IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

SOCIAL MEDIA AND IDENTITY THEFT: THE NEW-AGE GLOBAL PANDEMIC

Radhika Gupta, LLM (Criminal Law) Amity University, Noida (AIALS)

Ayushi Goyal, LLM (Criminal Law) Amity University, Noida (AIALS)

ABSTRACT

Identity theft is a global phenomenon that has been the subject of investigation and reportage. As a result of the neoliberal economic policies and technology adaptation that are today the standard across all industries, people's perspectives are changing at a rapid rate. Despite diverse outcomes, the value of information technology has been progressively growing. Due to the rapid growth and improvement of the nation's information technology infrastructure in recent years, identity theft has become a growing problem. Due to the fact that identity theft targets personal information, this is the case. A person commits social media identity theft when they create a phoney social media profile in another person's name using their images and personal information. Regardless of whether the conduct is performed in jest or with the intent to deceive others, it reflects negatively on the one who committed it. There are several reasons why con artists perpetrate this form of theft against their victims. The purpose of this study is to examine the many sorts of identity theft that may occur in India as well as the existing legislative framework for combating and preventing these types of crimes.

Keywords: Identity Theft, Phishing, Hacking, Information Technology, Social Media

INTRODUCTION

Social media is quickly becoming one of the most powerful tools for social interaction and presence. Almost everyone in the world uses at least one of the several social media networks. While social media may appear to be safe, identity theft is a common concern. It has grown as we have integrated social media into our daily lives.

Identity theft is a documented phenomenon on a global scale. Innovation has been quickly changing people's mindsets thanks to the industrial revolution, neoliberalism, and digital adaptability that are today dominating all industries. Information technology's significance has progressively increased, with both beneficial and bad consequences. Due to the advancement and innovation of information technology in the nation, identity theft has been a steadily increasing worry in recent years. Social media identity theft occurs when someone makes a fake social media account using the pictures and personal data of another individual. Whether it is carried out as a joke or in an effort to deceive others, it is wrong and damning. Scammers have a variety of reasons for carrying out such a theft[1].

Although some are interested in utilizing your stolen social media identity to demand money from you, others seek your close companions and directly request money using this fictitious account. They could even utilize a fake account to propagate offensive or political comments, making your relatives and close acquaintances turn against you.

Only biometrics have the potential to be utilized as an identity theft tool. A breach of private information can occur if a lot of sensitive information is obtained through a phony biometric device. If a person's biometrics get into the incorrect hands, it might enable thieves to profit from any transactions made in the latter's name[2]. In addition, most victims don't even recognize that such a violation of private details has occurred, and by the moment they do, it can already have been too late to recoup the process of recovering from these identity thefts can take months or even years, and the overall performance is quite low.[3]

This paper attempts to explore the numerous types of identity theft that occur in India as well as the current legal system in place to battle and prevent them.

LEGISLATION TO PREVENT IDENTITY THEFT

Let us just pick the top 2 identity fraud methods, ATM skimming and spamming, out of the numerous varieties that exist.

Explaining ATM skimming - The concept of "cash anywhere, anytime" has prompted the installation of devices that would make it simple for authorized account users to withdraw money. Automated teller machines (ATMs) quickly took over as the main and most important service that banks offered to their individual clients. Since many years ago, ATM fraud has been committed in a number of ways, including by installing keypad replacements, hacking installed cameras in booths, and mounting cameras within the machine itself.

This term includes the theft of private information that is sensitive through ATM skimming and the resulting financial loss. Nonetheless, there is still space for improvement in the classification of sensitive data and the severity of the punishment to be applied depending on the loss that resulted from carelessness and insufficient protection by such data processors or data fiduciaries.[4]According to Section 66 of the Information Technology Act, 2000, every violation covered by Section 43 is punished by a period of three years of incarceration, a fine that may reach five lakh rupees or both. This includes ATM skimming, which really is criminal culpability for other offenses. Conversely, Sections 66C and 66D cover the penalty.

