WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Identity Theft in Cyberspace in India

Malaika Gupta

Uttaranchal University

ABSTRACT

The significance of identity theft in the current time is the burgeoning importance of identity-related information in e-governance, social interaction as well as economy. An excellent personal relation and a good name dominated business as well as daily transactions. With the transformation to face-to-face identification in electronic commerce, it was rarely possible, and, as an outcome, identity-related information became much more relevant for participation in social and economic interaction. The requirements of non-physical ways of identification are becoming the standard for e-governance or e-commerce businesses these days. For example, while purchasing an item online, when the purchaser enters their credit or debit card details, that not only identifies the customer but also legitimizes the transfer of payment from the so-identified customer security. This ease of carrying out transactions, lack of proper cyber education, and lapses in cybersecurity cause identity theft, where the digital identity of the unknown victim is misused.

1 Introduction

Theft of personal information, also known as criminal identity theft, is a crime when a hacker or a thief steals your personal information to effectuate a fraud. Identity theft means the fraudulent use of a person's name and personal information to obtain credit, loans, etc. Identity theft uses the identity of another person to receive financial or other benefits on behalf of that person. This is when thieves steal your information to get your bank account or use the information to commit a crime or crime. [1]

Identity theft Statistics

According to expert research:

- 50% of Asia-Pacific surveyed businesses have seen an increase in fraud losses in the last 12 months since accounting and accounting - both of which could damage the brand's reputation.
- Fraud loss was highest in India as reported by 65 percent.
- In India, 87 percent of businesses have expressed serious concern about the harmful effects of fraud on their businesses.
- 71% of people in India say that security is the best way to use the internet, easily tracked and customized, by 15 percent and 14 percent.
- 64% of consumers in India rely entirely on businesses to protect them and use modern security measures.
- Theft of personal information contributes to 28 percent of total fraud in India.
- Fraud rate is very high on credit cards, and two-wheelers have a very low fraud rate.
- Delhi and West Bengal have the highest levels of fraud, followed by Punjab, Uttar Pradesh, and Haryana.

Types of Identity theft

- **Criminal Identity theft**

Theft of crime occurs when a convicted felon identifies himself as another person, using the personal information and details of that person. This leads to the imposition of a criminal record on the victim who may not be aware of the crime committed or may learn about the crime until it is too late or when summoned by the court. It ought to be difficult for the victim to erase their records as the dominion of all the cases is different, and it will be very tough to

[1] Scott Thiel, William Gibson, Father of Cyberspace, 17 Mar 1948, and Gibson William, Neuromancer, Newyork: Ace Books (1984) p.69.

find out who the suspect is as it may need to find the police and who will identify the victim and the Court after an investigation that will clear the charges. [2]

- **Financial Identity theft**

Theft of personal information means that the criminal takes the victim's account by obtaining their personal information. Therefore, the theft of financial information is the result of ID theft. The main purpose of the criminals is to get a credit card in the name of the victim or withdraw money from the victim's account.This includes taking loans from the victim, writing cheques on behalf of the victim, or transferring money to the victim's account.

- **Synthetic Identity theft**

Synthetic identity theft is a common theft when original ownership is done in whole or in part. It is perpetrated by criminals by combining fake credentials with the victim's official details to create a fake document. This false document can be used by a criminal to apply for a loan, get a duplicate license, apply for a loan, etc. This is especially true for lenders who offer credit to fraud. Victims are less affected when their names are confusing, and identity or negative ratings can affect their credit score.

- **Identity cloning and concealment**

Identity cloning and concealment occurs when someone uses another person's identity to hide their identity. It is widely used by foreigners, usually expatriates or migrants. A person can apply for a visa using false information and hide their original identity. Terrorists use Identity cloning to impersonate another person.

Therefore, instead of using someone else's identity for financial gain or committing a crime, the criminal lives the victim's life[3]..

- **Medical Identity theft**

Medical identity theft occurs when a one-person uses another person's information to see a doctor, to obtain drugs that are available on prescription, or to seek insurance benefits. As a result, criminal medical records are included in the victim's record. Therefore, this has a significant impact on the records of the victim's medical record.

