STATE OF IDENTITY FRAUD REPORT

2024

2024 EDITION

A look into the most prevalent fraud tactics, data insights, and future-proof technologies to combat fraud.

AUTHENTICID

This might sound familiar: fraud was on the rise in 2023. The trend doesn't show any sign of slowing, and identities have never been both more valuable and more difficult to protect.

Our 2024 report is full of the latest fraud trends, tactics, and technologies. Plus, we are providing valuable insights from both business leaders and consumers in the realms of identity fraud, business challenges, and technology adoption.

Identity Fraud Report provides a pulse check for business and consumer identity fraud and identity verification sentiments as well as a look ahead at the threats and technology that will make a big impact in the coming year.

ABOUT OUR DATA

This report includes internal proprietary data anonymized and analyzed from our platform's identity verification, biometric authentication, and watchlist technology and processes. Plus, insights from our annual fraud surveys conducted in Q4 2023. Our business survey included responses from 103 fraud fighters and technology professionals in the financial services, telecom, retail and gaming industries. Our consumer survey includes insights from 455 respondents in North America.

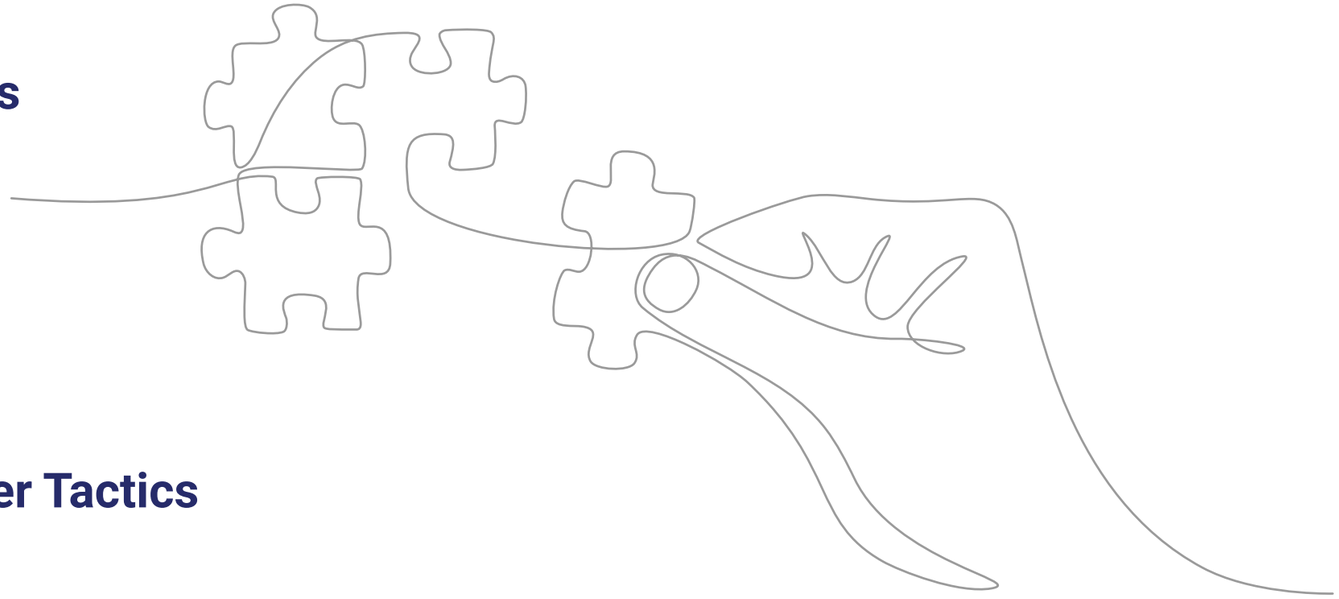
Created in Partnership with PEAK iDV

PEAK iDV

Steve Craig
Founder & Chief Enablement Officer

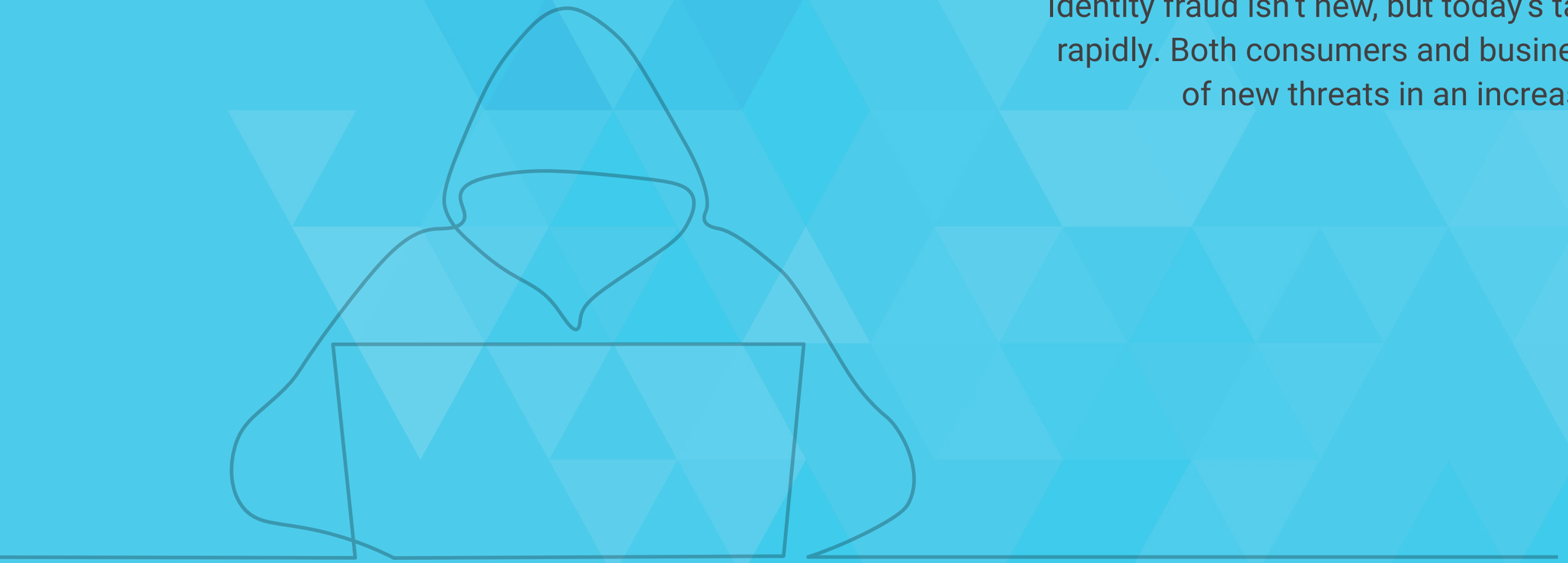
Steve Craig is an independent expert in digital identity and has worked in the technology industry for over 20 years. Prior to founding PEAK iDV, Steve held leadership positions at three top companies in identity verification across roles in product, strategy, and sales. PEAK iDV is a community-powered learning hub that enables providers, practitioners, and investors to level up their knowledge and expertise in the rapidly changing digital identity industry in topics ranging from identity verification, artificial intelligence, biometrics, fraud, regulatory compliance, and more.

CONTENTS



THE LATEST
FRAUD EVOLUTIONS

Identity fraud isn’t new, but today’s tactics are changing rapidly. Both consumers and businesses face a variety of new threats in an increasingly digital world.



HIGHLIGHTING THE TOP FRAUD TRENDS FOR 2024

Consumers and businesses alike are facing new challenges in today's digital existence, from considering the ramifications of digital identity to grappling with the use and prevalence of new tools like generative AI. In the meantime, the explosion of AI has also pushed identity fraud into a new frontier that will become a potential global shift in the coming year.

Identity crime has led to record levels of breaches and business attacks, and consumer identity fraud is growing at an alarming rate. In fact, it's predicted that in 2024, cybercrimes will cost the world **$9.5 trillion**.[1] At this critical juncture, it's time to take a strategic look at taking control of identity, technology, and shifts in consumer behavior to stop the global identity fraud crisis.

Businesses reporting growth in **data and security breaches** from 2022 to 2023[2]

Consumers who had their **personal information exposed** in 2023[3]

[1] "Cybercrime To Cost The World $9.5 Trillion USD Annually In 2024," Cybercrime Magazine, October 2023
[2] AuthenticID Consumer Fraud Survery 2024
[3] AuthenticID Consumer Fraud Survery 2024

IDENTITY-BASED FRAUD

Long gone are the days of poorly made fake IDs. Today, identity-based fraud is sophisticated, difficult to detect, and scalable by bad actors.

16% Increase in fraudulent IDs detected by AuthenticID technology compared to 2022.

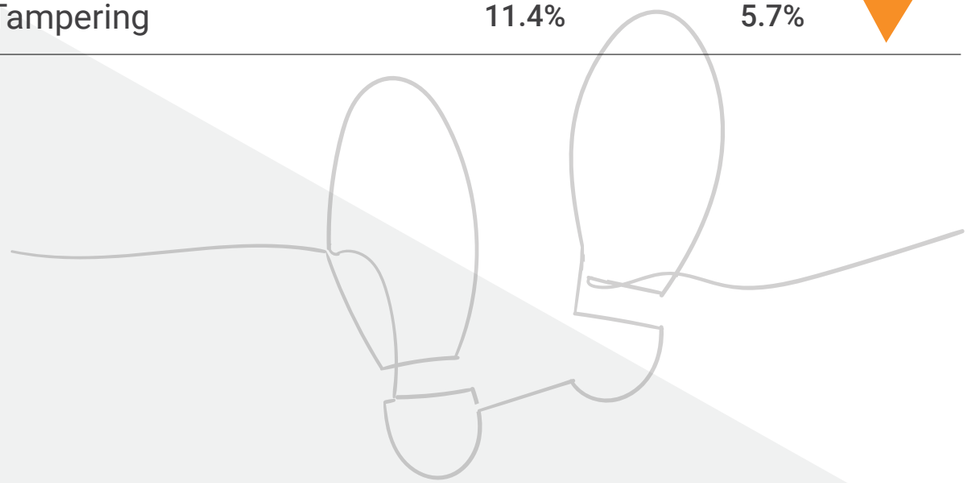
68% of people said the threat of identity fraud and scams impacts how they make purchases, open accounts, and do business.