The following day, the plaintiff sent a petition to the State Bank of Patiala requesting repayment of the Rs. 40,000 that was wrongfully deducted from her accounts. But the responses disobeyed. As a result, the individual that was hurt filed a customer complaint. The ATM system had been compromised by a third party, which had then resulted in illicit activities, the court found from the portions of proof that had been provided before the Honourable Courts.[5]

[1] Anderson, Keith B., et al. "Identity Theft." The Journal of Economic Perspectives, vol. 22, no. 2, 2008, pp. 171–92.

[2] Bisogni, Fabio, and Hadi Asghari. "More Than a Suspect: An Investigation into the Connection Between Data Breaches, Identity Theft, and Data Breach Notification Laws." Journal of Information Policy, vol. 10, 2020, pp. 45–82

[3] Archer, Norm, et al. "Understanding Identity Theft and Fraud." Identity Theft and Fraud: Evaluating and Managing Risk, University of Ottawa Press, 2012, pp. 14–42.

[4] SOVERN, JEFF. "Stopping Identity Theft." The Journal of Consumer Affairs, vol. 38, no. 2, 2004, pp. 233–43.

[5] Romanosky, Sasha, et al. "Do Data Breach Disclosure Laws Reduce Identity Theft?" Journal of Policy Analysis and Management, vol. 30, no. 2, 2011, pp. 256–86.

The body corporate involved in such financial institutions profited from the money wrongfully withdrawn from the complainant's accounts and was in charge of covering up the loss to the affected party. Since it was the banks' job to guarantee that the ATM machines just weren't modified and ensured adherence with the level of security, this decision clearly outlined the extent of the lender's culpability for Skimming has emerged as one of the most sophisticated and dangerous types of financial crime among all of these. Identity theft is regarded as the starting point as it spreads to other types of offences; hence, a full series of circumstances might result in financial losses.

No official legal definition of ATM skimming has been given, however ATM Mounting a device that is often invisible to ATM users that discreetly collects bank account information when the user enters an ATM card into the specific machine is known as "skimming," and it is regarded as criminal conduct the exploitation of such ATMs.

With the use of such a thorough technique, the thieves might encode the stolen information onto a fresh ATM card so they can withdraw cash from the account holder's bank account.

In examining the scope of such offenses, it is essential to think about the appropriateness of regulation and responsibility for such high-end, heinous crimes as ATM skimming.

The Information Technology Act of 2000 and the Information Technology (Amendment) Act of 2008 is the only statutes that, to some degree, address offenses linked to ATM cloning.

According to the court's ruling in the situation of Commissioner of Income Tax versus NCR Corporation Pvt Ltd., ATMs are subject to cyber-criminal laws because any computer scheme that is component of an ATM machine processes information that is used to perform the primary function of cash exemption or money transfer. Hence, under terms of the Information Technology Act of 2000, ATMs can be regarded as computer systems.

There are relatively few rules that are compliant with and apply to cyberattacks like ATM machine skimming in India since there is so little legislation that controls cyber law there. Sections 43 and 66 of the Information Technology Act of 2000 address the offense of ATM skimming. Once the Information Technology Act, 2008, as amended, other clauses including Section 420 of the Indian Criminal Code and Sections 43A, 66C, and 66D were inserted in addition to each of these two.

According to Section 43 of the Information Technology Act of 2000, any person who, without the current owner or the responsible individual of access's approval, e-books, copies, introduces a virus, damages, interrupts, or causes disruptions, denies access, grants access to any unauthorized person in accordance with the act, or fees the services used by any person to the bank statement of another is subject to civil responsibility.

These Section 43 provisions are common in Sections 63 to 74 of the IT Act, 2000. It should be emphasized that clauses (i) and (j) include more serious offenses including tampering with computer source code and altering, damaging, or erasing any data contained in the computer system. Regrettably, Section 43 only defines third-party personal responsibility, rather than a data controller or operator.

There have been attempts in the most recent Personal Data Protection Legislation, 2019, to also include damage and the standards by which these scammers can be held liable. The Personal Data Protection Bill, 2019, does not describe harm or destruction directly, but it defines "harm" as any circumstance that results in psychological or bodily harm, destruction, distortions, impersonation, economic damage, or property damages. This definition is more inclusive of the important features of ATM skimming and serves to better clarify the standards by which such offenders can be penalized. It is logical that concerns about data privacy and company responsibility exist.[6]

[6] STAFFORD, MARLA ROYNE. “Identity Theft: Laws, Crimes, and Victims.” The Journal of Consumer Affairs, vol. 38, no. 2, 2004, pp. 201–03. JSTOR, http://www.jstor.org/stable/23860545. Accessed 30 Mar. 2023.

