2022

IDENTITY THEFT REPORT

**Table of Contents**

[**Introduction** 3](#_Toc113055066)

[**Cyber Identity Theft in the US** 4](#_Toc113055067)

[**Rights and Ethics of Dealing with Identity Theft** 5](#_Toc113055068)

[**Implications and Limitations of US Federal National Law Effectiveness** 7](#_Toc113055069)

[**Implications and Limitations of Investigative Tools** 9](#_Toc113055070)

[**Victims, Harm, Perpetrators, and Social Perception** 10](#_Toc113055071)

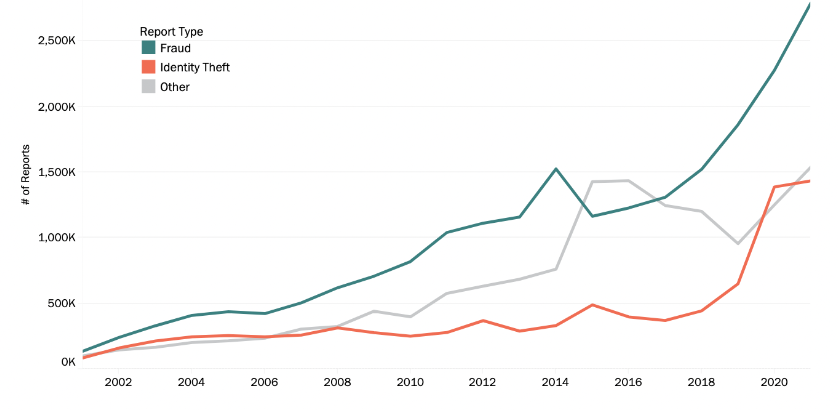
[**Conclusion** 13](#_Toc113055072)

# **Introduction**

The evolution of technology and the internet has provided unique affordances for cybercrime activities globally. Significant catalysts of increased cybercrime activities include the ease of information dissemination and anonymity (FTC, 2022). Online identity theft has swiftly grown as a more prevalent and substantial threat to the United States (US) economy, e-commerce, businesses, and the privacy of many citizens. Identity theft has multiple direct and indirect implications, including reputational damage to the victims, fraudulent transactions, and financial losses (FTC, 2022). According to the National Council of Identity Theft Protection, Americans lost approximately $5.8 billion to identity theft in 2021. In 2020, nearly half of American citizens were victims to unique forms of identity theft, including imposter scams, account takeovers, and financial identity theft (FTC, 2022). The statistics highlight that identity theft is a prevalent and a fast-evolving cybercrime that should be innovatively and effectively addressed. This report presents a comprehensive analysis and critical discussion pertaining aspects of cyber identity theft in the US, primarily using current statistics, rights and ethics considerations, as well as showcasing the implications, limitations and effectiveness of US Federal National Law. The report also presents the implications and limitations of various investigative tools and addresses concerns of identity theft victims, perpetrators, and social perception.

# **Cyber Identity Theft in the US**

The Federal Trade Commission developed a database (Consumer Sentinel Network) for receiving fraud reports from consumers and law enforcement agencies. Industry members and non-profit companies can also report fraudulent activity on the database. Presently, 25 states contribute to the Sentinel. In 2021, consumers lost approximately $5.8 Billion to fraudsters, representing a 70% annual increase (FTC, 2022). The FTC received 2.8 million reports from consumers in 2021, mainly of imposter scams and online shopping scams. In 2021, Sentinel received approximately 5.7 million reports, these included identity theft reports (approximately 1.4 million) and fraud reports (FTC, 2022).



**Figure 1: Number of Reports by Type** (National Council on Identity Theft Protection, 2022)

Figure 1 depicts the number of reports received on FTC's Consumer Sentinel Network from 2002 to 2020. This graph indicates that the numbers of fraudulent activity and identities that theft grew significantly over this period. The National Council on Identity Theft Protection (2022) state that US identity theft cases occur every 22 seconds and studies predict this ratio may increase in 2022 (Helser and Hwang, 2021).

**A picture containing bar chart

Description automatically generated**

**Figure 2: Percentage of Reports by Type** (National Council on Identity Theft Protection, 2022)

Figure 2 shows the percentage of fraud (48.6%) is higher than identity theft (25%) in the US. Statistics also show that one third of US citizens are victims of identity theft, the number of identity theft incidents in the US is three times higher than in any other country (FTC, 2022).

