INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 4 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

SOCIAL MEDIA AND IDENTITY THEFT: AN EMERGING GLOBAL PANDEMIC

AUTHOR - LUV KUMAR* & AKSHAY KUMAR**

* STUDENT AT LAW COLLEGE DEHRADUN, FACULTY OF UTTARANCHAL UNIVERSITY. EMAIL - SINGHSLUV689@GMAIL.COM

** ASSISTANT PROFESSOR AT LAW COLLEGE DEHRADUN, FACULTY OF UTTARANCHAL UNIVERSITY. EMAIL - AKSHAYKUMAR@UUMAIL.COM

BEST CITATION - LUV KUMAR & AKSHAY KUMAR, SOCIAL MEDIA AND IDENTITY THEFT: AN EMERGING GLOBAL PANDEMIC, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 5 (4) OF 2025, PG. 1121-1129, APIS – 3920 – 0001 & ISSN - 2583-2344.

Abstract

"Identity theft represents a widespread issue that has garnered significant attention in both scholarly research and media coverage. The implementation of neoliberal economic policies, coupled with the adaptation of technology that has become ubiquitous across various industries, is contributing to a significant and rapid transformation in individuals' perspectives. The value of information technology has exhibited a consistent upward trajectory, notwithstanding the variability in outcomes observed across different contexts. The recent advancements and expansion of the nation's information technology infrastructure have contributed to the increasing prevalence of identity theft. Identity theft is characterised by its focus on personal information, which substantiates this assertion. Social media identity theft occurs when an individual establishes a fraudulent social media profile under the name of another person, utilising their images and personal information without consent. The nature of the conduct, whether executed humorously or with the intention to mislead, yields adverse implications for the individual responsible for the action. This form of theft is perpetrated by con artists for a variety of reasons, which can be analysed to understand the underlying motivations and mechanisms involved in such fraudulent activities. This study aims to investigate the various forms of identity theft that can occur in India, alongside an analysis of the current legislative framework designed to combat and prevent these criminal activities."

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

INTRODUCTION

Social media is rapidly emerging as a significant instrument for facilitating social interaction and establishing presence within various communities. A significant proportion of the global population engages with at least one of the various social media platforms available. Despite the perception of safety associated with social media platforms, the prevalence of identity theft remains a significant concern among users. The integration of social media into daily life has resulted in significant growth.

Identity theft represents a well-documented phenomenon that occurs on a global scale. The rapid evolution of innovation has significantly influenced societal mindsets, driven by the forces of the industrial revolution, neoliberal economic policies, and the pervasive adaptability of digital technologies, which currently shape various sectors. The significance of information technology has progressively escalated, yielding both advantageous and detrimental consequences. The progression and innovation of information technology within the nation have contributed to a notable rise in concerns regarding identity

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 4 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

theft in recent years. Identity theft within social media contexts transpires when an individual creates a fraudulent account utilising the images and personal information of another person. The execution of the process is contingent upon various factors.

The act of employing humour or deceitful tactics is fundamentally unethical and carries significant negative implications. Individuals engaging in fraudulent activities possess numerous motivations for executing acts of theft.

While certain individuals may aim to exploit your compromised social media identity for financial gain, others may target your immediate social circle, employing this fraudulent account to solicit monetary contributions directly. The potential for the use of a fictitious account to disseminate derogatory or politically charged remarks exists, which may result in the alienation of one's relatives and close acquaintances.

Biometrics represent a unique category of technology that may be employed as a mechanism for identity theft. The acquisition of sensitive information through a fraudulent biometric device poses a significant risk of private information breaches. The unauthorised access to an individual's biometric data poses significant risks, as it may facilitate fraudulent activities, allowing perpetrators to exploit financial transactions conducted under the victim's identity.

Furthermore, a significant number of victims fail to acknowledge the occurrence of a violation concerning their private information. By the time they become aware of such an incident, it may already be too late to initiate recovery efforts. The process of recuperating from identity theft can extend over months or even years, with overall success rates remaining notably low.

This study investigates the various forms of identity theft prevalent in India, alongside an examination of the existing legal framework designed to combat and mitigate these offences.

LEGISLATION TO PREVENT IDENTITY THEFT

This study focusses on two prevalent methods of identity fraud: ATM skimming and spamming, selected from a wide array of existing techniques.