A corporate body that owns deals with, or handles any "sensitive personally identifiable information" is guilty of negligence in putting in place or preserving "data protection practices and procedures," which further results in any least partly responsible or willful misconduct, and shall be held accountable for damages to the harmed party. This is clearly outlined in Section 43A of the Information Technology Act, 2008.

As mentioned in the justification, data protection standards and methods may be established by accord, through any applicable legislation, or as specified by the centralized administration in accordance with professional guidance as it may think appropriate.

One such interpretation must provide a quick sketch of what might be considered a legitimate practice and process rather than a full meaning. Appropriate security methods and standards, as indicated in the rationale, may emerge by agreement, any existing legislation, or as specified by the centralized administration in accordance with expert opinion as it deems proper. The nation-state has been given considerable authority and leeway to assign a proper interpretation to private and sensitive information that hasn't yet been categorized under the Act. In the Personal Data Protection Bill of 2019, an attempt was made to define "personal data" and "sensitive personal data" while fully removing Section 43A. In addition, the obligation of a company incorporated has been divided into the liabilities of a data processor as well as a data trustee.

Case Illustration - Kumar versus Whiteley

In this case, the accused got unauthorized access to the JANET, or "Joint Academic Network," and thus deleted, introduced additional files, and changed passwords to prevent those with permission from using the network. Following an investigation, it was determined that Kumar, the accused, was connecting to the BSNL internet connection as a registered genuine user and modifying the computer database of the customers' internet user profiles.

Based on a complaint made by the Press Information Bureau, which also identified inappropriate broadband Internet usage, the Crime Investigation Bureau was compelled to launch a cybercrime case against Kumar and undertake examinations. The complaint further said that the subscribers had lost roughly Rs. 39,000 as a consequence of Kumar's actions. He has formerly "hacked" webpages from Bengaluru, Madras, and other locations as well, the Press Information Bureau reports.[7]

N.G.A. Kumar, a computer expert from Bengaluru, was found guilty of violating Sections 420 of the Indian Penal Code (IPC), which deals with cheating, and Section 66 of the Information Technology Act, which regulates computer-related offenses. The court decided that the appellant should serve a one-year strenuous prison sentence as well as a penalty of fifty thousand.[8]

Similar to this, employees of Tata Indicom were imprisoned in the case of Syed Asifuddin & Ors. Versus State of AP for changing the digital bit identifier that is programmed in mobile phones that have been expressly stolen with permission from Reliance Infocomm. The Court determined that this modification with the software's code contravened Section 65 of the Information Technology Act of 2000.[9]

[7] BAILEY, RISHAB. “Censoring the Internet: The New Intermediary Guidelines.” Economic and Political Weekly, vol. 47, no. 5, 2012, pp. 15–19

[8] Kiran Prasad. “E-Governance Policy for Modernizing Government through Digital Democracy in India.” Journal of Information Policy, vol. 2, 2012, pp. 183–203.

[9] Duraiswami, Dhiraj R. “Privacy and Data Protection in India.” Journal of Law & Cyber Warfare, vol. 6, no. 1, 2017, pp. 166–86.

WHAT CAUSES SOCIAL MEDIA IDENTITY THEFT?

Criminals can perpetrate identity theft in a variety of ways using social media. Below are some of the most typical causes of such an event.

1. Anonymity

Criminals use this to get access to your social media or even other digital platform accounts and steal your personal details and photographs. They build a phony account on social networking sites and give it a legitimate appearance using this data. They want to dupe your family and friends into approaching this account in this fashion.

2. Fraudulent emails from corporations

You could receive phishing or fraudulent emails from certain con artists asking for personal data. They could impersonate a buddy or a staffing firm. If you provide them with your information, they will use it to create a phony social media account and start scamming people.