# **Rights and Ethics of Dealing with Identity Theft**

Experts and scholars have developed unique definitions of the term identity theft. According to Gross & Acquisti (2005), identity theft is the unauthorized use of personal data that is publicly available. Personal data includes phone numbers, dates of birth, personal images, and current addresses (Vilic, 2019). Piquero et al (2021), conversely, defines identity theft as the online misappropriation of identity tokens mainly for financial gains, tokens that can be misappropriated include usernames, passwords, and email addresses.

From a cyberspace perspective, identity theft is a form of fraud that involves using personal and financial data to achieve malicious goals and objectives (Vilic, 2019). The leading modus operandi of identity theft are hacking, phishing, spoofing and pharming. Phishing is a prevalent form of identity theft in the United States and globally. When phishing, a cybercriminal sends an email to the user claiming to be an authorized person or legitimate legal entity (Vilic, 2019). The main objective of phishing emails is to collect private and confidential information from the target users, unsuspecting users replying to such emails are vulnerable to various forms of identity theft. For instance, users may provide secure personal information such as credit card numbers, usernames, and passwords (Blackwood-Brown, 2018). Cybercriminals may also use phishing emails to direct users to fake sites designed to collect their data, including social security numbers and bank details (Vilic, 2019). Due to the sensitivity of the data involved, rights and ethics should be considered when dealing with identity theft.

Businesses and consumers are directly and indirectly affected by identity theft. Successful identity theft involves sensitive data being obtained without the owner's consent, including usernames, passwords, and credit card numbers (Vanhee, 2022). Payne and Kennett‐Hensel (2017) proposed that the government should implement a law like the Fair Credit Billing Act to address identity theft in the US. This policy could be in the form of federal legislation or simply a business guiding principle transferring the burdens of identity theft from consumers to corporations.

A principle of ethical approach for dealing with identity theft is that upper management and relevant law enforcers should be liable and accountable for implementing data security plans (Payne and Kennett‐Hensel, 2017). Liquidated damages should be imposed on upper management for the compromise of personal information. Imposing such penalties will ensure that managers implement effective measures to secure personal data from compromise (Burnes, DeLiema, and Langton, 2020). The above suggests that personalizing liability and accountability in developing and implementing data security plans can minimize incidents of identity theft and related cybercrimes in an organization.

# **Implications and Limitations of US Federal National Law Effectiveness**

Previous studies have extensively investigated the implications of identity theft and the effectiveness of national laws in the US. For instance, a study by Hole (2022) demonstrates the challenges facing law enforcement agencies that deal with different sovereign states, presenting legal challenges for investigators and prosecutors. Adults, 65 and older took approximately $2.5 Billion in financial monetary losses (DeLiema, Burnes, and Langton, 2021). Most of those vulnerable to out-of-pocket costs are the unmarried, of lower incomes, and of low educational attainment (Burnes, DeLiema, and Langton, 2021). In addition to direct financial losses, some victims have also incurred legal credits and ruined credit. This showcases how financial losses caused by identity theft can also include indirect costs to the victims.

The psychological implications of successful identity theft could can have heavy psychological effects on victims. In a study by DeLiema, Burnes, and Langton (2021), respondents were asked to rate their distress level on the misuse of personal data. A significant number of respondents (34%) indicated that it was moderately or severely distressing. States have developed and implemented different laws and regulations to address identity theft, the laws under 18 USC § 1028 criminalize misuse of one's identifying information, whether financial or personal. The Identity Theft and Assumption Deterrence Act was also passed in 1998 with the primary objective of enhancing the fight against identity theft in the US (EG, 2022). This law penalties anyone who knowingly falsifies personal data or documents.

According to the aforementioned law, anyone convicted of federal identity theft involving, producing or transferring identification, may face penalties of hefty fines and up to 15 years in jail. Federal identity theft for drug trafficking can include penalties of up to 20 years in federal prison and identity theft involving domestic and international terrorism may attract up to 30 years in jail (EG, 2022). The US Federal National Laws are designed sufficiently but fail to address the menace of identity theft effectively, the Identity Theft and Assumption Deterrence Act mentioned above is one such law (EG, 2022). This notion is supported by the constant increase in various forms of identity theft, including imposter scams, fraudsters and online shopping scams (DiNapoli, 2021).

