AUTHENTICID

2025 State of Identity Fraud Report

From Insights to Action:
Key Data, Trends, and Innovations Shaping 2025

Change is here, change has come.

In 2024, identity fraud threats continued to grow.

It's easy to chart the expected but still shocking rise in fraud threats. The biggest question for businesses: can you stop it?

The 2025 edition of our State of Identity Fraud report offers the latest in identity fraud tactics, trends, and technologies. Also inside, get valuable insights from business leaders and consumers, how they view and experience fraud, business challenges, and new technology adoption, including AI and biometrics.

About Our Data

This report uses a combination of external business and consumer surveys conducted in Q4 2024 with internal proprietary data anonymized and analyzed from our platform's identity verification, biometric authentication, and watchlist technology and processes. Together, the 2025 State of 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.

SME Contributors

Eva Velasquez

President and CEO, Identity Theft Resource Center

As a recognized leader in the field of identity compromise and crime, cybercrime, and fraud, Eva has been featured on CBS Mornings, NBC Nightly News, Fortune, The Associated Press and numerous other media outlets.

Dan Giurescu

President and CEO, Credivera

A pioneer in the technology space, Dan's vision for Credivera is to empower people in the ways in which they manage, share and control their digital information for work and life.

CONTENTS

01

The Fraud That Has Changed the Game–and the Fraud That Will Change It Again

DEEPFAKES

ACCOUNT TAKEOVER

PAYMENT FRAUD

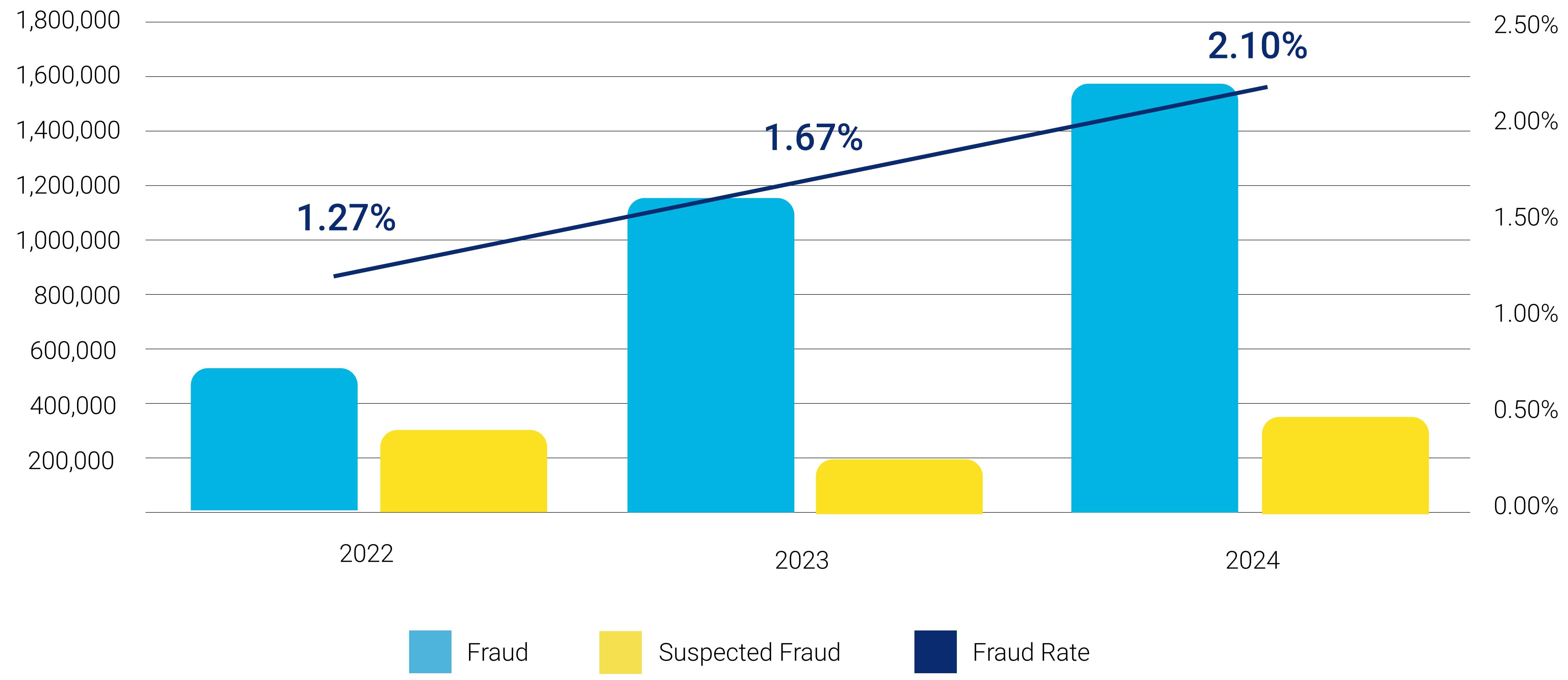
SOCIAL ENGINEERING SCAMS

WORKPLACE FRAUD

Over the past 3 years, we've tracked the most pertinent fraud threats: from the emerging threats that bypass organizations' traditional methods of cybersecurity and identity verification to the standbys of bad actors that continue to successfully target businesses and consumers alike.