Stealthy Progress: IDs Get More Sophisticated

In 2023, the explosion of AI tech didn't just make it hard to discern if something was written by ChatGPT. It gave the same cutting-edge abilities to fraudsters who now use AI to create fake IDs seamlessly, with convincing, computer-generated or stolen headshots and nearly undetectable document composition. As a result of advancements in fake IDs, companies like AuthenticID must stay ahead of fraudsters who use the latest technology to steal identities, whether by authenticity checks, liveness detection, anti-spoofing technology, and more.

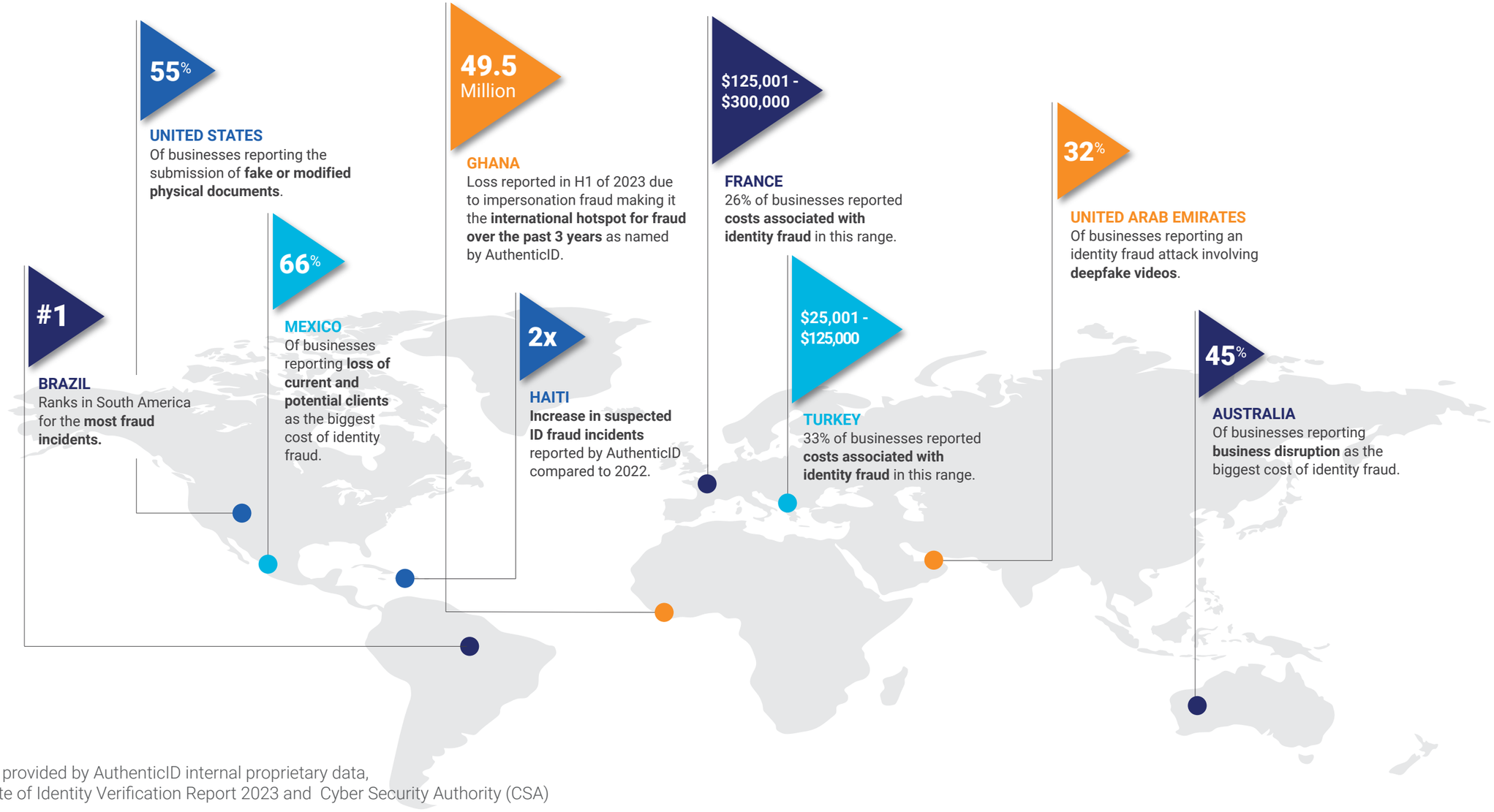
Trends of Identity Fraud Attacks at AuthenticID[4]

	2022	VS.	2023	
Fraudulent Biometrics Detected	5.4%		15.3%	▲
Headshot Manipulation	10.5%		8.8%	▼
Material Analysis (Paper or Digital Screen Detection)	63.4%		69.1%	▲
Barcode Manipulation	14.3%		16.0%	▲
Text Tampering	11.4%		5.7%	▼



[4] AuthenticID Internal Data Fraud Analysis from 2023

THE GLOBAL IMPACT OF IDENTITY FRAUD



* Datapoints provided by AuthenticID internal proprietary data, Regula State of Identity Verification Report 2023 and Cyber Security Authority (CSA)

SPOTLIGHT: Synthetic Fraud Continues to Change

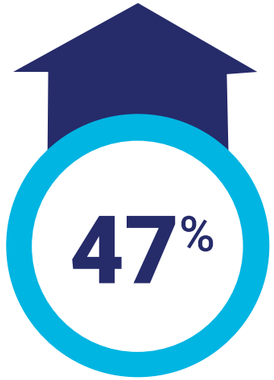
Over the past several years, synthetic identity fraud– those synthetic identities that are created via a combination of personally identifiable information (PII) of one or more real people with false information, which can include data created by generative AI–has skyrocketed.

How it's changed

Today, synthetic fraud has exploded with the proliferation of generative AI, as well as the impact of bad actors in the credit repair industry: a small but mighty number of unscrupulous companies will convince individuals in debt to functionally erase a bad credit history and create a new identity using "credit profile numbers," unissued Social Security numbers or someone else's Social Security number.

In addition, these synthetic identities are used for attacks on DDAs (demand deposit accounts) as well as savings and investment accounts. Retail banks and fintechs are at special risk as bad actors have increasingly focused on synthetic fraud in lending.

With an increase in data breaches, the pool of stolen data will only allow synthetic fraud to continue to grow. The growth has also fueled the rates of other fraud types, including account takeovers. Last year, account takeover comprised more than **one-third** of all fraudulent activity reported to the FTC.[5]



Businesses reporting growth in **Synthetic Identity Fraud** in 2023

Synthetic Identity Fraud comprises 85% of all identity fraud cases

[5] "Consumer Sentinel Network Data Book," FTC, February 2023
[6] AuthenticID Consumer Fraud Survery 2024
[7] "Credit Repair Firms Driving $20B Synthetic ID Fraud Crisis," BankInfoSecurity, November 9, 2023

AI GENERATED FRAUD

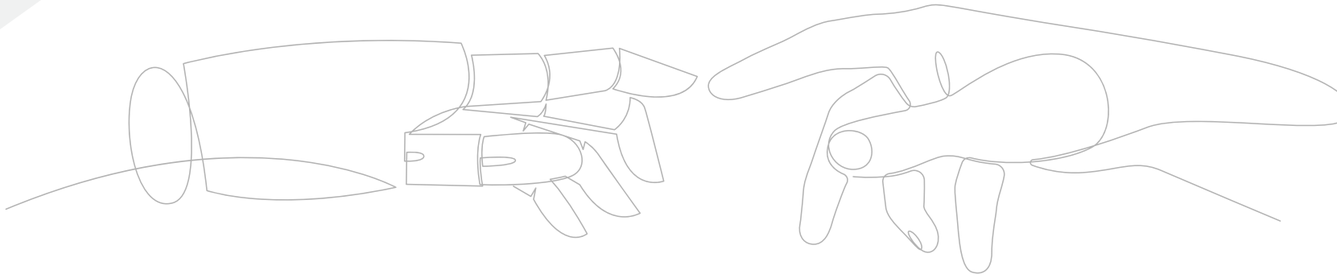
Can you spot the fakes?

Here are six headshots created with generative AI tools.
Five are fake. One is real. ***Can you figure it out?***

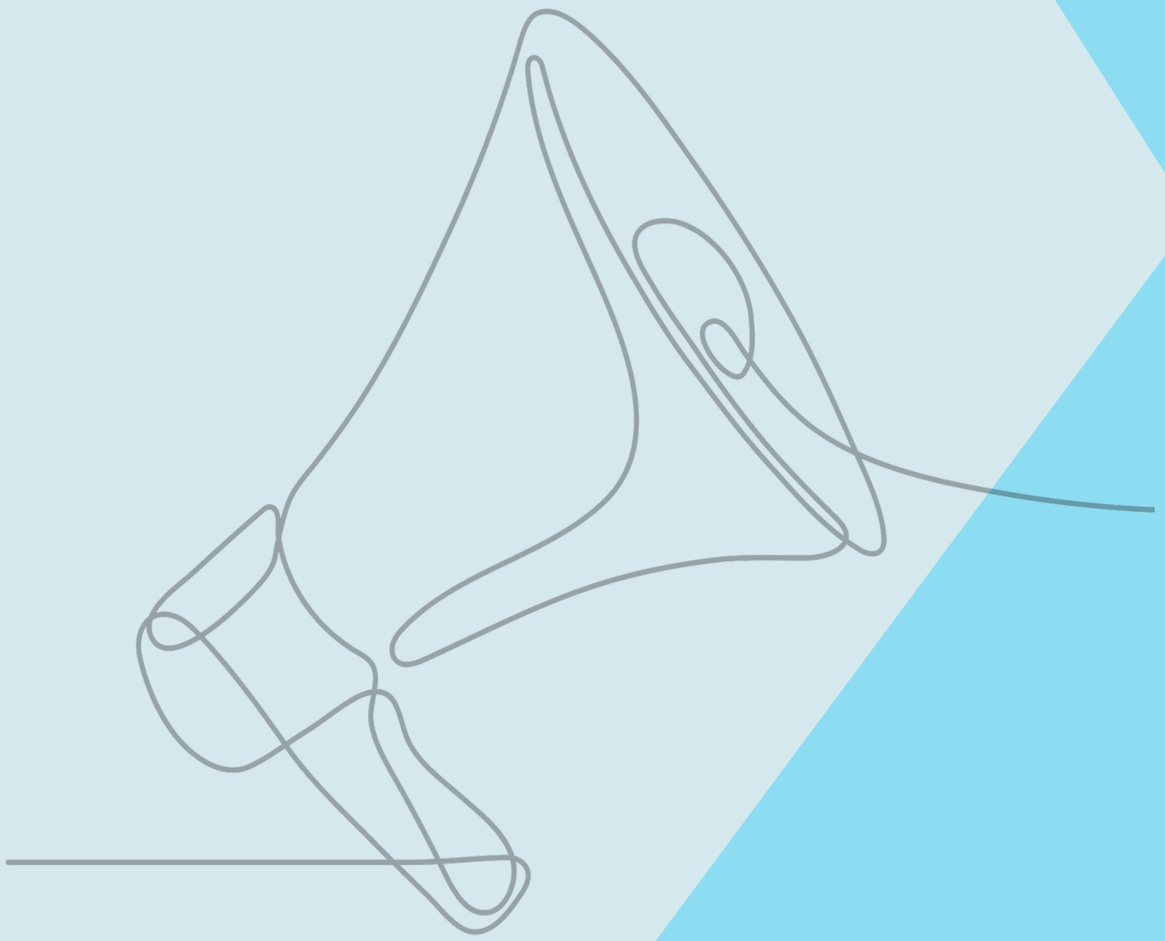
(Find the answer on page 35)

Deepfake & Generative AI Technology

Knowing that someone is truly real has never been harder, which leaves the door open for fraud. These technologies can be used for nefarious purposes, including blackmail, harassment, and identity fraud. A powerful tool for fraud, especially social engineering, and synthetic identity fraud, AI can be used to generate images, synthesize voices, and customize an identity based on publicly available data and dark web information. Such realistic deep fakes aren't expensive for bad actors to make, and they can be catastrophic for victims.