This article provides an overview of ATM skimming, a method employed by criminals to illegally obtain card information from unsuspecting users. The process typically involves the installation of covert devices on ATMs that capture data from the magnetic stripe of a card, often in conjunction with a hidden camera to record PIN entries. The implications of such activities are significant, leading to financial losses for individuals and institutions alike. Understanding The notion of universal access to cash has led to the implementation of devices designed to facilitate the withdrawal of funds for authorised account holders. Automated teller machines (ATMs) have rapidly emerged as the primary and most significant service provided by banks to their individual clients. For several years, various methods of ATM fraud have been perpetrated. These methods include the installation of replacement keypads, the hacking of cameras installed in booths, and the mounting of cameras within the machines themselves.

This term encompasses the illicit acquisition of sensitive private information via ATM skimming, along with the consequent financial repercussions. Despite existing frameworks, opportunities for enhancement remain in the categorisation of sensitive data and the corresponding severity of penalties imposed, which should be contingent upon the extent of loss incurred due to negligence and inadequate safeguarding by data processors or data fiduciaries.Section 66 of the Information Technology Act, 2000 stipulates that any infringement addressed by Section 43 is subject to a penalty of imprisonment for a duration of three years, a monetary fine that may amount

to five lakh rupees, or a combination of both sanctions. This encompasses ATM skimming, which constitutes criminal liability for additional offences. In contrast, Sections 66C and 66D address the imposition of penalties.

On the subsequent day, the plaintiff submitted a formal petition to the State Bank of Patiala, seeking the reimbursement of Rs. 40,000 that had been improperly deducted from her accounts. However, the responses did not conform to expectations. Consequently, the affected individual submitted a formal complaint regarding the incident. The analysis revealed that the ATM system was infiltrated by an external entity, leading to unauthorised activities, as determined by the evidence presented to the Honourable Courts. The body corporate associated with these financial institutions derived profits from the unauthorised withdrawals from the complainant's accounts and was responsible for concealing the resultant losses to the affected party. Given that it was the responsibility of the banks to ensure that the ATM machines remained unaltered and complied with established security standards, this decision distinctly delineated the scope of the lender's liability for Skimming has been identified as a highly sophisticated and perilous form of financial crime within the broader spectrum of illicit activities. Identity theft is considered a precursor to various other criminal activities, leading to a comprehensive range of situations that may culminate in significant financial losses.

There is currently no officially recognised legal definition for the term ATM skimming; however, ATM The act of installing a device that remains largely undetectable to ATM users, which surreptitiously gathers bank account information upon the insertion of an ATM card into the machine, is referred to as "skimming." This practice is classified as criminal behaviour, representing a significant exploitation of automated teller machines.

The implementation of a comprehensive technique enables thieves to encode stolen information onto a newly issued ATM card, facilitating unauthorised cash withdrawals from the account holder's bank account.

The examination of the scope of offences necessitates a consideration of the appropriateness of regulatory measures and the assignment of responsibility for severe criminal activities, such as ATM skimming.

The Information Technology Act of 2000, along with the Information Technology (Amendment) Act of 2008, represents the sole legislative framework that, to a certain extent, addresses offences associated with ATM cloning.

The court's ruling in the case of Commissioner of Income Tax versus NCR Corporation Pvt Ltd. establishes that cash machines (ATMs) fall under the purview of cyber-criminal laws. This determination is based on the premise that any computer scheme integral to an ATM machine is responsible for processing information essential to executing its primary functions, which include cash withdrawal and money transfer. Consequently, in accordance with the provisions of the Information Technology Act of 2000, automated teller machines (ATMs) may be classified as computer systems.

The regulatory framework governing cyberattacks, specifically those involving ATM machine skimming in India, is notably limited due to the scarcity of legislation addressing cyber law in the region. The provisions outlined in Sections 43 and 66 of the Information Technology Act of 2000 pertain to the criminal activity known as ATM skimming. The enactment of the Information Technology Act, 2008, along with its subsequent amendments, resulted in the incorporation of additional provisions, specifically Section 420 of the Indian Penal Code, as well as Sections 43A, 66C, and 66D, complementing the existing legal framework.

Section 43 of the Information Technology Act of 2000 delineates the civil liabilities incurred by

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 4 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

individuals who engage in unauthorised actions concerning digital information. Specifically, it addresses behaviours such as accessing, copying, introducing malicious software, damaging, interrupting, or causing disruptions to digital services without the consent of the current owner or responsible individual. Furthermore, it stipulates that denying access or granting access to unauthorised persons, as well as misusing services related to another individual's bank statement, constitutes a breach of the act, thereby rendering the perpetrator liable for civil consequences.

The provisions outlined in Section 43 are prevalent within Sections 63 to 74 of the Information Technology Act, 2000. It is important to highlight that clause (i) and (j) encompass more severe violations, which involve tampering with computer source code as well as altering, damaging, or erasing any data within the computer system. It is unfortunate that Section 43 provides a definition solely for third-party personal responsibility, without addressing the roles of a data controller or operator.

