pen ACCLAIMS

Volume 11, July 2020 ISSN 2581-5504

"The Act of Stealing You from You: Identity Theft"

Aashima Sakhuja
UILS, Panjab University, Chandigarh

****Harsh Rana***
UILS, Panjab University, Chandigarh

Charu Singh, an aspiring young airhostess was completely aghast by the unwelcomed decision of her instructor of dismissing her from her training sessions. The decision did come as a shocker for her, and left her with a sense of ambiguity as to what triggered to be the reason which marred her career.

More appalling was the news that someone had hacked into her Facebook account and exchanged a couple of nasty communications with anonymous people pretending to be the face of the account. A case filed at the Gurugram Cyber cell and subsequent probe unearthed the fact that her roommate was the actual culprit, who later claimed it to be a benign prank.[1]

The above incident, may appear, at first glance to be just a passing illustration of a genial prank by a friend but if dug deeper it is one of the most unnoticed and unassuaged forms of fraud, undertaken by circumventing technology and breaking into what is otherwise considered as robust systems. In other words, it is the ***modern technology driven version of the crime known as IDENTITY THEFT.***

Often cited as *the 'Crime of the New Millennium'*, it is nothing but a direct attack on the victim's privacy where the criminal garners an abundant amount of characteristic data to impersonate the former in banks, credit card companies and other monetary concerns, appending to it the malefactor also relinquishes the benefit of supplemental non-pecuniary concerns correlated to the heisted data.

Breaking it down to the simplest form of words- *'Identity Theft' the term is intentional use of someone's personal data, fraudulently, to obtain an advantage over the victim's plight.* 'Identity Theft' the term coined in 1964 is in itself an oxymoron, 'Identity was believed to be something that could not be stolen', nonetheless the rapid development of certain labyrinthine technological systems has successfully deconstructed the word 'Impossible' to 'I am possible', pioneering this new genus of fraud employing identity as *its modus operandi*.

Yet, there are scholars who claim that this fraud is not entirely data driven and dates back to 1800's where ballot stuffing in the elections was a run of the mill, following which a trend of forging ids by teenagers to grab a glass of grog became prevalent which further acted as an appendage to the growing crime. The invention of computers and propagation of digital economies added the much required vigor to this trend which grew in leaps and bounds

[1] https://is.gd/829rHU (June 10, 2020 at 1:45 am)

Volume 11, July 2020 ISSN 2581-5504

compelling the American Congress to pass **The Identity Theft Assumption Deterrence Act of 1998**[2], officially declaring identity theft as a Federal Crime. When it comes to contemporary India *every 4 of 10 (39%) Indians have experienced identity theft.*[3]

The Indian Subcontinent has seen a rapid increase in Cyber Crimes, the culprits, if caught are the ones that usually mix up in the society as civil beings. There are numerous anonymous examples ranging from circulation of indecent images of a Kannada film actress by the mysterious critter to siphoning an amount of rupees 1,90,000 from legislator's bank account. The savagery of these maven men does not have an end chalked out.[4]

The possibility of digital divide narrowing in India is still a far-fetched reality with only 25.3% as the *rural internet density* to 97.9% in the urban areas. Factually 66% of country's population is still based in suburbs[5], clearly the idea of *Data Protection* to them is as outlandish as the notion of sun setting in the east. As wide as this world of automation is, it cannot be denied that the culprits work with an unvaried attitude that aids the researcher to club and categorize the offence of 'Identity Theft' into different types.

Identity Theft Resource Centre[6], a non-profit victim support initiative in Sans Diego, California, graded identity theft in five different types, the first one being:

Identity Cloning and Concealment; can a person live his whole life pretending to be someone else? Definitely in case the latter wantonly enshrouds his actual self. Herein the culprit seems to be like any other common next door neighbor you vouch to know about but may be the name he told you is not his, may be the identity he feeds you stolen from someone somewhere around the globe who is still struggling because some fraudster stripped him off his own identity. It is usually used as a tool by sleeper cells to get off the ground with their terrorist's ideologies, so this seemingly superficial offence sometimes paves a way for a much greater threat to National Security. Subtly, illegal immigrants also use this as a way to enter lands they are blacklisted from, isn't actor *Irfan Pathan's 'Angrezi Medium'* an ideal example of identity theft arrayed fair.

