Engineering and Technology Journal e-ISSN: 2456-3358
Volume 09 Issue 01 January-2024, Page No.- 3353-3360
DOI: 10.47191/etj/v9i01.15, I.F. – 7.136
© 2024, ETJ

A Study of COVID-19 Effects on the Identity Theft Landscape

Trang Thi Thu Horn[1], **Mahmoud Yousef**[2]
[1,2]University of Central Missouri

ABSTRACT: This research studies the impact of COVID-19 on the identity theft landscape using historical data published by the Federal Trade Commission. The data set included information about the number of identity theft reports for each state per year over a 6-year period, 2017 -2022. The dataset also included the number of reports for each identity theft category, providing a holistic view of the identity theft landscape. The data showed a significant increase in the number of identity thefts across all the states in 2020 compared to 2019; the percentage increase ranged from 45% to 1,801.1%. This coincided with the pandemic, which started in December 2019. The top 5 states that had the highest percent increase in 2020 are Kansas, Rhode Island, Maine, Washington, and Illinois. Moreover, in the year 2020, there was a dramatic increase across all the states in the number of identity theft reports related to government documents or benefits fraud, ranging from 207.7% to 33,236% increase compared to the year 2019. This was due to the sudden increase in available funds to help Americans during the pandemic, including unemployment benefits, stimulus checks, small business loans, etc., along with the expedited process to distribute the funds, which created ideal conditions for cybercriminals, especially identity thieves.

KEYWORDS: cybercrime, identity theft, benefits fraud, phishing, COVID-19

INTRODUCTION

COVID-19 has had a great impact on various aspects of our society, ranging from public health to the national economy, and created a significant increase in cybercrimes. Due to COVID-19, small and local businesses downsized or went out of business, causing widespread economic hardship and contributing to a huge increase in unemployment. Many economic sectors, including service and travel industries, faced high unemployment rates due to sharp decreases in demand or shutdowns. Reports of anxiety and depression worldwide were also on the rise (World Health Organization, 2022). In response to such unprecedented challenges, the government had several assistance programs to help individuals, families, and businesses. In addition, remote working created challenges for small and medium-sized companies since they were often not well prepared for the surge in cybercrimes. The sudden move to remote working and learning made individuals who were not sufficiently prepared in complex cyber environments easy targets for cybercriminals. These conditions created a perfect storm for cybercrimes, especially identity theft.

PHISHING AND IDENTITY THEFTS

The very first confirmed case of COVID-19 in the United States was reported in January 2020, and in the same year, the FBI Internet Crime Complaint Center received about 791,790 complaints of cybercrimes, an increase of over 300,000 complaints compared to 2019 (Federal Bureau of Investigation, 2021). It was also reported that the total loss to cybercrimes in 2020 was over $4.2 billion. During the peak of the pandemic, the number of phishing incidents increased by 220% compared to the yearly average (Warburton, n.d.).Phishing attacks are a type of attack that uses emails or text messages to trick the victims into giving their personal and financial information (Federal Trade Commission, n.d.). For example, a person receives an email that appears to come from a reputable source, which can be a company, a financial institution, or a government agency. The email then warns them of an issue that needs their attention immediately, which will encourage them to click on a link or a button to go to the website. These sites can be phony sites that mimic legitimate sites or actual company sites with popup windows that will appear for the purpose of harvesting sensitive personal information (The Office of the Comptroller of the Currency, n.d.). Then they might be asked to update their account information and provide information about their social security number, account number, passwords, or other information to verify their identity. Phishing attacks are commonly utilized to harvest data for identity theft attacks.

Identity theft is a type of fraud that involves stealing and using someone else’s sensitive personal or financial information without permission (Federal Trade Commission, n.d.). The sensitive information can be name, address, social security information, credit card information, bank account information, etc. Identity thieves can buy things with the victim’s credit card information, get new credit cards in the victim's name, open new accounts with the stolen information, steal tax refunds, etc. (Federal Trade Commission, n.d.). In addition, identity thieves can take out loans or even a driver's license in the victim's name, causing financial and reputational damages to the victims, which can take the victims years to recover (The Office of the Comptroller of the Currency, n.d.). In 2020, it was reported that identity theft complaints related to government benefits increased by 3,000%, causing troubles and challenges for both individuals and the federal government (Pandemic Oversight, n.d.). In fact, it took the Internal Revenue Service (IRS) 260 days to resolve a case of identity theft of a citizen, causing a long wait for the taxpayer and holding up their tax refund and stimulus check. (Pandemic Oversight, n.d.)

