Mid-Year
IDENTITY FRAUD REVIEW
2024 Trends and Insights

AUTHENTICID

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

Introduction

In 2024 staying ahead of fraud has been even tougher. One reason: new technology allows bad actors to put new spins on existing fraud methods. Businesses have a huge fraud problem, and they're falling behind as bad actors make huge gains.

AuthenticID, powered by proprietary research and innovations from our Identity Fraud Taskforce, has a unique lens into the battle between fraudsters and fraudfighters, both using the same technologies and techniques to stay one step ahead.

Our Mid-Year Report looks at the trends, fraud threats, and technology updates businesses need to know to safeguard their data and assets as well as their customers for the rest of 2024 and beyond.

About Our Data

This first half report includes internal proprietary data anonymized and analyzed from our platform's identity verification, biometric authentication, and watchlist technology and processes. We also utilized data from our consumer fraud survey, which received 500 responses and was conducted in June 2024.

Contents

AT A GLANCE:

FRAUD TRENDS at Mid-Year 2024

Bigger, better, faster.

Fraudsters are armed with the latest technology, shifting the way businesses must approach identity and security. In 2024, key trends are shaping up, with the headlines to match.

DEEPFAKES & INJECTION ATTACKS

Deepfake technology has quickly emerged as a powerful threat, fueled by the rise of generative AI technology. In the hands of bad actors, this technology is a frightening tool that allows fraudsters to create more convincing fakes than ever- at a fraction of the time and cost. Deepfakes are convincing biometrics, images, videos, and content that are generated by AI and Machine Learning. And now they're being used as weapons in injection attacks, when they are "injected" into an identity verification workflow.

DEVIOUS USE CASE OF DEEPFAKES

IN THE NEWS – British engineering giant Arup was recently revealed to be the company that was the target of a deepfake scam that led to a $25 million payout. An employee at the multinational company was tricked by advanced deepfake technology of an individual claiming to be the company's chief financial officer in a video call, wherein multiple staff members were deepfake recreations.[2] The Hong Kong-based crime highlights the new ways deepfakes and injection attacks can wreak havoc on victims.

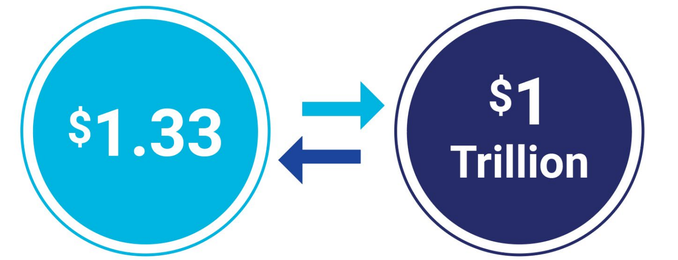
7 CENTS

The amount malicious actors spend to reach 100,000 social media users with a weaponized deepfake.[1]

[1] "Scammer paid Facebook 7 cents per view to circulate video of deepfake Jim Chalmers and Gina Rinehart," The Guardian, 30 November 2023.
[2] "Finance worker pays out $25 million after video call with deepfake 'chief financial officer'" CNN, February 4, 2024.

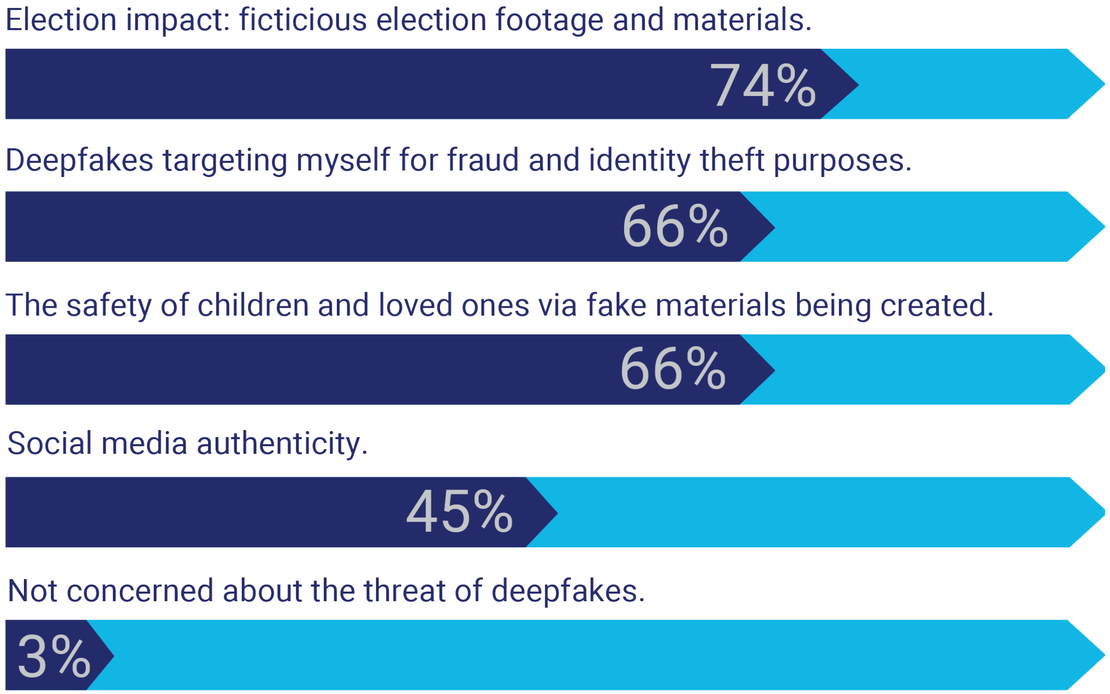
THE DEEPFAKE ISSUE: CAN IT BE STOPPED?