SPOTLIGHT: How Authorities, Regulators & Businesses Respond to AI



With AI-powered fraud escalating, some think tanks are predicting that police will make the first arrest of an individual for using AI to impersonate someone in 2024.[8] In the meantime, governments worldwide are grappling with how best to legislate the technology while it is still quickly evolving. Identity fraud is a key focus for the U.S. government, with 2023 hearings spilling over into 2024 as conversations continue.

New AI Regulations in EU and China: The Artificial Intelligence Act (AI Act) was introduced in the European Union in December 2023. The regulatory framework aims to make sure AI systems are safe and respect the fundamental rights of people and businesses. The legal framework is based on four levels of risk: minimal risk, high risk, unacceptable risk, and specific transparency risk. Oversight and regulations is specific to the category the AI system falls under.

Furthermore, the Cyberspace Administration of China (CAC) released Generative AI regulations in April, 2023.

Fraud Fighting Tip

Fight AI fraud threats with more AI: When authenticating users, liveness detection can distinguish between genuine human motions and interactions versus those being performed by a bot or AI. Liveness detection can also detect injection attacks during the verification process.

[8] "'We Think It's Overhyped': AI Is in For a Humble Reality Check in 2024, Analysts Say," Entrepreneur, Published October 11, 2023

REAL-TIME FRAUD, REAL-TIME PAYMENTS

Popular with consumers, real-time payments are now commonly used by many large financial institutions as well as fintechs and other apps. Customers enjoy a nearly friction-free experience. But instant transactions leave little time for institutions to detect fraudulent purchases and activity, and their lack of reversibility poses an issue when fraudulent activity occurs. As a result, authorized push payment (APP) fraud has grown. In APP fraud, bad actors use traditional hacking and/or social engineering methods to pose as a legitimate payee in nearly instantaneous fraud.

Fraud Fighting Tip

To stop real time fraud, monitoring (including behavioral biometrics and analytics), setting transaction limits, machine learning models that can spot irregular behavior, as well as creating watchlists for bad actors, must all work in tandem. As with most fraud types of today, there is no silver bullet to solve it, and a variety of agile tools are required.

Annual Growth Projections for real-time payment transactions

63%

$511 billion

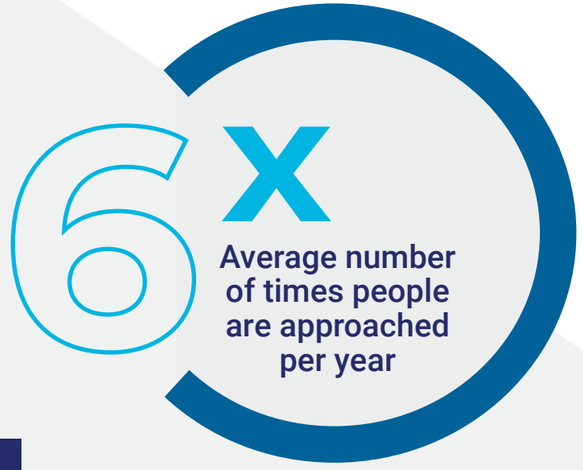
Growth Prediction by 2027 [9]

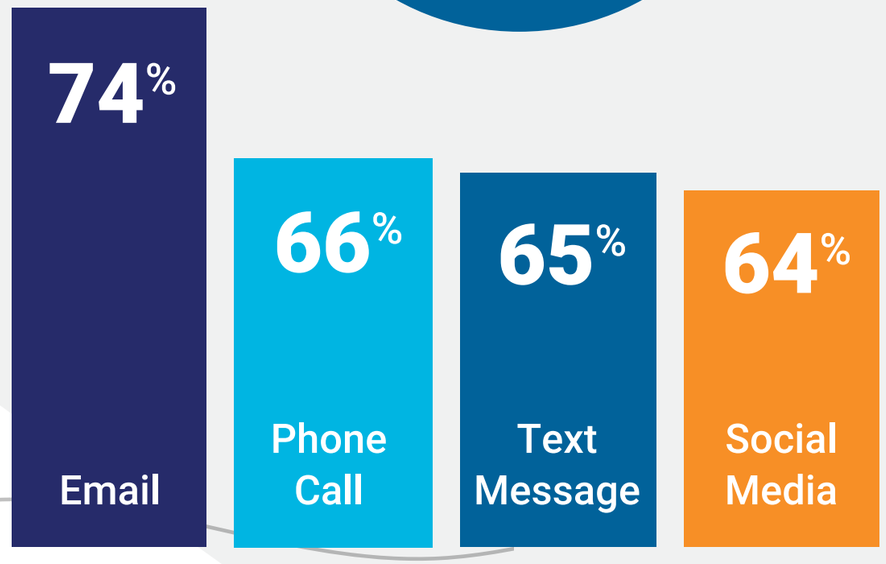
[9] "Prime Time for Real-Time Global Payments Report," ACI Worldwide, Published 2023.

SOCIAL ENGINEERING ATTACKS

A traditionally-used identity fraud method, social engineering is increasingly complex, multi-layered, and reliant upon spoofing.

Nearly all of us have experienced a social engineering attack, probably even within the last year, most likely via phishing across a variety of channels: email, text messages, and robocalls. Today, these attempts are getting more difficult to discern, and are often automated by bad actors, leading to an even more widespread impact.





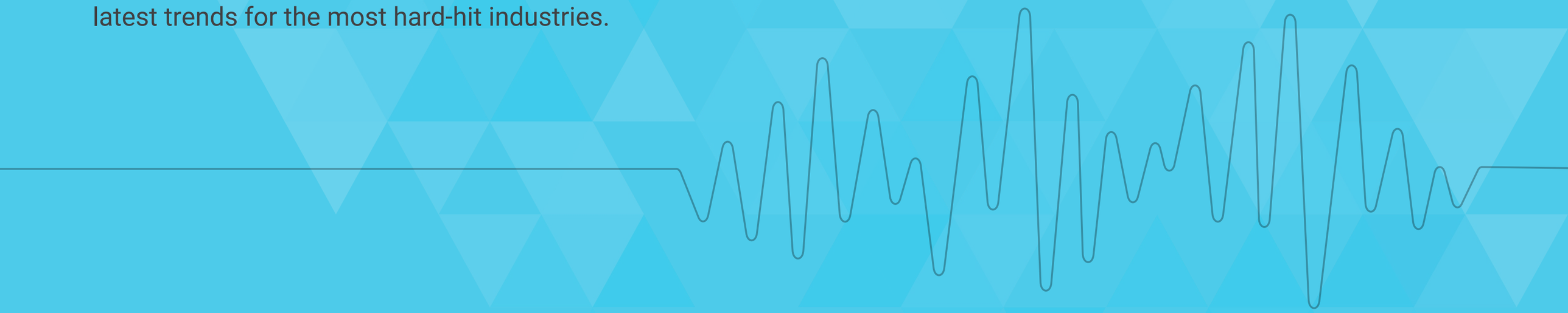
How Fraudsters are Targeting Consumers in 2023[10]

[10] AuthenticID Consumer Fraud Survery 2024

FRAUD TRENDS

BY INDUSTRY

While no industry escapes the threat of identity fraud, several industries remain at particularly high risk for both customer information and sensitive company data. Bad actors attack at various points of the customer journey, from account creation to re-authentication. Here are the latest trends for the most hard-hit industries.



FINANCE

Identity fraud in finance skyrocketed in 2023, and the trend shows no sign of slowing, even as consumers expected high levels of security from their banking partner.

HOW FINANCE IS FIGHTING BACK

Data. Data use across the customer journey, including device recognition and image verification will slash fraud in real-time.

Biometrics can prevent some of the most commonly seen fraud types in the financial sector, including account take-over (ATO) and card not present (CNP) fraud. The banking sector is set to see the **largest number of identity verification checks in 2024 at 37 billion**.[11]

Quick hits on top threats

Synthetic Fraud hits the financial sector the hardest, and it's the fastest-growing fraud type in that sector.

Personalization

AI has made phishing schemes to get financial information from consumers more convincing than ever before due to the ability to craft and customize deceptive messages.

