Journal of Engineering, Science and Technological Trends (JESTT)

Vol. 2, Issue 1, February 2025
DOI: https://doi.org/10.48112/jestt.v2i1.10

Review

Identity Theft in the Digital Age: Legal Gaps, Enforcement Challenges and the Need for Global Reform

Sidra Raza[1]* and Shaista Naznin[1]

[1]Department of Law, Abdul Wali Khan University, Mardan, Pakistan

*Corresponding Email: sidraraza82@gmail.com (S. Raza)

Received: 02 December 2024 / Revised: 18 January 2025 / Accepted: 04 February 2025 / Published online: 28 February 2025

ABSTRACT

Identity theft has grown into a major international issue that hurts everyone from individual people to banks and government departments. This research examines international legal frameworks designed to combat identity theft. The study examines critical laws such as the Identity Theft and Assumption Deterrence Act, Theft Penalty Enhancement Act, Fair Credit Reporting Act, and Fair and Accurate Credit Transactions (FACT) Act, among others. The study reveals that inconsistencies in enforcement across jurisdictions reduce the effectiveness of identity theft laws. According to analysis, identity theft keeps growing as one of today's most common crimes because people conduct financial transactions online and cyber security poses significant weaknesses. The results call for better consumer security measures plus stronger connections between federal and state agencies along with new anti-fraud technology. The findings recommend that governments create better data security laws while working together across borders and building better support for victims of identity theft. Ongoing improvement of identity theft laws plus education about it helps victims avoid both monetary loss and emotional distress.

Keywords*:* Identity Theft; Cyber Fraud; International Law; Consumer Protection; Financial Crime, Legal Framework; Data Security; Fraud Prevention; Digital Crime; Cybersecurity Policy

1. Introduction

The main objective of Digital Law is to educate people about the theoretical thoughts relating to the Law and Economics issues in the Digital Environment [1]. Digital identity theft poses serious problems worldwide that affect both individuals and official organizations. The digital revolution has brought unparalleled connectivity and accessibility [2]. Cybercriminals exploit vulnerabilities in digital systems and online transactions to commit identity theft on a large scale [3]. Identity thieves use stolen personal data to rob people of both money and trust, which can lead to legal and financial problems for victims. Identity theft functions through many methods such as stealing credit cards and personal data from databases to create false social security numbers. Identity theft presents more significant problems than just money loss. Thieves can misuse identity information to create false charges, submit fake tax reports, and open medical treatment accounts under false names [4]. Law enforcement finds it difficult to catch up with cybercriminals so governments must create effective anti-crime rules to stop these activities and keep customers safe [5]. The presence of just laws, rules, and regulations that are applied fairly is a sign of good governance [6]. Several different laws operate globally yet challenges like uneven enforcement and legal boundaries make it hard to stop identity theft completely. This research analyzes global identity theft laws, including the Identity Theft and Assumption Deterrence Act, Theft Penalty Enhancement Act, the Fair Credit Reporting Act, and the Fair and Accurate Credit Transactions Act. It evaluates how these laws fight identity theft while showing their weak points in stopping advanced internet fraud. This analysis examines two major aspects of how law enforcement and consumer protection regulations tackle identity crimes. However, there are still gaps in the global legal framework despite the existence of different regulations. With the absence of uniformity of policies between jurisdictions, cybercriminals can exploit the lack of enforcement mechanisms [7]. In addition, there are no strict data security regulations in many regions allowing people and businesses to be breached. The solution to these problems requires internationally coordinated efforts, better legal tools, and improvements in cybersecurity technology.

Objectives of the Study

1. To examine how international laws help to address identity theft and financial fraud.

2. Gaps in the existing legal frameworks are identified to propose strategies for the prevention of global identity theft.
3. To assess the effectiveness of consumer protection laws in shielding people from identification fraud.

2. International Laws on Identity Theft

The majority of states have laws against identity theft that make it illegal to misuse someone else's identifying information [8]. It makes no difference whether the information is financial or personal under the majority of the US state legislation. Social Security numbers, credit histories, and banking PINs are examples of the kind of information that are frequently obtained by:

1. The criminal's unauthorized use of financial and governmental databases to obtain information
2. Identity, credit or debit cards, wallets, and handbags, lost or stolen mail

Identity theft is one of the fastest-growing crimes in the U.S. [9]. Internet usage is common among identity thieves. Nevertheless, they can also get critical personal information from unprotected places like garbage cans, database hacks, and frauds. Identity theft may be prosecuted as a misdemeanor or a felony, depending on your location and the specifics of the offense. For instance, first-time offenders in Illinois may be charged with misdemeanors. According to the Department of Justice, the offense may be considered a felony in several situations under federal law. A person may also face charges of wire fraud, mail fraud, or several other offenses depending on how the offense is carried out. Fraud involving credit cards may also be a part of the offense.

