A study on Identity Theft: the modern crime.

Ummey Safia Begum

Faculty of Law, Cotton University, Guwahati, Assam, India.

Abstract

'Identity theft makes thousands of victims!' is a typical headline of the current scenario. Identity criminals do not steal identities in real life; instead they use identity as a tool to steal money. And the crime is not usually noticed by the typical victim until long after the criminal has booked a one-way ticket to the tropics. A good reason to look at the terminologies of identity 'theft', identity fraud, and identity-related crime is that they are often used in parlance. With the increasing dependency of people on the internet and the cyber world these crimes can be seen in every walk of life in this generation. This article studies on how people fall prey to such notorious crimes and the impacts that are left on people. Information Technology (Amendment Act, 2008) Act along with various provisions of Indian Penal Code of 1872 tries to bring those culprits under the purview of law and punish them accordingly.

Keywords: *Identity Theft, Identity fraud, Identity related crimes, Cyber world, Information Technology (Amendment Act, 2008), Indian Penal Code 1872*.

Methodology

As a secondary tool for study, books of eminent authors, articles in research journals, newspaper reports have been scanned and analyzed. Several online databases and internet search engines have been used to keep the study updated.

Introduction

Identity refers to information intrinsic to a specific individual. Publicly available information, such as a person's telephone number and street address, as well as confidential information, such as Aadhar Card number in India that contribute to a person's identity. By acquiring access to that information, an identity thief can impersonate himself to be someone else to commit fraud. Identity theft is often associated with the fraudulent use of another's identity for financial gain (i.e., the theft of money) and it can also be used to acquire unauthorized entry, privileges, or benefits.

In the present world with the invasion of mobile phones, computers and the internet in our lives, a man's identity has ceased to be his physical appearance. The nature of the internet constitutes a lack of visibility. It grants immense privacy to its users. In the world of the internet, netizens communicate, interact, transact and even romance without coming face to face with one another. Identities on the internet are through user-names of netizens assigned to email accounts, and passwords. Credit card details, social security number, passwords and username constitute the commercial identity of an individual and not his physical being, in today's world. He interacts and transacts using the above identifiers to identify himself. In India we have the Information Technology (Amendment Act, 2008) Act (IT Act) that deals with these kinds of crimes and are punishable under the law.[1]

Consumers fall victim to these schemes due to a variety of reasons. Consumers are vulnerable because they lack specific information regarding the product or service being offered in many cases. Some are also naive and find it difficult to believe that unscrupulous businesses can thrive and flourish. Similarly, many people are too busy or tired to be on guard against fraudulent or deceptive business practices. Additionally, some victims may be experiencing personal problems such as grief, loneliness, depression, substance abuse etc. that impair their decision-making abilities.

[1] Vivek Sood, Nabhi's Cyber Crimes, Electronic Evidence & Investigation: Legal issues (Nabhi Publications, New Delhi, 1st Revised edn., 2008).

During February 2022 several Indians complained on social media that unaccounted loans have appeared in their credit history even as they never borrowed any money from India bulls-owned a company named Dhani Loans and Services. The permanent account number (PAN) details of the people have been used by the fraudsters reportedly to avail instant loans from the Dhani app. Some complained that they were facing show-cause notices by collection agents for loans they never took, others said their credit scores too had been impacted as credit reports have listed loans they had never availed as defaults, and Actor Sunny Leone is one such affected party.[2]

Identity related crimes

There are many things that a person can do with the identities of others. One can not only use someone else's identity, but also can swap identities or destroy identities and the like. However, such things can also happen accidentally without any intentions and it should be emphasized that these activities need not be unlawful but there are perfectly legitimate reasons for doing such things with identities, only a subset of what Rost, Meints, and Hansen have termed 'the rearrangement of identity linkage' is unlawful. The typology developed by them offers a useful starting point to delineate the various forms of 'bad things that can be done with identities'. Identity-related crime' as an umbrella term can be used to describe this overall category covering all punishable activities having identity as a target. Rost, Meints, and Hansen distinguished four partly overlapping – types of modifying the link between an identifier and the person identified by this identifier:

- identity collision, that is when two people have the same name, or when a wrong email address is used; this usually occurs unintentionally;
- identity change, when someone intentionally takes on another identity;
- identity deletion, that is revoking a digital-signature certificate, or reporting the death of Mark Twain in a newspaper ;
- Identity restoration, that is restoring the link between identifier and person, e.g. when Mark Twain tells the world that reports of his death are grossly exaggerated.