In 2024, we witnessed how AI can transform the capabilities of bad actors and fraudsters, coupled with shifts in digital identity and consumer trends that make identity authentication and security a critical piece of the identity fraud puzzle.

Fraudulent Transactions Year-over-Year*



*AuthenticID State of Identity Fraud Surveys, 2024

As the intertwined worlds of digital identity and fraud continue to evolve in tandem, it's crucial to evaluate the impacts of fraud on consumers and businesses, as well as how fraudsters are changing.

Identity fraud looms large for both businesses and consumers: Over 68% of people say the threat of identity fraud impacts their behavior online some or all of the time.[1] In a recent analysis of a subset of our direct clients, 2024 saw a rise in both confirmed and suspected fraudulent transactions. The **overall fraud rate climbed to 2.10%**, marking the highest level observed in the past three years.

DEEPFAKES: BLURRING REALITY

Convincing deepfakes are here–and they're one of the most difficult types of fraud both to detect and to fight.

40 BILLION

46% of businesses surveyed by AuthenticID **reported a year-over-year increase in deepfake and generative AI fraud**, while 50% observed consistent levels, and only 4% noted a decrease. 96% of those businesses believe deepfakes and generative AI are a fraud threat to their organization.

60% of Americans consider the spread of misleading audio and video deepfakes the most concerning use of AI.[1]

Generative AI will enable $40 billion in losses by 2027, up from $12.3 billion in 2023. That's a 32% compound annual growth rate.[2]

Deepfakes Are No Longer Theoretical—Businesses Must Act

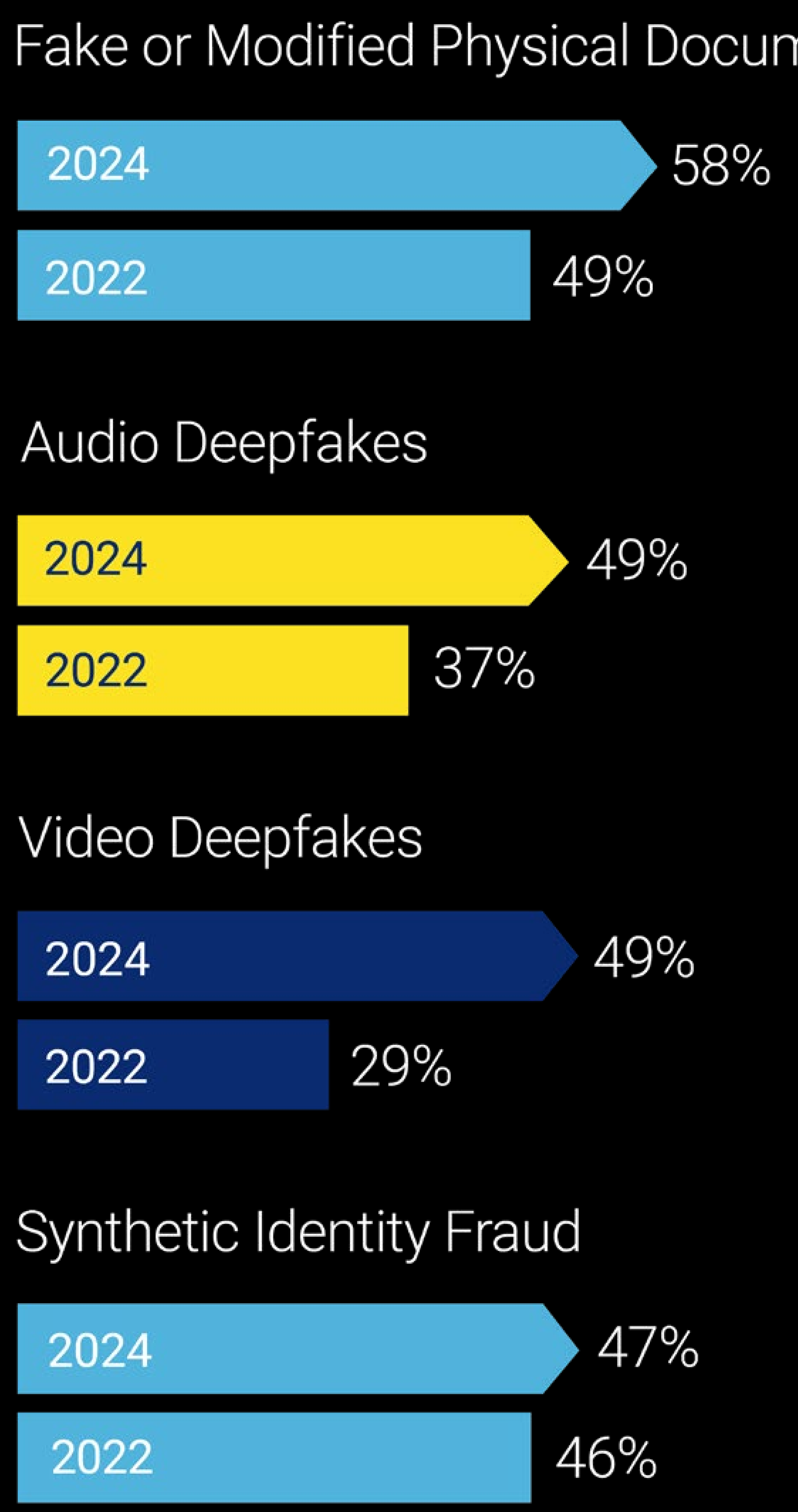
The rise in deepfake incidents, as reported in AuthenticID's 2024 fraud survey and corroborated by external sources, underscores the urgent need for enhanced detection and prevention measures. What was once a concern has rapidly become a reality, materializing faster than many experts predicted.