COVID-19 effects on identity theft

This study will focus on studying the effects of COVID-19 on identity theft. This research utilizes historical data, which involves the use of publicly available datasets provided by the Federal Trade Commission (FTC). The FTC is an agency of the United States government with the mission of protecting consumers (Federal Trade Commission, n.d.). The agency collects reports from individuals who have been victims of identity theft, then analyzes and disseminates the data through reports and its publicly available database. Besides, it also has a dedicated identity theft website that provides resources and guidance for prevention and addressing identity theft. The data set used in this research contained information about the number of identity theft reports across all the states for the years from 2017 to 2022. It also contained information about the number of reports for each category of identity theft for each state each year, providing a holistic view of the identity theft landscape over the years. There was a total of seven categories of identity theft, including credit card fraud, bank fraud, phone or utility fraud, loan or lease fraud, employment or tax-related fraud, government documents or benefits fraud, and other identity theft fraud. The data was then extracted and put into an Excel spreadsheet for further analysis.

Overall, there was a significant increase in the number of identity theft reports from 2019 to 2020 across all the states.

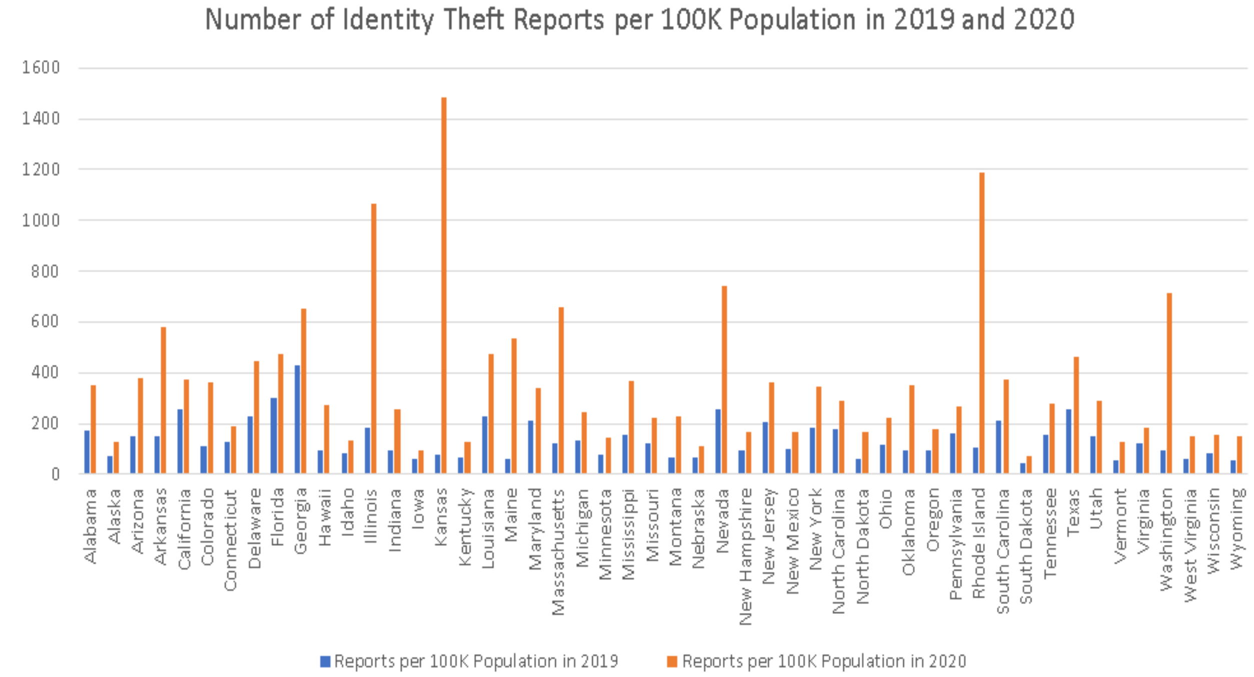
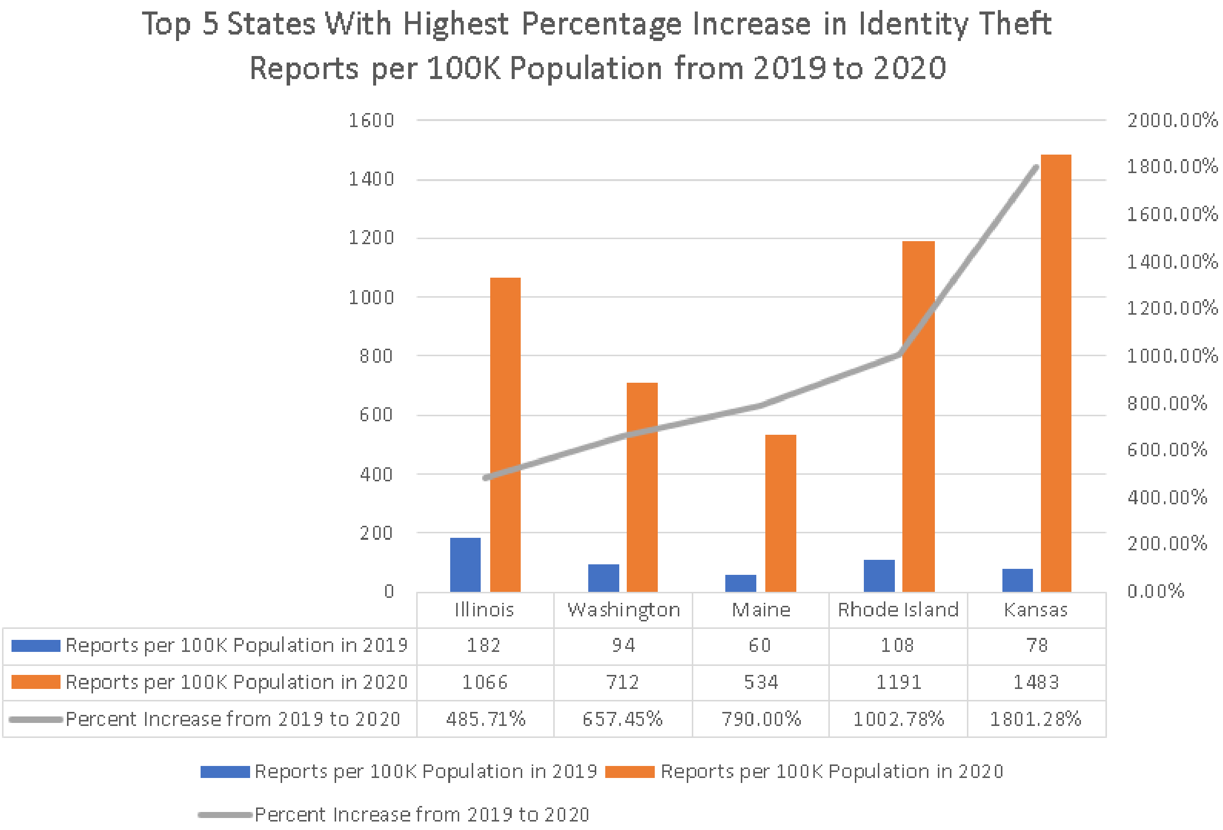