There's no silver bullet to stop any type of fraud completely. But there are powerful algorithms we can use: in June, AuthenticID announced a comprehensive set of algorithms aimed at stopping deepfakes by using text, visual, and behavior-based algorithms. These algorithms can be used for the myriad ways bad actors can use deepfakes: from text to headshots, in addition to selfie and video deepfakes.



Average cost of **creating a deepfake** in 2024[3]

Expected global **cost of deepfake fraud** in 2024[3]



When surveyed, 91% of people could not select a real person from a line of deepfake headshots.

[3] "AI-assisted fraud schemes could cost taxpayers $1 trillion in just 1 year, expert says, Fox News Digital, June 20, 2023.

The headlines tell the tale:

“AI IS THE FINAL BLOW FOR AN ID SYSTEM WHOSE TIME HAS PASSED”
– Forbes

“A NEWLY-STREAMLINED PROCESS FOR FAKE IDS SAYS IT’S USING AI”
– The Verge

“AI WILL MEAN AN ARMS RACE OF FAKE IDS”
– Diginomica

FAKE IDs: BETTER, CHEAPER, EVERYWHERE

Generative AI isn’t just making an impact in deepfakes. Fake IDs are now being developed cheaply and at scale using AI: even worse, they are convincing enough to thwart traditional identity verification methods. These IDs are not just used to get underage youths into a bar. They are also used in scams that can cost businesses millions. These fakes can even duplicate some often-used security features, including barcodes, holograms, and background patterns.

ACCOUNT TAKEOVERS ARE A GROWING THREAT

Once again, AI is fueling another fraud surge: this time, in Account Takeover attacks. Reports have found that 28.7% percent of fraud in 2023 was third-party account takeover – and human-initiated attacks increased once again. From banking accounts to social media, fraudsters are targeting weaknesses with improved abilities to circumvent traditional security measures.

70%

Percentage of security leaders who view account takeover attacks as the greatest concern to their organizations, ahead of threats like ransomware and phishing.[4]

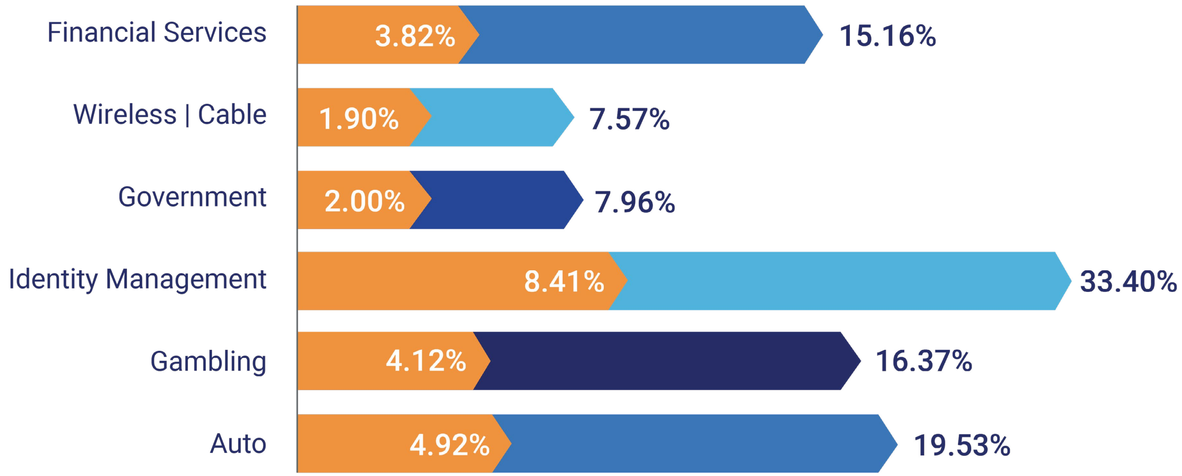
[4] “Azure account takeover campaign targets senior execs,” SC Media, February 13, 2024.