The important thing here is when these acts constitute a crime, or should be considered a crime and for this purpose, the identity change and identity deletion are the most interesting. The category of identity collision usually happens accidentally, but if it is done with intent, it is likely that it falls into the category of identity change. Similarly, identity restoration is perfectly acceptable unless and until it is conducted without the consent or knowledge of the person whose identity is being restored and therefore again a matter of identity change. From a criminal perspective identity deletion is an interesting category. Severe consequences may occur when someone has his/ her identity deleted by someone else, for instance, when a hacker destroys important records in a company's computer system. Such an act should be made with an intent to cause damage to the particular company, else it would be simply considered as data interference as mentioned in Article 4 of the Convention on Cybercrime.[3] Most instances of unlawful identity deletion will actually fall in traditional categories of crime such as slander as per Section 499 of Indian Penal Code (IPC) 1872. This may also be well considered as unlawful when someone destroys part of his or her own identity. For example, in some countries, they have criminalized destroying an official ID, and consider it unacceptable when asylum seekers destroy their passport before arrival. But on the other hand according to Rost, Meints, and Hansen the latter could be seen as building up a new identity rather than merely destroying an old identity that could be again handled within the category of identity change. However, when compared to the category of identity change, the category of identity deletion should not be overlooked when researching identity-related crime, but an overseable and perhaps minor phenomenon which in its criminal guise is as 'identity fraud'.[4]

Causes or techniques of identity theft

In such circumstances of a case intent/mens-rea is mostly drawn from it. An interference of a guilty mind is the prima-facie norm. The presence of mens-rea at the inception is believed in most criminal cases. To determine mens-rea or guilty mind the use of information and data by the accused is the most important circumstance.

There are various ways by which a victim falls prey to such notorious acts.

---

[2] Sunainaa Chadha, *Explained: What is identity theft and how you can protect your personal data online*, The Times of India, March 3rd 2022. https://timesofindia.indiatimes.com/business/india-business/explained-what-is-identity-theft-and-how-you-can-protect-your-personal-data-online/articleshow/89968866.cms

[3] See http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

[4] Ronald E. Leenes, *Identity theft, identity fraud and/or identity-related crime*, Researchgate (2006). https://www.researchgate.net/publication/257703479_Identity_theft_identity_fraud_andor_identity-related_crime

Data Breaches

A data breach is when a thief or hacker is able to access the data without receiving the proper authorization. The information of a company may be accessed by the hackers which may have sensitive information stored in a central location. In many cases, the thief focuses on getting credit card or Social Security numbers, as well as the complete names of the owners for committing mischief. Files may also contain other information that can be highly sensitive particularly because that information can be used to correlate the identity of each person.

In 2019, there were around 1,506 data breaches in the United States of America, resulting in the exposure of 164.68 million sensitive records. Similarly, various data breaches have been committed by the fraudsters in India as well. For example, in May 2023 a ransomware gang abused a zero-day exploit to compromise the security of over 2,000 organizations worldwide according to a report from Emsisoft. These included New York City's public school system, British Airways and BBC or in October, resecurity, an American cyber security company, said that the personally identifiable information of 815 million Indian citizens, including Aadhaar numbers and passport details, were being sold on the dark web and the like.[5]

Malware Activity

A hacker can accomplish any number of things with the help of malware, or malicious software from taking over a computer system to controlling a network, providing backdoor access and more. It can also be used specifically to steal personal information. To spy on the target's computer activity is the most common way malware is used to execute identity theft or fraud by programming it. With a phishing email or other trap designed, the attack may begin to get the user to click on a link or image installing the malware automatically.

There are many ways how the attacks can be performed, for instance key loggers, which can keep track of which keys a user strikes. The key logger can record their keystrokes and report them back to the thief when the user accesses a particular website or logs in to their computer. The attacker can thus ascertain their password to a specific site, workstation, or application. Thus, they may be able to collect the target's personal information once the attacker uses that login information,

Credit Card Theft

One of the simplest ways a thief can steal your identity is credit card theft. The card itself is enough to make purchases under the target's identity once they have access to your credit card and they often do not need any other aspect of your identity. The thief can buy and sell the item to someone else at a steep discount, banking a profit along the way. This kind of theft can also be used to grab card numbers for resale on the dark web. The thief also sells to someone else once they get your credit card information.

The company's stores a long list of credit card information to help their customers make quicker purchases. Basically, when customers first do business with the company, information of the credit cards are obtained and kept in a secure location. And because their card information is already in the company's system, their next purchase is quicker and easier. But this convenience comes at a cost when they can get a storehouse of account numbers and information.

Mail Theft

Identity thieves were busy taking people's personal information and using it for their benefit even before the invention of the internet. A common method was that of mail theft. The thief grabs the target's credit card or other information from their mailbox which is a method used in this kind of attack. They then try to use it to make purchases or sell it by using such information. A thief always does not have to go into your mailbox to take your credit card or gather personal information as it is just as easy to go through trash. Often, people have a habit of throwing out letters, notices, or account statements that contain sensitive information. Although information in the trashed document is not enough to execute a complete theft of your identity, it can be used by the thief to confirm who you are.