Hopping on to the next bracket of the crime- '**The Medical Identity Theft'-** the growing pace of life and disregard towards the concept of 'work life balance' has led to the development of variegated infirmities among the employed folk necessitating medical insurance. The Incurred Claim Ratio[7] of 2017 is tabulated to be 70%[8] in healthcare sector

[2] The act became effective on October 30, 1998, punishing identity theft with penalties up to 15 years of imprisonment and maximum fine up to $2,50,000.
[3] https://is.gd/KeEFur (June 8, 2020 at 4:30 pm)
[4] https://www-firstpost-com.cdn.ampproject.org (June 12, 2020at 5:15pm)
[5] https://is.gd/yn6AM5 (June 14, 2020 at 2:10 pm)
[6] Identity theft resource Centre is a United States non-profit organization for consumer assistance in 1999 by Linda Foley in San Diego, California. It was a recipient of National Crime Victim Service Award in 2004.
[7] ICR refers to the total amount of claims paid by a general insurance company divided by the total amount of premium collected during the same period.
[8] https://is.gd/3M7ObQ (June 11, 2020 at 4:30 pm)

Volume 11, July 2020 ISSN 2581-5504

which is huge but of this is questionable and suspected to be pseudo usage of someone else's identity and information to get prescription drugs, visit a doctor or claim an insurance benefit falls within the ambit of medical identity theft, the ramification of which is suffered by the sitting target of the culprit whose medical records stands altered.

Akin to it is **'Child Identity Theft'** wherein the imposter uses a child's identity to stockpile the illegal benefits in the name of a bairn. It is often seen that technologically advanced minors these days in their inquisitiveness to know more and ignorance about the prevalent threat get trapped in the well laid strategies of the culprits.

For a simple man with no intent to harm anyone, his name appearing in criminal records without any awareness of the same can be distressing. Well that's what a criminal identity yegg does to the innocent. Feigning someone else using his specifications in the order to prevent arrest or conviction is not all nefarious for the wrongdoer nor does the fact that maybe a law-abiding citizen has to bear the brunt of the former's deeds makes him even a tad bit of guilty conscious, but the act definitely exploits the faultless in the eyes of law. This is called as the **Criminal Identity Theft .**

Finally, yet importantly the most popular yet widely exercised fraud of **'Financial Identity Theft'.** It is by far one of the most highlighted cybercrimes across the world. Doping someone of their hard earned money, furnishing credit cards, writing erroneous cheques, sniveling banks money through loans borrowed without any intention to payback, corrupting the victim's CIBIL score are a part of this identity theft. A spike in the financial identity theft is an auxiliary to the growth of digital banking operations in the country.

Apart from the above classifications, there are a great deal of diversified criminal activities that have popped up in the contemporary times due to the explosion of financial services over internet, such as mortgages, credit cards, bank accounts etc. further provide a sense of anonymity to these potential thieves always on a look out for unsecured identity credentials, inventing new strategies in order to deceit the official organizations acting as watchdogs over them.

Dear PAYPAL valued member, it has come to our attention that your account information needs to be updated. If you could please take out 5-10 minutes of your time and renew your records you will not run into any future problems ……[9]

The above mail, initially seems to be a legitimate request of update made by **PayPal** to one of its account holders , but actually is a spoof mail , an exemplar of the newest form of Identity Theft i.e**. PHISHING.**[10] It is basically a scam where the phisher broadcasts an e-mail which

[9] I received this e-mail as I way conveniently working on this piece of work, It is reprinted exactly as I received it and includes that emails punctuations and grammatical errors , which were less glaring as compared to the original , this caught my attention because I am a PayPal account holder .

[10] The word Phishing comes from an analogy drawn from fishing, the e-mail is used as a bait to lure the fish from the sea of internet users. The **F** is changed to **PH** according to the computer hacking traditions.