3. Malware and Hacking

It's possible for a scammer to get your personal data by hacking into your profile on social media, laptop, or cellphone. They can infiltrate your devices and steal data using this approach. They can also get personal data by hacking into the company web.

4. Hacking of the internet services

If you link your cell phone to the web via public Wi-Fi, you have the potential of enabling scammers' access. Cybercriminals will be able to snoop on your unreliable connectivity. Every time you input a passcode or social network information hackers might gain access to it.

IDENTITY THEFT ON SOCIAL MEDIA: THE GUIDE TO AVOID

One might wonder how to protect yourself against identity theft on social networks. Below are a few pointers to assist you in doing the same.

1. Avoid sharing excessively online.

Always keep all of your data to yourself. If you don't know enough about social media websites, there won't be much for a scammer to take. Even the most basic knowledge about social media might end up saving you a lot of time and hassle. You may just input your country of residence and remove the city if you don't want to see any specific details.

Furthermore, you may apply a similar strategy when browsing other websites. Avoid using personally identifiable information like a phone number or an email address unless it is absolutely necessary. It will help you avoid giving the fraudster important personal information.

2. Be aware of whom you're adding

When utilizing social media, you must be wary about sharing your personal information with fraudsters. You should avoid adding strangers to your friend list for this reason. If you inadvertently add a fraudster, they will most likely get access to your profile without your awareness. They learn more about your email and try to guess your security questions.

Always keep an eye on your friend requests and review the profile data to confirm that the person is whom you believe they are. Check your buddy list on a regular basis to see if you accidentally added an unexpected individual to your account. Your passwords will get increasingly difficult to guess. You can also delete information from your social media account that you believe may reveal personal information.

3. Keep Your Privacy Settings Safe

Every social networking site provides some level of privacy and security. It is vital to analyze and customize these options. Take care to conceal the bulk of your personally identifiable information, such as your birthdate, current location, profession, and so forth. Additionally, try to keep your account hidden from anyone who isn't on your friend list.

If you are not cautious about your privacy, every stranger on the social networking site will have access to your information. They will also have privy to some of your most confidential material and will be capable to utilize it to harm you.

4. Limit the number of posts you make.

Most social networking sites now allow users to hide their accounts from strangers. Be ensure that your profile is only available to your close friends and family. You may also restrict who has access to your profile and posts. This can help keep unwanted scammers away from your social media activities.

Before you share photographs, videos, or anything else that may be deemed personal, make sure to check the privacy settings. It should only be viewable to your pals, not the wider public. Also, by changing your privacy settings, you may limit who can see your future postings.

5. Avoid Visiting Live Places

It is usually best not to share live whereabouts on any social networking platform. You should not mention your true location on your account for this purpose. You may also avoid marking your present location when sharing photos, videos, or status updates. If your profile is public, you should avoid including any location information.

This information may expose your house and family to fraudsters. They will find out where you are right now, putting your safety in jeopardy. For example, if you publish that you are alone at a park, a criminal can mug you there. As a result, avoid marking the precise address on social media.

6. Authentication and strong passwords are recommended.

Check that the social networking site you choose has robust authentication methods in place. It will help you create login details and passwords that your cybercriminals will find difficult to guess. Additionally, ensure that the authentication system allows you to get warnings if suspicious logins to your accounts are undertaken from different devices.

The bulk of users of social media favour permanent passwords over one-time credentials. As a result, choosing the right combination of words, digits, and special characters is crucial for constructing a memorable password. This method will never allow fraudulent scammers to guess your passcode.

7. Make use of Internet Security Software.

Whether surfing the online or utilising social media platforms, Internet security software can secure your identity and IP address. You may occasionally click on links that wind up installing malware to your system and stealing your private info. But, computer security can help you tackle this problem.

Installing authentic antivirus software on your device is recommended to avoid such problems. To prevent identity theft, most security software combines anti-keyloggers, secure settings, and encoded password management.

IF YOUR SOCIAL MEDIA IDENTITY HAS BEEN STOLEN, WHAT SHOULD YOU DO?