[1] AuthenticID State of Identity Fraud Surveys, 2024.

[2] "Majorities of Americans are concerned about the spread of AI deepfakes and propaganda," YouGov, Published September 12, 2023.

Surge in Identity Fraud Tactics Over the Past 2 Years*

Businesses report fraud methods they've observed.



*Regula's 2024 Deepfake Trends Study

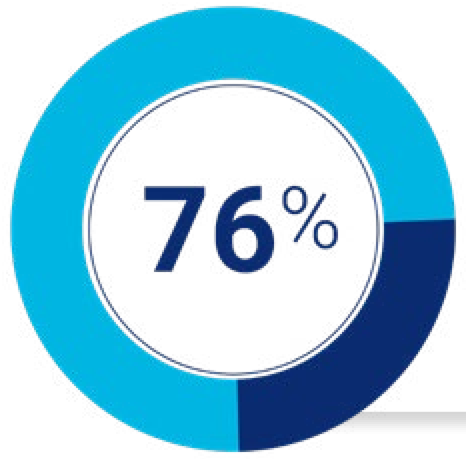
DEEPFAKES: BLURRING REALITY cont’d

Outdated customer identification, identity verification, and customer due diligence protocols mean companies are at risk of exposure by deepfake scams.

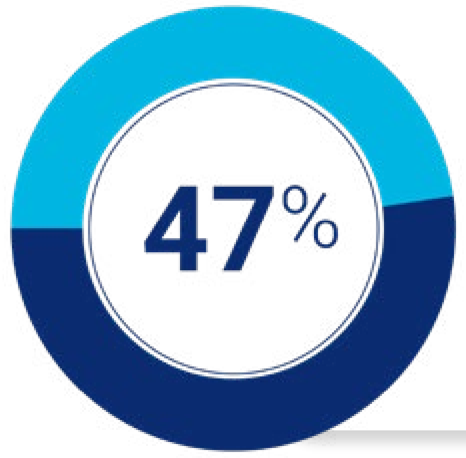
The situation is serious enough to warrant a FinCEN Alert focused solely on deepfake attacks.[3] Here’s what FinCEN says are the driving factors of these attacks:

- ✓ **Low barrier to entry**
- ✓ **Fraudsters use them to create IDs, photos, and videos to trick platforms**
- ✓ **Institutions face financial losses and compliance challenges from these attacks**
- ✓ **There’s no silver bullet to mitigate**

By the time an organization detects a digital injection attack using deepfakes, it’s already too late.



Business **owners** who are confident in their business’ ability to detect deepfake threats.*



Employees who are confident in their business’ ability to detect deepfake threats.*

**The survey results between business owners and employees at a business suggest a meaningful gap between confidence and competence in detecting deepfakes.*

*Regula’s 2024 Deepfake Trends Study

> *Despite the sophistication of deepfake technology, subtle clues in language and context can sometimes betray their authenticity. As the battle against misinformation intensifies, the quest for effective safeguards and consumer education against deepfakes remains imperative.*
>
> – Blair Cohen
> President & Founder, AuthenticID

[3] FinCEN Alert on Fraud Schemes Involving Deepfake Media Targeting Financial Institutions, Issued November 13, 2024.

THE TECHNOLOGY THAT FUELS DEEPFAKES: AI AND ITS PROGRESS

2024 in review: AI-fueled deepfakes

JANUARY

PRESIDENT JOE BIDEN

Robocalls using deepfake voice generation impersonated President Biden told recipients not to vote in New Hampshire's primary.

TAYLOR SWIFT

Pornographic, AI-generated images of the American pop star Taylor Swift spread across social media.

FEBRUARY

HONG KONG EXECUTIVE

British engineering company Arup was the victim of a deepfake fraud after an employee was duped into sending HK$200m (£20m) to criminals after fraudsters used deepfake technology to impersonate the company's chief financial officer and other staff during a video conference call.

MAY

ADVERTISING EXECUTIVE

Fraudsters impersonated the CEO from WPP, the world's largest advertising and public relations company. They used a fake WhatsApp account, a voice clone and YouTube footage to virtually meet and try to convince a colleague to set up a new business to solicit money.

AUGUST

ELON MUSK, JEFF BEZOS, & WARREN BUFFET

New York Attorney General Letitia James issues investor alert about scams target victims online with AI-manipulated videos and social feeds that show wealthy individuals like Elon Musk, Jeff Bezos, and Warren Buffet apparently touting the scammers' investment schemes, which often involve cryptocurrency.

SEPTEMBER

MEMES

AI-generated portraits and videos of presidential candidates flooded social media.

70%

THE FEAR IS REAL

70% of people are moderately or extremely worried about the threat of generative AI-based fraud and deepfakes online.[4]

[4] AuthenticID State of Identity Fraud Surveys, 2024.