CONSUMER & BUSINESS FRAUD OBSERVATIONS

BUSINESSES ARE STRUGGLING TO KEEP UP WITH SOPHISTICATED FRAUD

Identity fraud spares no industry. While financial services are prime targets for identity theft, with big payouts, other industries also can offer big windfalls for fraudsters. In fact, synthetic identity fraudsters target the auto lending industry the most of any lending type.[5] Bad actors also target car rentals as a prime place to steal identities. The big business of online gaming and gambling also provides big benefits to fraudsters, who can use account hacking and chargeback fraud on platforms with weak security and verification protocols. Simply put, the amount of fraud all industries are seeing continues to skyrocket in 2024, with no signs of slowing.

Fraud Percentage Rate by Industry vs Percentage of Total Fraud Detected by Industry



63% of financial firms reported an overall fraud increase of at least 6% within 12 months, with digital channels accounting for half of the overall fraud losses.[6]

[5] "Synthetic ID Fraud Rises 98% in Auto Lending Industry," BankInfoSecurity, May 10 2024.
[6] LexisNexis® True Cost of Fraud™ Study: Financial Services and Lending Report — U.S. and Canada Edition, 2024.

BREACHES

Major data breaches, especially in healthcare, have added to the massive amounts of PII available on the Dark Web, available for purchase for just pennies. Techniques like Imposter Scams continue to plague businesses, according to the FTC, with losses of $2.7 billion in the United States alone.

BIOMETRIC ADOPTION IS INCREASING

As the speed and accuracy of biometric authentication methods has increased, so too have use cases. In fact, several high-profile uses of biometrics have been implemented over the past year, from American Airlines using facial biometrics to Disney parks implementing biometric fingerprint scanners to palm screening payment technology at Whole Foods retail locations.[7] Consumers are accepting these trends: In AuthenticID's consumer survey,

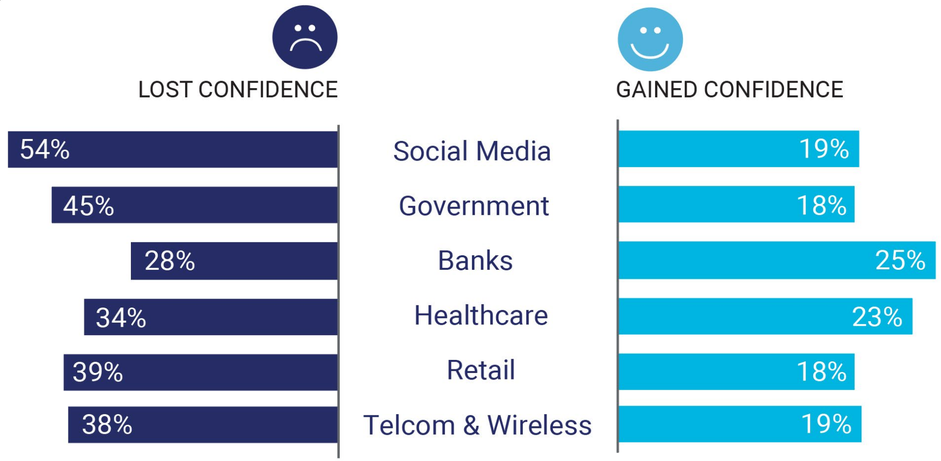
65% of people chose biometric authentication as their preferred authentication method, even over passwords.

[7] "SDM TOPICS ACCESS CONTROL & IDENTIFICATION INTEGRATION & NETWORK SOLUTIONS Facing the Future With Biometrics," SDM, March 2023.