After you've acquired everything there is to understand regarding social media identity theft, you'll really have to know what to do in the event that you end up a victim. The best actions to consider if you suspect identity theft are listed below.

a. Locate the source

Investigate the source when you hear about theft from a relative or close friend. You will be forwarded to a fake account that is attempting to steal your data. Your pals who interacted with this phony account might help you locate it. An online search can also be necessary.

b. Account Information

Users on most of social media platforms may report spam or objectionable information and accounts. If you suspect that a fraudulent account is utilizing your name and information, you may simply report it to the platform. Even if you do not have a username on the relevant network, you may still report profiles by visiting the platforms' government sites.

c. Passwords should be changed, and suspicious accounts should be removed.

If you're still skeptical, try a run with your 'friends' list. Identify and delete questionable accounts from this list. After that, modify your credentials to make them more challenging to guess. You can also delete material from your social network account that you believe may be harmful.

d. Feel free to contact the Cyber Cell

The police department's cyberspace cell is in charge of investigating incidents and disputes using social media and the internet. If the identity theft is significant, you will notify it to the local police station's cyber unit. They would ask to provide detailed about the situation and investigate your account to locate the fraudster.[10]

It is apparent that social media networks are quite bad at stealing data. This piece made the point that fraudsters are always looking for ways to acquire your data and create fictitious identities online. You must heed the recommendations in this post if you want to keep similar scenarios from occurring on your account.[11]

This data may make your home and family vulnerable to scammers. They will discover your current location, exposing your protection in peril. If you post the fact that you're alone at a campground, a criminal may mug you there. As just a result, avoid posting the exact location on social media. Encryption and password protection are strongly advised.

In brief, in the globalized world of today, where everything is connected and accessible and anonymity is a characteristic feature in order to prevent risks from the rising number of identity theft instances, the following precautions are recommended:

- Use of secure encryption or a concealed authentication combination is required.
- Passwords must be changed on a frequent basis.
- Staying away from dubious or dubious sites and connections;
- Desist from providing anyone else with your individual data;
- Documentation and crucial data security;
- Using an approved security barrier to prevent unauthorized access to digital equipment;
- Preventing the disclosure of credit/debit cards and other sensitive information.

It is crucial to get in touch with the closest nearby police department as soon as possible if someone has been the victim of identity theft, then file a complaint with the local Cyber Cell Police Station and the relevant institution. In order to understand this, let us take the recourse of an example , Stuti should get in connection with the bank's regulators if her bank information has been hacked and undesired transactions have taken place without his permission. Stuti is the designated cardholder.[12]

[10] Sruti Chaganti. “Information Technology Act: Danger of Violation of Civil Rights.” Economic and Political Weekly, vol. 38, no. 34, 2003, pp. 3587–95.

[11] ADVANI, PRITIKA RAI. “Intermediary Liability in India.” Economic and Political Weekly, vol. 48, no. 50, 2013, pp. 120–28

[12] KRAUSE, JASON. “STOLEN LIVES: Victims of Identity Theft Start Looking for Damages From Companies That Held Their Personal Financial Information.” ABA Journal, vol. 92, no. 3, 2006, pp. 36–64.

CONCLUSION

A user's confidentiality has been greatly violated by identity theft, which has had an impact on the victim's emotional and social well-being. Identity theft, meanwhile, has an effect beyond the person; it also can be harmful to companies and other entities. Considering from a legal perspective, Indian laws are inadequate in regard to protecting identity fraud, or the data of a person or business, leaving a great deal of room for enhancement in terms of laws, rules, and procedures pertaining to identity theft.

The lack of explicit rules acts as a catalyst for a slew of deceptive offences that have skyrocketed in the previous two decades. A robust system with an effective pyramid of jurisdiction is required to enable appropriate application of current legislation and equal monitoring of the circumstance.

It is also vital to limit resource redundancy and to engage compassionate workers. Finally, the state must raise consumer knowledge of measures to preserve confidential and private information and conduct safe online activities. Additionally, they must be taught about their entitlements and the many redressal processes accessible to them in the event of identity theft. People should also keep track of their credit files and sensitive information everywhere it is used to lessen the damage and early detection of identity theft, and they should seek clarity here about why such data is required and how secure it is.