WHAT'S NEXT FOR **DEEPFAKE REGULATION?**

There's growing momentum as numerous countries and U.S. states look to regulate how AI and deepfake technology can be used. In 2025, additional states could enact similar disclosure requirements. The highlights:

Congress is currently considering a number of bills as they tackle the GenAI issue, including the DEEPFAKES Accountability Act, the DEFIANCE Act of 2024, and the Protecting Consumers from Deceptive AI Act.

Several states have enacted legislation to regulate deepfakes, including Texas, Florida, Louisiana, South Dakota, New Mexico, Indiana, Washington, Oregon, Mississippi, and Tennessee.

Colorado AI Act, a deployer of a high-risk AI system that is a substantial factor in making consequential decisions concerning Colorado residents must provide a description of the AI system, its purpose, and the nature of each consequential decision.

Utah AI Act, businesses that use GenAI to interact with an individual must clearly and conspicuously disclose to the individual that they are interacting with AI.

California: AB 2355 effect January 2025 requires political ads using AI-generated content to include a disclosure, and SB 942, effective January 2026 requires GenAI systems with over a million monthly visitors make available a free AI detection tool for users to assess AI-generated content.

EU AI Act, deployers of high-risk AI systems that assist in making decisions related to individuals must inform individuals that they are subject to an AI system.

ACCOUNT TAKEOVER ATTACKS

In 2024, **Account Takeover scams rose by 250%.**[5] A typical victim of this fraud method loses about $180, and 40% of victims also experienced identity theft, adding insult to injury.[6] In the last several years, this method has skyrocketed, with accounts like social media, banking, email, and even ecommerce as common targets. Social media accounts are a serious score for bad actors, containing the types of personal information and access to other potential victims that fraudsters are looking for. In 2025, experts predict this type of fraud will overshadow other tactics like ransomware.

PAYMENT FRAUD

Beyond the threat of fraud that instant payment platforms may pose, new techniques are emerging to make identity fraud even more complex than ever. At the end of 2024, the Consumer Financial Protection Bureau (CFPB) sued the operator of Zelle as well as three of the nation's largest banks for failing to protect consumers from fraud on the platform, an indicator that payments fraud is a bigger issue than ever.[7] As consumers seek easier access to payments and funds and cheaper deals, the opportunity for fraud is high. The culprit? Organizations who don't offer robust identity verification methods, ignore fraud red flags, or who are too slow to track bad actors who bank hop. In fact, APP (authorized push payment) scams have skyrocketed and are popular with organized crime groups, in part due to their large windfall and ease of completion in fast payment systems.

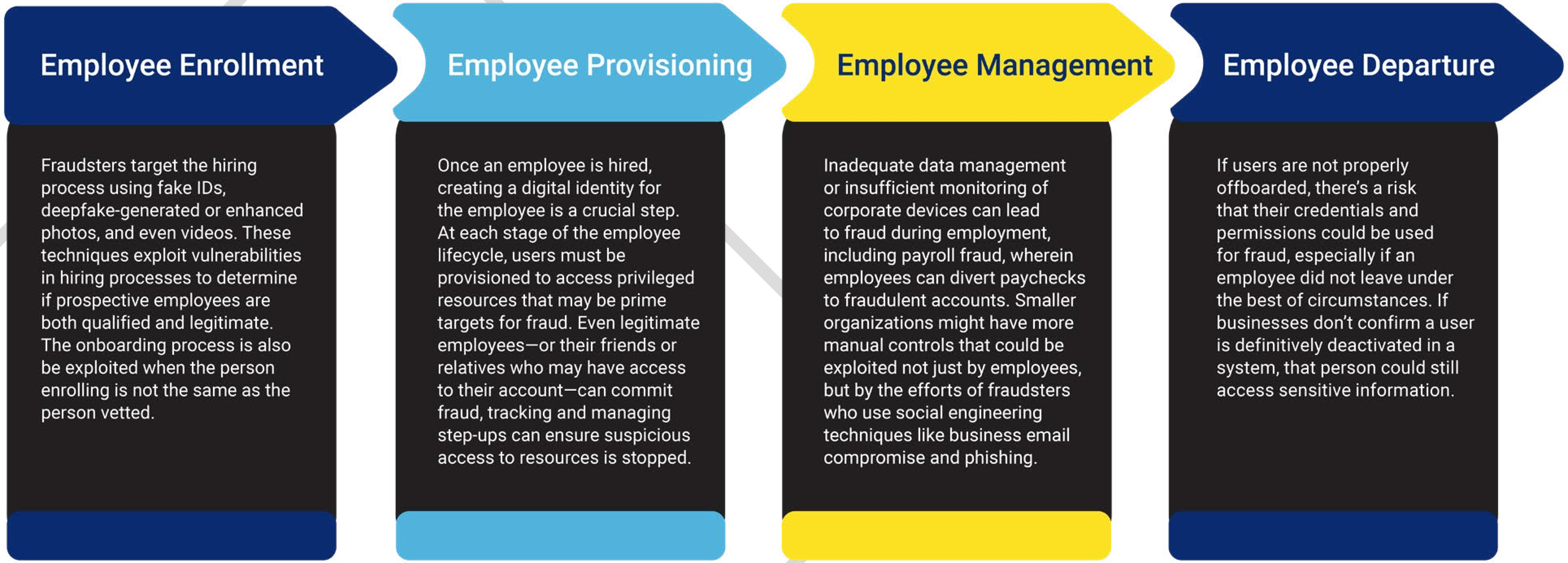
[5] "Identity Fraud in the Age of AI: Account Takeover Scams Soar 250%," Finance Magnates, Published February 11, 2024.
[6] "Account Takeover Incidents are Rising: How to Protect Yourself," Security.org, Published January 2, 2025.
[7] "CFPB Sues JPMorgan Chase, Bank of America, and Wells Fargo for Allowing Fraud to Fester on Zelle," Published December 20, 2024.