CONSUMERS ARE STILL WORRIED — FOR GOOD REASON

HOW BUSINESSES RESPOND TO THREATS MATTERS

The perception of how you're safeguarding your customers' identity data matters. We surveyed consumers: *Over the last year, have you gained or lost confidence in the following industry service providers to safeguard your identity data?*[8]



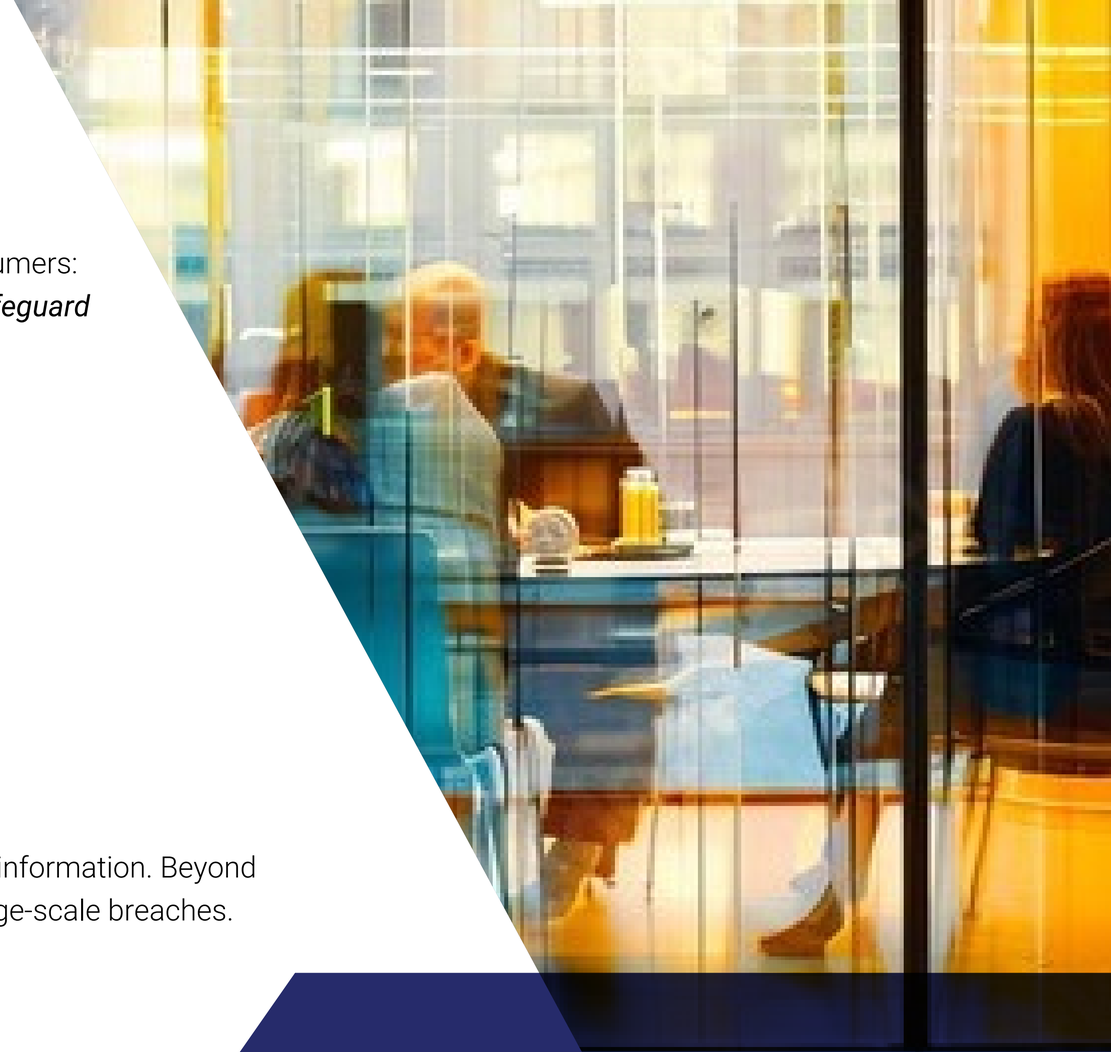
Consumers are concerned about the growing rate of data breaches and the impact on their personal information. Beyond just a username and password, consumers are more frequently seeing critical PII data exposed in large-scale breaches.

40% respondents who say their personal data has already been involved in a data breach this year.

23% respondents who've had their Social Security Number Exposed.

25% respondents who've had personal Credit Card or Payment Information Exposed.

22% respondents who've had their Username/Password Exposed.



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

[8] AuthenticID Mid Year State of Fraud Survey, June 2024.

