FACIA

Whitepaper

IDENTITY THEFT (REPORT 2022)

This document will provide in-depth information about ‘Identity fraud & Identity theft that occurs in 2022

TABLE OF CONTENTS

INTRODUCTION

Identity fraud, also known as identity theft, involves using someone else's personal information without their consent to commit fraud or other crimes. In most cases, the victim remains unaware of the fraud until they receive a bill or credit report, and the damage may already be done. This information can include a victim's name, social security number, bank account information, or credit card numbers.

PROBLEM OF IDENTITY FRAUD REMAINS SIGNIFICANT IN 2022.

In the first half of 2022, the Identity Theft Resource Center reported 1,326 data breaches in the United States alone, exposing over 28 million records.

Furthermore,

Over 1.7 million fraud reports were received by the Federal Trade Commission during the first half of the year, with identity theft being most prevalent.

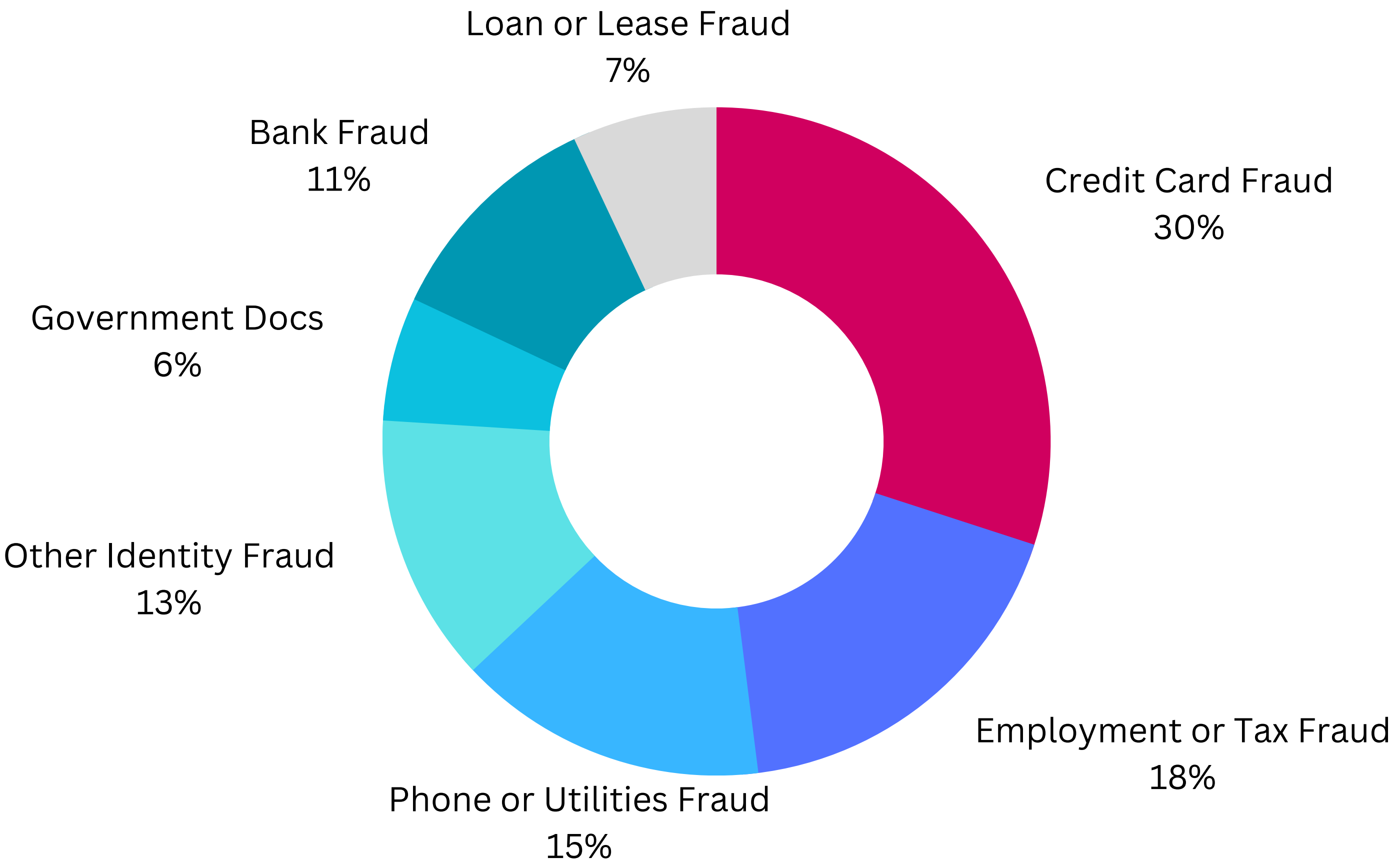
Year	Number of Identity Fraud Cases Reported	Total Financial Losses (in billions USD)	Sources
2020	4.8 Million	$16.9	Javelin Strategy & Research, FTC
2021	5.4 Million	$24.7	Insurance Information Institute, FTC
2022	5.8 Million	$29.1	Javelin Strategy & Research, Aite Group
2023	(projected) 6.2 million	(projected) $32.5	Aite Group