3. The Identity Theft and Assumption Deterrence Act

Congress in 1998 passed the Identity Theft and Assumption Deterrence Act due to high incidences of identity theft and the unenthusiastic reaction from the government towards its victims [10]. Regarding its statute identity theft is now a federal crime. It is a federal offense if an individual ‘‘knowingly and with intent to defraud transfers or uses without lawful authority a means of identification of another person for any unlawful purpose or for obtaining any benefit, advantage or privilege. ” These statutes make it clear that using other people’s identity for unlawful purposes or for obtaining unlawful benefit is a federal offense. One of them under this Act is Identity theft, whereby a person’s information is used to impersonate that particular individual. For a person to be able to perform such an act he/she has to have access to other pieces of information apart from the name of another person. Such other details are the date of birth of a person, social security number, credit card number, and bank account number. It is possible to have several identification documents and identifying numbers, for instance, a driver’s license number. It can involve various forms of Personally Identifiable Information (PII) [11]. The following are the penalties for fraud using identifying document violations: The penalties for using fraudulent identifying document violations depend on the particular offense as well as the type of document that has been violated. For instance, the offender can be fined, or receive a prison term of up to fifteen years if they use the identity of another individual to engage in any unlawful act if they receive anything of value in the aggregate amount of $1000 or more in one year for the commission of the crime. For other offenses, the term in prison is three years. However, if the offense is committed in connection with a violent crime or to facilitate the commission of a drug trafficking felony then the punishment could be up to twenty years. Crimes that are committed with the intent to aid international terrorism are punishable by up to 25 years in jail.

4. The Theft Penalty Enhancement Act of 2004

The Identity Theft Penalty Enhancement Act was passed on July 15, 2004. It amends the identity theft provisions presently in Title 18 of the United States Code and delineates, and prescribes punishment for aggravated identity theft. The law defines aggravated identity theft as a person who ‘knowingly transfers, possess or uses, without lawful authority, a means of identification of another person’ in connection with the commission of specifically listed felonies. In addition to the punishment for the initial felony, aggravated identity theft carries a mandatory two-year prison sentence. In addition to these requirements, the act also provides the US Sentencing Commission with the power to review and amend its guidelines and policy statements to ensure that the guideline offense levels and enhancements adequately punish the identity theft offenses involving abuse of position, and to enforce the laws. The act raised the fines for identity theft at the same time enabled the Justice Department to receive $2,000,000 for the investigation and prosecution of identity theft and related credit card and other fraud cases constituting felony violations of law for FY2005 and $2,000,000 for each of the 4 succeeding fiscal years.

5. Fair Credit Reporting Act

While identity theft is not mentioned in the FCRA, the act can be used to request that the credit reporting agency remove negative information about fraudulent charges or accounts. About the balancing of confidentiality, accuracy, relevancy, and proper use of such information the FCRA seeks to make consumer reporting agencies adhere to reasonable procedures that ensure that needs for consumer credit, personnel, insurance, and other information are met fairly and reasonably to the consumer. Additionally, according to the FCRA, any individual who furnishes information has to ensure that it is accurate and the same applies to consumer reporting agencies regarding the information that they disseminate. According to the Fair Credit Reporting Act (FCRA), consumers have a claim against credit reporting agencies that provide false information about them. An identity theft victim can sue a credit reporting service for negligence in not verifying the information in the consumer report and passing on information that is false due to identity theft. The consumer may sue under the recently amended FCRA at the latest within two years from the time that the plaintiff knew of the violation that led to such liability or within five years from the time the violation occurred [12].