DIGITAL, PHYSICAL IDENTITY CREDENTIALS. A SPLIT IN SENTIMENT

A shift in how we think about identity, whether physical or digital, has been underway for some time. In 2024, there's been a continued growth of two intertwined trends: in the US, mobile driver's licenses (mDLs), and, globally, verifiable credentials. Momentum behind mDLs is gaining steam, with 15 states already offering mDLs or in the implementation stage, with over a dozen more in the legislative phase to move these digital initiatives forward. In fact, in New York, mDLs can now be used as proof of age in bars and restaurants.[9] Globally, the use of verifiable credentials, a digital, cryptographically-secured version of credentials that can be presented digitally for verification, has growing use cases in healthcare, education, and government. Countries including Singapore, with its National Digital Identity (NDI) system, Sweden's BankID system, and Estonia's eID, among others, are standouts in digital identity innovation globally.

Consumers are ready:

Consumers reporting they're open to adopting an mDL when it becomes available (Combines *yes, yes, but not right away, and maybe need more info*) **78%**

Consumers reporting they won't adopt an mDL. **13%**

But when it comes to digital identity credentials versus physical identity documents, consumers are a bit more likely to hold on to their physical wallets:

47% of consumers prefer a physical over digital wallet.

19% of consumers prefer a digital wallet alone.

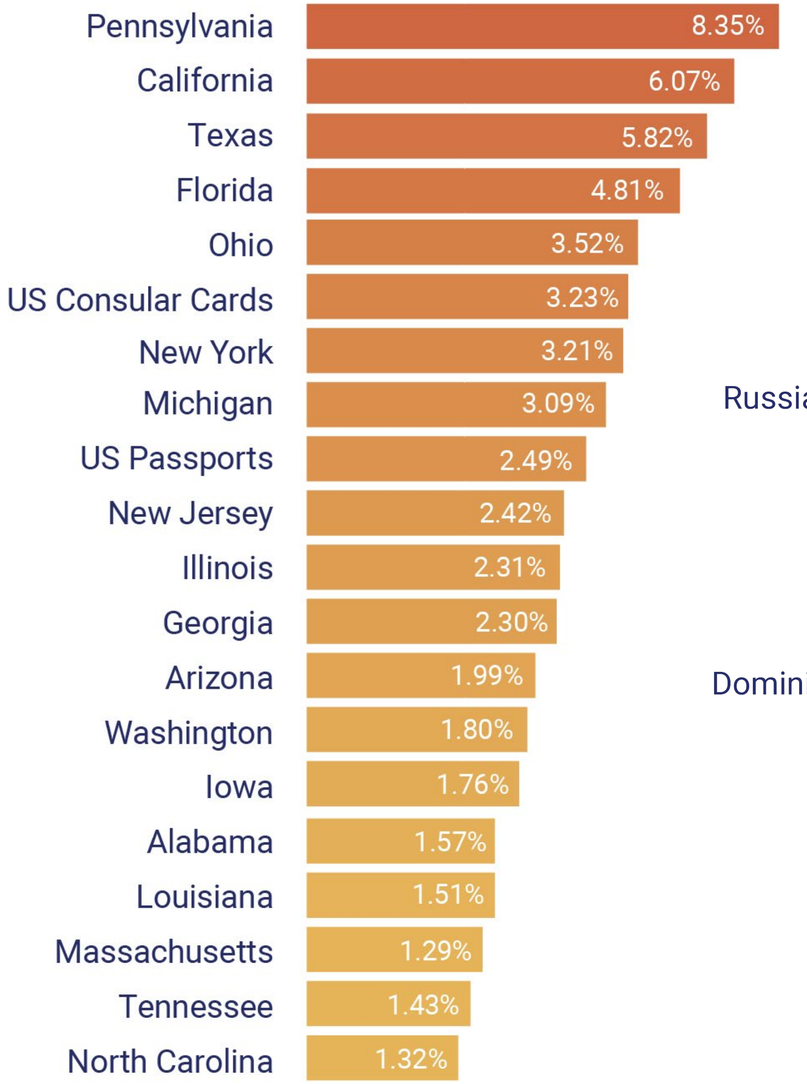
32% of consumers say they'd use both, depending on the circumstances.

The key to improving sentiment? Consumer protection against fraud threats. This includes adopting the very latest in fraud-fighting technology to ensure fraud attacks are stopped. There's no shortage of attack vectors, but there is also crucial technology available to stop bad actors. Identity verification has never been more important – but it's more than just checking an ID. From behavioral biometrics to the use of watchlists, there are more ways than ever to protect your organization and your customers. Check out the mechanisms on page 13 to improve your organization's defenses against fraud.