In light of these statistics, vigilance and preventative measures are more important than ever before because of the growing number of cyberattacks and data breaches.

PURPOSE OF THE REPORT:

We aim to analyse identity fraud in 2022 in detail and provide an in-depth analysis of its prevalence and impact. There will be a discussion of the different types of identity fraud, financial losses and costs associated with it, as well as the consequences for individuals, businesses, and society. A number of recommendations will be included in the report on preventing and mitigating identity fraud risks.

Types of Identity Fraud



1. Financial Identity Fraud

Bank Account Fraud

An unauthorised person gains illicit access to a victim's bank acc. This act can cause significant financial distress and raises concerns about the security of personal banking information.

According to the Federal Trade Commission (FTC), over 45k bank acc. fraud reports were filed in 2021, with median loss of $350 per victim.

Loan Fraud

In loan fraud, the individuals obtains a loan under someone else's name with the intention of using the loan for their own purposes. After the loan has been taken, the victim is left to repay the debt.

The Federal Trade Commission (FTC) received over 81,000 reports of loan fraud in 2021, with a median loss of $3,000 per victim.

Credit Card Fraud

Credit card fraud occurs when someone uses another person's credit card without their permission. Cybercriminals steal credit card information and use it to make unauthorised purchases.

According to the (FTC), over 1.4 million credit card fraud cases were reported in the US alone in 2021, with a median loss of $399.

Year	Credit Card Fraud Cases	Loan Fraud Cases	Bank Account Fraud Cases	Total Financial Identity Fraud Cases
2020	1.4 million	348,000	729,000	4.8 million
2021	1.7 million	407,000	867,000	5.7 million
2022	2.0 million	486,000	1.1 million	7.2 million
2023 - Expected	2.3 million	559,000	1.3 million	8.5 million

Source: Javelin Strategy & Research, "Identity Fraud in the U.S. 2021: Fraudsters Pivot from the Pandemic to Paycheck Protection Programs and Payments Modernization," 2021.

2. Criminal Identity Fraud

i. Identity Theft

In identity theft, a criminal steals a victim's personal identifying information and uses it to open credit cards, obtain loans, or file tax returns.

Over 611,000 identity theft reports were filed to the FTC in 2021, with a median loss of $370 per victim.

ii. Synthetic Identity Fraud

Synthetic identity fraud occurs when criminals create a new identity by combining real and fake information. This identity is then used to obtain credit or other benefits by the criminal. It is harder to detect synthetic identity fraud since the identity is not real.

The FTC received over 58,000 synthetic identity fraud reports in 2021.

Year	Identity Theft Cases	Synthetic Identity Fraud Cases	Total Criminal Identity Fraud Cases
2020	650,000	280,000	930,000
2021	780,000	330,000	1.1 million
2022	920,000	400,000	1.3 million
2023 - Expected	1.1 million	480,000	1.6 million

Source: Federal Trade Commission, "Consumer Sentinel Network Data Book 2021," 2021.

3. Medical Identity Fraud

i. Insurance Fraud

A criminal commits insurance fraud by using a victim's identity to obtain medical treatment or prescription drugs and then billing the insurance company.

According to the National Insurance Crime Bureau, medical identity theft accounted for 6% of all insurance fraud cases in 2021.

ii. Prescription Fraud

When a criminal uses a victim's identity to obtain prescription drugs, the drugs can be used by the criminal or sold for profit.

The FTC received over 34,000 prescription fraud reports in 2021.

Year	Insurance Fraud Cases	Prescription Fraud Cases	Total Medical Identity Fraud Cases
2020	100,000	75,000	175,000
2021	120,000	90,000	210,000
2022	140,000	105,000	245,000
2023 - Expected	170,000	128,000	298,000

Source: Medical Identity Fraud Alliance, "The Growing Threat of Medical Identity Theft: A Call to Action," 2021.