Lending threats are growing

The large bank of stolen/breached PII is a ticking time bomb for most citizens. Two particular industries are also poised for a huge fraud break-through. **Auto loan fraud increased over 38%** in the past year and has been on the rise for the past three years, partially due to higher credit limits and easier means to secure loans online.[12] In addition, organized crime has hit mortgages, with publicized cases of mortgage fraud in cities like Toronto, with over $200 million in fraud claims in just two years, a new phenomenon.[13]

Consumers reporting they had their **credit card or payment information exposed** in 2023. **30%**

Consumers reporting that **keeping personal information safe** is extremely important to them when choosing a financial instrituion. **56%**

[11] "70bn Digital Verification Checks in 2024 To Combat Rise in Fraud," DigitNews, Published October 2, 2023
[12] "Auto Lending Industry Is New Frontier for Synthetic ID Fraud," BankInfoSecurity, Published September 11, 2023
[13] "How organized crime has mortgaged or sold at least 30 GTA homes without owners' knowledge," CBC, Published January 23, 2023

TELECOMMUNICATIONS

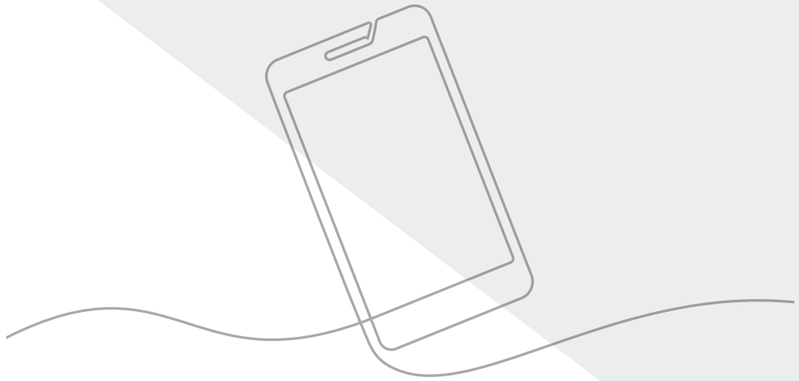
In today's digital world, telecommunications is integrated with a variety of sectors, interconnecting people, organizations, and industries. The telecommunications industry remains a massive target of fraud, with phones' use for two-factor authentication a lynchpin for fraud vectors.

FRAUD TRENDS

SIM Swapping continues to impact the industry, with more organized crime rings prosecuted for this each year. Because SIM swapping relies on successfully tricking a telecom employee into switching a victim's account onto a card the fraudster owns, the use of AI is also a factor in successful impersonations of IT staff or customers..

Application-to-Person (A2P) Fraud is on the rise. Fraudsters use grey routes (when an SMS text is sent through a "backdoor" route at some point on its journey, rather than a route sanctioned by mobile operators) to deliver an SMS and avoid termination fees. Bad actors also use artificial inflation of traffic (AIT) in the form of spam messages to lure individuals to exploit billing gaps

Subscription Fraud drives much of the fraud now seen in telecommunications, both in terms of credit mules and applications, corresponding with both a global downturn in economic conditions as well as new technology and digitization.

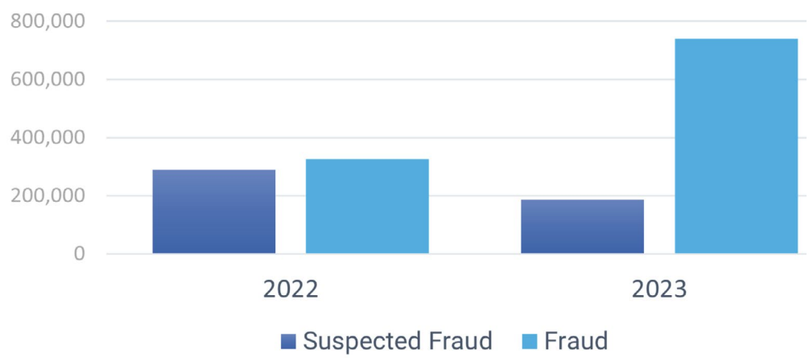


927K = **$4 billion**

Counterfeit IDs Stopped in 2023 for AuthenticID Telecom Customers

Savings in Estimated Fraud Loss Based on Average Cost Per Incident

Year-over-Year Comparison, AuthenticID Telecom Customers



* Datapoints provided by AuthenticID internal proprietary data.

OTHER INDUSTRIES OF NOTE

GIG & SHARING ECONOMY

Nearly **1 in 4 Americans** have been victimized by identity fraud while using these platforms and services.[14] What's more, there are over a billion gig workers – a huge industry with fraud prevention that is not yet mature.

FRAUD TRENDS

Business is booming, and so is fraud: With continued shifts in consumer behavior toward the gig and sharing economy, it's no surprise fraud is increasing, with **payment fraud** once again the top fraud type.

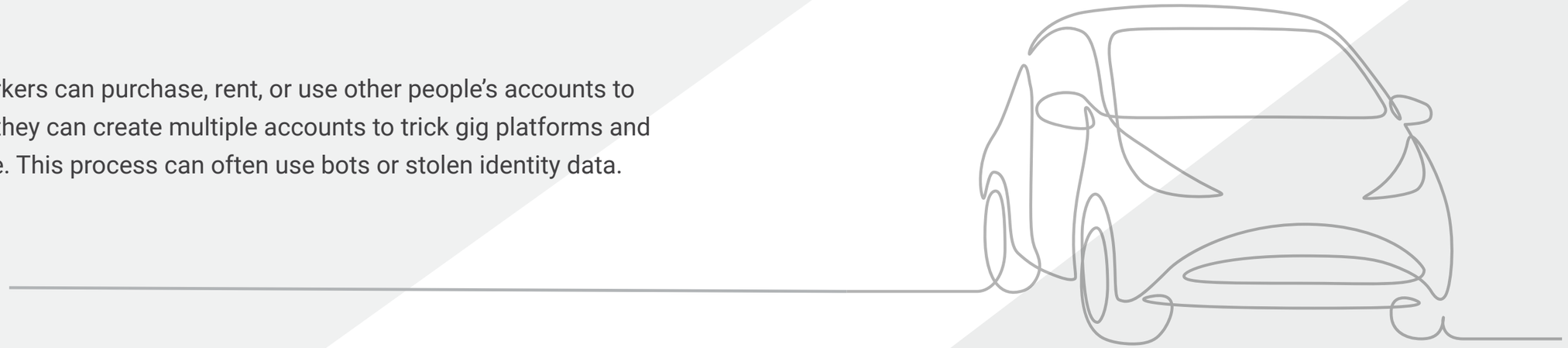
Account Fraud

Unscrupulous workers can purchase, rent, or use other people's accounts to get more gigs, or they can create multiple accounts to trick gig platforms and gain an advantage. This process can often use bots or stolen identity data.

ON THE HORIZON

Better Identity Verification Needed

Over **28% of people** say biometric authentication would make them feel safer using these platforms, and with the current proliferation of fraud, the industry will need to shift toward better identity verification methods in 2024.



[14] 2023 U.S. Gig Economy Report, Transunion, Published October 4, 2023

RETAIL / eCOMMERCE

Online shopping and payment platforms continue to grow, and with that growth comes escalating fraud risks.

> Bad actors infiltrate both small and large businesses regularly, resulting in billions of dollars in losses for retailers each year.
>
> – Blair Cohen for Total Retail, July 2023 [15]

TOP THREATS

Synthetic Shoppers

Synthetic fraud has hit the retail industry hard, and in retail, it takes a new twist. A synthetic identity can use a real, stolen credit card purchased via the dark web to attach to this new identity, hoping to bypass retailers' controls.

Buy Now, Pay Later (BNPL) Fraud

With over **45 million** people using Buy Now, Pay Later in the US alone, it's no surprise it's a huge fraud target. And as the payment method is still evolving, regulations are not as robust as they are for other payment methods just yet, leading to yet another golden opportunity for bad actors.

Return Fraud

Nearly half of returned transactions are fraudulent, with some returns being actual stolen goods returned to get a full refund with no receipt.

ON THE HORIZON

Real-Time Detection

eCommerce moves quickly due to customer demand for seamless transactions, and as such, retailers must deploy advanced AI identity verification, payment card verification, and machine learning models to ensure detection at the speed of fraud.

[15] "Fraud is Taking a Financial Toll on the Retail Industry," Total Retail, Published July 20, 2023

GOVERNMENT

Identity fraud and tax and benefit fraud are still rampant in local, federal, and state governments, even after the Covid-19 pandemic saw record numbers of relief-specific schemes.

In fact, the true cost of Covid-19 fraud still is debated, and the estimated number continues to rise.

TOP TRENDS

Tried and True

Benefits and tax fraud remain huge issues to people's identity, with continued high rates of fraud in these programs.

Document Tampering

Like most industries, tools like generative AI mean forging documents has never been easier for fraudsters- leading to an uptick in fraud in other categories.

ON THE HORIZON

A Push Toward Coordination

A recent Pandemic Response Accountability Committee report found that a critical vulnerability was the lack of a centralized entity to assist victims of identity crime involving government programs. The committee is working with Executive Branch officials and Congress to find a solution.

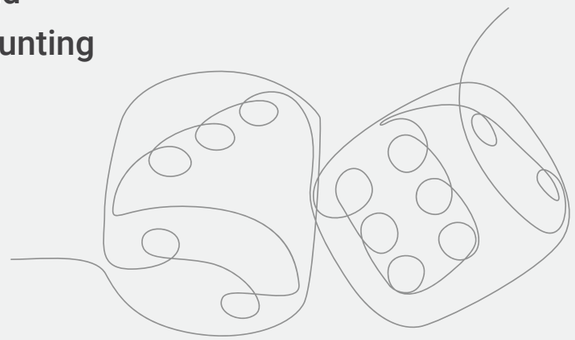
Digital Licenses

As more identity thieves target licenses, the push toward digital licenses and IDs has never been more relevant, with a number of states looking to implement the process in the coming years.

GAMING & GAMBLING

FRAUD TRENDS

- ✓ Multiple Accounts Fraud
- ✓ Gnoming or Multi-accounting
- ✓ Bonus Abuse
- ✓ Credential Stuffing



ON THE HORIZON

AML Matters

Gaming and gambling operators must abide by anti-money laundering regulations, and with an increase in identity fraud threats from bad actor groups, the costs of not abiding by regulations have been high. In 2023, Australian courts approved a **$300 million fine for a casino operator** for breaking AML laws.[16]

Age Verification

In the US and abroad, governments are considering implementing regulations to ensure operators can verify the age of an individual, not just to combat fraud, but to combat unauthorized access or purchase by minors, as well as human trafficking risks.

[16] "Australia court approves $300 million money-laundering fine for Blackstone's Crown Resorts," Reuters, Published July 11, 2023

HEALTHCARE

With some of the most valuable information on the dark web- personal health information (PHI) – healthcare remains a huge target for fraud.

FRAUD TRENDS

Medical Identity Theft

A perennial problem, medical identity theft has also escalated via new tactics. In one such tactic, bad actors can not just target your personal information, but also can target your coverage, while you foot their medical bills.

Phishing

In 2023, new warnings arose about the growth in smishing, or phishing via SMS text, that targeted hospitals and healthcare.