Phishing and Spam Attacks

In this kind of act an attacker may send an email or text message that imitates a legitimate source and often fools the target. And then after the target clicks on a link that has been sent they are taken to a fake website that asks you

5 The Hindu Bureau,*Top cybersecurity data breaches in 2023*, The Hindu, Dec. 16, 2023. https://www.thehindu.com/sci-tech/technology/major-cybersecurity-data-breaches-in-2023/article67644589.ece

for your username, password, or other personal information like your Social Security or credit card number. The hacker can then use that information to assume your identity or make purchases.

Wifi Hacking
When we use our computer or mobile device on a public network, it may be vulnerable to a hacker that can eavesdrop on communications with the network. At places like coffee shops, department stores, or airports where anybody can get onto the network, often without a password they can be easy targets. The hackers are specifically after social security, credit card, or bank account number to purchase or sell anything by using the credentials.

How Identity Theft Can Affect You

Data and information are chameleons that can be grossly misused to falsely implicated innocents. False cases of data theft are likely to be galore in the times to come. Just as the nature of intellectual property makes stealing luxuriously simple, it is just as simple to accuse a person especially those who are employees or providers of services and more of the same.
There are several ways identity thieves can use personal information to their advantage from stealing money to impersonation and so on. However, the impacts on the victims sometimes cause them to be fatal. Some of effects are discussed below -

Financial
The financial hardships caused by identity theft may last for months or years after the personal information is exposed. The hurdles in the recovery process in this type of loss can include depending on the type of data identity thieves put their hands on, activity in credit files and working to restore good credit, cleaning up and closing compromised bank accounts, and opening new ones.
They can also take over investment and other financial accounts by getting into bank accounts, the impacts of which could affect retirement, mortgage, child's education etc. And it becomes worse when they get handy over some sensitive personally identifiable information like social security number etc.

Emotional
A host of emotional reactions can trigger relating to Identity theft. Anger is the first thing a victim may experience. A challenging and long-term emotion may come into play after the initial shock. Because the thief who steals identity can commit crimes in the victim's name, which can directly harm the reputation and is often stressful to be fixed. For example, while applying for a job if a criminal record pops up in a background check, it may affect not only employment opportunities but also feelings of self-worth. Moreover, it could lead to arrest before getting any time to clear up the confusion.

Physical
Identity theft issues could also manifest as physical symptoms because if someone uses others name and identity to commit crimes, it is obvious that the law enforcement would make arrests, which is a highly stressful event. And it would affect everything from employment to housing options down the road. For example, one could lose home if the credit and mortgage are affected. One could lose a job if the work is affected etc.

Social
The Internet is another way identity thieves can gain access to personal information in today's cyber world like passwords to your email and social media accounts where the hackers could damage a person's reputation or put job on the line by using current accounts or even creating new, fraudulent accounts in which they post while pretending to be the target. It could also affect personal relationships as the thief would pretend and can communicate with the target's friends or family.[6]

Laws Governing Identity Theft

The words data theft, data breach, identity theft and phishing are commonly used in common parlance. These crimes have elements of theft and cheating if we see them from a legal perspective. And these crimes can be huddled together under a class that could be called data crimes or data related crimes from the legal and academic perspective. The IT Act brings into existence the offense of data theft even though not encapsulated in a medium such as CD, computer pen drive or floppy which would basically fall under the purview of theft of movable property as per

[6] 4 Lasting effects of Identity Theft, https://lifelock.norton.com/learn/identity-theft-resources/lasting-effects-of-identity-theft (Last visited on 28th March' 2024).

section 378 of Indian Penal Code[7]. Clause (b)[8] and (j)[9] section 43 with the new version of Section 66 of IT Act incorporates the offense of data theft in the true sense of expression from the legal perspective.

Similarly, the crimes which falls under the category of criminal breach of trust as per section 405 IPC[10], dishonest misappropriation of property defined in section 403 IPC[11] and cheating section 415 IPC[12] are together dealt with sections given in the IT Act which can be said to apply to data crimes or data related crimes.

- Section 66 B of IT Act which says that "Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both".
- Section 66 C provides Whoever, fraudulently or dishonestly make 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 with may extend to rupees one lakh.
- Section 66 read with 43 (b) that whoever downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium without the permission of owner or person in charge shall be liable for punishment upto three years of imprisonment or with fine upto five lakh rupees or both.
- Section 66 read with 43(h) states charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network shall be liable for punishment upto three years of imprisonment or with fine upto five lakh rupees or both.

In the case of ***Binod Sitaram Agarwal vs the State of Maharashtra (2018)[13]***, the applicant was charged with offences that violated sections 43 and 66 C of the Information Technology Act 2000. Sections 408 of the Indian Penal Code and section 70 of the Information Technology Act were also added.