Figure 1- Numbers of identity theft reports per 100K population in 2019 and 2020

The percentage increase in the number of identity theft complaints ranges from 45% to 1,801.1% for all the states from the year 2019 to 2020. The top five states that had the highest percentage increase in identity theft complaints are Kansas, Rhode Island, Maine, Wahington, and Illinois. Specifically, the number of identity theft reports increased by 1,801.1% in Kansas, 1,001.3% in Rhode Island, 790.1% in Maine, 663% in Washington, and 483.6% in Illinois.



	Illinois	Washington	Maine	Rhode Island	Kansas
Reports per 100K Population in 2019	182	94	60	108	78
Reports per 100K Population in 2020	1066	712	534	1191	1483
Percent Increase from 2019 to 2020	485.71%	657.45%	790.00%	1002.78%	1801.28%

Figure 2-Top five states with highest percentage increase in identity theft reports per 100k population from 2019 to 2020

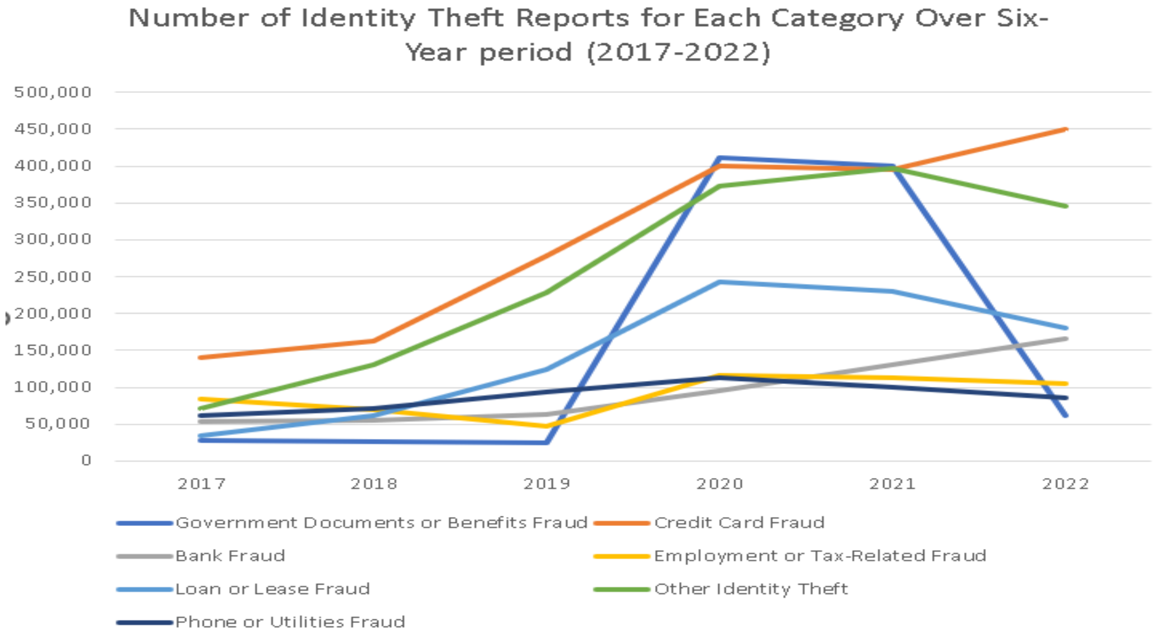
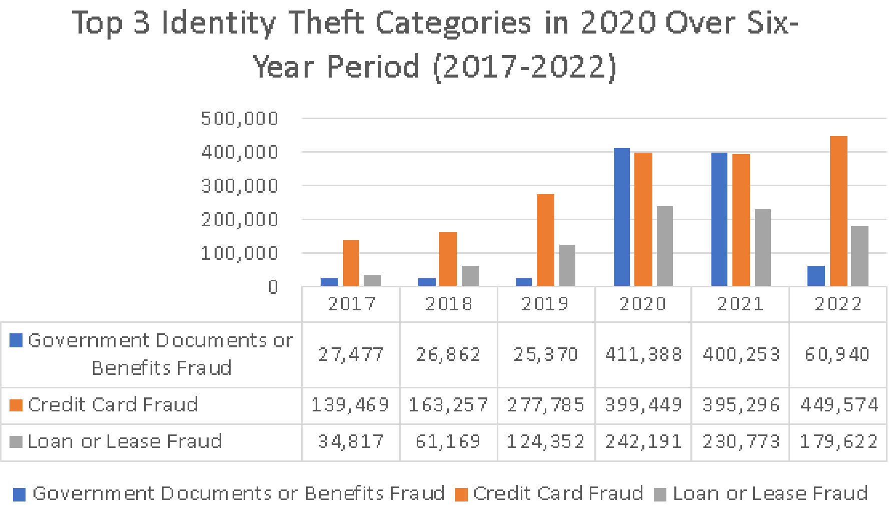