Data Breaches

The demand for high-value health records and medical information continues to drive attacks on healthcare systems.

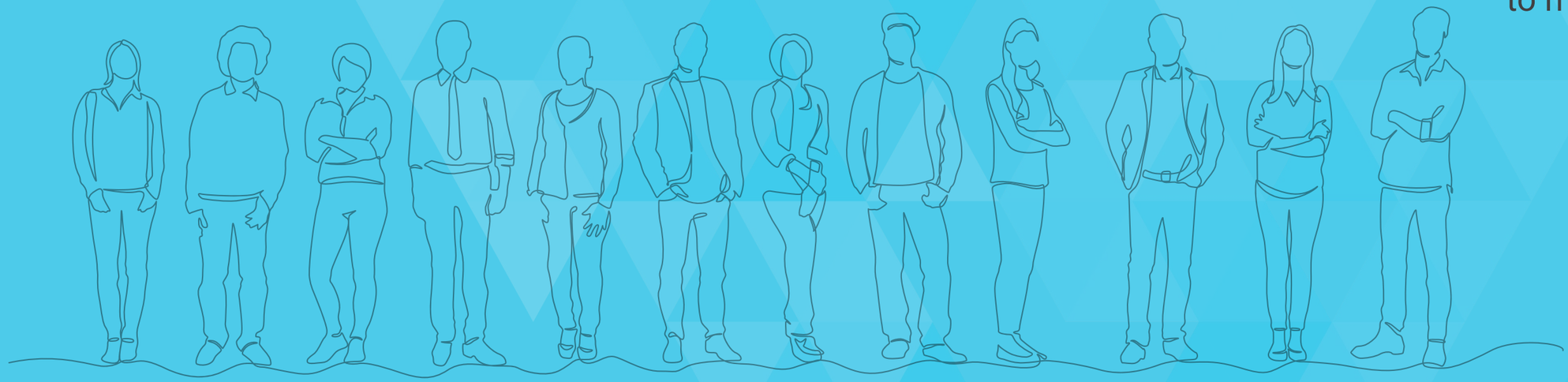
ON THE HORIZON

Better Authentication, Better Experience: The continued growth of telemedicine and virtual access of medical records has also corresponded with patient demand for a smooth experience with the highest security levels for sensitive data. As such, a continued push toward multi-layered verification techniques will help curb some fraud threat trends.

TOOLS OF THE TRADE:

FRAUDSTER TACTICS

The category of fraudsters includes individual actors, organized crime syndicates, and everything in between. For fraudsters of any level, identity theft can be a lucrative and, in a digital world, a nearly faceless crime. The people who commit fraud have the opportunity to make big money.



ORGANIZED CRIME CONTINUES TO DRIVE FRAUD

For crime syndicates both in the US and worldwide, identity fraud is a big business and often funds a variety of other nefarious activities, including human trafficking.

The reach of organized crime is vast and growing: in one 2023 case, a Chinese crime gang targeted Texas driver's licenses: taking stolen information from the deep web, allowing them to correctly answer security questions and successfully obtain replacement licenses. As a result at least 4,000 fraudulent accounts were created and 2,400 licenses were shipped to third-party address, according to the Texas Department of Safety.

ORGANIZED CRIME GROUPS IN THE SPOTLIGHT

A number of organized hacking groups made headlines in 2023, using techniques like SQL injections and malware to exploit vulnerabilities in a number of high-profile attacks.

Scattered Spider

A collective operating out of Russia, Scattered Spider uses techniques like social engineering, phishing, MFA fatigue, and SIM swapping to target large organizations. Active since at least 2022, the collective has targeted identity credentials from companies like Okta, MailChimp, DoorDash, and successfully attacked MGM Casino and Caesars Entertainment.[17]

GambleForce

Based in the Asia-Pacific region, this group exploits CMS (content management systems) of gambling, government, retail, and travel businesses to steal credentials. Using open source tools and SQL injections to bypass authentication measures, GambleForce successfully accessed data from a number of global organizations.[18]

Charming Kitten APT

This Iranian hacking group has targeted government, defense, military, and diplomacy systems with a new strain of malware and by employing social engineering, including impersonating US officials.[19]

FIN8

Active since 2016, FIN8 deploys ransomware through a backdoor and is constantly evolving. Financially motivated, FIN8 resurfaced after a hiatus with updated backdoors and malware.

[17] "FBI shares tactics of notorious Scattered Spider hacker collective," Bleeping Computer, Published November 16, 2023
[18] "New Threat Actor Uses SQL Injection Attacks to Steal Data From APAC Companies," Security Week, Published December 14, 2023
[19] "Top 5 Notorious Cyber Threat Groups Making Headlines," SISA, Published July 2023

TOP TOOLS USED BY FRAUDSTERS

Fake customers, real threats. As these tools continue to grow and hone skills with the use of a greater number of data sets, the threats will continue to become both more sophisticated and faster as bad actors can scrape personal information at record speed. What's more, AI allows fraudsters to better personalize their schemes. Black hat AI tools like WormGPT are now readily available.

The Dark Web

The Dark Web is a treasure trove for bad actors: stolen PII, hacked account data, credit card information, medical information, government data, and even fake IDs are available anonymously, for a price. Any individual's personal information is worth around $1,000 on the dark web.

Fraud as a Service (FaaS)

Identity fraud is so large that bigger crime syndicates can specialize in a particular part of identity theft crimes and still make substantial sums of money. Larger groups sell products or services related to identity fraud, including stolen personal information or account information, pre-made synthetic identities, or even deep fake or phishing kits to lone actors or smaller groups.

Generative AI & Deep Fakes

Knowing someone is real has never been harder due to the increased use of generative AI, which allows fraudsters to spoof headshots, videos, and even the voices of real individuals.

Convincing Fake Profiles

The result of a wide array of tools and dark web-housed personal and business information means that fake profiles – ranging from social media profiles to phony businesses to fake websites – are even harder to detect for many consumers.

Location Masking Tools

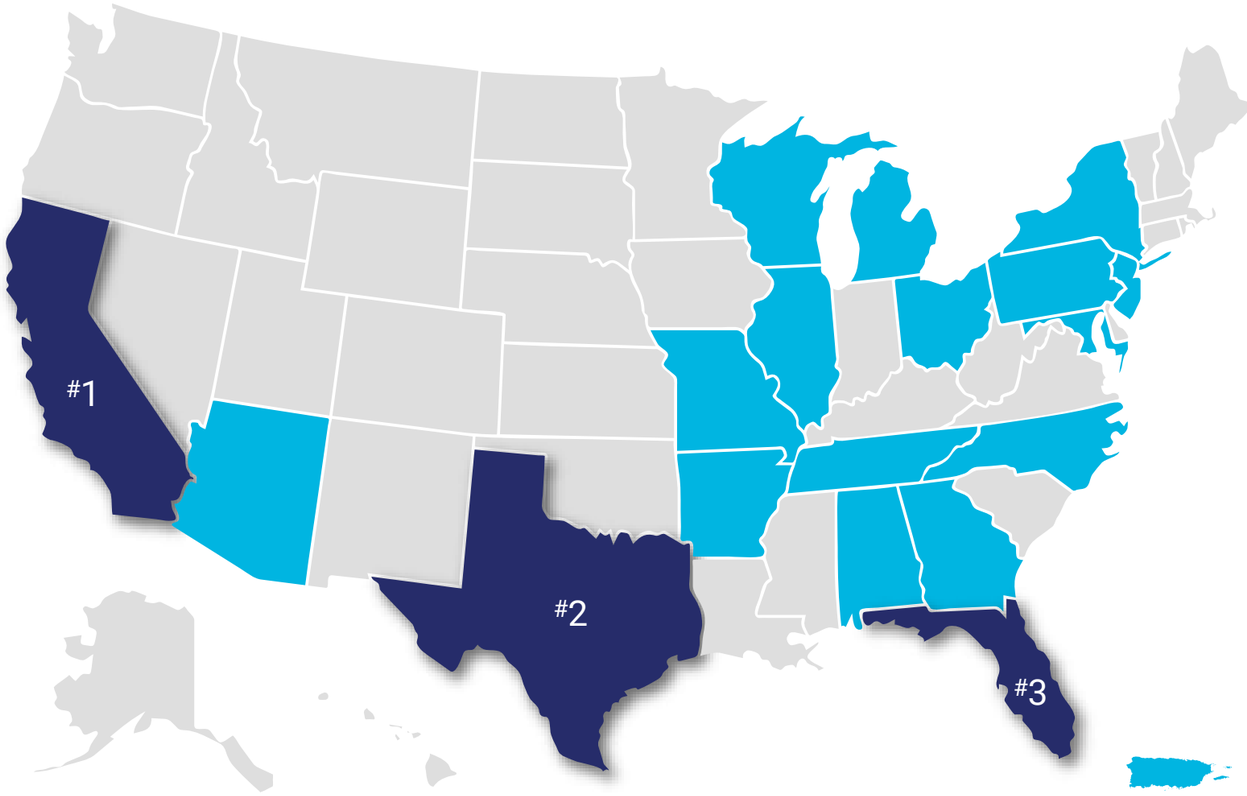
It's harder to catch a fraudster whose location is unknown. Via tools like remote desktops, VPNs, GPS spoofing apps, and emulators, bad actors can bypass many legacy authentication systems.