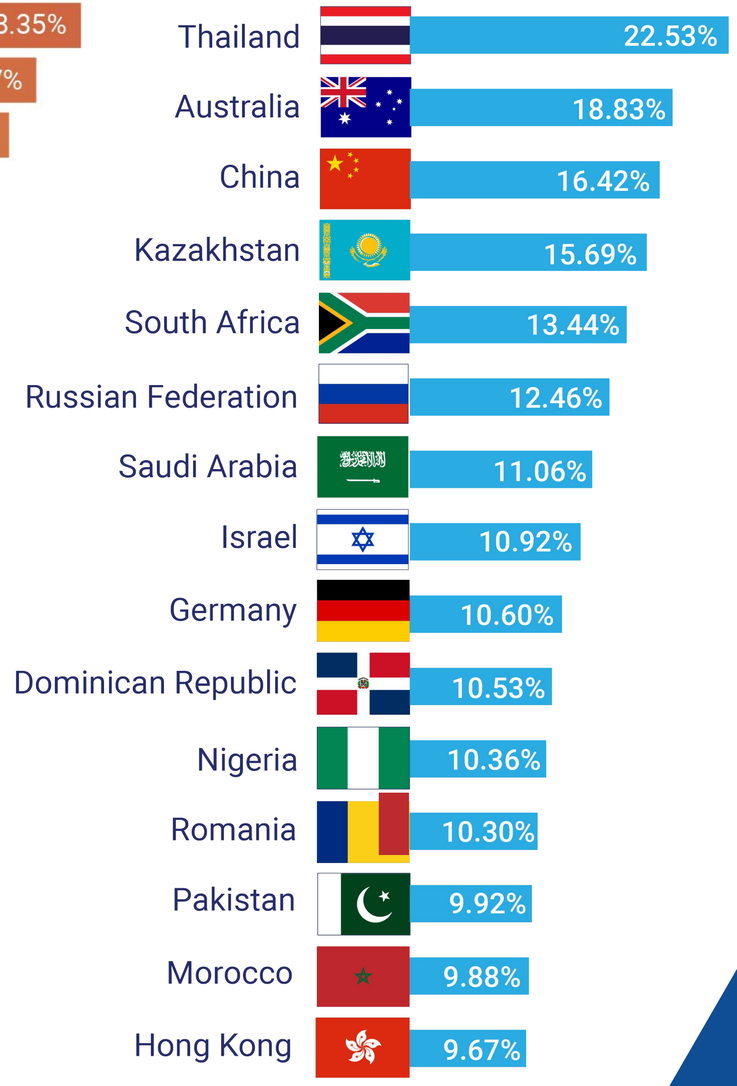
[9] "Mobile driver's licenses continue to pick up speed," Biometric Update, June 12, 2024.