- **Child Identity theft**

When a child's identity is used by any other person to obtain illegal profits is known as child identity theft. A swindler can be anyone, a stranger, a friend, or a family member who is directly involved in the children's life.

Remedies for corporate data theft in cyberspace

In the age of the cyber world, as the use of electronics increased, so did technology, and people began to enjoy the term 'cyber' as an opportunity for everyone to have access to any information, data collection, analysis, etc., using advanced technology.

Due to the rapid increase in the number of web users, cybercrime has had a major impact, making cybercriminals in this country and abroad.

Since the word "Crime" has the same meaning as "a legal case that may be associated with criminal activity that could lead to prosecution," while "crime" may be an illegal act where the machine is a weapon or a victim or both. "

2 What falls under the ambit of Cyber Crimes?

It can be hackers, access to split documents, steal trade secrets, or use the Internet through IP law. It might also contain 'denial of services' and viruses that prevent normal traffic from visiting your site. Cybercriminals are not limited to outsiders, except for malware cases and the problem of common security attacks on employees of the same organization who have easy access to corporate passwords and data storage for their benefit. Cyber-attacks also include activities involving the use of devices to promote crime, namely, financial crime, fraudulent sales, pornography, online betting, IP crime, email, fraud, fraud, cyber slander. Cyber fraud, unauthorized access to a computer device, electronic record abuse, email explosion, physical, etc. [4]

Outstanding IT developments bring new threats to the law. These challenges are not limited to any kind of common law, but they do exist, for example, criminal law, property law, contract law, and violence. One of these challenges is the growing threat of data theft. It is a term used when any information in the form of data is copied or illegally obtained by a company or another person without their consent or consent.

Data is an important asset in this new age of information technology (IT). Data is a significant raw material for call centers and IT businesses. Data has always been an important tool and arm for companies to win big market shares. Due to the amount of Data in the current era, its security has become a major problem in the Information Technology industry. Data theft is a challenge posed by Information Technology players who spend millions to compile or purchase data in the industry. The money they earn depends on data protection.

[2] Martin Bryant "20 years Ago Today, World Wide Web was Born-TNW Insider" 6 Aug 2011. (Retrieved on 12 Jul 2016)
[3] GS Bajpai, On Cybercrime and Cyber Law, Serials \Publication, New Delhi, 2011
[4] HarperCollins, Collins English Dictionary – Complete and Unabridged, HarperCollins. Publishers 1991, 1994, 1998, 2000, 2003, 2006, 2007, 2009, 2011, 2014.

Temporary companies rely heavily on their IT networks to perform the many functions of their business. In exchange, they have more information to look at online. In contrast, some information may be freely accessible, confidential information such as customer and employee information, trade secrets, intelligence, email messages, service delivery skills, etc. It should be protected to reduce the financial and historical risks associated with data failure.
Unlike the European General Data Protection Regulation and US sector law, India does not have a protected data protection code. The Protection of Personal Information Bill was established in Parliament, but it should be considered how the law itself will work. To date, IT Act, 2000, IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Regulations, 2011 (later called SPDI Rules), and IPC, 1860, provide both amendments. Organizations and individuals involved.

3 Challenges

A major problem regarding data theft is its international status, e.g., systems that can be easily accessed in the USA, data exploited in China, and impacts felt in India. The result of this is that different powers, environments, laws, and regulations can begin to work, which is a problem in itself. Moreover, in some cases, the collection of facts has become another matter, as the prosecutor in three different places, one of whom may have disagreed, is almost impossible, and knowledge of the weakness of our police will add to the problem. The discrepancy between the various investigative frameworks and the unsafe migration process is another topic. However, the worst part of all these problems is the lack of clear laws in the country where the case is being prosecuted because even if the perpetrator is caught, he can still flee by choosing and choosing other different positions in the law.
Computers are used in a field where cyberspace gives equal opportunities for economic success and self-improvement for all as the use of cyberspace grows more complex and the growth of internet communication increases, cybercrime, which means violations of online contracts, cybercrime, etc. For this reason, a cybercriminal must set strict rules to control cybercrime and ensure adequate justice for the victim of cybercrime. With the new cybersecurity situation, there is a strong need to control cybercriminals and, in particular, in cases of cyberterrorism and hackers, cyber laws must be made more stringent.