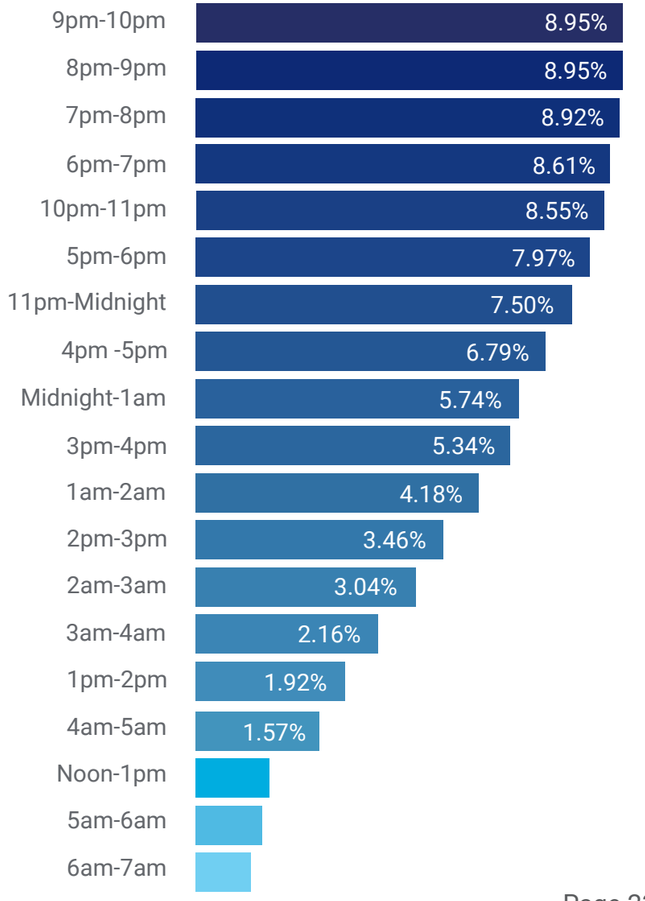
THE WHERE, WHEN, AND HOW OF IDENTITY FRAUD

of all Fraud Attacks take place between **4pm and midnight**

Top 19 U.S. States Where Fraudulent Transactions Happen

1 California
2 Texas
3 Florida
4 Illinois
5 Michigan
6 New York
7 Georgia
8 Puerto Rico
9 Maryland
10 North Carolina
11 New Jersey
12 Pennsylvania
13 Arkansas
14 Tennessee
15 Arizona
16 Ohio
17 Missouri
18 Wisconsin
19 Alabama

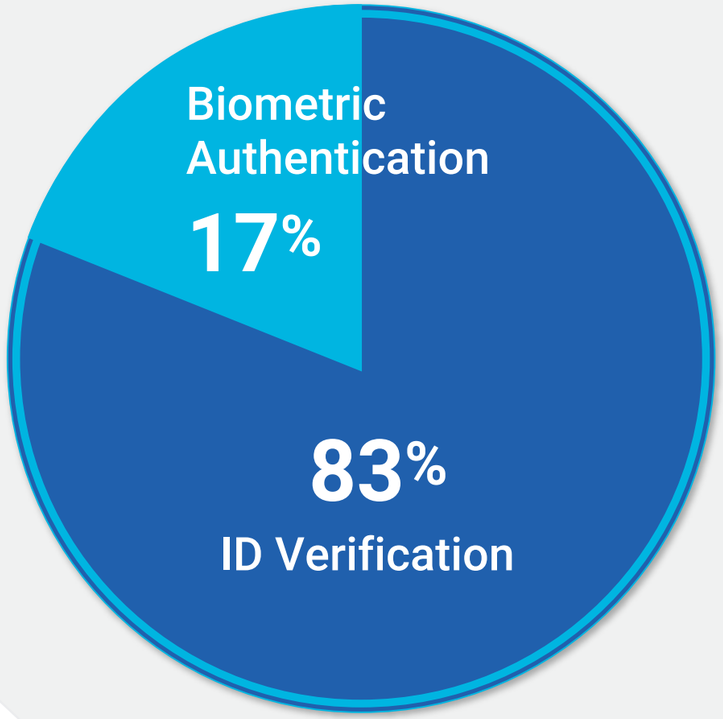




* AuthenticID Internal Data Fraud Analysis from 2023

Increases in Fraud Rates by Channel

2023 Fraud Detection at AuthenticID
ID Document Verification vs. Biometric Authentication



* AuthenticID Internal Data Fraud Analysis from 2023

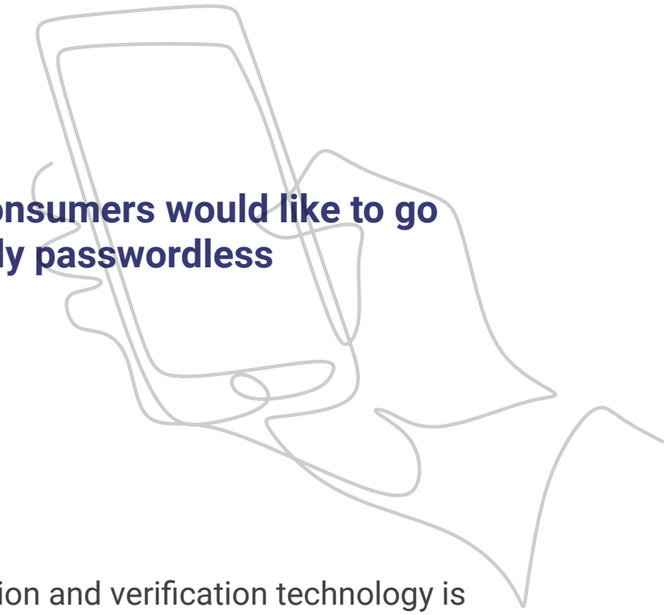
NAVIGATING THE TRANSFORMATIVE FUTURE OF DIGITAL IDENTITY

The increased interconnectedness and digitization of our existence hasn't just led to an increase in fraud. It has also generated advances and conversations about how to control and protect a secure digital identity. Taking greater control of digital identity is crucial over the coming years.

HOW DIGITAL IDENTITY IS EVOLVING

Going passwordless is gaining steam. Most companies across all industries are chasing a balance of convenience and security in their account enrollment, onboarding, and re-authentication processes across a variety of in-person and digital channels.

of consumers would like to go totally passwordless



Several trends are shaping the current state of digital identity in the US and abroad

PASSWORDLESS AS GOAL

With both the US and Europe cracking down on stolen credential market-places in 2023, password-based authentication is highly vulnerable. The quest to move past this authentication method toward something that is secure with minimal friction is an ongoing process. Many organizations have not yet adopted passwordless solutions due to internal implementation obstacles. However, FIDO-based passwordless solutions have seen an uptick at various organizations as phishing-proof authentication is crucial. To protect digital identity, organizations must employ better authentication practices as they make a shift toward passwordless methods.

BEHAVIORAL BIOMETRICS

On the forefront of authentication and verification technology is behavioral biometrics, which allows organizations to distinguish and measure human behavioral patterns and physical biometrics (such as face, fingerprint, or voice). These patterns can be analyzed to determine legitimate users in a dynamic, continuous fraud prevention system. Even better, a system based entirely on the characteristics of a real person's behavior and immutable features provides built-in digital trust. Device fingerprinting, device-based gestures and kinesthetics are powerful means to determine the authenticity of an individual, even when devices are stolen or misused. For the financial, ecommerce, and social media sectors, behavioral biometrics is a critical tool to verify identity when layered with analytics and other data.

HOW DIGITAL IDENTITY IS EVOLVING con't

DIGITAL IDs/mDLs

The proliferation of sophisticated fake IDs underscores the importance of transitioning to digital options that provide greater control over one's identity and support an infrastructure for inclusive development. Europe has led the charge toward digital IDs, but in the US, 11 states have rolled out mobile driver's licenses (mDLs), with nine other states in progress, and 12 others actively exploring programs. Digital IDs and mDLs can also allow for greater control of identity via age verification and on-device behavioral biometrics for fraud protection. Expect a year of rapid growth in 2024 as the move toward digital IDs continues.

FRAUD CONSORTIUMS

Given the universal prevalence of fraud, as well as the interconnectedness of payment rails and businesses, operating in a silo no longer works. That's why in 2023, new independent fraud consortiums were created: to share data transactions and information between groups of similar merchants/ businesses. By doing so, these businesses have access to data analytics and knowledge about common bad actors; often, they're hitting similar businesses within a vertical. Identifying fraud patterns alerts the entire consortium. This data plays a huge role in centralizing the authentication of individual identities.

QUANTUM COMPUTING

Over the past year, quantum computing has drawn the attention of not just IT and cybersecurity professionals, but also a variety of governments. While quantum computing is still in its early phases of development, it has huge ramifications for digital identity, both positive and negative. Quantum computing could be a game-changer for fraud detection when combined with machine learning. However, quantum computers could easily break crypto-graphic keys, compromising the security of biometric ID documents, financial data, passwords, and other sensitive information. As with AI, the rapid development of this technology could expose vulnerabilities in digital identity systems. In 2024, draft standards are expected to be released for quantum-safe algorithms by the National Institute of Standards and Technology (NIST).

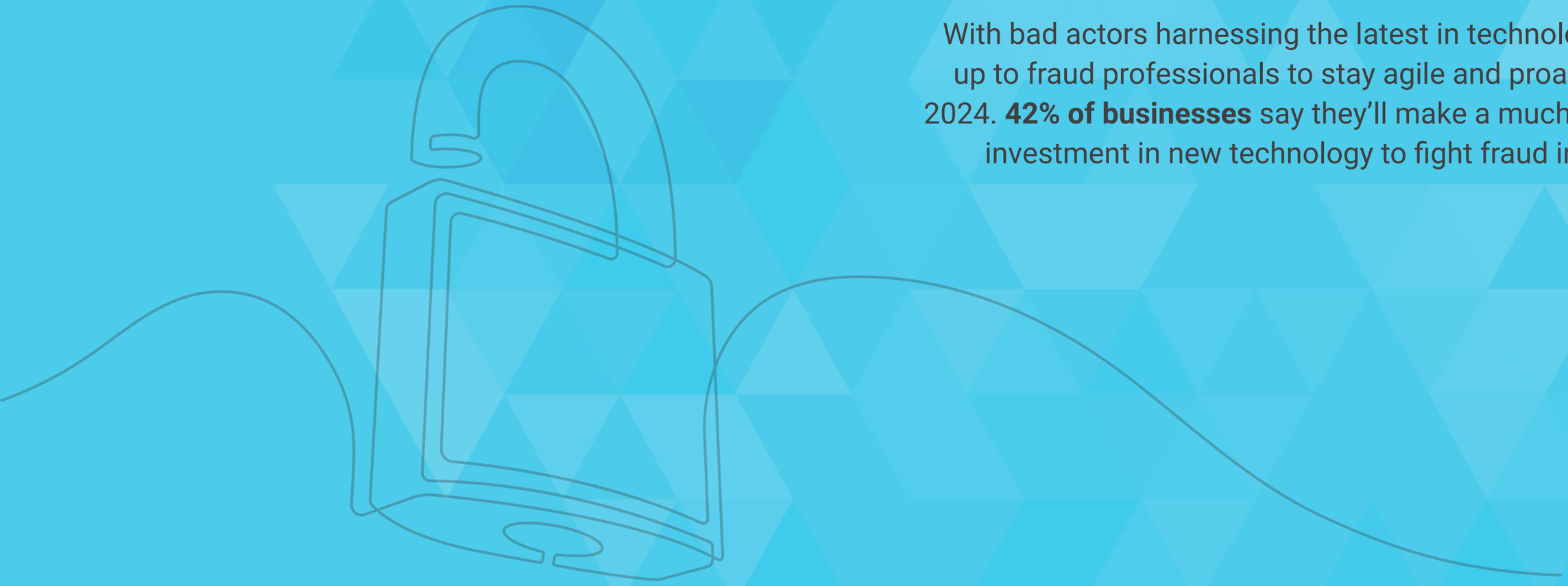
of people reporting they've used or plan to use generative AI tools*

of people reporting they've already used or plan to adopt a mobile driover's license*