Figure 3-Number of identity theft reports for each category over a six-year period (2017-2022)z

Among various types of identity theft, government documents and benefits fraud had the highest increase from 2019 to 2020, with a 1,521% increase. As can be seen from the figure, before the pandemic started, government documents or benefits fraud remained the lowest among other categories of identity theft. There was a decrease in the number of reports of government documents or benefits fraud from 2017 to 2019. However, after the pandemic started, there was a dramatic increase from 2019 to 2020 across all the states for government documents or benefits fraud category, ranging from 207.7% to 33,236% increase compared to 2019.



	2017	2018	2019	2020	2021	2022
■ Government Documents or Benefits Fraud	27,477	26,862	25,370	411,388	400,253	60,940
■ Credit Card Fraud	139,469	163,257	277,785	399,449	395,296	449,574
■ Loan or Lease Fraud	34,817	61,169	124,352	242,191	230,773	179,622

Figure 4-Top three identity theft categories in 2020 over a six-year period (2017-2022)

In fact, most identity theft cybercrimes reported in Kansas, which has the highest increase in identity theft, are related to government documents or benefits fraud. The Kansas Department of Labor experienced a record-high number of fraudulent applications, causing the agency to temporarily shut down its website to hinder the criminals' activities (O'Brien, 2021). The Kansas Department of Labor and the audit division of the Kansas Legislature were highly confident that from January 2020 to February, during the COVID-19 health emergency, $380 million was fraudulently obtained by individuals personating others (Carpenter, 2021). Moreover, there was less convincing evidence concerning $306 million in payments flagged as suspicious. The auditor identified a potential loss totaling $686 million, equally distributed between the federal unemployment fund and the state's unemployment trust fund (Carpenter, 2021). The article pointed out that the cause could be the mistakes made in responding to COVID-19 and the surge in joblessness compounded with the rapid expansion of aid programs, which overwhelmed the system. Furthermore, the legislature's post division of post-audit stated that the issues stemmed from its outdated mainframe computer that relied on a patchwork of the old and new programming languages, which was inadequate for processing claims (Carpenter, 2021). It was also noted that a significant accumulation of valid and fraudulent claims was fueled by Congress's introduction of complex temporary relief programs and the surge in the state's unemployment rates (from 2.9% to 12.6%). Specifically, the number of claims the Department of Labor handled soared from 3,000 in February 2020 to 66,000 in March 2020, with over 200,000 Kansans filing initial claims within seven weeks due to Covid-19 (Carpenter, 2021). The tremendous workload strained the piecemeal system, causing periodic failures and making it impossible to predict the errors with any modification. Besides, integrating new federal unemployment programs caused issues in the systems that were hard to detect and resolve (Carpenter, 2021).