4 Does India have adequate Laws to prevent data theft?

The issue of data theft, which turns out to be one of the biggest crimes in the world, is being ignored by lawmakers in India. Contrary to the UK Data Protection Act. In 1984, there was no clear law in India to solve this problem, although India prided itself on its IT law, 2000, to address the ever-increasing challenge of cybercriminals, including data theft. The fact is that the IT Act, 2000 is not well prepared to deal with these cases. [5]

5 Remedies available to an affected organization

Currently, Indian law does not provide a precise definition of data theft. Accordingly, in most cases provided for in section 43 of the IT Act, 2000, subsection (b) means the uploading, copying, or extracting of any data, data, or data from a computer device, computer network, or storage device without permission.
Permission from the owner and any person in charge of the system, network, or device. In the same category, paragraph (j) explicitly seeks to steal, conceal, damage, or alter the source code of a machine to damage.
Specifically, "data theft" may be defined as an unauthorized act of copying or stealing private or confidential information from an organization without the necessary permissions. As mentioned above, data fraud can occur in the sense of client records, source codes, trade secrets, personal and employment information, etc. It has been shown extensively that existing employees of the organization are involved in data theft. It is also clear that, although employees are the largest asset of the organization, they may end up being its major liabilities. It also recommends that organizations should adopt a strict set of information security policies that support the applicable principles of non-disclosure and confidentiality in their employment agreements.
When an organization finds someone, who has been involved in data theft, social and criminal solutions are used.

Civil Remedy

The organization may sue the person referred to in terms of Section 43 (b) of the Information Technology Act, 2000. Section 46 states that the judiciary must fight IT judges. However, an IT judge can only decide in cases where the injury or injury claim does not exceed five crores. In the case of claims weighing more than five pounds, the company concerned must file a similar action in the appropriate court. In addition, subject to employment agreements, an organization may institute a breach of contract under the Indian Contract Act, 1872. [6]

Criminal Remedy

For similar offenses provided for in Section 43 of the IT Act 2000, Section 66 provides for imprisonment for up to three years or a fine of up to five lakhs or both. Sections 405 and 408 of the Indian Penal Code, 1860, are also sections that may be used to steal information. Section 405 describes the violation of

[5] Mark Goodman, Future Crimes: Inside the digital underground and the battle for our connected world, Pub Anchor, reprintedition(2016)
[6] Anna Kohnke, Dan ShoeMaker, Ken E. Singler, The Complete Guide to Cybersecurity, Risks, and Controls, Auerbach Publications, (2016)

criminal finances, while Section 408 provides for criminal prosecution by a clerk or clerk. Section 408 provides for imprisonment for up to 7 years on the obligation to pay a fine. [7]

Another interesting clause could be Section 378 of the Indian Penal Code, 1860, which states the theft of movable property. For this reason, for this section to apply, it must first be determined by the courts whether digital data or data can be treated as movable property.

6 Remedies available for an affected individual whose data has been stolen.

Section 43A of the Information Technology Act, 2000 provides that if an entity fails to enforce and maintain proper policies and procedures that result in improper loss or unfair gain to any person, they shall be liable to pay compensation to that person concerned. Here, "acceptable safety policies and procedures" are considered binding if the company has a data monitoring system and complies with the same understanding as ISO 27001: 2013, as set out in Regulation SPDI 8. However, for this section to apply, attorneys.