WORKFORCE FRAUD: ON THE RISE

Workforce and employee fraud is increasing, as fraudsters are targeting various points along the employee identity lifecycle. Fraud can occur at any point in an employee's tenure, merging both external and internal threats.

Bad actors can use a wealth of stolen PII, synthetic identities, and AI technology to convince employers they're a legitimate, qualified employee with a valid identity—and once they have access to your organization's systems, they can commit significant fraud. With the median global loss due to employee fraud at $145,000 in 2024, making it the world's most costly type of financial fraud, it's crucial for organizations to ensure their workforce is who they say they are.[8]

Here's where workplace systems may be vulnerable:



Employee Enrollment

Fraudsters target the hiring process using fake IDs, deepfake-generated or enhanced photos, and even videos. These techniques exploit vulnerabilities in hiring processes to determine if prospective employees are both qualified and legitimate. The onboarding process is also be exploited when the person enrolling is not the same as the person vetted.

Employee Provisioning

Once an employee is hired, creating a digital identity for the employee is a crucial step. At each stage of the employee lifecycle, users must be provisioned to access privileged resources that may be prime targets for fraud. Even legitimate employees—or their friends or relatives who may have access to their account—can commit fraud, tracking and managing step-ups can ensure suspicious access to resources is stopped.

Employee Management

Inadequate data management or insufficient monitoring of corporate devices can lead to fraud during employment, including payroll fraud, wherein employees can divert paychecks to fraudulent accounts. Smaller organizations might have more manual controls that could be exploited not just by employees, but by the efforts of fraudsters who use social engineering techniques like business email compromise and phishing.

Employee Departure

If users are not properly offboarded, there's a risk that their credentials and permissions could be used for fraud, especially if an employee did not leave under the best of circumstances. If businesses don't confirm a user is definitively deactivated in a system, that person could still access sensitive information.

[8] Association of Certified Fraud Examiners, Occupational Fraud 2024: A Report to the Nations.

Trend To Watch

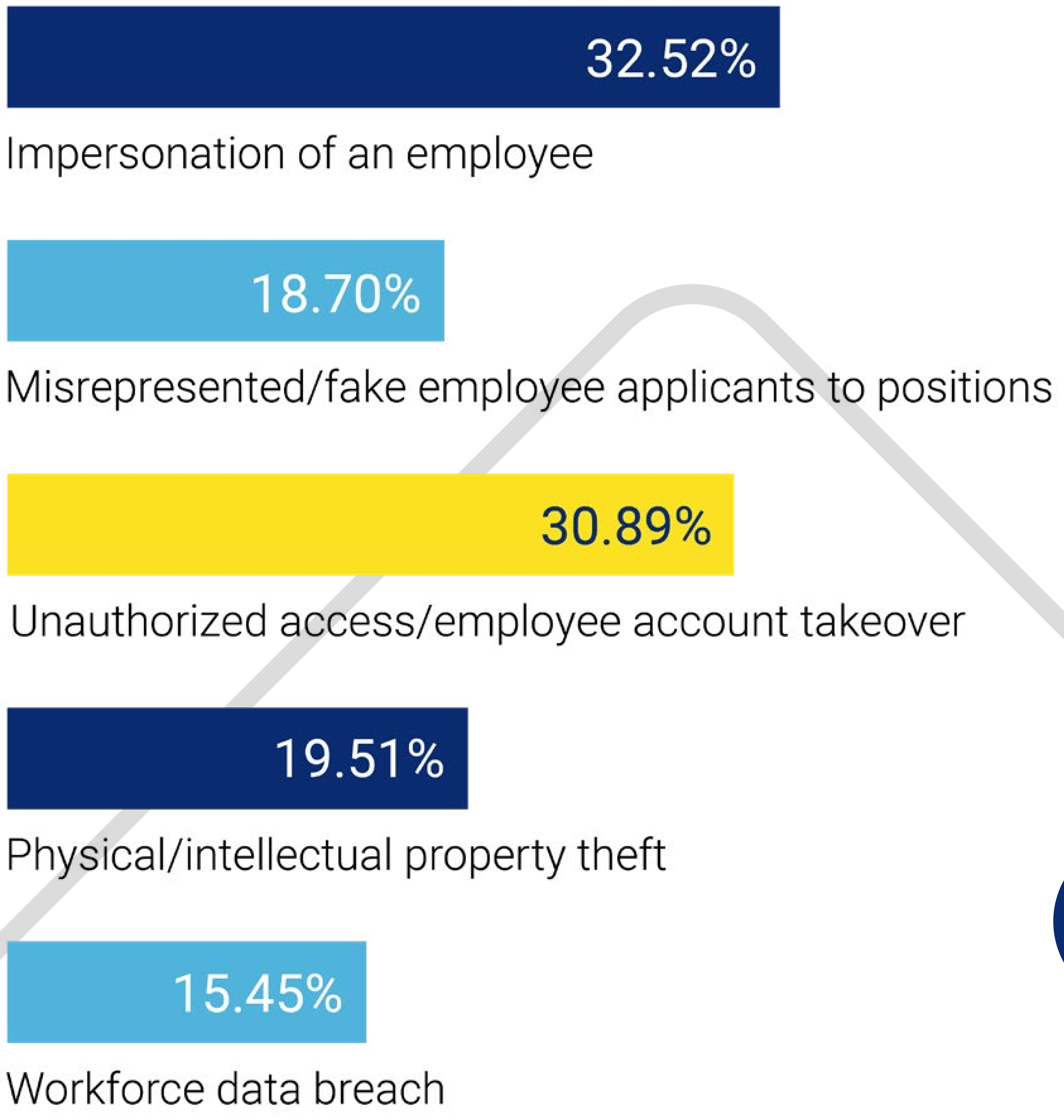
Account recovery-related fraud is on the rise as fraudsters try new ways to scam workers into giving away their credentials. Account recovery processes can be tricky for businesses to implement, as ease is important as to not create excess friction for locked-out employees, but too much ease creates opportunities for fraudsters. If an email or phone has been compromised, a bad actor can thus "recover" an account. In addition, fraudulent account recovery requests can trick employees into giving away access to their work accounts.

