred money from the various bank accounts of The Citi Group customers to the freshly opened bank accounts at the Indian banks using the PIN numbers and other account information they had acquired while working for Mphasis. The Indian authorities were alerted to the scam by a bank from the United States in April 2005, and they soon identified the perpetrators.

[4] The Harris Poll, NORTON CYBER SAFETY INSIGHTS REPORT GLOBAL RESULTS,https://now.symassets.com/content/dam/norton/campaign/NortonReport/2021/2021_NortonLifeLock_Cyber_Safety_Insights_Report_Global_Results.pdf., 2021.

[5] *Id at 4.*

[6] Syed Asifuddin and Ors. v/s. The State of Andhra Pradesh, 2006 (1) ALD Cri 96, 2005 CriLJ 4314

When the accused tried to withdraw money from the fabricated accounts, police caught them. Of the $426,000 that was stolen, $230,000 could be recovered. The Court determined that Section 43(a) applied in this case since carrying out such transactions requires illegal access Technology Act, 2000.[7]

VI. CONCLUSION:

A person's privacy has been greatly violated by identity theft, which has had an impact on the victim's mental and social well-being. Identity theft, however, has an effect beyond the person; it also poses a threat to businesses and organizations.

Anyone can become a victim of identity theft, therefore it's critical to take the recommended precautions. Seniors and college students should exercise extra caution when it comes to identity theft because these groups make easy targets for thieves. While those who use shared computers are likewise at risk, everyone in today's society has the potential to be vulnerable. However, people become more irresponsible when they handle personal information carelessly and ignore warning indications. Long-term effects from identity theft may not only hurt victims individually but can negatively impact the economy and businesses.

[7] Lawctopus, https://www.lawctopus.com/academike/tag/pune-citibank-mphasis-call-center-fraud/ , (Last Visited August 7, 2014)