State of Fraud 2023

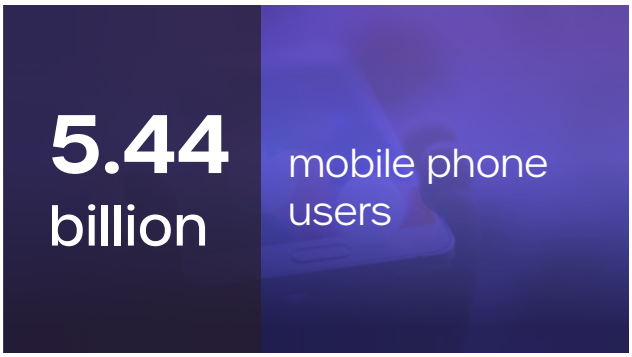
acuant & IDology
GBG companies

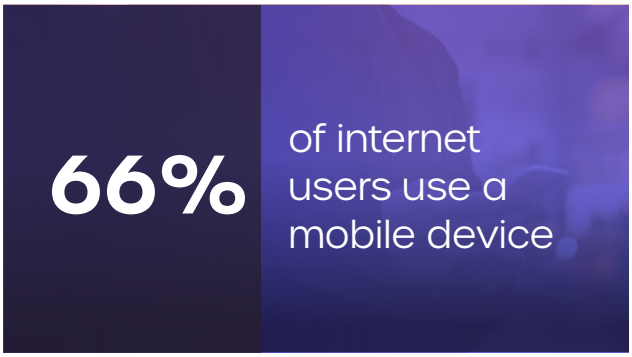
More people online opens the door to fraud

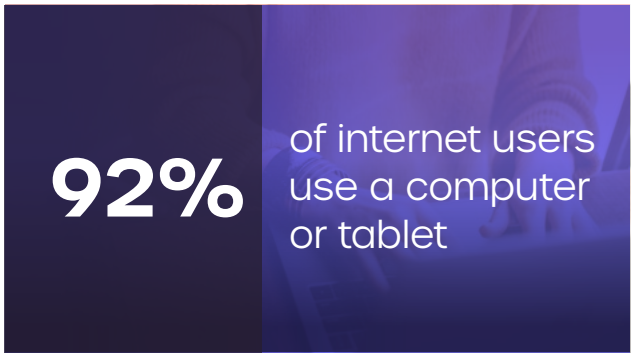
It's estimated that **64.4%** of the world's total population is using the internet, with that number suspected to grow by the end of 2023. With a rapidly evolving digital landscape comes more users, more online services and more fraud.

With the digitalization of services, from digital banking, online dating, telehealth, shared economy apps, eCommerce and more—and fraudsters evolving their methodologies to adapt to advancing technologies—companies must be proactive in their approach to detecting and preventing fraudsters' attempts at fraud, cybercrime and financial crime.