THE HR DIGITAL TRANSFORMATION IS NOW

While the workforce has shifted toward digital, HR processes haven't always followed suit. In 2025, expect several trends to impact how HR departments shift processes and workforce identity.

More HR departments and leaders will automate daily tasks, meaning not only will certain processes be streamlined, but the reduction in manual processes will lead to a better ability to mitigate fraud. Processes in accounts and onboarding are especially susceptible to fraud, and integrating identity authentication, including biometrics, into these processes can help.

Workplace Related Fraud*



*AuthenticID State of Identity Fraud Surveys, 2024.

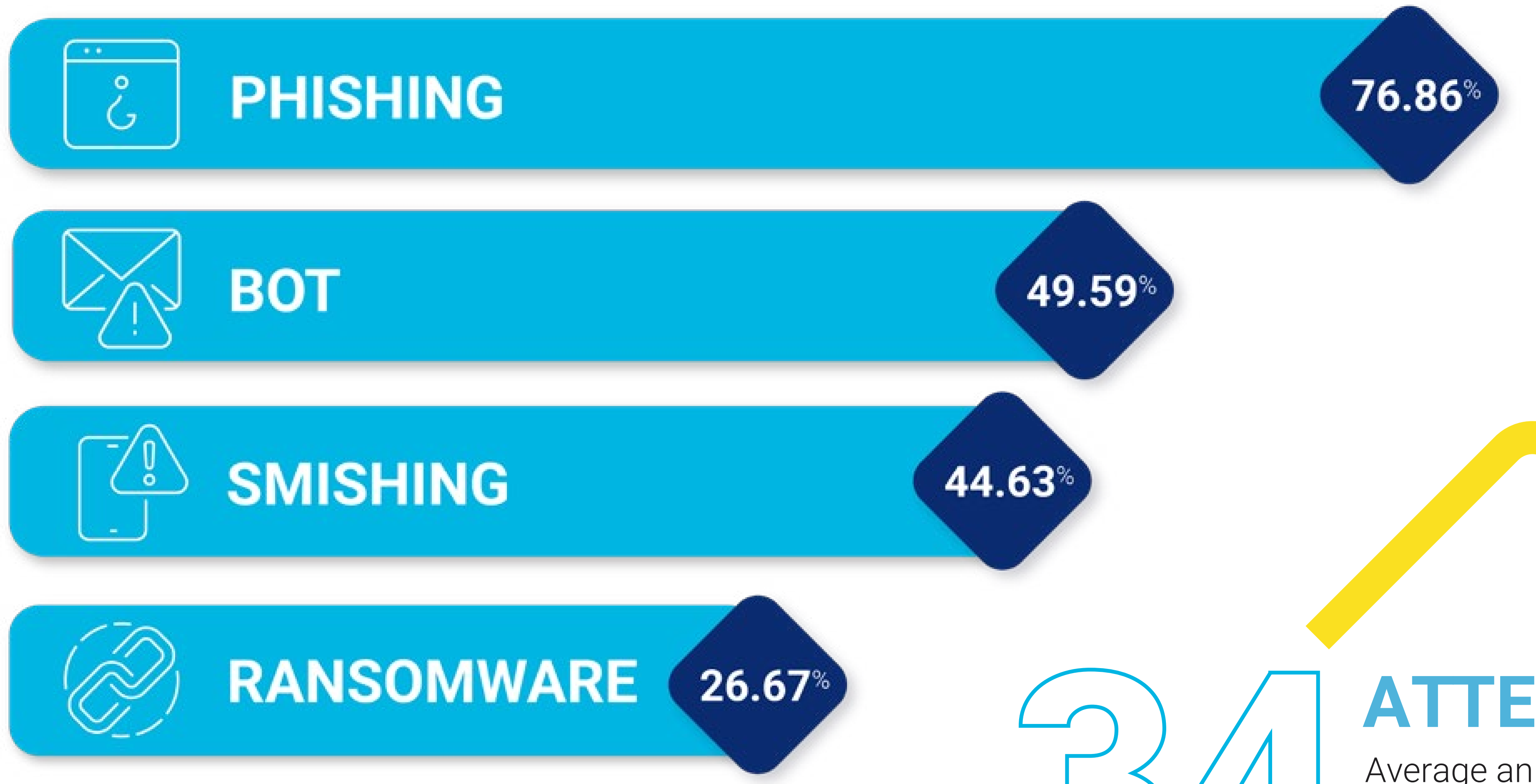
SOCIAL ENGINEERING: CLASSIC TACTIC, NEW WORRIES

In 2024, more than **90% of cyberthreats** were driven by social engineering.[9]

Social engineering attacks aren't new, but they're entering a new era: hyper-personalization. As AI tools continue to develop, it's increasingly easier for bad actors to hone in on believable, realistic human behaviors, emotions, and actions to not only mimic authentic individuals, but to manipulate victims' behavior.

The ability of attackers to impersonate legitimate individuals, organizations and/or requests is getting better, with a number of new tactics to aid them.

The Increase of Fraud Types in Business*



*AuthenticID State of Identity Fraud Surveys, 2024.

34 ATTEMPTS

Average annual suspicious communications targeting personal data or account access.*

[9] Q2 2024 Cybersecurity Trends: Rising Threats from Ransomware, Social Engineering and Identity Theft, Gen Digital, Published October 15, 2024.

RISING & EVOLVING TACTICS

Phishing

Phishing attacks have risen each year we've completed the State of Identity Fraud Report, with bad actors exploiting weaknesses in identity and access management systems. Phishing attacks now use AI to not just impersonate, but automate, with a rise in both voice phishing, tailored campaigns with lookalike domains, and AI-generated chatbots. New tools in the phishing arsenal now include commodity attacks, which impersonate big brands to trick users into clicking on malicious, fake promotions.

Business Email Compromise (BEC)

In this form of social engineering, bad actors pose as a legitimate company executive or a known vendor to trick individuals into performing illegitimate transfer of funds requests. Targeting both large and small businesses, BEC rose in 2024, with the FBI issuing a warning that these scams' attempts at employee deception were succeeding via use of techniques like pretexting.[10]

Ransomware