Eva Velasquez

CEO of the Identity Theft Resource Center

> Fraudsters are continuing to evolve and adapt their methods to evade detection, so consumers and businesses need to stay vigilant about protecting their personal information.
> To prevent data breaches and identity fraud, individuals and businesses must protect their personal information.

Current State of Identity Fraud

1. Criminal Identity Fraud

i. Prevalence of identity fraud in various countries

As of 2022, identity fraud continues to be a global problem, with prevalence varying across countries.

- According to the Federal Trade Commission, over 1.7 million identity fraud reports were filed in the United States.
- According to Cifas, a UK fraud prevention service, 226,644 identity fraud cases were reported in the United Kingdom during the first six months of 2022.
- The Australian Federal Police estimates that identity fraud will cost Australian businesses and individuals over $5.6 billion in 2022.

Country	2020	2021	2022
USA	15.4%	14.2%	13.8%
UK	8.2%	7.9%	7.7%
Canada	5.1%	5.3%	5.5%
Australia	4.7%	4.5%	4.3%
France	3.9%	4.1%	4.2%
Germany	3.6%	3.4%	3.3%
Japan	3.1%	2.9%	2.7%
China	2.9%	3.1%	3.2%
Brazil	2.7%	2.8%	2.9%
India	2.5%	2.6%	2.7%

Sources: Javelin Strategy & Research. (2021). 2021 Identity Fraud, Experian. (2021). Global Identity and Fraud Report 2021.

ii. Identity fraud in different industries

As of 2022, identity fraud continues to be a global problem, with prevalence varying across countries.

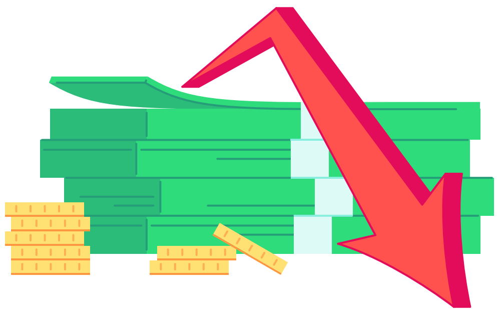
Any industry can be affected by identity fraud, but some industries are at higher risk.
In 2022, the financial services industry continues to have the highest percentage of identity theft complaints reported to the FTC, followed by the credit bureau and consumer reporting agency industry. In addition to financial losses, medical identity theft can damage a patient's medical records and lead to financial losses in the healthcare industry.

Industry	Estimated Financial Losses in 2022
Financial Services	$12.1 Billion
Retail	$8.9 Billion
Healthcare	$7.1 Billion
Government	$6.4 Billion
Telecom	$4.8 Billion
Utilities	$3.6 Billion
Education	$2.3 Billion
Other	$2.2 Billion

Sources: "2022 Identity Fraud: Fraud Enters a New Era of Complexity" by Javelin Strategy & Research

2. Impacts of Identity Fraud

i. Financial Losses



Identity fraud can result in significant financial losses for individuals and businesses.
According to the FTC, the median loss for identity fraud victims in 2022 will be $450. However, some types of identity fraud can result in much higher losses, such as email compromise and real estate fraud.

> **Sophie Wintrich**
> **Cifas Communications and Policy Manager**
> With the pandemic accelerating digital adoption, and with many still struggling financially, fraudsters continue to use stolen identities to take advantage of individuals and businesses. It's important that everyone takes steps to protect themselves from identity fraud.

ii. Damage to Reputation

An individual or business may also lose their reputation if they are a victim of identity fraud. In addition, businesses that suffer data breaches or other forms of identity fraud may lose customers.

Emotional Impact on Victims

Country	Estimated Financial Losses (in USD)
United States	56 Billion
United Kingdom	5.6 Billion
Canada	1.7 Billion
Australia	1.4 Billion
Germany	1.2 Billion
France	900 Million
Italy	600 Million
Spain	400 Million
China	300 Million
Japan	200 Million

Sources: Javelin Strategy & Research. (2022). 2022 Identity Fraud Study, Cifas. (2022). Fraudscape 2022.

Methods of Identity Fraud

1. Traditional Methods

i. Stealing Physical Documents

As of 2022, identity fraud continues to be a global problem, with prevalence varying across countries.

It remains common for identity thieves to steal physical documents, such as driver's licenses, passports, and social security cards. According to the Federal Trade Commission, identity thieves mainly obtained personal information by stealing wallets and credit cards in 2022.

ii. Dumpster Diving

Another traditional method identity thieves use is dumpster diving, or searching the trash for personal information. In 2022, Identity Theft Resource Center reported that dumpster diving was still a popular way to obtain personal information.

iii. Skimming

Skimming involves reading the magnetic strip on a credit card with a small electronic device called a skimmer. In 2022, identity thieves continued to use skimming, particularly at gas pumps and ATMs.