6. Fair and Accurate Credit Transactions (FACT) Act of 2003

Among other things, the FACT Act passed on December 4, 2003, makes several changes to the FCRA to combat identity theft and assist victims [13]. Most of these new regulations that set a national approach to dealing with consumers’ complaints on identity theft and other related frauds are in concordance with legislation enacted by state legislatures. A new FCRA provision also provides for specific steps that credit card issuers, who use consumer credit reports, should follow if they receive a request for an additional or replacement card within a short period after receiving a known change of address for the same account. Other new laws require that social security numbers must be shortened in consumer credit reports if requested by the consumer and credit card account numbers must be truncated in electronically printed receipts to further curb instances of identity theft. Consumers can request fraud alerts on their credit files if they have been victims of identity theft or suspect potential fraud. The new regulations stipulate that a customer may request a fraud alert from one consumer-reporting agency and that agency shall notify the other agencies across the country that the alert has been put in place. Fraud alert records are nor-

mally maintained for ninety days, but the customer can request an extended alert, which is maintained for seven years at most. All the users of the given report are aware of the fraud alert since it is a part of the consumer's credit file. Any created credit score must moreover include the alert. Fraud notice is also given to identity theft victims and at this rate information, related to the crime is deleted from the credit reports of the victims. Upon receiving such proof of the consumer's identity, a copy of the identity theft report, identification of the allegedly fraudulent information, and a statement from the consumer to the effect that the information is not related to any transaction conducted by the consumer, a consumer reporting agency is required to stop all such information from being reported and notify the furnisher of the information in question that it might be the result of identity theft. It is also necessary to provide further consumer reporting agencies to which requests for information blocking can be addressed. The victims of identity theft are also allowed to ask for information concerning the alleged offense. An application and business transaction records of a business entity wherein any transaction which the recipient seeks to assert is a result from identity theft must, upon request of the victim or any law enforcement agency investigating the theft and which is authorized by the victim to receive the records, produce copies of the application and business transaction records to the victim or such law enforcement agency.

7. Fair Credit Billing Act

The Fair Credit Billing Act (FCBA) grants customers an opportunity to have charges that were made by an impostor removed from their accounts and also an opportunity to receive an explanation of the charges that have been made and confirmation of such charges [14]. However, it is not a statute that was put in place to deal with identity theft in particular. The FCBA was adopted to safeguard the consumer against misleading and unjust credit billing and credit card practices Consumers are explained and protected by law against unfair billing problems within consumer credit transactions. According to the FCBA, billing error refers to an unauthorized charge, a charge for goods or services for which the consumer has requested an explanation or confirmation in writing, or charges for products and services that were never furnished or received by the consumer. To have billing irregularities rectified, a customer can claim the FCBA from the creditor. Thus, the customer is not bound to pay the protested amount, the creditor is prohibited to attempt to collect any part of the protested amount together with the interest, and other expenses incurred in connection with the extension of credit. The act also prescribes how such matters should be addressed and it provides that the consumer's claims should be considered. If the creditor finds the existence of the stated billing error, he or she will be in a position to correct the mistake and credit the consumer's account with the amount in dispute inclusive of finance charges.

8. Electronic Fund Transfer Act

The Electronic Fund Transfer Act, like the Fair Credit Billing Act, though does not mention identity theft, does provide customers with a legal way to challenge transactions that they did not authorize and to have their accounts replenished in the case of error. The Electronic Fund Transfer Act (EFTA) aims to give the fundamental architecture that sets the rights, duties, and risks of users in EFT systems [15]. The EFTA also limits consumer's responsibility for any unauthorized electronic fund transfers, for example. The consumer's responsibility is capped at $50 or the amount of the unauthorized transfers before the institution receives the consumer's notice of the loss or theft of a debit card or other device used in making electronic transfers, which must be given within two business days of discovery. The financial institutions must also provide a customer with a confirmation of any electronic fund transfer, which the customer initiated from an electronic terminal. A financial institution must examine a potential mistake, find out whether or not it has happened, and notify the consumer of the findings and determination in writing or by mail within ten business days if it is provided with an oral or written communication from the consumer to the effect that the documentation forwarded to the consumer contains an error within sixty days from the date of forwarding such documentation. The consumer's name and account number must be included in the notice to the financial institution, together with the following information: the consumer's perception of an error, the actual amount of the error, and the justification for perceiving the error in the paperwork. Financial institutions are required to investigate errors and resolve disputes promptly under relevant regulations. If the financial institution cannot finalize the investigation within ten business days, they may recredit the customer's account for the amount in question as a temporary measure. This will help in the conclusion of the investigation and dismissal of the chance of an error being made.

