Volume 8, January 2020 ISSN 2581-5504

"Identity Theft in Cyberspace with Special Reference to India"

Ankita Shrivastava,
Kalinga University,
Raipur

ABSTRACT

The reason for the relevance of identity theft in the present times is the burgeoning importance of identity-related information in the e-governance, economy as well as in social interaction. In the past, a "good name" and good personal relations dominated business as well as daily transaction. With the transformation to electronic commerce, face-to-face identification was hardly possible, and, as a result, identity-related information became much more relevant for the participation in social and economic interaction. The requirements of non- physical way of identification is becoming the norm for e-governance or e-commerce businesses. For instance, while purchasing any item online, when the purchaser enters their card details that just not only identifies the customer, but it also legitimises the transfer of payment from the so identified customer. This is ease of carrying out transactions, lack of proper cyber education and lapses in the cyber security causes cybercrime of identity theft where the digital identity of the unwitting victim is stolen or by authorised access to victim's account is made to make unlawful financial gains.

INTRODUCTION

> *"Security is, I would say, our top priority because for all the exciting things you will be able to do with computers - organizing your lives, staying in touch with people, being creative - if we don't solve these security problems, then people will hold back."*
>
> BILL GATES

Cybercrimes are those "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)"[1]. It is a crime of recent times which involves illegal activities in cyber space, where any electronic communication device or information system, or internet is used as a tool or target or both. *Cyberspace* is a virtual place where communication over computer network takes place and hence, it is a space with no geographical location and is available to anyone, anywhere in the world with access to the internet.[2] In the modern times with the growing dependence on computer, internet and allied technology and with the digitalization of various services, cybercrimes are also on rise and becoming a menace which needs to be urgently contained. Like any other technology, internet and allied technology also have negative and positive sides associated with them. There are undeniably many benefits of internet but at the same time it has made easier the

[1] Halder and Jaishankar, Cyber Crime and Victimization of Women: Laws, rights and Regulations, 2011, ISBN no. 978-1-60960-830-9

[2] Dr SR Myneni, Information technology law (cyber laws), 1st Edition, Asia law house, Page no. 33

commission of certain crimes. And one such crime is of identity theft in cyberspace. *Identity theft* is a cybercrime whereby the identity of a person is stolen to acquire unlawful monetary gain or to deceive others and, in some cases, it may cause threats to victim's personal safety. When identity theft is committed over cyberspace, it is called as online identity theft or identity theft in cyberspace.The name of the offence is slightly misleading as when a thing is stolen the victim gets dispossessed whereas if a person's identity is stolen, that doesn't render them identity less. The identity of a person, whether alive or deceased, here means and include their personal information for instance, name, date of birth, e-mail ID, data relating to bank account, IT return forms, medical insurance and other such accounts. The commonly interchangeable terms Identity theft and identity fraud are used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain".[3]The ways in which this offence is committed are many such as hacking accounts, phishing, spear phishing, denial of service, distributed denial of service, data theft, installation of spyware, cookies, e-mail/SMS spoofing and many novel ways are coming up with each passing day.

The reporting, determination of Jurisdiction, investigation and trial of these crimes are unlike conventional crimes. Thus, law enforcement agencies are required to have a specific knowledge and expertise in the working of computer and internet to tackle such crimes for enabling speedy trial and just punishment for the perpetrators of crime. The prevalence of such crime is rapidly increasing and causing substantial economic loss to private companies and governments in India and around the world. According to National Crime Record Bureau, India recorded 9622, 1192, 12317 and 21796 cybercrimes in the years 2014, 2015, 2016 and 2017 respectively[4]. And according to the same bureau, the year 2018 recorded 27248 cybercrimes out of which, 55.2% (15,051 out of 27248) were registered for the motive of fraud[5]. According to the Norton Cyber Security Insights Report 2016, 49% of India's online population, or more than 115 million Indians, are affected by cybercrime at some point making the country ranking second in terms of highest number of victims. And with the growing use of cloud computing which provides multiple access to files stored making the stored data more vulnerable to such kinds of cybercrimes. These trends itself shows that an efficacious and robust Legal Redressal machination as well as preventive measure must be devised to curb this millennial crime and facilitate India's growth into a trillion-dollar economy. And one of the ways this can be achieved is by educating the general public about risk associated with using internet and application of common preventive techniques such as using secure WIFI network, firewall, not sharing password etc. which are widely disregarded.

[3] Easttom and Taylor (2011)

[4] https://www.livemint.com/companies/news/cyber-crime-cases-in-india-almost-doubled-in-2017-11571735243602.html

[5] National Crime Record Bureau, Crime Report 2018, Page no.- xiii

IDENTITY THEFT UNDER INFORMATION TECHNOLOGY ACT, 2000

The IT Act Amendment, 2008 has inserted section 66-C to the IT Act, 2000, which defines and prescribes punishment for the offence of identity theft as follows-

Definition*: 'Whoever, fraudulently or dishonestly make use of the electronic signature*[6]*, password or any other unique identification feature of any other person*

Punishment*: 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.'*

The offence under this section is cognisable and bailable and triable by the court of magistrate of First Class. The terms dishonestly and fraudulently are defined under sections 24 and 25 of the Indian Penal Code,1860 (hereinafter referred as IPC). A combined reading of above three provision suggest that identity theft is an offence whereby a person or a group intentionally make use by downloading, extraction or copying of the electronic signature, password or any other unique identification by feature of the victim to cause wrongful loss to him/her. An electronic signature is a method of authenticating an electronic record by affixing e-signature.