THE LATEST IN DATA INTELLIGENCE: Our Analytics

Top 20 States in the U.S. with the Highest Rate of Fraud

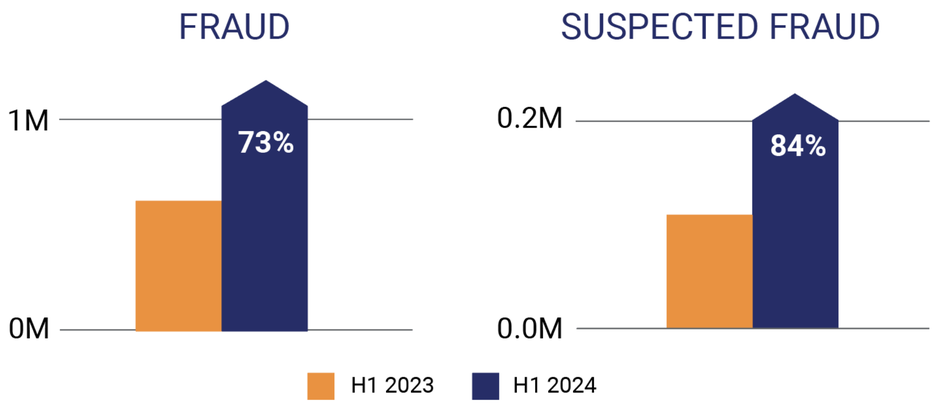


Top 15 Countries with the Highest Rate of Counterfeit IDs

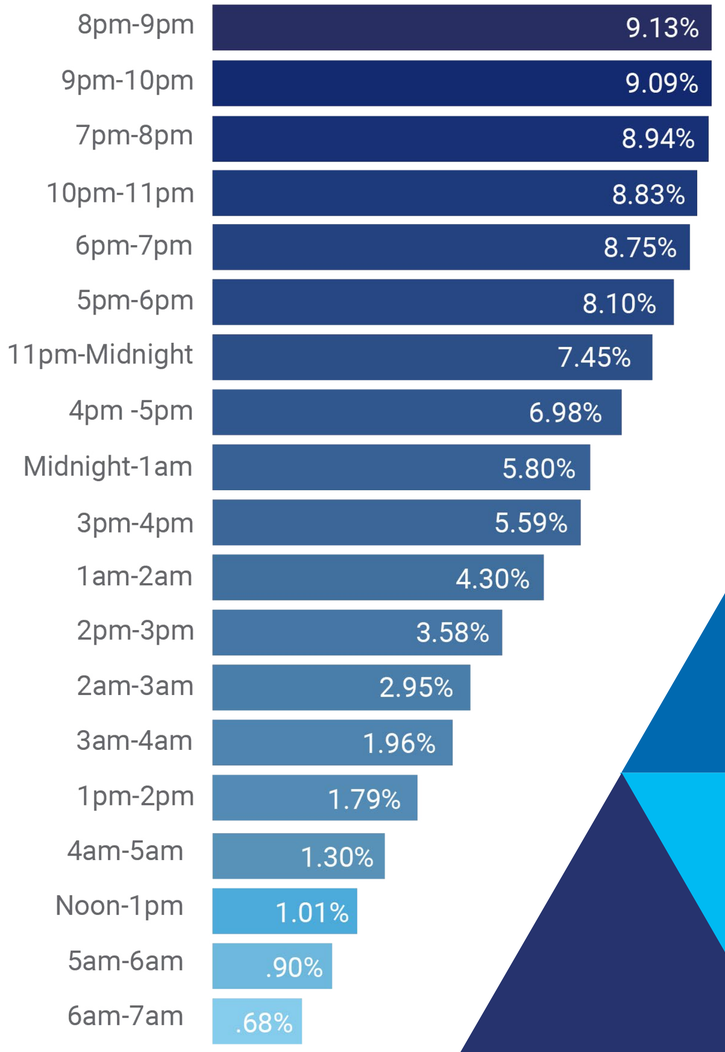


Volume and Variety of Fraudulent Attacks

Based on data extracted from our client transactions, we've observed a significant increase in fraudulent activity so far in 2024. Comparing H1 2023 to H1 2024, there's been a 73% rise in the number of fraudulent transactions and an 84% increase in suspected fraudulent transactions.



When does fraud occur?



Total Fraudulent Activity

Biometric Authentication Fraud

- SELFIE MATCH
- FRAUD SHIELD WATCHLISTS
- LIVENESS DETECTION
- DEEPFAKE INJECTION ATTACKS

22% VS **78%**

ID Verification Fraud

- HEADSHOT MANIPULATION
- FAKE SIGNATURES
- BARCODE TEXT ANALYSIS
- VISUAL OCR ANALYSIS
- TEXT TAMPERING

AUTHENTICID

Identity Fraud *Taskforce*

Moving at the Speed of Fraud

AuthenticID's Identity Fraud Taskforce is the driving force behind our innovative identity verification platform. Comprised of a diverse team of experts, the Taskforce has a mission to move at the speed of fraud.

With over 40 patents, this Taskforce ensures we can detect fraud before it breaches our clients' systems, equipping us and our clients to fight the future of fraud and stay ahead of bad actors, no matter what techniques and tactics they use.

So far this year, the Identity Fraud Taskforce has pushed the boundaries of what identity verification platforms have previously done, ensuring sophisticated attacks are stopped quickly.

Learn more about our **Identity Fraud Taskforce**.

Problems & Solutions

AuthenticID released product enhancements the first half of this year to solve these crucial challenges in identity verification.

Synthetic Signatures

SOLUTION

Does the signature look a little too perfect, or is it perhaps anomalous upon a closer, AI-driven view? False, AI-driven signatures can be detected by machine learning, catching differences that don't always jump out to the naked eye – or traditional verification systems.

False Rates in Authentication

SOLUTION

Our team has automated most of the thresholding retraining process, improving the number of False Acceptance Rates (FAR) and False Rejection Rates (FRR) our system detects. It's all about accuracy – even as new attempts test your verification platform.