---

[7] See Indian Penal Code, 1872.

[8] Information Technology Act,2000 (Amendment Act of 2008) Sec. 43 (b) Whoever, downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium without the permission of owner or person in charge.

[9] Information Technology Act,2000 (Amendment Act of 2008) Sec. 43 (j) Whoever, steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage.

[10] I.P.C., 1872, Sec. 405 Criminal breach of trust.—Whoever, being in any manner entrusted with property, or with any dominion over property, dishonestly misappropriated or converts to his own use that property, or dishonestly uses or disposes of that property in violation of any direction of law prescribing the mode in which such trust is to be discharged, or of any legal contract, express or implied, which he has made touching the discharge of such trust, or wilfully suffers any other person so to do, commits "criminal breach of trust".

[11] I.P.C Sec. 403 Dishonest misappropriation of property. -

Whoever dishonestly misappropriated or converts to his own use any movable property, shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both

[12] I.P.C. Sec. 415 Cheating.-

Whoever, by deceiving any person, fraudulently or dishonestly induces the person so deceived to deliver any property to any person, or to consent that any person shall retain any property, or intentionally induces the person so deceived to do or omit to do anything which he would not do or omit if he were not so deceived, and which act or omission causes or is likely to cause damage or harm to that person in body, mind, reputation or property, is said to "cheat".

[13] Criminal Bail Application No. 3027 of 2018.

In another case ***K Sudhakar vs N Balaji (2017)[14],*** K. Sudhakar, the father-in-law of respondent N. Balaji obtained his savings account statement from HDFC Bank without consent. The respondent filed a private complaint stating that he has a savings account in HDFC Bank, Thillai Nagar Branch, Tiruchirapalli which makes the petitioner committing offences punishable under sections 66 B and 66 C of the Information Technology Act read with section 406 and section 416 of IPC.

The court held that if the said bank had issued the bank statement to the petitioner without the consent of the respondent he can ask for the relief that is available under the law against the bank authorities. He cannot therefore prosecute the petitioner in court instead. The court viewed that continuance of the proceedings against the petitioner would result in an abuse of procedure of the court, and hence, ordered to quash the proceedings.[15]

Conclusion and suggestions

Identity theft is one of the most common consumer complaints all over the world. In recent years, data breaches have jeopardized the personal information of millions of people by committing various kinds of mischiefs. A losing identity is like losing themselves and if any liability occurs during identity theft, it falls under the person who has been deceived and is innocent, without any knowledge being what had happened. Identity theft may result in serious monetary loss, mental suffering, and injury to one's reputation, and loss of credit. It's critical to be diligent in securing one's personal information, maintaining the security of passwords, and routinely checking credit reports in order to prevent identity theft.

Various use of services and tools like fraud alerts and credit freezes can assist in detecting and recovering from identity theft. By protecting our identity we can lessen the chance of falling victim to this kind of crime by taking proactive steps.

1. By updating passwords regularly, changing net-banking or ATM passwords. Passwords are like keys to a locker. While setting passwords, one should avoid easy credentials that anyone can guess easily. A strong password will enhance online security," says Adhil Shetty, CEO of Bank Bazaar.
2. It is cautioned to avoid saving login credentials. Personal devices may be given for maintenance or service checks or left open or get stolen in such cases it is unsafe to save passwords, cautions Singh. Moreover, while making online transactions, it is always necessary that the platform or website is secured. Websites and mobile apps from trusted entities should be used. Accessing net banking or other sensitive accounts in public places like cybercafés or libraries should be avoided.
3. Using updated Browser & Software is recommended. Software should be updated regularly. "Older software will not withstand sophisticated digital attacks", said Shetty.
4. Banks or financial institutions never ask for sensitive data like passwords or login details, and therefore, one should not share sensitive data online or disclose it on the phone without full disclosure of the person's identity such as who they are, what firm they represent, and why they are calling.
5. Avoid unsafe ATMs either inside a bank or where the guard protects the premises.
6. Opting two-factor authentication for credit and debit cards is helpful in securing data. Banks should take proactive measures in keeping their customers updated with the latest developments in the cyber security space by sending regular communication through SMS, Emails, and in-app notifications. "Considering the pace at which digital payments in India are growing, organizations must look at cyber security as an integral part of the overall organizational stack and not merely a tick-in-the-box," said Stanley Johnson, Executive Director, and AGS Transact Technologies.[16]

[14] Crl. OP.NO. 16669 of 2019.

[15] What Is Identity Theft and Its Laws in India? https://www.writinglaw.com/what-is-identity-theft-and-its-laws-in-india/ (Last visited on 28th March' 2024).

[16] Supra note 2.