Another section of the aforesaid act which punishes for cheating by impersonation is section 66-D[7] which defines the offence and prescribes the punishment for it as follows-

Definition: *'Whoever, by means for any communication device or computer resource cheats by personating,*

Punishment*: 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 one lakh rupees.'*

The offence under this section is cognisable, bailable and triable by the Magistrate of the First Class. The instances where cloned websites are created and used for defrauding unsuspecting victims comes within the purview of this section. Other cases of e-mail frauds, creation of fake profiles in social media websites or application for the purpose of cheating, e-mail forgeries, data theft, breach of privacy by unauthorised access and other such cases are punishable under this section.

In the case of *Samdeep Varghese v, State of Kerala*[8], a complaint filed by the representative of a Company, which was engaged in the business of trading and distribution of petrochemicals in India and overseas, a crime was registered against nine persons, alleging offences under Sections 65, 66, 66-A, 66-C and 66-D of the Information Technology Act, 2000 along with Sections 419 and 420 of the IPC. The said company had a website-

[6] Defined under section 2(1) (ta) of the IT ACT, 2000 as "electronic signature" means authentication of any electronic record by a subscriber by means of the electronic technique specified in the Second Schedule and includes digital signature

[7] Added by Information Technology Amendment Act, 2008

[8] I.L.R. 2010 (3) Kerala

'www.jaypolychem.com' but another website with the name '*www.jayolychem.org*' was made by the accused Samdeep @ Sam (who was dismissed from the company) in conspiracy with other accused persons. Defamatory and malicious matters were published in the website. The first accused and others would send e-mails from fake e-mail accounts to customers, directors of company, suppliers, bank with the intention to malign the name of the company. The first accused along with other known and unknown persons colluded to cheat the company and committed other acts of forgery, impersonation and defamation which resulted in financial loss to the tune of several crores of rupees to the company.

TYPES OF IDENTITY THEFT

The age digitization has brought with it ease in doing business and accessing government services such paying electricity bill, filing IT returns but on the flip side of the coin, it has also made our financial and personal data susceptible to such cybercrime. The types[9] of identity theft can be categorised as follows-

1. Criminal identity theft
2. Financial identity theft
3. Identity cloning and concealment
4. Synthetic identity theft
5. Medical identity theft

The *criminal identity theft* is the most common type of identity theft. Here, the perpetrator illegally uses the stolen identity of the unwitting victim to commit any crime or sells it in the black market.

In *Financial identity theft,* the perpetrator uses the financial identity of the victim to commit fraud or cheating relating to bank accounts, insurance and such others. with

In *Identity cloning and concealment*, perpetrators can use the information they obtained to hide their real identity. They can request and use identification instruments to mislead investigation or use the victim's bank account to launder money. In addition, they can circumvent identification and terrorist prevention measures by using obtained identities.[10]

The *Synthetic identity theft* is a kind where the perpetrator uses the fake information along with stolen identity to create a new identity which is used for illegal activities. Sometimes multiple information is stolen from various people to create a synthetic identity. For instance, such constructed identity can be used to obtain a credit card which in turn is used for making purchases online or offline. At times this kind of identity theft also leads to lowering of credit score of victims as the use of their banking account information is involved.

[9] https://www.securitas.in/globalassets/india/files/about-us/news---related-documents/identity-theft-is-the-largest-contributor-to-fraud-in-india.pdf

[10] Un handbook on identity theft

In *Medical identity theft,* the perpetrator illegally avails the victim's health care or medical insurance benefits or sometimes it is sold to hackers. The stolen identity is also used for filing and using fraudulent claims. The victims of this kind of identity theft crime like others may also suffer denial of service attack.

CONCLUSION

The crime of identity theft should be curbed and cabined before it becomes it gets deeply rooted in the Indian soil. Unlike other crimes, this crime can be prevented by following simple practices of cyber hygiene. One of the ways is to periodically check the accuracy of personal documents stored in computers or phones and quickly resolving any discrepancies, if found any. Portable storage devices should be carefully regulated, and a regular inventory of their use and location kept. Another important area in which government may make rules is regulation of employee and the number of employees who has access to data also needs monitoring with the granting of access based on the work responsibilities of the employee. Another strategy to tackle this crime is creation of awareness programmes in schools, workplaces and villages to educate people about the prevention and redressal of this crime. A national database of loss identity software should also be developed which would act as the nodal point connected with all important government offices, banks and such other places to detect any illegal use of those lost identity. Following few simple practices would go a long way in curbing the crime of identity theft and save time and unnecessary hassle.