Slow Verifications and Abandonment

SOLUTION

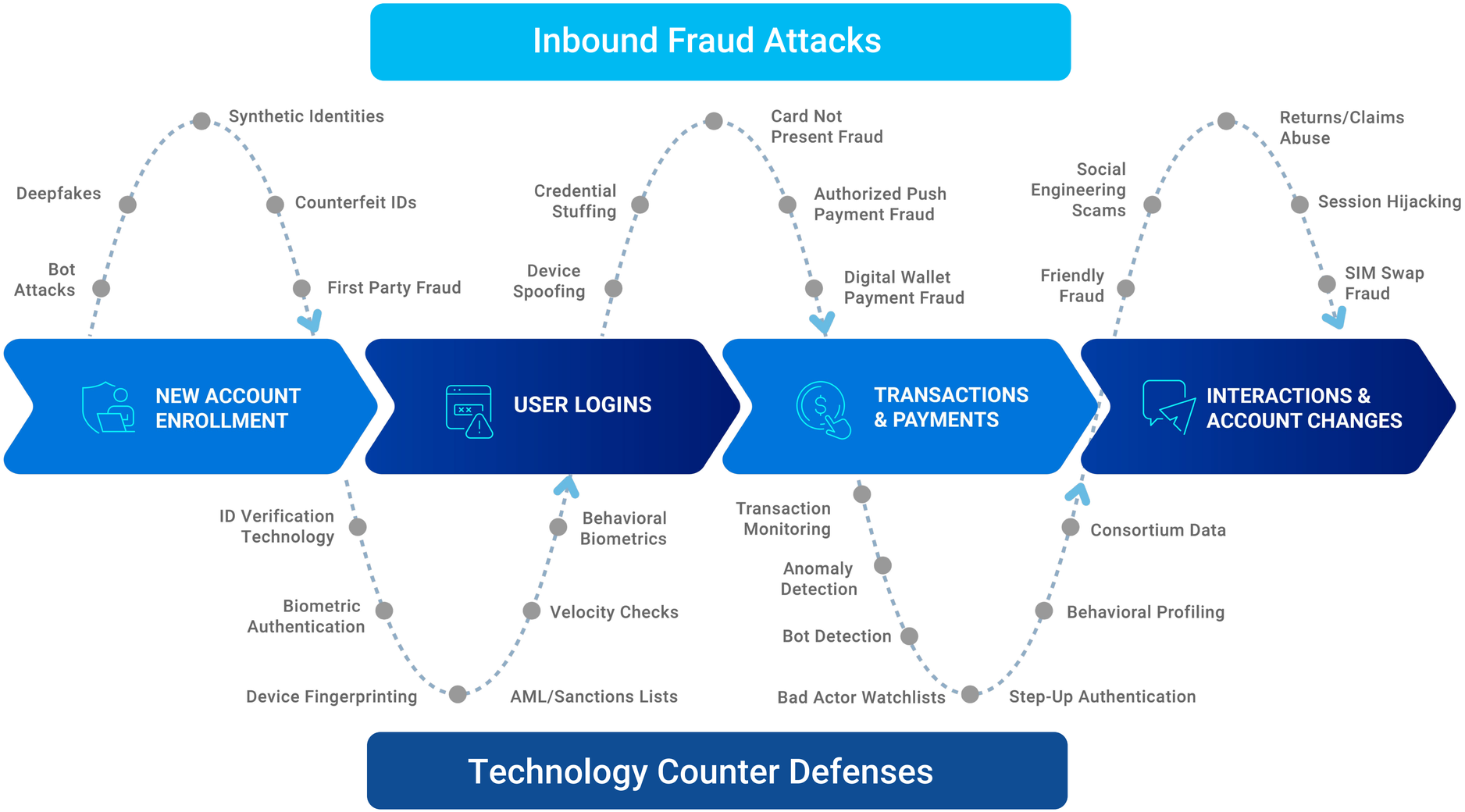
With automated AI-based decisioning, and recent updates to our document classifier you can get a Yes or No decision in just seconds, eliminating the concern for UX friction and abandonment.

Deepfakes are a Worry

SOLUTION

A combination of new, proprietary algorithms can detect both deepfakes and generative AI injection attacks. Visual fraud algorithms detect counterfeit and synthetic elements, text fraud algorithms detect errors within false documents, and behavioral algorithms focus on activity during the ID capture and submission.

At every stage of the customer journey, fraudsters are finding new ways to target customers' identities and sensitive data. Fraudfighters have been working hard to develop the technology and platforms to stop each type of inbound fraud attack when and where they occur. A comprehensive approach to tackling these dangerous threats has never been more important.



STAY AHEAD OF FRAUD:
Innovative Technology Can Help

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 over 2,000 unique computer vision data models to verify an ID's authenticity.

AUTHENTICID

Request your private **FRAUD CONSULTATION AND DEMO** of our identity verification solutions.

© 2024 AuthenticID Inc. All Rights Reserved.