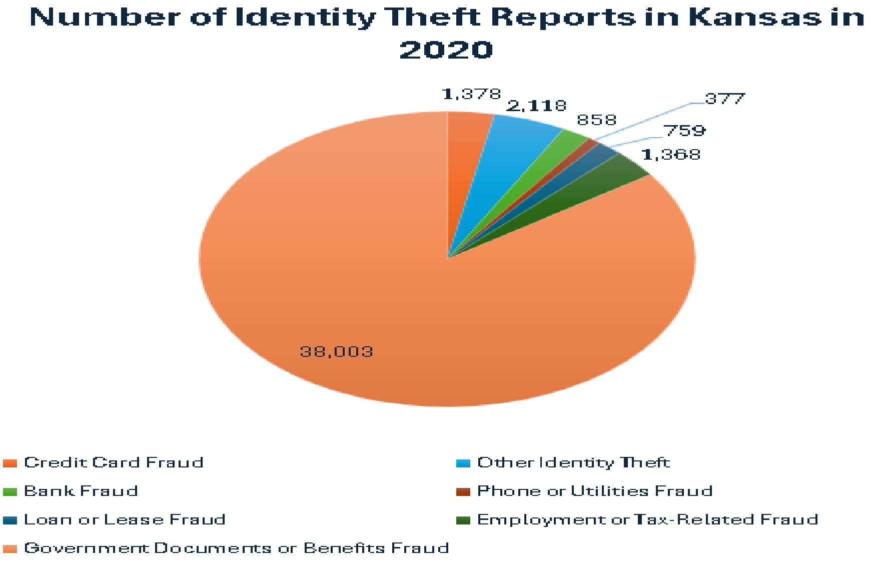
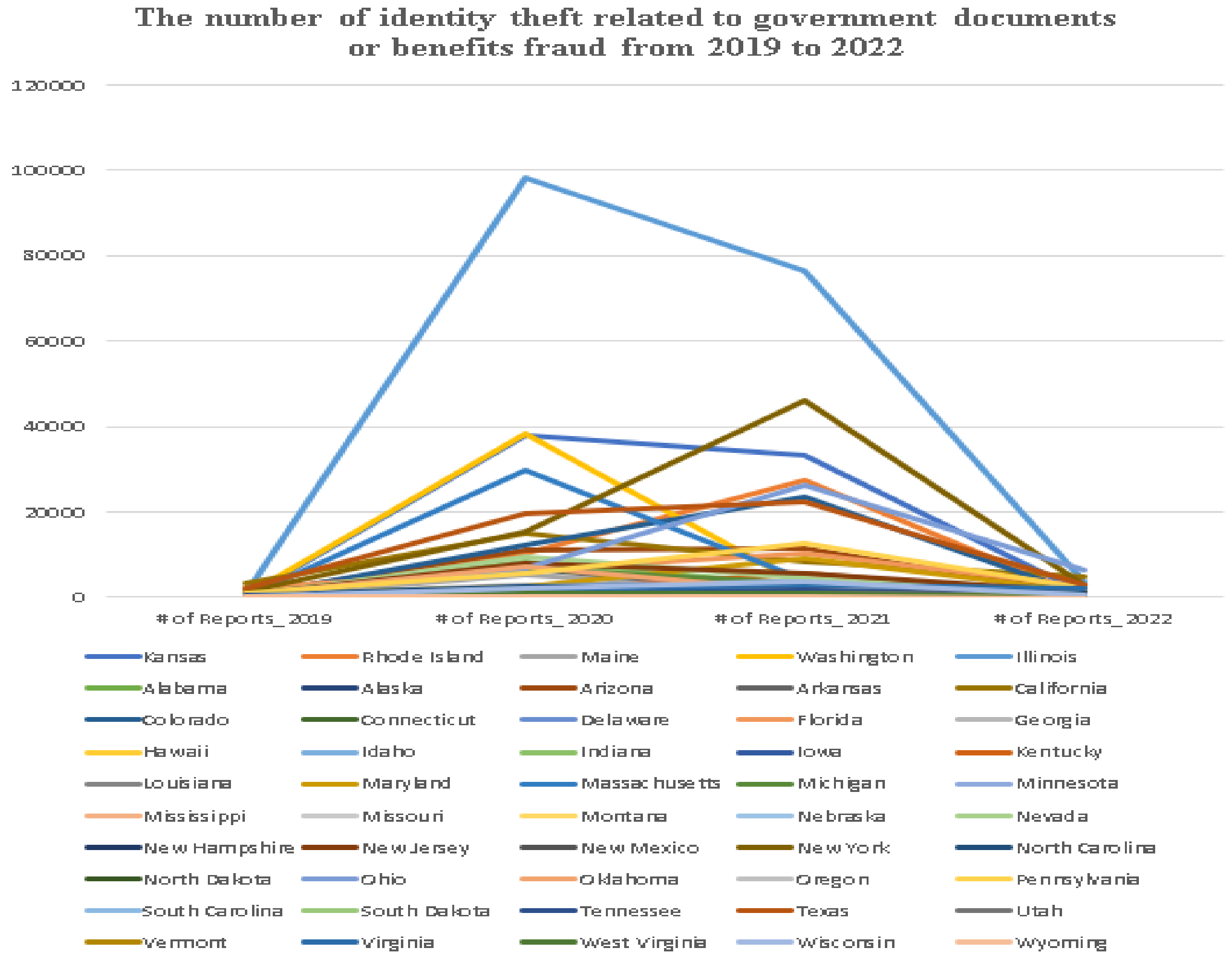