The most recent Personal Data Protection Legislation, 2019, has made attempts to incorporate provisions regarding damage and the criteria for holding scammers accountable for their actions. The Personal Data Protection Bill, 2019, does not explicitly define harm or destruction; however, it characterises "harm" as any situation that leads to psychological or physical injury, destruction, distortions, impersonation, economic loss, or damage to property. This definition encompasses a broader range of critical characteristics associated with ATM skimming, thereby enhancing the clarity of the criteria utilised for the penalisation of such offenders. Concerns regarding data privacy and corporate responsibility are both rational and warranted.

A corporate entity that possesses, manages, or processes any sensitive personally identifiable information may be deemed negligent if it fails to implement or maintain adequate data protection practices and procedures. Such negligence could lead to partial or wilful misconduct, rendering the entity liable for damages incurred by the affected party. The provisions are explicitly detailed in Section 43A of the Information Technology Act, 2008.

As outlined in the justification, data protection standards and methodologies may be established through consensus, relevant legislation, or as determined by the centralised administration in alignment with professional guidance deemed appropriate.

This interpretation necessitates a concise overview of what could be regarded as a valid practice and process, rather than an exhaustive definition. Security methods and standards that are deemed appropriate may arise through consensus, existing legislation, or directives issued by the centralised administration, based on expert recommendations as considered suitable. The nation-state possesses significant authority and discretion in determining an appropriate interpretation of private and sensitive information that has not yet been classified under the Act. The Personal Data Protection Bill of 2019 sought to establish definitions for "personal data" and "sensitive personal data," concurrently eliminating Section 43A from the legislative framework. The obligations of an incorporated company have been categorised into the liabilities associated with a data processor and those pertaining to a data trustee.

WHAT CAUSES SOCIAL MEDIA IDENTITY THEFT?

Identity theft can be executed by criminals through various methods facilitated by social media platforms. The following delineates several of the most prevalent factors contributing to the occurrence of such an event.

1. The concept of anonymity

Individuals engaged in criminal activities exploit this method to gain unauthorised access to social media and various digital platform accounts, thereby facilitating the theft of personal information and photographs. The

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 4 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

construction of a fraudulent account on social networking platforms is executed by utilising this data to create a facade of legitimacy. This account appears to be designed to mislead individuals, potentially influencing family and friends to engage with it in a specific manner.

2. Fraudulent communications originating from corporate entities

Individuals may encounter phishing or fraudulent emails originating from specific con artists soliciting personal information. The potential exists for individuals to assume the identity of a peer or a recruitment agency. The provision of personal information may lead to the establishment of a fraudulent social media account, subsequently facilitating the perpetration of scams against individuals.

3. Cyber Threats and Intrusion Techniques

Scammers can potentially acquire personal data by infiltrating user profiles on social media platforms, as well as accessing information stored on laptops or mobile devices. This approach enables the infiltration of devices, facilitating the unauthorised acquisition of data. Personal data can also be acquired through unauthorised access to the company's web infrastructure.

4. Compromise of internet services

The connection of mobile devices to the internet through public Wi-Fi networks presents a significant risk, as it may facilitate unauthorised access by malicious actors.

Cybercriminals may exploit vulnerabilities associated with unreliable connectivity to conduct surveillance activities. Each instance of entering a passcode or social network credentials presents an opportunity for unauthorised access by hackers.

IDENTITY THEFT ON SOCIAL MEDIA: THE GUIDE TO AVOID

This inquiry raises important considerations regarding the protective measures individuals can implement to safeguard their identities from potential theft within social networking platforms. The following points are presented to facilitate the achievement of the same objective.

1. It is advisable to limit the extent of personal information shared on online platforms.

It is advisable to maintain the confidentiality of personal data. Insufficient knowledge regarding social media platforms may result in minimal opportunities for exploitation by scammers. A fundamental understanding of social media can significantly reduce time expenditure and mitigate potential complications. It is possible to input only the country of residence while omitting the city in order to avoid the display of specific details. Additionally, a comparable approach may be employed when navigating alternative websites. The utilisation of personally identifiable information, such as phone numbers or email addresses, should be minimised and employed only when deemed absolutely essential. This approach is designed to mitigate the risk of disclosing critical personal information to potential fraudsters.

2. It is essential to exercise caution regarding the individuals being added to one's network.

The utilisation of social media platforms necessitates caution regarding the dissemination of personal information, particularly in relation to potential fraudulent actors. The addition of unfamiliar individuals to one's social network is discouraged due to potential risks associated with privacy and security. The inadvertent addition of a fraudulent individual may result in unauthorised access to one's profile, often occurring without the individual's awareness. Their analysis of your email facilitates attempts to deduce your security questions.