**A screenshot of a computer

Description automatically generated with medium confidence**

**Figure 3: Identity Theft Arrests and Convictions in New York** (DiNapoli, 2021)

Figure 3 shows the number of identity theft arrests and convictions in New York from 2010 to 2020. The total number of convicted-sentenced reduced from 554 in 2016 to 201 in 2020, these statistics highlight the effectiveness of New York’s identity theft laws.

The ineffectiveness of national law is a recipe for various challenges, the FBI and the Department of Justice are involved in investigating and addressing identity theft crimes in the US (EG, 2022). The Department of Justice makes convictions and executes penalties on criminals convicted of identity theft. Effectiveness of national laws could be enhanced by ensuring that the responsible agencies are equipped with sufficient resources to execute their roles and responsibilities. For instance, strengthening the relationship between the FBI and the local law enforcement agencies would lead to more successful investigations (Zaeem and Barber, 2021).

# **Implications and Limitations of Investigative Tools**

Various investigative tools have been developed and implemented to address identity theft in the US, these investigative tools have unique implications and limitations. According to Piquero et al. (2021), individuals involved in frequent online transactions are more vulnerable to identity theft. Those who spend more time in chat rooms and on social media networks are also at risk of identity theft as are those engaging in routine computer communication and e-commerce (Piquero et al., 2021). Cybercriminals can use social networks to collect personal data from target users, they also use online platforms to execute phishing activities to collect information for various forms of identity. Therefore, investigative tools should focus on specific platforms linked with identity theft. Guedes, Martins, and Cardoso (2022) used the Routine Activity Theory (RAT) to expound online identity theft risk factors, RAT is one of the most empirically tested criminological theories explaining online identity theft (Guedes, Martins, and Cardoso, 2022). As a result, exposure to risky online activities and proximity to offenders increases identity theft vulnerability. An increase in online activities and a lack of capable guardians increase one's vulnerability to online identity theft. Users of credit cards and frequent visitors of risky content online were also proven more vulnerable to online identity theft (Hole, 2022).

The US's leading identity theft investigative report tools include IdentityTheft.gov, Bureau of Justice Statistics (BJS), Consumer Sentinel, FBI, and the FTC (US Department of Justice., 2022). Consumers can report identity theft cases to the FTC using the IdentityTheft.gov website or phone line. The BJS includes identity theft data in their National Crime Victimization Survey, while the Consumer Sentinel is a unique investigative cyber tool that enables consumers to report and access identity theft reports. The FBI however, remains the chief investigative unit of the Department of Justice in cases of fraud (US Department of Justice., 2022).

The investigative tools in the US appear effective in addressing identity theft, for instance, the FBI partners with state and federal agencies to investigate identity theft cases. The FTC also has a secure site that enables consumers to file identity theft complaints and receive personalized recovery plans. The Internet Crime Complaint Center (IC3) additionally partners with the FBI to provide current fraud statistics, including identity theft. Enhancing the partnership between these agencies and providing sufficient resources will enhance their effectiveness (US Department of Justice, 2022).

# **Victims, Harm, Perpetrators, and Social Perception**

Successful monetary gain as a result of identity theft can result in a unique kind of harm being subjected on victims. For instance, credit and debit card misuse victims may encounter financial losses as well as reputational damage. Victims of such fraud may also be blacklisted unfairly by financial institutions, including banks and creditors. Using stolen identity information to create new accounts has contributed to a considerable increase in tax return fraud (Finklea, 2010). Identity theft has the capacity to adversely affect US national security, the US economy and many other economies globally (Finklea, 2010). Given the consequential severity, victims of identity theft should absolutely take whatever precautionary measures possible and report misuse of their identity information to relevant agencies for action.

Expansion of the internet and an increase in globalization have made it complicated for law enforcement agencies to identify and comprehend perpetrators of identity theft. For instance, perpetrators may be operating domestically or internationally. The lack of delineation in international laws regarding identity theft makes dealing with both international and domestic cyber criminals complex (Finklea, 2010). Responsible law enforcement agencies need to innovate more methods of dealing with perpetrators of identity theft and ensure that victims find Justice.