Figure 5-Numbers of identity theft reports in Kansas in 2020

The sudden increase in available funds, such as unemployment benefits, stimulus checks, small business loans, etc., and the expedited distribution process created ideal conditions for cybercriminals. Michael Horowitz, the Justice Department Inspector General who oversaw Covid-19 relief spending, told "NBC Nightly News" that Covid-19 relief programs were organized in ways that made them attractive targets for scammers (Dilanian & Strickler, 2022). The article also pointed out that according to experts, as much as $80 billion was lost to theft, which was approximately 10% of the $800 billion handed out in the Covid-19 relief plan known as the Paycheck Protection Program (PPP) (Dilanian & Strickler, 2022). In addition, an estimate of $90 billion to $400 billion was believed to have been stolen from the $900 billion Covid-19 unemployment relief program. On top of that, another $80 billion was potentially stolen from a separate Covid-19 disaster relief program (Dilanian & Strickler, 2022).

The quick disbursement of over 5 trillion in federal pandemic response funds created a "perfect storm" for identity fraud (Pandemic Oversight, 2022). The FTC received a 2920% increase in the number of identity theft reports related to government documents or benefit fraud in 2020 (Pandemic Oversight, 2022). Due to the urgent need for financial assistance, the program was rolled out quickly. It might have lacked adequate levels of verification and security measures, creating opportunities for cybercriminals to exploit the weaknesses in the system. In addition, due to the social distance and lockdown policy in place, the sudden shift to online and remote environments created challenges for individuals who were not well prepared for complex cyber networks, making them vulnerable to cybercrimes, including identity theft. Besides, people might not be fully aware of the need to protect their personal information, especially in times of crisis. The pandemic led to perfect opportunities for fraudsters to create new social engineering scams, taking advantage of the chaotic crisis and various government aids that were available.

From the year 2020 to 2021, we saw a decrease or a smaller percentage increase compared to the increase from 2019 to 2020 for government documents or benefits fraud category, the percentage increase ranging from 5.3% to 341.2%. Meanwhile, from 2021 to 2022, we saw a decrease in the number of government documents or benefit frauds across all the states except for Connecticut. However, the percentage increase in Connecticut from 2021 to 2022 was much smaller compared to the percentage increase from 2019 to 2020.



On July 2023, the Connecticut Department of Labor (CTDOL) Commissioner warned Connecticut employers and residents of the rise in unemployment benefit fraud due to identity theft. During the pandemic, stolen identities were sold for about one dollar on the dark web, which was still being mined to purchase names, social security numbers, date of birth, and other sensitive data (Connecticut Department of Labor, 2023). This information can be used to apply for credit cards, unemployment benefits and bank loans (Connecticut Department of Labor, 2023). CTDOL suspected that about 75% of the several thousand claims they received daily were fraudulent, and they withheld the payment. CTDOL has worked closely with federal agencies and law enforcement to prevent unemployment fraud and protect the employer-funded Trust Fund.

For other categories of identity theft, we also saw an increase in the number of loan or lease fraud related identity theft reports across all the states from 2019 to 2020, as well as employment or tax-related fraud category. The increasing percentage ranged from 31.6% to 634.6% for those categories, which were much smaller compared to the percent increase in the government documents or benefits fraud category. Please see the summary table 1 for more information on other categories of identity theft.

Table 1 – Summary of Identity Theft Categories Over the Years from 2019 to 2022

Identity Theft Categories	**2019-2020**	**2020 - 2021**	**2021-2022**
Credit Card Fraud	Most of the states showed an increase from the year 2019 to 2020 across all the states. Percentage increase ranged from 0.5% to 181.1%, except for New Hampshire, which had a 5.7% decrease	Except for Iowa, Louisiana, and New Mexico, most of the states showed a decrease in 2021 compared to 2020 or a decrease in percent increase compared to the previous increase in 2019-2020	Showed an increase from the year 2021 to 2022, except for Georgia, Louisiana, Maryland, and Tennessee
Bank Fraud	Except for Idaho, most of the states showed an increase in the bank fraud category. The percent increase ranged from 16.8% to 306.3%	Except for New York, New Jersey, Ohio, and Pennsylvania, most of the states show an actual decrease in 2021 compared to 2020 or a decrease in percentage increase compared to the previous increase in 2019-2020	Stayed the same or showed an increase across all the states. The increase percentage ranged from 1% to 289.7%, except for New York, Rhode Island, New Jersey, Florida, Oklahoma, and Mississippi
Phone or Utility Fraud	Showed an increase for 40 out of 50 states, the remaining states showed a decrease from 2019 to 2020	Show a decrease in 2021 compared to 2020 or a decrease in percent increase compared to the previous increase in 2019-2020 except for Maine, Idaho, and North Dakotas	Showed a decrease for 30 out of 50 states
Loan or Lease Fraud	Showed an increase across all the states, the percent increase ranged from 56.6% to 429.4%	Stayed the same or showed a decrease or a decrease in percent increase compared to the previous increase in 2019-2020	Stayed the same or showed a decrease across all the states except for Indiana, Montana, and New Hampshire
Employment or Tax-Related Fraud	Showed an increase across all the states. The percent increase ranged from 31.6% to 634.6%	Stayed the same or decreased or decreased in percent increase compared to the previous increase in 2019-2020	Most of the states stayed the same or showed a decrease in the number of reports related to employment or tax-related fraud, except for Texas, Maine, New Mexico, Virginia, Missouri, and Idaho
Other identity theft	Showed an increase from 2019 to 2020. The percent	Showed a decrease in 2021 compared to 2020 or a decrease in percent	Showed a decrease for 39 states out of 50 states