3. It is essential to consistently monitor incoming friend requests and to thoroughly examine the profile information to verify the identity of the individual in question.

It is advisable to routinely review the list of contacts associated with your account to identify any unintended additions of individuals.

The complexity of passwords is expected to increase, thereby enhancing their resistance to unauthorised access attempts. It is advisable to remove information from social media accounts that may potentially disclose personal details.

4. Ensure the Security of Your Privacy Settings

Each social networking platform offers varying degrees of privacy and security measures. It is essential to conduct a thorough analysis and tailor these options accordingly. It is essential to minimise the disclosure of personally identifiable information, including but not limited to one's birthdate, current location, and profession. Furthermore, it is advisable to maintain the privacy of your account by restricting access to individuals who are not included in your friend list.

Failure to exercise caution regarding privacy may result in unrestricted access to personal information by unfamiliar individuals on social networking platforms. Access to highly confidential materials may be granted to individuals, enabling them to potentially exploit such information to your detriment.

5. The frequency of posts should be minimised.

Currently, a significant number of social networking platforms provide users with the option to conceal their accounts from individuals who are not in their network. It is imperative to ensure that one's profile is accessible solely to close friends and family members. Access to one's profile and posts can be restricted to specific individuals or groups. This intervention may serve to mitigate the intrusion of undesirable scammers within the realm of social media engagement.

Prior to disseminating photographs, videos, or any other content that could be classified as personal, it is imperative to review the privacy settings. Access to this content should be restricted to a select group of individuals, rather than being available to the general public. Furthermore, adjusting privacy settings may restrict the visibility of future postings to a selected audience.

6. Refrain from Attending Live Venues

Sharing live locations on social networking platforms is generally advised against due to potential privacy and security concerns. It is advisable to refrain from disclosing one's actual location within the account for the intended purpose. It is advisable to refrain from indicating one's current location when disseminating photographs, videos, or status updates. In the context of online privacy, it is advisable to refrain from incorporating any location details if one's profile is set to public.

The dissemination of this information has the potential to increase the vulnerability of residential properties and their occupants to fraudulent activities. The current location of an individual may be determined, potentially compromising their safety. The dissemination of information regarding one's solitary presence in a public space, such as a park, may inadvertently increase vulnerability to criminal activities, including theft or assault. Consequently, it is advisable to refrain from disclosing the exact address on social media platforms.

7. It is advisable to implement authentication measures alongside the use of robust password protocols.

It is imperative to verify that the selected social networking platform implements comprehensive authentication mechanisms. This approach facilitates the generation of login credentials and passwords that are challenging for cybercriminals to predict. Furthermore, it is imperative that the authentication system is designed to provide alerts in the event of suspicious login attempts to user accounts from various devices.

A significant proportion of social media users demonstrate a preference for permanent passwords in comparison to one-time credentials. The selection of an appropriate combination of alphanumeric characters and symbols is essential for the formulation of a password that is both secure and memorable.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 4 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

This method effectively prevents fraudulent actors from successfully guessing your passcode.

8. Utilisation of Internet security software is recommended.

The utilisation of internet security software is essential for safeguarding one's identity and IP address while engaging in online activities or utilising social media platforms. There exists a possibility that users may inadvertently engage with hyperlinks that result in the installation of malicious software on their systems, subsequently compromising their private information. However, the implementation of computer security measures can assist in addressing this issue.

The installation of legitimate antivirus software on devices is advised to mitigate potential issues. In order to mitigate the risk of identity theft, contemporary security software typically integrates a combination of anti-keylogger technologies, secure configuration settings, and encrypted password management systems.

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

Upon acquiring comprehensive knowledge about social media identity theft, it is imperative to understand the appropriate actions to take should one become a victim. The following actions are recommended for individuals who suspect they may be victims of identity theft.

- **Identify the origin of the information.**

It is imperative to conduct a thorough investigation into the source of information when allegations of theft involving a relative or close friend are presented. The user will be redirected to a fraudulent account that seeks to unlawfully acquire personal data. Individuals within your social circle who engaged with this fraudulent account may assist in its identification. The necessity of conducting an online search may arise in various contexts.

- **Account Information**

Individuals utilising various social media platforms possess the capability to report instances of spam or content deemed objectionable, as well as accounts associated with such material. In instances where there is a suspicion that a fraudulent account is operating under one's name and utilising personal information, it is advisable to report the matter to the respective platform. Individuals lacking a username on the respective network retain the ability to report profiles by accessing the official government sites of the platforms.