Cyber Policing in India

In the current context, cybercrime is rampant in our country. These cases are intensifying after demon possession, as demon possession has increased online banking transactions. The growth of these criminals has led to the establishment of the Cyber and Information Security Division (C&IS), dealing with issues related to Cyber Security, Cyber Crime, National Information Security & Guidelines, and the implementation of NISPG and NATGRID, etc. [8]

Crime and Criminal Tracking Network and Systems (CCTNS)

In 2009, the department was established under the C&IS approved by the Cabinet Committee to build a national intelligence infrastructure. It includes around 15,000 police stations. The Cyber police station uses a trained officer and equipment to track and analyze digital crime.

Predictive Policing

Predicting the police requires using data mining, statistical modeling, and machine learning in crime-related archives to find areas where the police can be involved. Starting in 2013, Jharkhand Police and the National Informatics Center began developing data mining software that could help them learn criminal attempts by scanning online records.

Delhi police, with the help of the Indian Space Research Organization (ISRO), is trying to develop a guessing tool known as CMAPS or Crime Mapping, Analytics, and Predictive System. The program will identify crime hotspots by combining Delhi police data with ISRO satellite imagery and map location. With the help of CMAPS, Delhi Police have reduced their analysis time from 15 days to 3 minutes.

Hyderabad City police are trying to create a database known as the 'Integrated People Information Hub,' which can provide a '360-degree view' of government officials, including their names, surnames, family details, addresses, and other docket details including passports, credit cards,Aadhar card, and driving licenses.

Anyone can lodge a complaint against an online crime reporting system known as Digital Police run by the Department of Home Affairs, Government of India. This is a SMART police initiative that provides a platform for citizens to file complaints online. The site also provides access to government-authorized authorities to use the National Database of Crime Records for crime investigations, policy formulation, data analysis, research, and the provision of citizen services.

Police also use various social media accounts to assist with their recruitment and investigation. People are amazed at how people can steal information using social media. Therefore, the police are trying to understand the machines and are trying to control crime through social media. 9

7 Cyber Crime Identity Theft Cases

Social Media plays an important role in people's lives. It is a tool that helps people stay in touch. Applications like Instagram, Facebook, Twitter, and Linkedin give us ways to stay connected all the time. Excessive use or distribution of these applications is dangerous as it could lead to identity theft.

There are various situations in which we can understand cybercrime:

[7] Fan Gaoyue, "Threats to Cyberspace and Responses", NAPS Net Special Reports, 13 Jun 2013, available at http://nautilus. org/napsnet-special-reports/threat-to-cyberspace and-responses. (Retrieved on 16 Jun 2016).

[8] Vinod Kumar Jaiswal, Cybercrime and Cyber Terrorism, Pub by RVS Books (2010)

[9] Moore, R., Cyber Crime: Investigating High-Technology Computer Crime, Cleveland Mississippi: Anderson Publishing (2005).

Pune Citibank MphasiS Call Centre Fraud

In this case, former employees of MphasiS Ltd defrauded American customers at Citibank for an estimated Rs. 1.5 characters. Unauthorized access to personal information in Electronic Account Space for customers has been used to commit fraud.
Under the Information Technology Act, the use of electronics in 2000 is considered an offense for the use of 'written documents,' 'breach of trust,' 'cheating,' 'conspiracy,' etc. Sections 66 and 43 of the Information Technology Act, 2000 and individuals must be arrested and fined and liable for damages.

Sony Sambandh Case

In this case, Sony India Private Ltd filed a complaint against non-resident Indians. The Sony Sambandh website has helped them send Sony products to friends and family in India after paying online.
It all started when Barbara Campa donated Sony Color Television and wireless headsets to Arif Azim in Noida. Finished payment by credit card, After the completion of all procedures, the company sent the items to Arif Azim. Later, the credit card company notified the company of the transaction. They told them that the real credit card owner had rejected the transaction and said the transaction was illegal.
The company filed a complaint with the Central Bureau of Investigation under Sections 418, 419, and 420 of the IPC. After an investigation, Arif Azim was arrested and told that while working at the call center, he was able to obtain a credit card number and misused it.
This was India's first case of cybercrime, and the CBI has acquired headphones and a television. The CBI testified in the case, and the defendant pleaded guilty. The court indicted Arif under sections 418, 419, and 420 of the IPC and showed tolerance for the boy as he was just a 24-year-old boy and was initially found guilty of keeping him in custody for one year.