2023 global stats



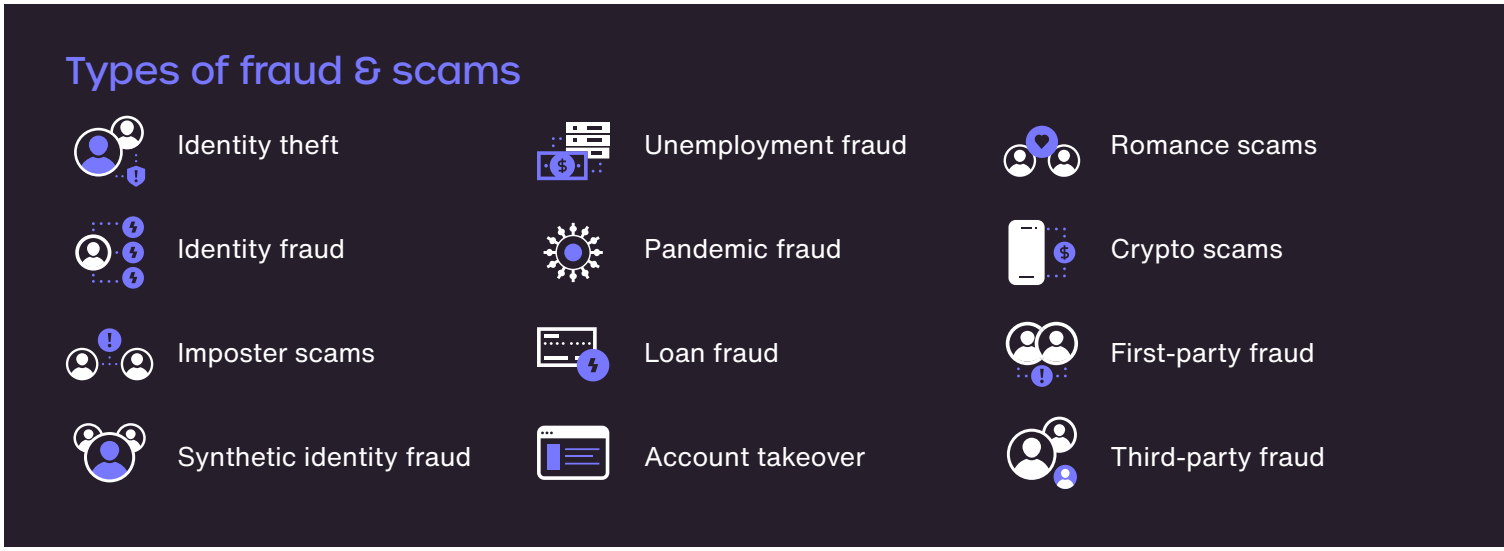




Fraud is still a problem

With more consumers online than ever, there is a wider net for fraudsters to cast when looking to illicitly access and exploit personally identifiable information (PII) for financial gain. And, there has been no shortage of a myriad of successfully executed fraud schemes—allowing fraudsters to get away with billions of dollars.

While some sectors might be seeing minimal year-over-year growth of fraud, the rapidly growing tech industry has seen a big increase since 2020. However, for organizations across industries, fraud continues to be a significant threat and many companies are being affected. A survey found that **46% of companies experienced some form of fraud in the past two years**, with cybercrime and customer fraud being significant contributing factors. Using multi-layered identity verification is essential for effectively preventing and detecting fraud and protecting one's business and customers.



There is no shortage of the different types of fraud and scams that fraudsters are deploying. Some of which includes:

Pandemic fraud: Three years on from the launch of federal and statewide Covid-19 relief programs in the US, it's suspected that between March 2020 and April 2022 at least **$45.6bn worth of unemployment payments** and **$4.6bn small business loans** were improperly paid out to fraudsters.

Synthetic identity fraud: Synthetic identity fraud is considered the fastest growing type of fraud and continues to be an issue.

- **70% of fraud executives** agree that **synthetic identities are a bigger challenge than traditional identity theft**.
- **23% of businesses** see **synthetic identity fraud as the most prevalent fraud scheme** in their industry.
- Synthetic identity fraud for unsecured US credit products resulted in **losses of $1.8bn in 2020**, with **losses expected to reach $2.94bn in 2025**.

Romance scams: In 2022, nearly **73,000 people** in the US **lost more than $1bn to romance scams**. And with **323 million people worldwide** using online dating apps, romance scams continue to be a significant and costly threat.

Cyberattacks threaten privacy

PII and other sensitive data continue to be extremely at risk and a prime targets for cybercriminals. Phishing, ransomware, data breaches and more have become a common occurrence across all industries—there were over **1,802 data-related compromises in 2022 for organizations in the US, impacting more than 422 million people,** and phishing attacks continue to be the top vector of attack. In fact, Q3 of 2022 was record-breaking for the number of global attacks in a single quarter: **1.27+ million total phishing attacks** in that short period of time.

Following cybersecurity best practices and having the protective protocols and policies in place to protect data and prevent illicit access, continues to be increasingly important.

1,802 data-related compromises in the US in 2022, impacting **422+ million** people

2022 saw a **38% increase** in global cyberattacks over 2021

1.27+ million total phishing attacks in Q3 of 2022

83% of organizations have been **breached more than once**

The average cost of a critical infrastructure breach is **$4.82m**

Types of cyberattacks

- Phishing
- Smishing
- Spoofing
- Ransomware
- Malware
- Password attack
- Social engineering
- Account takeover fraud
- Business email compromise
- Data breaches
- Data leaks

Data privacy becomes more of a focus

More states are implementing their own data privacy legislation as part of efforts to secure and protect PII and other sensitive data. In addition to focusing on the ramifications of cybercrime, the laws focus on restrictions when it comes to the handling and sharing of consumer data.