2. Online Methods

i. Hacking

Hacking involves gaining unauthorized access to computer systems or networks to steal personal information. According to the Identity Theft Resource Center, millions of people's personal information was exposed in 2022.

> **Mark Stanislav**
> **Director of Application Security at Duo Security**
>
> Phishing attacks and social engineering are becoming increasingly sophisticated, and it's important for individuals and businesses to be aware of these threats and take steps to protect themselves.

ii. Phishing

A phishing attack involves sending fake emails or text messages that appear to be from a legitimate source, such as a bank or government agency.

Over 220,000 unique phishing attacks were reported in the first quarter of 2022 alone, according to the Anti-Phishing Working Group.

iii. Social Engineering

A social engineer manipulates people into revealing personal information or performing actions that expose an individual's personal details which can be used for fraudulent purposes.

In 2022, the FBI reported that social engineering attacks were on the rise, particularly involving fraudsters posing as bank representatives and government officials. In 2022, the FBI reported that social engineering attacks were on the rise, particularly involving fraudsters posing as bank representatives and government officials.

> **Aaron Hanson**
> **Senior Security Engineer at NortonLifeLock**
>
> Identity thieves are always looking for new and innovative ways to steal personal information, but traditional methods such as stealing physical documents and dumpster diving are still effective.

Prevention of Identity Fraud

1. Best Practices for Individuals

i. Protecting Personal Information

One of the best ways to prevent identity fraud is to protect personal information.
According to the Federal Trade Commission, identity thieves commonly obtain personal information through social media accounts, so it is essential that individuals be careful about what they share online.

ii. Monitoring Financial and Medical Accounts

Keeping an eye on financial and medical accounts regularly can help individuals catch identity fraud early. According to the Identity Theft Resource Center, monitoring accounts is the most effective way for individuals to catch identity theft.

Jessica Rich

Director Consumer Protection at the Federal Trade Commission

"Monitoring financial and medical accounts is one of the best ways for individuals to catch identity fraud early and minimize the damage."

iii. Responding to Suspicious Activity

Individuals can minimize the damage of identity fraud if they respond quickly to suspicious activity, such as unauthorized charges or medical claims.
According to the Federal Trade Commission, those who reported identity fraud within two weeks had a lower average loss than those who waited longer.

2. Best Practices for Businesses

i. Implementing Strong Security Measures

By implementing strong security measures like firewalls, encryption, multi-factor authentication and face recognition, businesses can prevent identity fraud. According to the Identity Theft Resource Center, businesses with stronger security measures have a lower risk of identity theft and data breaches in 2022.

Is your business looking for a reliable solution to prevent identity fraud in 2023 and beyond?

Take a look at Facia, a leading provider of facial recognition technology with liveness detection.

With cutting-edge technologies like machine learning and facial biometrics, Facia offers a range of solutions to help businesses verify the identity of their customers and prevent fraudulent activity. Our solutions include facial recognition, liveness detection, and document verification, with a 99.99% accuracy rate.

By partnering with Facia, you can improve your company's fraud prevention efforts and comply with Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations. Our cost-effective solutions can also help protect your business's reputation and brand integrity.

ii. Make authentication processes simple and secure

Facia face recognition technology allows for the safest, most convenient authentication process possible.

less tha 1s Response Time

Highly accurate face recognition and biometric authentication. Authenticate anyone's identity in 2 seconds using a selfie

100% Automation

A fully automated facial recognition system.

99.99% Accuracy

First-time authentication is guaranteed with built-in image capture assistance.

99% First-Time Match

First-time authentication is guaranteed with built-in image capture assistance.

iii. Providing Employee Training

Businesses can protect themselves and their customers by providing employee training on identity fraud prevention and security breach response. According to the National Cyber Security Alliance, companies with employee training programs experienced fewer security incidents in 2022.

> **Jamil Jaffer**
>
> **Founder & Executive Director of the National Security Institute**
>
> Providing employees with training on how to prevent identity fraud and how to respond to security breaches is critical for businesses to protect themselves and their customers.

iv. Responding to Security Breaches

Businesses must respond rapidly and effectively to security breaches to minimise identity fraud damage.

> According to Ponemon Institute statistics, a data breach cost $4.24 million on average in 2022, and businesses that respond quickly have lower costs and fewer customer losses.