	increase ranged from 10.6% to 544.3%	increase compared to the previous increase in 2019-2020 except for Alaska, Iowa, Pennsylvania, Nebraska, Maryland, Virginia, North Dakota, Colorado, and Louisiana	

RECOMMENDATIONS

Nowadays, most of an individual’s information and data are online. Even though life is more convenient with the internet and online transactions, it creates opportunities for cybercriminals to steal and use individual’s personal information. In 2022, the FTC received more than 1.1 million reports of identity theft. The time to recover from an identity theft depends on the type of identity theft fraud involved. For example, if the criminal just uses a credit card without a person’s authorization and does not get any other sensitive information, it may just be a short amount of time for the person to report it and get a new credit card in his/her mail (Luthi, 2019). However, with more serious and complex types of identity theft, such as using the victim’s social security number to open a new credit account, causing a tax debt, or committing crimes, it could take years for the victim to recover from the damage (Luthi, 2019).

There are several ways that people can protect themselves from identity theft. The golden rule here is never to provide personal information, financial information, health plan information, or any sensitive information, whether over the phone or the Internet, in response to a communication that a person did not initiate (Attorney General of Texas, n.d.). Keep documents with your personal or financial information in a safe place at home and work. Make sure to shred documents that have sensitive information, such as receipts, loan applications, bank statements, etc., if no longer needed. For electronic devices that are used to store a person’s personal information, it is essential to get rid of all the personal information stored in your laptop, desk- computer, or mobile device before selling or giving away the devices (Attorney General of Texas, n.d.). In addition, users need to be aware of phishing scams. Emails and phony sites crafted by cybercriminals might appear to be exactly the same as the real ones. Even fake websites may have a fake padlock icon that is originally used to denote a secured website (The Office of the Comptroller of the Currency, n.d.). Furthermore, individuals can sign up for an identity theft protection service, which will help with alerting, limiting the damage, and helping victims recover sooner. Identity theft protection subscription will monitor credit reports, financial accounts, medical information, dark web, etc. Identity theft protection companies also provide recovery services that are up to $1 million and access to attorneys or investigators to restore the victim’s credit or reputation (Kinney, n.d.). Moreover, two-factor authentication plays an essential role in protecting individuals from becoming victims of identity theft. Enabling two-factor authentication on devices helps to protect the user’s account when the password is stolen since the criminal can’t get into the user’s account without another factor of authentication, which can be a one-time password received by the user’s phone, fingerprint, etc. Also, users should never provide passwords to anyone or to unsolicited requests over the Internet or over the phone. Users should use strong, complex, and unique passwords for each account. A password manager can be a good solution to consider. It is necessary to regularly review the user’s account activities for any suspicious transactions. In case of falling victim, the user should contact the institution immediately. If sensitive information is disclosed, the user should contact the major credit bureaus and discuss whether he/she needs to put a fraud alert on their file to prevent the cybercriminals from opening an account under their name (The Office of the Comptroller of the Currency, n.d.)

Organizations should have all the secure measures such as intrusion detection systems, encryptions, firewalls, etc., in place to protect the sensitive data collected from their customers. Identity theft can stem from data breaches where customers' information is exposed or sold on the dark web to criminals. Humans are always the most vulnerable element in cybersecurity; therefore, regularly training employees on security awareness and best practices is necessary. Systems should always be kept up to date with the latest security patches. Also, organizations should always implement verification procedures that involve the use of sensitive information or financial transactions. It is necessary to conduct more campaigns educating the public about the risk of identity theft and how to protect themselves against identity theft. Collaborations among different report agencies are needed to share information on vulnerabilities and cyber threats. Also, cooperation between different agencies such as Social Security administrations, the IRS, and law enforcement is needed to help streamline the response and recovery process. In the case of Covid-19, understanding that rapid response is crucial during a crisis, however, it shouldn’t come at the expense of security. Future aid programs in similar situations should strive for a balance to ensure that aid is distributed quickly and protected against fraudulent activities. Addressing cybercrimes, especially identity theft, requires collaborations across different sectors, including government, financial institutions, law enforcement, and the public, for more effective prevention and response strategies.