9. Identity Theft Task Force

In April 2007, the President's Identity Theft Task Force released its final report with a plan to combat identity theft. The plan focuses on using government resources, protecting personal data, assisting law enforcement, educating businesses and consumers, and improving security measures in both public and private organizations [16]. The Plan focuses on four main areas of improvement: protection of consumer's identity from identity thieves due to improved security and awareness; making it difficult for the thief to get consumer's data, helping the victims of identity theft to recover, and deterring identity theft through more active pursuit and punishment. To ensure that more offenses of identity theft can be prosecuted at the federal level, the Task Force provided the following recommendations that targeted filling up perceived gaps in federal criminal laws. They are listed below:

1. Expand the list of predicate offenses for aggravated identity theft offenses
2. Reform the statute that enshrines electronic data theft law by doing away with the provisions that state that the information should have been stolen through interstate communication [17].
3. Sanction the makers and disseminators of the nasty spyware and keyloggers.
4. Extend the cyber-extortion statute to capture other forms of cyber-extortion.
5. Provide for the possibility of an enhanced sentence for identity thieves who defraud data belonging to companies and organizations.

10. Real ID Act of 2005

The DHS made the final rule on January 11, 2008, about the REAL ID Act of 2005 on State-issued driver's licenses and ID cards that federal agencies would be allowed to accept for official use starting May 11, 2008. The Real ID Rule lays down mechanisms for meeting the REAL ID Act's basic standards. These standards are regarding the various aspects that surround the overall procedure of issuing an identity document; the information and the security aspects that should be incorporated into each card; the identity, U. S. citizenship or legal resident status of the applicant; the validation of the source documents which the applicant presents; and the security features about offices wherein the cards are issued. Any state that has presented its petition before the last date of the year December 31, 2009, will have its extensions granted. In

addition, the second renewal is also possible up to May 10, 2011, if some conditions concerning the security of the license and identity procedures, as well as the credentials of the states, are met. For persons born after December 1, 1964, the Rule brings the enrollment period to December 1, 2014, and for those born on or before December 1, 1964, the enrollment period is on December 1, 2017, to replace all licenses that are to be used for official purpose by the states that have been deemed to comply with the act by the DHS to have all their cards to The policy took effect beginning of the fiscal year on the 31st of March 2008 (Stevens, Federal laws related to identity theft, 2008).

11. Key Findings

International identity theft laws are analyzed to show significant gaps in legal enforcement, cross-border cooperation, and consumer protection. Incentives and enforcement are needed when regulations are not enough [18]. The most important finding is the inconsistency of identity theft laws in different jurisdictions. In the United States, the Identity Theft and Assumption Deterrence Act and the Theft Penalty Enhancement Act impose strict penalties for offenders, but many countries have no such legal frameworks that would enable cybercriminals to take advantage of the lack of regulatory environment. This disparity gives rise to a shelter for international criminals operating in several countries who are difficult to track and prosecute by law enforcement agencies. A major issue with identity theft legislation is its reactive nature. Most legal frameworks are geared towards punishment rather than preventing identity theft in the first place. Fair Credit Reporting Act (FCRA), and Fair and Accurate Credit Transactions Act (FACTA) only afford some consumer protections, but they are only useful to victims after the fraud has occurred. Data security laws are still largely absent of proactive measures, leaving individuals and businesses vulnerable to continued risk in the face of ever-changing cybercriminal tactics. Stronger data protection measures are necessary including stronger encryption, biometric verification, real-time fraud detection systems, and so on. Furthermore, identity theft laws are still only enforced with difficulty. Extradition and prosecution are difficult in jurisdictions where legal action is minimal or nonexistent, allowing many offenders to operate. An increasing trend in trade and investment is determined by several factors [19]. Financial institutions tend to prioritize business efficiency in preference to robust security, which results in weak authentication processes that do not detect fraudulent activities. The increase in identity theft cases has greatly contributed to the failure of institutions to adopt stringent cybersecurity protocols.

12. Conclusion

Identity theft is a global economic and security threat, not an individual crime, and it demands urgent coordinated legal intervention. While the existing legal frameworks deal with some aspects of identity theft, they are not comprehensive and proactively oriented. Without strong global cooperation, identity thieves will continue to exploit legal loopholes, leading to financial and psychological distress for victims. To address this problem, governments should stop using punitive measures and focus instead on preventive measures, like data encryption, stricter authentication protocols, and international cooperation in tracking cyber criminals. Consumer data security must be a priority for financial institutions to secure consumer data and implement stronger verification measures, along with speedy responses to fraud reports. Identity theft must move from reaction to prevention, with a strong focus on data security, consumer protection, and international legal cooperation. Identity theft can only be curtailed and its devastating consequences can only be diminished through comprehensive legal reform and technological improvements.