Volume 11, July 2020 ISSN 2581-5504

is an exact lookalike of the one sent by the official E- Commerce websites .To make the con all the more believable, the culprit puts to use the company logo's and trademarks to eliminate any sense of doubt that might trigger in the minds of the receivers of the mail. Once the data demanded is proffered it will obviously be misemployed, as of the update the targeted customer awaits, it was never mend to happen.

Phishing, more than anything else has far reaching consequences than any other form of identity thefts, for it imposes an additional societal cost i.e. *Loss of consumer confidence in conducting business online* and obliterates the idea of digital economy perceived by the governments of almost all the countries of the world.

Another shrouded but soon to be glaring issue in context of Identity Theft is **lack of Biometric Privacy** in the corporate world. Biometrics i.e. Finger Prints, Retina Recognition,

Face Identification etc. seemed to be the ultimate solution for the pertaining problem, for finger prints are sui-generis in nature but then no one should underestimate the people who are cash poor and time rich. Every lock has a key and that is why this unshakable way of *identification is now a tool of identity theft.*

Prevalence of biometric scanners almost everywhere from offices to gymnasiums further fueled the concerns. The 2017 judgment of K.S. Puttaswamy[11] is somehow considered as a reflection of those unsettled issues and a wakeup call for the authorities to fortify their defenses against data leakages considering the heavy dependence of the latter on biometric particulars of its citizens.

Calling attention to the already conceived laws in the country in context of Identity Theft and as offshoots the other cybercrimes that takes place, **The Information Technology Act of 2000[12]** is the main legislation governing them. Before its amendment in 2008, *section 43* of the act imposed a civil liability [up to rupees 1 crore] for any unauthorized access to network in order to assist in committing an illegal act. Though the term identity theft was used for the first time in Indian law in 2008 but prior to it *section 66* used to criminalize any activity under *section 43* done with a fraudulent intention .Section 66A, now deemed to be unconstitutional punished phishing, which was declared to be an illegal act in the landmark case of *Nasscom vs Ajay Sood and others.*[13]

Section 66 C specifically defines identity theft and punishes the same with a fine up to rupees 1,00,000 or an imprisonment up to 3 years. Although it is not covered within the ambit of section 378 [theft] of IPC 1860, but with the inclusion of electronic records the scope of inclusion of computer data related crimes have broadened. Therefore, Forgery {*section 464*},

[11] (2017) 10 SCC 1

[12] The IT Act, 2000 is an act of Indian parliament notified on 17 October 2000. It is the primary law in India dealing with cybercrimes and electronic commerce.

[13] National Association of Software ... vs Ajay Sood and Ors. on 23 March, 2005 Equivalent citations: 119 (2005) DLT 596, 2005 (30) PTC 437 Del

Volume 11, July 2020 ISSN 2581-5504

Forgery for the purpose of cheating {*section 468*}, Forgery for the purpose of harming reputation {*section 469*} can all be coupled with the IT Act. Further *section 419* can be put to use in case the accused impersonates the victim for the purpose of cheating. An expert committee on amendment to IT act headed by Shri Kisan, president Nasscom suggested an amendment in *section 417A* prescribing 3 years of punishment for cheating using Unique Identification but those recommendations are yet to be incorporated.

In an attempt to draw parity between Indian and American Data Privacy Laws, India still surfaces with lacunae in certain spheres. Indian law is absolutely silent when the attacker is non Indian citizen, with no extradition treaty is signed, there is no way out there to punish those criminals. Secondly the compensation awarded is deemed inadequate within upper limit of 1crore and 5 crore for individuals and corporations respectively, the losses inferred on the other hand are much greater.[14]

A cyber-attack is a four cornered attack on the victim namely Financial, Emotional, Physical and Social. The *doer does not realize the damage done*, he can only be punished, provided he is caught. **Digital awareness coupled with Innovation** as perceived by our honorable Prime Minister are our only defenses towards this **BLOODLESS WAR.**

[14] http://racolblegal.com/identity-theft-a-critical-and-comparative-analysis-of-various-laws-in-india/#_ftn32 (June 12, 2020 at 6:15 pm)