It is recommended that passwords be updated regularly, and any accounts deemed suspicious should be eliminated from the system.

For those who remain unconvinced, it is advisable to conduct an evaluation using your list of acquaintances. The process involves the identification and subsequent removal of accounts deemed questionable from the provided list.

Subsequently, it is advisable to enhance the complexity of your credentials to reduce the likelihood of unauthorised access. It is advisable to remove content from one's social network account that is perceived to be potentially detrimental. Individuals are encouraged to reach out to the Cyber Cell for further assistance.

The cyberspace cell of the police department is responsible for the investigation of incidents and disputes that occur within social media platforms and the internet. In cases where identity theft is deemed significant, it is imperative to report the incident to the cyber unit of the local police department. The individuals involved would request a comprehensive account of the situation and conduct an investigation into the user's account to identify the perpetrator of the fraudulent activity.

Evidence suggests that social media networks exhibit significant deficiencies in safeguarding user data. This analysis highlights the persistent efforts of fraudsters to obtain personal data and construct false identities in the digital realm. It is imperative to adhere to the recommendations presented in this post to prevent the recurrence of analogous scenarios on your account.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 4 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

The information presented herein has the potential to expose households and their members to the risks associated with fraudulent activities. Their actions may lead to the identification of your present location, thereby compromising your security measures. The dissemination of information regarding one's solitary presence at a campground may increase the likelihood of victimisation by criminal elements, such as robbery. Consequently, it is advisable to refrain from disclosing precise locations on social media platforms. The implementation of encryption and password protection is highly recommended to enhance security measures.

In summary, within the contemporary globalised context characterised by interconnectedness and accessibility, alongside the prevalent feature of anonymity aimed at mitigating risks associated with the increasing occurrences of identity theft, the following precautions are advised:

- The implementation of secure encryption methods or a hidden authentication combination is essential.
- The frequency of password changes is a critical security measure that must be implemented consistently.
- Avoiding engagement with questionable websites and connections; - Refraining from sharing personal information with others; - Ensuring the security of documentation and critical data; - Implementing an authorised security barrier to safeguard against unauthorised access to digital devices;
- Preventing the exposure of credit/debit card information and other sensitive data.

It is imperative to establish contact with the nearest police department promptly in instances of identity theft. Subsequently, it is essential to file a formal complaint with the local Cyber Cell Police Station as well as the pertinent institution. To elucidate this matter, it is pertinent to consider a specific scenario: Stuti should establish communication with the regulatory authorities of the bank if her banking information has been compromised and unauthorised transactions have occurred without her consent. Stuti has been identified as the designated cardholder.

CONCLUSION

The breach of a user's confidentiality through identity theft has significantly affected the emotional and social well-being of the victim. Identity theft exerts repercussions that extend beyond the individual victim; it also poses significant risks to corporations and various organisations. From a legal standpoint, the current framework of Indian laws appears insufficient in addressing the complexities associated with identity fraud and the safeguarding of personal and business data. This inadequacy highlights a significant opportunity for the development and refinement of laws, regulations, and procedural mechanisms related to identity theft.

The absence of clearly defined regulations serves as a significant driver for a range of fraudulent activities that have surged dramatically over the past twenty years. A comprehensive framework characterised by a well-defined hierarchy of authority is essential for the proper implementation of existing laws and the equitable oversight of the situation.

Limiting resource redundancy and engaging compassionate workers are essential considerations in optimising operational efficiency and enhancing workforce dynamics. In conclusion, it is imperative for the state to enhance consumer awareness regarding strategies for safeguarding confidential and private information, as well as promoting safe practices in online activities. Furthermore, it is imperative that individuals receive education regarding their entitlements and the various redressal mechanisms available to them in cases of identity theft. It is imperative for individuals to monitor their credit files and sensitive information across all platforms to mitigate potential damage and facilitate the early detection of identity theft. Furthermore, individuals should seek to understand the necessity of such data and the measures in place to ensure its security.

REFERNCE

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
6. STAFFORD, MARLA ROYNE. "Identity Theft: Laws, Crimes, and Victims." The Journal of Consumer Affairs, vol. 38, no. 2,2004, pp. 201–03. JSTOR,
7.Sruti Chaganti. "Information Technology Act: Danger of Violation of Civil Rights." Economic and Political Weekly, vol. 38, no.34, 2003, pp. 3587–95.
8.ADVANI, PRITIKA RAI. "Intermediary Liability in India." Economic and Political Weekly, vol. 48, no. 50, 2013, pp. 120–28
9. 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.