It’s important to note that consumers and victims have unique perceptions surrounding identity theft. Social perceptions significantly influence how consumers deal with issues that increase the risk of identity theft. Hole (2022) states that the use of online commerce is influenced by the consumer’s perception of the risk of identity theft. For instance, consumers may fail to utilize commerce platforms because they perceive that sensitive, financial information can be stolen. Consumers concerned about identity theft may fail to buy products and services online, therefore perception and safety must be visibly addressed to manage the challenge of identity theft effectively.

Digital forensic evidence is currently being used in the US to investigate and effectively address identity theft. The authorities investigating identity theft and fraud, including the FBI and other law enforcement agencies, have adopted digital forensic technologies to enhance effectiveness and accuracy in flagging identity theft activities. According to Barik et al. (2022), the digital forensic investigation involves five phases: identification, preparation, analysis, documentation, and presentation. During the identification phase, both relevant data considered as evidence and the location of occurrence are identified, all digital forensic evidence must be carefully handled following the recommended procedures (Fakiha, 2020). Various tools and techniques are used to generate data during the preparation phase, law enforcement accepts three primary acquisitions; forensic duplications, live acquisitions, and mirror images (Barik et al., 2022). The evidence is then analysed, documented and presented to the digital crime investigation agencies, using digital forensic evidence ensures that identity theft victims and perpetrators are accurately identified.

Presently, several digital forensic investigative tools are used by law enforcement agencies dealing with identity theft in the US. The leading tools include Autopsy, Bulk Extractor, and Digital Forensics Framework (DFF). Autopsy is a digital forensic platform for time analysis, keyword search, and hash filtering (Zbrog, 2022). The open-source tool is effective for extracting digital evidence and recovering deleted files on computers and smartphones. Whereas Bulk Extractors can be used to process digital media for forensic evidence, including smartphones, hard drives, and optical drives. DFF is an open-source platform for digital investigations of identity theft and fraud (Zbrog, 2022). The FBI and other agencies involved in the investigation of US identity theft use more sophisticated tools and technologies to collect and analyse digital forensic evidence.

Despite availability of various digital forensic tools and techniques, users must take more precautionary measures to avoid becoming victims of identity theft. Kim et al. (2022) argue that users are vulnerable to identity theft if they fail to properly manage their data on devices such as computers and smartphones. Experiments have also shown that data deleted on Android, for example, may be compromised by cybercriminals (Kim et al., 2022). Unauthorized access to sensitive data such as credit cards and usernames may also be used for identity theft, putting a significant risk on the victim's reputation (Hole, 2022) victims may also encounter financial losses and related challenges. As a result, law enforcement agencies and other relevant agencies must collaborate to ensure that perpetrators are dealt with according to applicable laws.

# **Conclusion**

In brief, this report highlights how cyber identity theft has significantly grown in the US, this rise is linked to various factors, including increased use of technology and the ability of perpetrators to remain anonymous. Various personal rights and ethical issues must be considered when dealing with identity theft, for instance corporate policies must be developed and implemented to ensure that upper management is held liable and accountable for failing to implement adequate data security measures to secure personal data. There is room to enhance the effectiveness of various US Federal National Laws in addressing identity theft, the existing laws should be improved to enhance the criminalization, apprehension, and prevention. Relevant agencies' investigative tools and technologies need to be reviewed, primarily that of digital forensic evidence, the objective of such review is to identify improvements in effectiveness to tools as well as addressing current limitations. Finally, the partnership of relevant agencies should be promoted to ensure that perpetrators of identity theft are dealt with according to the law and to ensure that victims find justice.

**References**

Barik, K., Abirami, A., Konar, K. and Das, S., 2022. Research Perspective on Digital Forensic  
Tools and Investigation Process. *Illumination of Artificial Intelligence in Cybersecurity and Forensics*, pp.71-95.

Fakiha, B., 2020. Digital Forensics: Crimes and Challenges in Online Social Networks Forensics. *Journal of the Arab American University, 6(*1), pp.15-33.