The Bank NSP Case

This is one of the most common cyber-crimes ever committed when a professional banker breaks up with his girlfriend. Later, the girl created a fake email and started sending emails to the boy's external clients from the bank's computer. This has led to the loss of corporate clients. The company took the bank to court and was charged with sending emails through the bank's server.

Andhra Pradesh Tax Case

In Andhra Pradesh, government officials exposed a businessman. He was the owner of a plastics factory and was arrested by the Department of Defense, and the Department received dollars. Twenty-two coins from his house.
Defendant used to file vouchers to show the legitimacy of his trade, but the security department used his computer to find out that the defendant had five businesses under the same company's fund and issued illegal or double discounts to represent his sales and tax records.

SMC Pneumatics Pvt. Ltd. vs. JogeshKwatra

This is the first case of cyber-defamation in India, with the suspect JogeshKwatra working for the plaintiff's company and began sharing with other employees and employers defamatory, defamatory, defamatory, and slandering other companies related to his company around the world to tarnish his reputation. The company and its MD, Mr. RK Malhotra.
The complainant filed a complaint in Court, and it is alleged that the emails sent to the suspects were degrading, insulting and defamatory. The lawyer added that the defendant only wanted to tarnish the plaintiff's reputation in India and the rest of the world. Therefore, the respondent is allowed to send those types of emails, and anyone who commits these types of actions will be fired.
After all disputes, the Court passes an initial withdrawal order to stop sending these types of emails, and the judge prohibits him from publishing, sending, or causing any form of harassment or harassment.

Bazee.com Case

In December 2004, a Be.com.com manager was arrested because his website sells CDs with questionable content. The CD was also available in Delhi markets. This case leads to the question of who should be paid here, an Internet Service Provider or a Content Provider. The senior manager was later released on bail to prove that he was a Service Provider, not a Content Provider. The case has raised several questions in cybercrime cases.

State of Tamil Nadu vs. SuhasKatti

The case is particularly important in cyberlaw cases as the trial process came to an end in less than seven months. In this case, the man who was a close friend of the divorced woman was sending abusive, derogatory, and derogatory messages about her. He was sending emails to the woman to collect

information about a fake account on behalf of the victim. As a result, many phone calls came from a woman who believed she was asking for it.[10]
In February 2004, the woman lodged a complaint, and police found the man and arrested him in the next few days. The defendant wanted to marry the woman instead of marrying someone else who later divorced. This caused the respondent to try to contact her again. He also convicted her of forcing the accused to start harassing her online.
The suspect is charged under Section 67 of the Informational Technology Act, 2000 and sections 469 and 509 of the IPC. The defense argued that some of the evidence listed here did not qualify as evidence under Section 65B of the Indian Evidence Act and that all emails could no longer be distributed by her ex-husband and ex-husband in an attempt to arrest the defendant. Instead, the Court hangs on the chief witness, the cybercafe owners, and on all the evidence.
As a result, the Court found the man guilty and sentenced him to life in prison, and fined both of them. This is the first conviction under Section 67 of the Information Technology Act, 2000.

Nasscom vs. Ajay Sood& Others

The case has a landmark decision as the case defines 'criminal identity theft' online as an illegal, disciplinary, and damaging act. The plaintiff, in this case, is the National Association of Software and Service Companies (Nasscom) which is India's main software company. The suspects were a private rental company hired by Nasscom to be tracked down and hired.
The suspects sent emails to third parties in the name of Nasscom to obtain confidential information that they could use in the search. Therefore, the crime of stealing sensitive information is an online scam where a person pretends to be an organization to extract his personal information from customers, such as passwords or access codes, etc. Therefore, the crime of stealing sensitive information collects personal information by misrepresenting it as a legal entity and using it for personal gain.[11]
The court appointed a committee to look into the whereabouts of the suspects, who received two hard drive emails sent by the suspects to customers. Bad emails are downloaded and counted as proof. The suspects used various fake IDs to avoid recognition and legal action.
Later, the defendant admitted their charges, and both parties sought to resolve the dispute amicably. The defendant had to pay Dollars. 1.6 million convicts have been convicted of felony criminal mischief.
This case is very important as it brings ‘sensitive identity theft’ to our legal system and proves that anyone who infringes intellectual property rights will pay damages. The case brought faith to the Indian Judiciary as they were able to protect intellectual property rights.