REFERENCES

1. Attorney General of Texas. (n.d.). *Help Prevent Identity Theft*. Retrieved from Attorney General of Texas: https://www.texasattorneygeneral.gov/consumer-protection/identity-theft/help-prevent-identity-theft
2. Carpenter, T. (2021, 08 30). *Legislative auditors revise Kansas unemployment fraud tally upward to nearly $700 million*. Retrieved from Kansas Reflector: https://kansasreflector.com/2021/08/30/legislative-auditors-revise-kansas-unemployment-fraud-tally-upward-to-nearly-700-million/
3. Connecticut Department of Labor. (2023, 7 20). *CT. Dept. Of Labor Warns of Uptick In Unemployment Fraud Due To Identity Theft*. Retrieved from Connecticut State Department of Labor Communications: https://portal.ct.gov/DOLCommunications/News/Press-Room/2023/CT-Dept-Of-Labor-Warns-of-Uptick-In-Unemployment-Fraud-Due-To-Identity-Theft
4. Dilanian, K., & Strickler, L. (2022, 3 28). *'Biggest fraud in a generation': The looting of the Covid relief plan known as PPP*. Retrieved from NBC News: https://www.nbcnews.com/politics/justice-department/biggest-fraud-generation-looting-covid-relief-program-known-ppp-n1279664
5. Federal Bureau of Investigation. (2021, 3 17). *FBI Releases the Internet Crime Complaint Center 2020 Internet Crime Report, Including COVID-19 Scam Statistics*. Retrieved from FBI: https://www.fbi.gov/news/press-releases/fbi-releases-the-internet-crime-complaint-center-2020-internet-crime-report-including-covid-19-scam-statistics
6. Federal Trade Commission. (2020). *Consumer Sentinel Network Data Book*. Federal Trade Commission.
7. Federal Trade Commission. (n.d.). *About the FTC*. Retrieved from Federal Trade Commission - Protecting American's Consumers: https://www.ftc.gov/
8. Federal Trade Commission. (n.d.). *How to Recognize and Avoid Phishing Scams*. Retrieved from Federal Trade Commission - Consumer Advice: https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams
9. Federal Trade Commission. (n.d.). *What To Know About Identity Theft*. Retrieved from Federal Trade Commission - Consumer Advice: https://consumer.ftc.gov/articles/what-know-about-identitytheft#:~:text=Identity%20Theft%20Insurance,What%20Is%20Identity%20Theft%3F,or%20medical%20insurance%20account%20numbers.
10. G., E. (2021, 4 07). *Government documents and benefits fraud surged 45 times in 2020*. Retrieved from atlasVPN: https://atlasvpn.com/blog/government-documents-and-benefits-fraud-surged-45-times-in-2020
11. Kinney, J. (n.d.). *10 Ways to Prevent Identity Theft*. Retrieved from U.S. News: https://www.usnews.com/360-reviews/privacy/identity-theft-protection/10-ways-to-prevent-identity-theft
12. Luthi, B. (2019, 7 23). *What to Know About the Effects of Identity Theft*. Retrieved from Experian: https://www.experian.com/blogs/ask-experian/how-long-can-the-effects-of-identity-theft-last/
13. O'Brien, S. (2021, 05 10). *Kansas had most identity theft reports in 2020, new study finds*. Retrieved from Fox4: https://fox4kc.com/news/kansas-had-most-identity-theft-reports-in-2020-new-study-finds/
14. Pandemic Oversight. (2022). *Key Insights: Identity Fraud Reduction and Redress in Pandemic Response Programs*. Pandemic Oversight.
15. Pandemic Oversight. (n.d.). *Identity Theft in Pandemic Benefits Programs*. Retrieved from Pandemic Oversight: https://www.pandemicoversight.gov/spotlight/identity-theft-in-pandemic-benefits-programs
16. The Office of the Comptroller of the Currency. (n.d.). *Phishing Attack Prevention: How to Identify & Avoid Phishing Scams*. Retrieved from The Office of the Comptroller of the Currency: https://www.occ.gov/topics/consumers-and-communities/consumer-protection/fraud-resources/phishing-attack-prevention.html#:~:text=In%20the%20worst%20case%2C%20you,driver's%20licenses%20in%20your%20name.
17. Warburton, D. (n.d.). *f5*. Retrieved from Phishing Attacks Soar 220% During COVID-19 Peak as Cybercriminal Opportunism Intensifies: https://www.f5.com/company/news/features/phishing-attacks-soar-220--during-covid-19-peak-as-cybercriminal
18. World Health Organization. (2022, 3 2). *COVID-19 pandemic triggers 25% increase in prevalence of anxiety and depression worldwide*. Retrieved from World Health Organization: https://www.who.int/news/item/02-03-2022-covid-19-pandemic-triggers-25-increase-in-prevalence-of-anxiety-and-depression-worldwide#:~:text=COVID%2D19%20pandemic%20triggers%2025,of%20anxiety%20and%20depression%20worldwide