Blackwood-Brown, C.G., 2018. *An Empirical Assessment of Senior Citizens' Cybersecurity Awareness, Computer Self-Efficacy, Perceived Risk of Identity Theft, Attitude, and Motivation to Acquire Cybersecurity Skills* (Doctoral dissertation, Nova Southeastern University).

Burnes, D., DeLiema, M. and Langton, L., 2020. Risk and protective factors of identity theft victimization in the United States. *Preventive Medicine Reports*, *17*, p.101058.

DeLiema, M., Burnes, D. and Langton, L., 2021. The financial and psychological impact of identity theft among older adults. *Innovation in Aging*, *5*(4), p.igab043.

DiNapoli, T., 2021. The Increasing Threat of Identity Theft. *Office of the New York State Comptroller*. Available from: https://www.osc.state.ny.us/files/reports/pdf/increasing-threat-of-identity-theft.pdf [Accessed 26 August 2022]

EG., 2022. Federal crime of identity theft – 18 USC § 1028. Available from: https://www.thefederalcriminalattorneys.com/federal-identity-theft# [Accessed 27 August 2022]

FTC., 2022. New Data Shows FTC Received 2.8 million Fraud Reports from Consumers in 2021. Available from: https://www.ftc.gov/news-events/news/press-releases/2022/02/new-data-shows-ftc-received-28-million-fraud-reports-consumers-2021-0 [Accessed 26 August 2022]

Helser, S. and Hwang, M.I., 2021. Identity theft: a review of critical issues. *International Journal of Cyber Research and Education (IJCRE)*, *3*(1), pp.65-77.

Gross, Ralph & Acquisti, Alessandro & III, H.. (2005). Information revelation and privacy in online social networks (The Facebook Case). WPES'05: Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society. *71-80. 10.1145/1102199.1102214*.

Guedes, I., Martins, M. and Cardoso, C.S., 2022. Exploring the determinants of victimization and fear of online identity theft: an empirical study. *Security Journal*, pp.1-26.

Hole, JW, 2022. Identity theft and its effects on victims, commerce, and society: Ideal systematic approach combatting identity theft involving a combination of prevention, education/outreach, detection, recovery, and enforcement components. Available from: https://minds.wisconsin.edu/bitstream/handle/1793/83033/Hole%2C%20Jeff.pdf?sequence=1&isAllowed=y [Accessed 22 August 2022]

Kim, H., Shin, Y., Kim, S., Jo, W., Kim, M., and Shon, T., 2022. Digital Forensic Analysis to Improve User Privacy on Android. *Sensors*, *22*(11), p.3971.

National Council on Identity Theft Protection., 2022. 2022 Identity Theft Facts and Statistics. Available from: https://identitytheft.org/statistics/ [Accessed 26 August 2022]

Payne, D. and Kennett‐Hensel, P.A., 2017. Combatting identity theft: A proposed ethical policy statement and best practices. *Business and Society Review*, *122*(3), pp.393-420.

Piquero, N.L., Piquero, A.R., Gies, S., Green, B., Bobnis, A. and Velasquez, E., 2021. Preventing identity theft: Perspectives on technological solutions from industry insiders. *Victims & Offenders*, *16*(3), pp.444-463.

US Department of Justice., 2022. Identity Theft – Special Feature. Available from: https://www.ojp.gov/feature/identity-theft/additional-resources [Accessed 225August 2022]

Vanhee, AJ, 2022. Increased Protection Versus the Cost of Increased Protection: Victimization and the Use of Protective Measures Against Identity Theft. *Criminal Justice and Behavior*, p.00938548221105824.

Vilic, V.M., 2019. Phishing and pharming as forms of identity theft and identity abuse. *Balkan Soc. Sci. Rev.*, *13*, p.43.

Zaeem, R.N. and Barber, KS, 2021. Economics of Cybercrime: Identity Theft and Fraud. In *Encyclopedia of Cryptography, Security, and Privacy* (pp. 1-4). Berlin, Heidelberg: Springer Berlin Heidelberg.

Zbrog, M., 2022. A guide to digital forensics and cybersecurity tools (2022-2023). *Forensics Colleges*. Available from: https://www.forensicscolleges.com/blog/resources/guide-digital-forensics-tools [Accessed 22 August 2022]