* AuthenticID Consumer Fraud Survery 2024

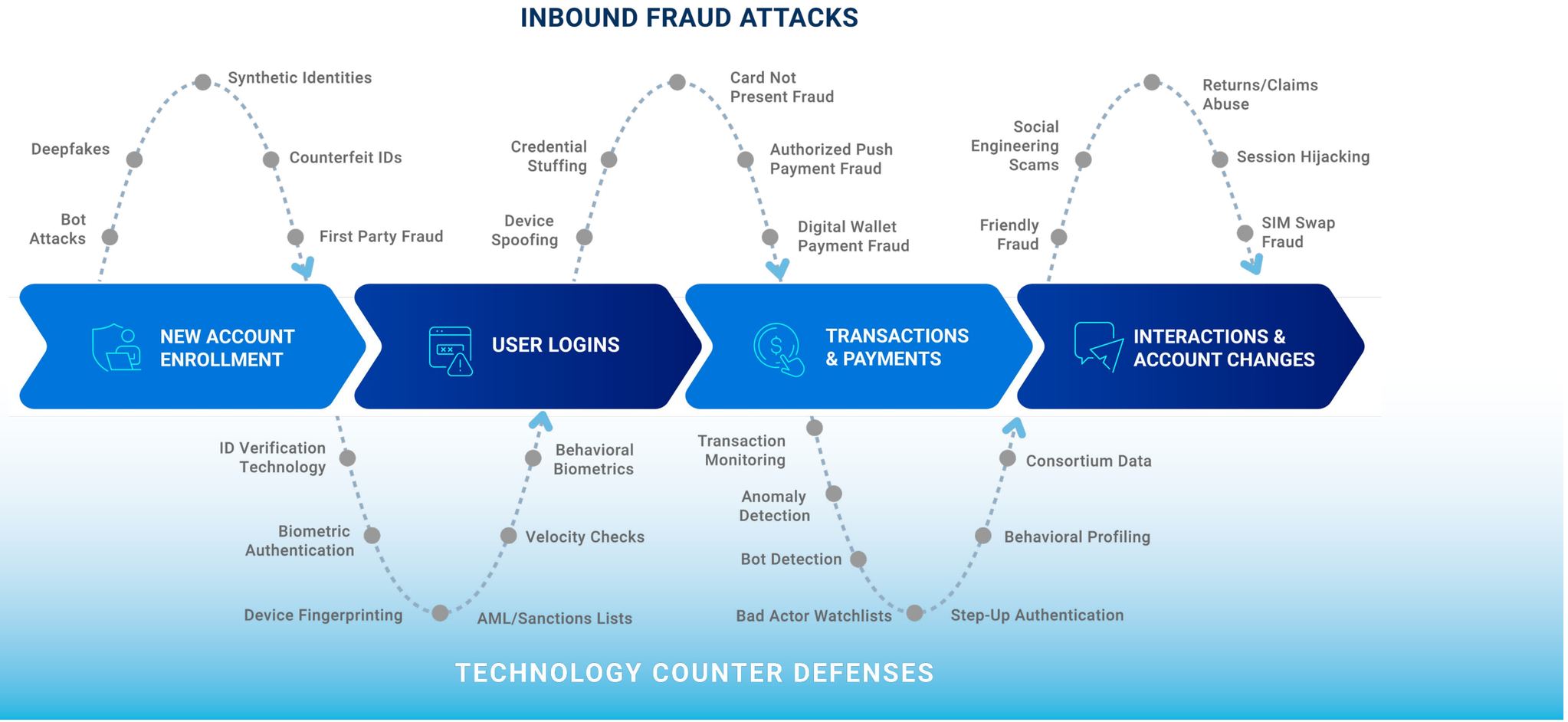
FUTURE-PROOF TECHNOLOGY TO COMBAT IDENTITY FRAUD

With bad actors harnessing the latest in technology, it's up to fraud professionals to stay agile and proactive in 2024. **42% of businesses** say they'll make a much higher investment in new technology to fight fraud in 2024.



Fighting Fraud Along the Customer Journey

Fraud attacks are relentless and infiltrate various channels and touchpoints within the customer journey. Effectively combatting this fraud requires a multifaceted, proactive, and adaptive approach. Here is a look at the most prevalent fraud attacks and recommended counter defenses.



IDENTITY PROOFING To Combat Fraud

Companies are not helpless against fraud – tools are available today utilizing the latest technology to stop multiple vectors of fraud attacks.

ID Verification

ID Verification technology can prevent identity fraud incidents while also providing a “smart” amount of friction – giving users peace of mind while ensuring they have a streamlined experience from account opening to re-authentication. A comprehensive identity verification solution with multiple layers is critical to fighting multifaceted fraud.

Automated identity document verification can catch sophisticated fraudulent documents and professional fraudsters. AuthenticID provides leading identity verification technology, including cutting-edge image capture technology offers the ability to capture and process low-quality images with the most challenging backgrounds and lighting. Additionally, OCR, 2D barcode, and MRZ data extraction technology has the highest accuracy in the industry, supports 7,300 global identity documents, and supports over 30 international languages.

Biometric Authentication

Biometric authentication offers a pathway for futureproof passwordless authentication and anonymized, un-hackable, and un-spoofable credentials. When paired with liveness detection to fight spoofing, identity could be confirmed with an action as simple as taking a selfie on a mobile device. With this simple, user-friendly way to authenticate an individual, you can match a person to the photo on a government-issued ID, profile picture, or any other image of a person’s face with complete accuracy. AuthenticID uses liveness detection and face match to ensure the person is actually present instead of a deep fake or spoof.

of people believe biometrics is the safest method for authentication*

Fraud Shield

Go one step beyond traditional identity verification with Fraud Shield: a biographic watchlist service that can be paired with biometric authentication for a powerful one-two punch. When a user tries to present an ID that is a fake, their IP address, name on the ID, ID number, and selfie are encrypted and then saved to flag for future fraud attempts. We have an ever-expanding network of bad actors that help our customers prevent fraud now and in the future. Fraud Shield’s Bad Document screening utilizes proprietary technology to manage a fraudulent document watchlist and unbiased, AI-based decisioning. Cut out the risk of identity verification processes with Fraud Shield. The Watchlist is updated in a matter of seconds so fraudsters don’t have time to submit multiple documents.

* AuthenticID Consumer Fraud Survery 2024

THE AuthenticID DIFFERENCE

Fighting fraud and maintaining a positive customer experience is a complicated process, and your business needs a partner that can do both. When choosing a partner for identity verification, consider these four factors:

1 TOUGH ENOUGH TO FIGHT FRAUD

Your identity verification technology should be designed to move at the speed of fraud, meeting the agile nature of bad actors. AuthenticID runs 500+ forensic checks on an ID using visual, text, and behavioral analysis to determine its authenticity.

2 SCALABLE FOR ENTERPRISE-LEVEL BUSINESS

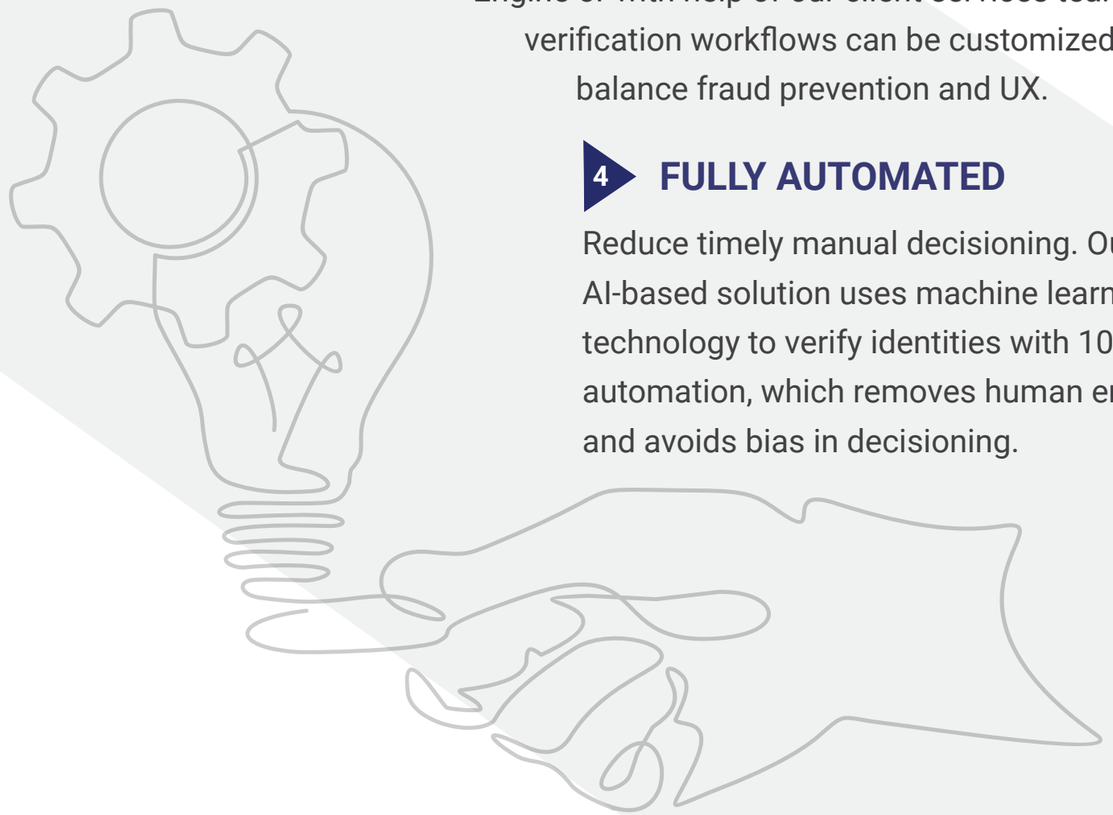
Your system needs to meet the high demands of customers and attacks from fraudsters. AuthenticID serves 8 out of the 10 major North American wireless carriers and top U.S. banks. Our dedication to the highest standards is reflected in our ISO/IEC 27001 and SOC2 certifications.