The difficulty for businesses in the US arises in the lack of a federal initiative—differing laws across state lines requires companies to stay up to date on evolving legislation in different states to avoid jurisdictional noncompliance and potential hefty fines. And more, for companies that operate globally, privacy on a national scale is not enough: compliance with international data privacy legislation like the EU's GDPR is also required.

5 states with comprehensive data privacy laws

Colorado | California | Virginia | Utah | Connecticut

> In 2022, **29 states considered comprehensive consumer privacy bills,** out of a total of 39 states since 2018

The state of global privacy laws

44	26	33	34
countries with legislation	countries with legislation	countries with legislation	countries with legislation
Europe	Americas	Africa	Asia-Pacific

The exploitation of crypto

While the volatile crypto market fluctuated throughout 2022 for a variety of reasons, the continued popularity of cryptocurrency has resulted in the industry being a prime target of exploitation. This includes, but is not limited to, the FTX money laundering and bankruptcy scandal that resulted in **the loss of an estimated $1-2bn** of contributors' crypto investments.

According to the FTC, at least **46,000 Americans have been scammed out of an estimated total of $1bn** worth of cryptocurrency since the beginning of 2021. **Crypto scams netted fraudsters $329m** from Americans in the first quarter of 2022 alone, with an estimated **$4.3bn crypto stolen** in the first eleven months of 2022.

46,000 Americans scammed out of **$1bn** worth of cryptocurrency since 2021

Over **$4.3bn crypto stolen** in 2022

Types of crypto scams

- **Investment-related fraud**
- **Romance scams**
- **Business imposters**
- **Government imposters**
- **Social media scams**

While the cryptocurrency industry is not as heavily regulated as other financial industries, this is changing. Regulators around the world have not only increased scrutiny on the crypto marketplace but are also enforcing new regulations as part of widescale Anti-Money Laundering (AML) efforts.

About Acuant + IDology

Acuant and IDology, GBG companies, deliver the industry's most comprehensive suite of identity verification and AML/KYC solutions to help businesses drive revenue, deter fraud and maintain compliance.

Dynamic and configurable workflows make verification as simple as possible for your business. Leverage thousands of diverse data sources, leading technology and orchestration that is powered by human assisted machine learning to give you the best, most trusted and transparent results—every time.

Regardless of your industry or location, our solutions can be implemented quickly to deliver first-class online experiences and verify the identity of almost anyone, anywhere in the world, at any time. Onboard more legitimate customers faster and with confidence.

acuant & IDology
GBG companies

acuant.com | idology.com

Sources

Page 2 | More people online opens the door to fraud

DataReportal (February 2023), *"Digital 2023: Global Overview Report"*

Page 3 | Fraud is still a problem

PWC, *"PwC's Global Economic Crime and Fraud Survey 2022"*

CNN, *"Pandemic unemployment benefits fraud may top $45 billion, federal watchdog says"*

GBG, *"The State of Digital Identity 2022"*

Aite-Novarica Group, *"Aite-Novarica Group survey of 46 financial services fraud executives, September 2020"*

Aite-Novarica Group, *"Synthetic Identity Fraud, Solution Providers Shining Light Into the Darkness: June 2022"*

Comparitech, *"Nearly 73,000 Americans lost more than $1 billion to romance scams in 2022"*

Page 4 | Cyberattacks threaten privacy

Identity Theft Resource Center, *"2022 Data Breach Report"*

CRN, *"The 10 Biggest Data Breaches Of 2022"*

Check Point Research, *"Check Point Research Reports a 38% Increase in 2022 Global Cyberattacks"*

APWG, *"Phishing Activity Trends Report: 3rd Quarter 2022"*

Security Magazine, *"$4.35 million — The average cost of a data breach"*

Page 5 | Data privacy becomes more of a focus

IAPP, *"Privacy Matters in the US States (2022 Wrap-Up Infographic)"*

UNCTAD (February 2023), *"Data Protection and Privacy Legislation Worldwide"*

Page 6 | The exploitation of crypto

FTC, *"Reports show scammers cashing in on crypto craze"*

Privacy Affairs, *"Cryptocurrency Scams in 2022 – Statistics & Trends"*