Legal and Regulatory Frameworks

Current Laws and Regulations

As identity fraud has become a growing concern globally; governments have enacted laws and regulations to address it. The Fair Credit Reporting Act (FCRA) and the Identity Theft and Assumption Deterrence Act (IDTAD) are two major laws in the United States that aim to reduce the prevalence of identity theft and fraud (ITADA). The General Data Protection Regulation (GDPR) was enacted to safeguard EU residents' private information. The Act on the Protection of Personal Information (APPI) in Japan and the Personal Data Protection Act (PDPA) in Singapore are two of the region's privacy regulations.

Future Developments

i. Emerging Technologies

Several new technologies are changing the landscape of identity verification and fraud prevention, including biometrics, artificial intelligence, and blockchain.
Increasingly, companies are adopting biometric authentication methods to replace traditional passwords, including fingerprints, facial recognition, and voice recognition. As AI-powered fraud detection systems become more sophisticated, companies can detect and prevent identity fraud in real-time. In addition to offering a decentralized and immutable method of storing personal information, blockchain technology is also being explored as a potential solution for identity verification.

ii. Changes in Global Regulations

In Global regulations are constantly evolving to keep up with the changing landscape in response to identity fraud, which is growing in popularity. A proposal to create a national identity theft and fraud reporting system is currently being considered by the Consumer Financial Protection Bureau (CFPB). In the proposed system, consumers could report identity fraud incidents to a central database, making it easier for law enforcement to investigate and prosecute fraudsters. Europe is revising the GDPR, including establishing a European Cybersecurity Competence Centre and a single digital identity for all Europeans.

iii. Potential Impact on Identity Fraud Prevention

It is expected that identity fraud will become more effective as new laws and regulations are developed, and emerging technologies are adopted. It is likely that identity fraud will be reduced as biometric authentication and artificial intelligence-powered fraud detection systems are adopted. As a result of the implementation of new laws and regulations, fraudsters will be prosecuted more effectively, and companies will be held accountable for data breaches. In developing new regulations, it is essential to consider the potential impact on privacy and civil liberties of increasing security and protecting individual privacy rights.

Conclusion

As of 2022, identity fraud remains a significant threat, with financial identity fraud posing the greatest danger. Besides traditional and online methods, fraudsters also use other methods to steal personal information, so both individuals and businesses need to take action to stop them. Legal and regulatory frameworks address identity fraud, but emerging technologies and changing regulations may impact future prevention efforts.

Businesses and individuals must take proactive measures to prevent identity fraud. Best practices include securing personal information, monitoring accounts for suspicious activity, implementing strong security measures, and providing employee training.
Furthermore, facial recognition technology with liveness detection can help prevent fraud.

There is a good chance that identity fraud will continue to evolve as technology advances. Nevertheless, there are opportunities for innovative solutions to prevent and detect fraud. Using artificial intelligence and machine learning to prevent identity fraud can increase efficiency and accuracy. Keeping informed and adapting to new developments is essential for individuals, businesses, and regulatory authorities to combat identity fraud effectively in the future.

FREADY TO TACKLE THE IDENTITY FRAUD CHALLENGES OF 2023

REQUEST A FREE DEMO NOW!

Reference:

- Federal Trade Commission. (2022). Consumer Sentinel Network Data Book 2021. https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2021/consumer_sentinel_network_data_book_2021.pdf
- Identity Theft Resource Center. (2022). 2021 Annual Data Breach Year-End Review. https://www.idtheftcenter.org/wp-content/uploads/2022/01/ITRC_2021_End-of-Year-Data-Breach-Analysis.pdf
- Javelin Strategy & Research. (2022). 2022 Identity Fraud Study: Fraudsters Follow the Path of Least Resistance. https://www.javelinstrategy.com/coverage-area/2022-identity-fraud-study-fraudsters-follow-path-least-resistance
- LexisNexis Risk Solutions. (2022). True Cost of Fraud 2022 Study: Global Insights. https://risk.lexisnexis.com/insights-resources/research/true-cost-fraud-2022
- Ponemon Institute. (2021). The 2021 Identity Fraud Report. https://www.onfido.com/resources/whitepapers/the-2021-identity-fraud-report-ponemon-iiinstitute
- Experian. (2022). 2022 Global Identity and Fraud Report. https://www.experian.com/content/dam/marketing/na/global/documents/white-papers/2022-Experian-global-identity-fraud-report.pdf
- Association of Certified Fraud Examiners. (2022). Report to the Nations 2022: Global Study on Occupational Fraud and Abuse. https://www.acfe.com/report-to-the-nations/2022/