3 CUSTOMIZABLE

Your business is unique, and AuthenticID's solution is not one size fits all. Through our Identity Decisioning Engine or with help of our client services team, verification workflows can be customized to balance fraud prevention and UX.

4 FULLY AUTOMATED

Reduce timely manual decisioning. Our AI-based solution uses machine learning technology to verify identities with 100% automation, which removes human error and avoids bias in decisioning.

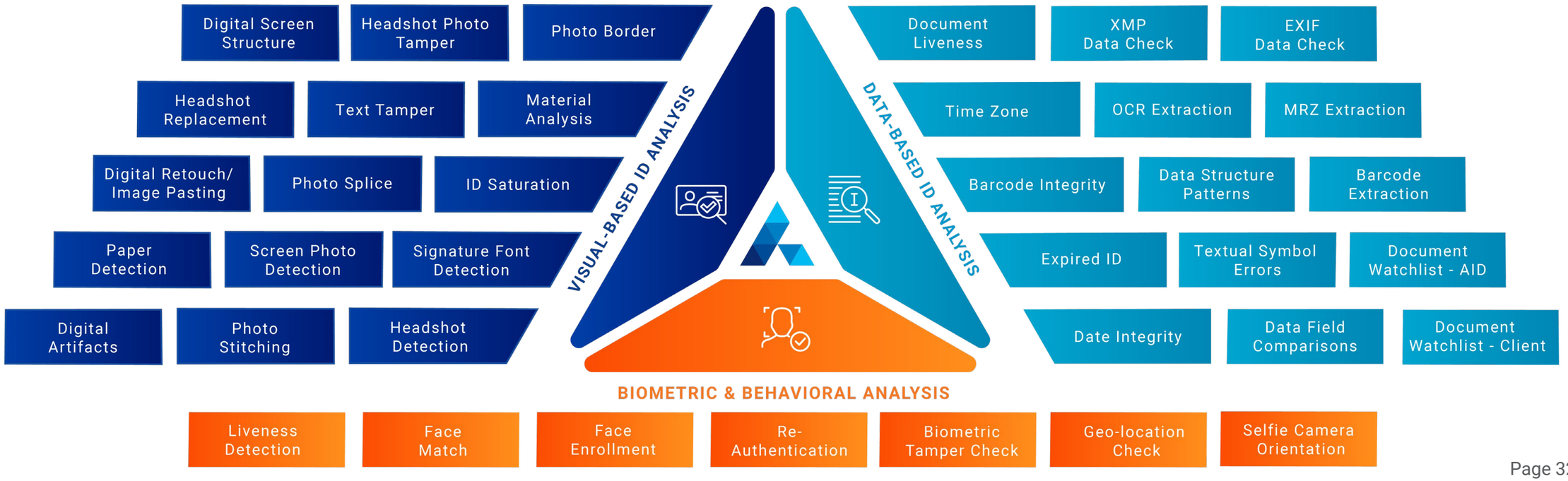


FIGHT FIRE WITH FIRE: AI, ML, AND FRAUD FORENSICS

Stop fraud, increase customer conversion, reduce operating costs and elevate security with thousands of proprietary machine learning and computer visualization models.

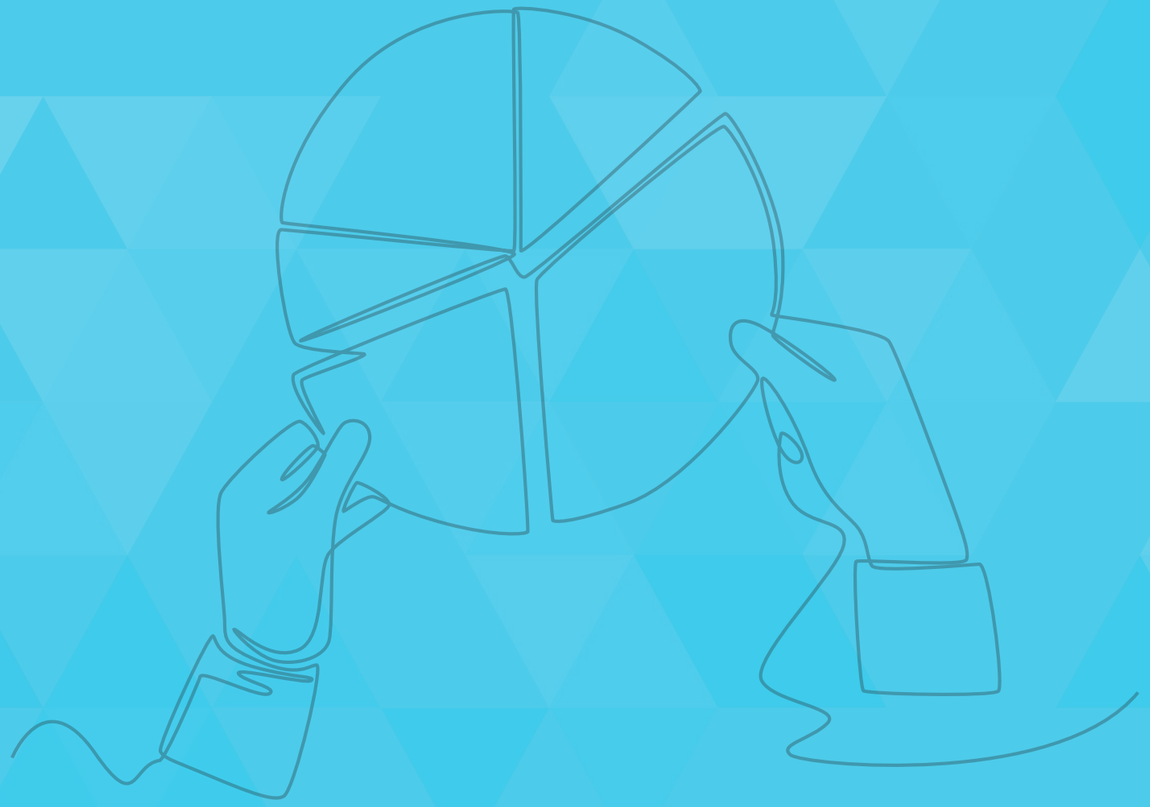
Our AI and machine learning technology provides **99%+ accuracy** in detecting even the most sophisticated fraudulent documents. AuthenticID's proprietary technology combines machine learning and AI to review hundreds of computer vision data models in seconds to verify an ID's authenticity.

500+ Fraud Forensic Checks to Block Fraudulent IDs & Synthetic Identities



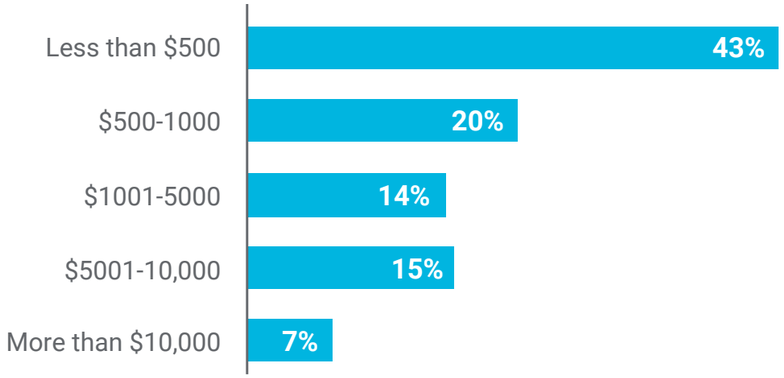
HIGHLIGHTS:

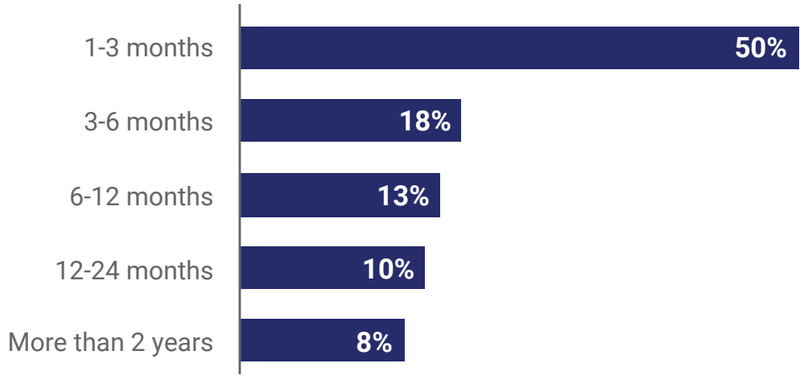
2024 CONSUMER & BUSINESS FRAUD SURVEYS



Financial Loss & Time to Recover

Survey respondents that were victims of fraud indicate the value lost from fraud and the time it took to clear up financial and credit issues from each incident.





When Transacting with Financial Institutions, Security & Fraud Prevention Concerns Outweigh User Experience Benefits

	NOT IMPORTANT	SOMEWHAT IMPORTANT	IMPORTANT	VERY IMPORTANT	EXTREMELY IMPORTANT
Quick, seamless account openings	5.3%	22.0%	31.6%	23.5%	17.6%
Frictionless access to online accounts and account recovery (forgot login info)	1.9%	15.2%	33.5%	24.7%	24.7%
Strong security measures to ensure unauthorized access to my account	1.1%	6.19%	14.76%	24.5%	53.3%
Trusted adherence to privacy and compliance regulation to keep my personal data safe	1.5%	4.4%	16.6%	21.2%	56.2%

Top Fraud Scams Survey Respondents Endured in 2023

1. **Personal Banking Fraud** – 50% of respondents
2. **Credit Card Fraud** – 49% of respondents
3. **Online Shopping Fraud** – 20% of respondents
4. **Mobile & P2P Payment Fraud** – 18% of respondents
5. **Social Engineering Attacks** – 17% of respondents
6. **Government-related Identity Theft** – 15% of respondents
7. **Online Account Takeover** – 12% of respondents

Customer and Business Perspectives on Security vs. UX

Fraud prevention and customer user experience can be a balancing act. Here is how consumers and business weigh the importance between each attribute.

Answer from Page 9

Request your private fraud consultation and demo of our identity proofing solutions.

IDENTITY **MADE SIMPLE**

Identity proofing anytime, anyplace, and on any device.

REQUEST CONSULTATION & DEMO

2024

STATE OF IDENTITY FRAUD REPORT

AUTHENTICID

Created in Partnership with PEAK iDV