Declaration

Competing Interests: The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgement: This article is extracted from chapter 3 of the thesis of Miss Sidra Raza (Crime of Identity Theft in Pakistani Law: A Critical Analysis, under the supervision of Dr. Shaista Naznin from Abdul Wali Khan University, Mardan, Pakistan.

Funding Statement: This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

References

[1] C. Yongmei and J. Afzal, "Impact of enactment of 'the Prevention of electronic crimes act, 2016 ' as legal support in Pakistan," *Acad. Educ. Soc. Sci. Rev.*, vol. 3, no. 2, pp. 203–212, 2023.

[2] A. Haider, A. Ali, and M. Zubair, "Chasing Dragons in the Dragon's Land: A Convoluted Struggle with Drugs and Deviance in Modern China," *Asketik J. Agama dan Perubahan Sos.*, vol. 7, no. 2, pp. 322–343, 2023.

[3] A. Haider, U. Yousaf, N. H. Shah, and W. Azeem, "UNTOC's Role in Combating Transnational Organized Crime: An International Response," *Pakistan J. Law, Anal. Wisdom*, vol. 3, no. 8, pp. 178–188, 2024.

[4] J. Afzal, C. Yongmei, A. Fatima, and A. Noor, "Review of various Aspects of Digital Violence," 2024.

[5] A. Haider, "Application of the United Nation Convention against Transnational Organized Crime: An Analysis," *Available SSRN 4686710*, 2024.

[6] J. Afzal and C. Yongmei, "Federal and provincial legislation regarding 'Right to Information for good governance in Pakistan," *Discov. Glob. Soc.*, vol. 1, no. 1, p. 12, 2023.

[7] A. Haider, S. Raza, and B. Z. Khan, "Organized Crime and the Objectives of the Islamic Penal System," *Al-Qamar*, pp. 63–82, 2023.

[8] G. R. Newman and M. M. McNally, "Identity theft literature review," 2005.

[9] S. B. Hoar, "Identity theft: The crime of the new millennium," *Or. L. Rev.*, vol. 80, p. 1423, 2001.

[10] M. A. Sabol, "Identity Theft and Assumption Deterrence Act of 1998-Do Individual Victims Finally Get Their Day in Court," *Loy. Consum. L. Rev.*, vol. 11, p. 165, 1998.

[11] P. M. Schwartz and D. J. Solove, "The PII Problem: Privacy and a new concept of personally identifiable information," *NYUL rev.*, vol. 86, p. 1814, 2011.

[12] F. C. R. Act, "Fair Credit Reporting Act," *Flood Disaster Prot. Act Financ. Inst.*, 2009.

[13] M. Epshteyn, "The Fair and Accurate Credit Transactions Act of 2003: Will Preemption of State Credit Reporting Laws Harm Consumers," *Geo. LJ*, vol. 93, p. 1143, 2004.

[14] A. J. Walden, "Closing the" No Further Responsibility" Loophole in Resolving Credit Billing Errors," *Wayne L. Rev.*, vol. 66, p. 321, 2020.

[15] L. M. Taffer, "The Making of the Electronic Fund Transfer Act: A Look at Consumer Liability and Error Resolution," *USFL Rev.*, vol. 13, p. 231, 1978.

[16] K. M. Finklea, *Identity theft: Trends and issues*. DIANE Publishing, 2010.

[17] A. Haider, "Beyond Borders and Bars: Exploring the Transformative Influence of the UN Convention against Transnational Organized Crime," *pjlaw.com.pk*, vol. 2, 2023, doi: 10.1080/09766634.2011.11885550.

[18] I. Ahmad, A. Haider, and B. Zeb, "In the Name of Nature: The Legal Frontiers of Environmental Preservation," *J. Asian Dev. Stud.*, vol. 12, no. 4, pp. 401–411, 2023.

[19] I. Ahmad, A. Haider, and J. Afzal, "The Geopolitical and Economic Impact of BRICS on the Middle East," *FWU J. Soc. Sci.*, vol. 18, no. 4, pp. 80–95, 2024.