pen ACCLAIMS

Volume 11. July 2020 ISSN 2581-5504

"Identity Theft"

Saptodwipa Sarkar
Symbiosis Law School,
Noida

Identity theft is the crime of obtaining the personal or financial information of the user with the motive of using his or her name in order to carry on transactions or purchases. Thus here, the identity of the user is used by someone else and have access to the credit cards, bank accounts. The imposter can also commit other crimes in the name of someone else's identity. Basically, the social media accounts generally require two essentials- email id or username and a password. The former is available to each and every person out there and even be similar for two or more accounts to a certain extent but the latter is exclusive and varies from person to person. When this exclusive password is leaked to someone, then the incident is termed as Identity Theft. Besides this, identity thieves often look forward to steal information like one's bank card number, birth certificates social insurance numbers and so on. To summarise, identity theft can be defined as stealing exclusive identifying information of a person in order to impersonate them and commit further crimes in that person's name.

To combat with a crime first we need to analyse the issue from several perspectives collectively resulting into the crime. Lack of stability in economic and political sphere increases the probability and scope of identity theft. Especially, the developed countries have to face a problem called illegal immigration and often these immigrants steal identities such as social insurance number or driving licence details in order to get employment in that particular country. Social factors and environment are also some contributing factors to identity theft. The common practice of uploading personal details on social media profiles significantly raises the risk of cyber-crimes. Criminals can also obtain our personal information through third-party applications. Most social media sites have apps ask for permission to access your account information before installation or even they need access to the device's gallery, audio and so on. This is one of the pathways to the hackers to steal your details to commit fraud. At times we share personal details that we would not share otherwise on our social media accounts not even understanding the gravity of such acts.

Now let us move forward to analysis of Indian policies and legislation to deal with identity theft especially in today's world of digitization. Identity theft basically involves two steps- first, dishonest or fraudulent downloading, copying or extraction of unique identification details of a person and secondly, fraudulent use of such stolen information. Section 24 and section 25 of IPC are used to determine this malicious intent (mens rea). The moment personal information is downloaded, extracted or copied with a dishonest intent; mens rea will come into existence. Thereafter, whether the person hacking such information uses it will be considered as actus reus i.e. physical element of the crime. The offense of Identity theft is covered under IT Act. As per section 66C of the IT Act, when a person fraudulently uses password, digital signatures etc of another person it may lead to imprisonment up to three

Volume 11. July 2020 ISSN 2581-5504

years of fine up to one lakh rupees or both. Further, section 66D of the same act talks about the punishment of cheating by personation using computer resource. As per this section, if a person cheats someone using computer resource or communication that can lead to imprisonment up to three years or fine up to one lakh rupees or both. In this context, we should remember that the offense requires fraudulent or dishonest inducement caused to the person whose information is stolen and as a result of that, the person either accept, deliver or transact data or even omits to do something of that sort which he would not omit under normal circumstances. It is observed that in most cases, both the components of Section 66C and 66D is present. It is thus imperative for the prosecution to understand the nature and thereby punishing the offender. Besides, IPC can also be applied to deal with cases of cheating, forgery and fraud.

The impact of Identity Theft is long lasting. Identity thieves want our money. Depending on time span taken to understand and react after one's identity is stolen, the amount of loss varies since there are certain banks that reimburse the clients for direct losses. But delaying to complain may result into more loss i.e. the person whose identity was stolen will have to pay for the fraudulent charges if he doesn't report within a stipulated time period. Further, legal and credit related troubles are also caused as a result of identity theft. Some incidents of identity theft go beyond charges made to existing accounts in our name. Thieves may open new accounts using our personal details, such as your Social Security number, your address and your name and may even commit further crimes presenting themselves with our names and identity. If the person being fooled is unaware of this activity and debts go unpaid, the lender might sue him for the balance." Thereafter the person has to fight a legal battle and he may win if he can prove that he was subject to identity theft. But in today's world of complicated technology it is indeed tough to catch such thefts. However, the cost of the legal battle will have to be incurred by the person himself and. Meanwhile, those unpaid accounts can have a disastrous effect on your credit score, driving it down 100 points or more for a single incident. In addition to all these devastating impacts, there exists much more harmful impacting factors of identity theft. Identity theft isn't just about money. There have been instances where identities of American citizens have been stolen to allow criminals to avoid capture and individuals seeking medical care to receive treatment under fraudulent names. Victims may find themselves faced with false arrest, erroneous medical records, or the loss of federal or state benefits. Hence, the impact is severe and long lasting in all aspects.

In general, some best possible ways to avoid becoming an identity theft victim is to exercise caution, prudence and diligence while protecting our sensitive and personal information. Some methods are discussed here. At first, the users must set up strong passwords for their social media accounts so that is it difficult to be hacked and the passwords need to be changed in fluctuating intervals. Further we should avoid giving personal details over the phone or to random websites in order to access them. In addition to that, one has to pay attention to the billing cycles. If he or she is not receiving scheduled monthly bill through mail, it often indicates that card essentials are stolen. Last but absolutely not the least, we need to be extra cautious in safeguarding our personal laptops, mobiles or any other

Volume 11. July 2020 ISSN 2581-5504

electronic device. This can be executed by using a safe and secure browser for safer online transactions, by not keeping financial details on the computer unless necessary, by avoiding automatic log in methods and by deleting all sensitive details from the machine before selling off or disposing it.

To conclude, it can be stated that, identity theft has been an issue of serious concern after the cybercrimes started increasing. The only way to deal with this is increasing cyber security. This should be done by the users and the intermediaries also besides the direct service providers. All of us must follow the above-mentioned methods to avoid being subjected to identity theft. We should always remember that identity theft is a crime of opportunity; thereby, if the opportunity is not there, the crime will also not take place. Lastly, we must not share personal information beyond necessary details on social media platforms. Hence, collective security and concern can curb this crime from the society.