In 2024, ransomware made a resurgence, driven by new attacks on businesses, governments, and individuals. Sharp spikes in the US, UK, Canada, and India were driven by new tactics, including double extortion, which threatens a victim with not only file encryption but the release of sensitive data if demands aren't met. Ransomware families like LockBit hit hard in 2024 via malicious email attachments.[11]

Hyper-Personalization Era of Scams

With a wealth of personal data available on the Dark Web, scammers can now combine personalized information with the ability to create convincing content, specifically targeted to the victim. The lines between legitimate and fake communications will continue to blur with bad actors more easily able to exploit human psychology and get victims to bite.

[10] FBI Public Service Announcement Alert Number I-091124-PSA, Business Email Compromise, Published September 11, 2024.
[11] "Ransomware attacks continue to increase in the US, UK, and Canada," Avast, Published September 4, 2024.

02

How Fraudsters Have Changed –and Why They Know Us Better Than We Know Them

The more things change, the more they stay the same: fraudsters continue to be savvy opportunists with a real interest in you. And with advancements in technology, it's unfortunately easier than ever for people to become a fraudster. The opportunity for big money with even less effort is upon us.

Despite best efforts to fight them, cybercrime rings continue to grow: research shows **there is a hacker attack every 39 seconds.**[12]

FRAUD & CYBERCRIME RINGS ARE EVOLVING

Over the past several years, the explosion of **Fraud as a Service (FaaS)** means fraud has been democratized. Thanks to the accessibility of generative AI technology, bad actors are not only committing fraud themselves, but selling the tools, infrastructure, and expertise to enable others to do the same. Even a wannabe fraudster with limited skills can create fake websites and IDs, send bulk emails, and harvest personally identifiable information at scale. Dark web FaaS platforms offer ready-made tools and tactics for new and seasoned bad actors, whether they're working alone or with a syndicate.

Today, cybercriminals are taking advantage of **mule herders and mule networks** that can move faster than ever, with the IRS issuing a warning to taxpayers in 2024 about this threat. In money mule networks, individuals move funds between accounts, varying currencies, and blockchains to avoid detection by law enforcement. These networks often recruit individuals under 35 years old via deceptive job offers and promises of instant cash.

39 SECONDS

The average frequency of a hacker attack.

[12] Clark School Report via Astra.

[13] “‘Darcula’ Phishing-as-a-Service Operation Bleeds Victims Worldwide,” Dark Reading, Published March 27, 2024.

[14] “AT&T, Verizon targeted by Salt Typhoon cyberespionage operation, but networks secure,” Reuters, Published December 24, 2024.