Cyber Attack on Cosmos Bank

In August 2018, there was a cyberattack on the Pune branch of Cosmos Bank that sank to R. 94 crores. The attackers broke into a large server and transferred money to a Hong Kong bank following the details of various Visa and Rupay cards.
The hackers found themselves using communication between the central system, and the payment method was disrupted, meaning that both bankers and account holders were unaware of the transfer.
This attack was huge and of its kind as the first malware that attacked destroyed all communication between the payment gateway and the bank. The attack caused extensive damage as there were 14,000 transactions in 28 countries using 450 cards and 2,800 transactions using 400 cards in India.

BSNL, Unauthorized Access

In this case, the Joint Academic Network (JANET) has been hacked to prevent access to authorized users by changing their passwords and deleting / uploading files to their accounts. The suspects also made changes to the BSNL database on their online user account.
The company filed a lawsuit against cybercrime, and the CBI launched its investigation and found that broadband internet was being used without permission. Different VPN suspects log in with a server from different cities.
The defendant was then jailed for one year and fined Rs. Five thousand as mentioned in Section 66 of the Information Technology Act, 2000 and Section 420 Indian Penal Code, 1860.

8 Conclusion

As the number of cyber frauds and crimes increases, Some laws are enacted to protect 'sensitive personal information through 'data protection and privacy policy.
While IT legislation, 2000, and SPDI regulations failed to address a series of key issues related to data security in the Indian cyber world, both emerged as the primary basis for providing solutions to organizations and individuals affected. As an organization's responsibility to ensure the confidentiality of any part of the data stored with it, data protection is no longer just a business problem. Failure to access the database not only affects the financial results associated with court actions and business shortages but also damages the company's reputation, especially in the markets.

[10] Vicky Nanjappa, "Cybercrime Rising: Is India doing enough?" Sep 28, 2015, available at : www .oneindia.com. (Retrieved on 23 Jun 2016)
[11] Share. N. Raj, "Evaluation Of Cybercrime Growth And Its Challenges As Per Indian Scenario," IJIFR Vol.2, Issue – 9, May 2015.

REFERENCES

- Amos N. Guiora "Cybersecurity: Geopolitics, Law and Policy," Routledge; 1 program (2017).
- Anirudh Rastogi "Cyber-LawOf Technology and Internet Technology," LexisNexis; The second plan. (2014).
- Apar Gupta, AkshaySapre"Commentary On Information Technology Act - About Laws, Regulations, Orders, Guidelines, Reports and Policy Documents." LexisNexis; First Edition (2015).
- Amita Verma "Cyber Crimes and Law," Public Publications, Allahabad, (2009).
- Anjali Kaushik, "Safe navigation in a cyber environment: Protect your identity and data," SAGE India; 1 program (2013).
- Atul Kahate "Cryptography and Network Security," Tata McGraw-Hill Education, 2013.
- Akash Kamal Mishra "Signature: The Need for Money Without Money". Create an Independent Publishing Platform for Space; 1 program (2017).
- Ananda Mitra, "Digital Security: Cyber Terror and Cyber Security (Digital World)" Chelsea House. ; 1 program (1 May 2010).
- Debarati Halder, K. Jaishankar. "Cyber Cases of Indian Women."SagePublications India Pvt. Ltd; 1 program (2016).
- Gurpreet S. Dhillon, "The Essentials of Cyber Security" Paradigm Books (14 May 2014).
- Harish Chander "Laws and cyber protection" Prentice Hall India Learning Private Limited (2012).
- Karnika Seth, "LexisNexis Computer, Internet and Technology Rules