TOP COUNTRIES FOR CYBERCRIME RING GROWTH*

- Thailand
- China
- Bangladesh
- Vietnam
- Cambodia
- Hong Kong
- Oman
- Singapore

*AuthenticID Internal Data Fraud Analysis from 2024

Sophisticated **Phishing as a Service (PhaaS)** platforms like ‘Darcula’ offer bad actors access to branded phishing campaigns for subscription prices of $250 per month. The access includes tools like JavaScript, allowing identity thieves to use iMessage and RCS (rich communication services) to bypass SMS security.[13]

Telecommunications companies faced one such cybercrime ring this year, as a Chinese-linked cyberespionage ring called **Salt Typhoon** attacked large telecom companies including AT&T, Lumen, and Verizon, as hackers gained access to networks to geolocate millions of individuals and record phone calls.[14] Salt Typhoon has also been linked to US presidential election campaign attacks. The ALPHV/BlackCat ransomware group was also responsible for 2024's breach at Change Healthcare–another heavy hitter that poses a threat to other organizations.

THE FRAUDSTERS TOOLBOX

Injection attacks and presentation attacks are among the most prevalent techniques used by fraudsters in identity verification workflows. Understanding how these tactics operate is crucial for developing effective defenses and safeguarding against fraud and the detection of AI-generated content and deepfakes.

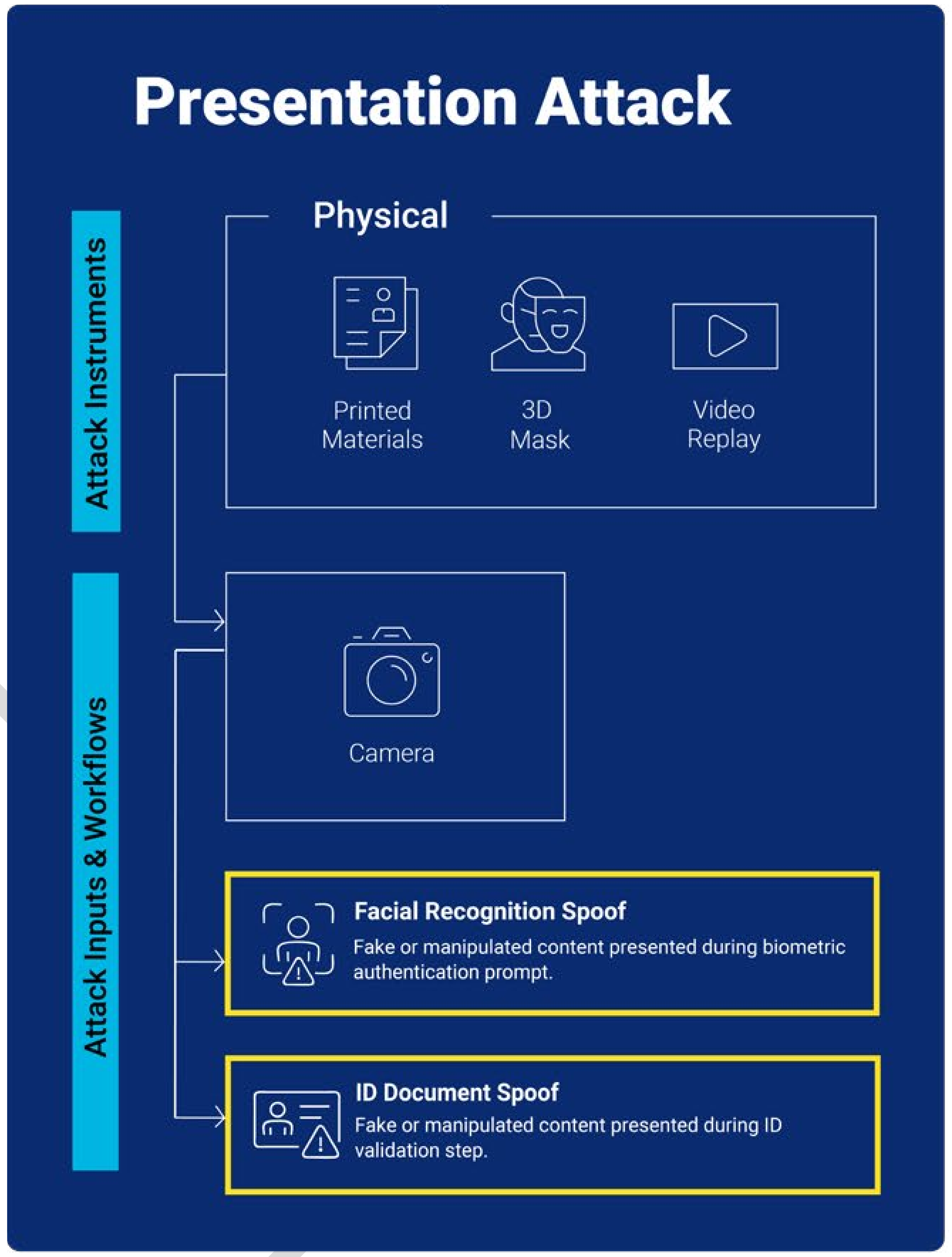
UNDERSTANDING THE DIFFERENCE

Presentation Attack

An attempt to deceive an authentication system by using falsified biometric or identity data in the capture process to create an account or grant access to an existing account.

Injection Attack

An attempt to manipulate the data stream itself by injecting false biometric or identity data into the system through software/hardware hacks, to bypass the normal capture process.



Presentation Attack

Attack Instruments

Physical

Printed Materials

3D Mask

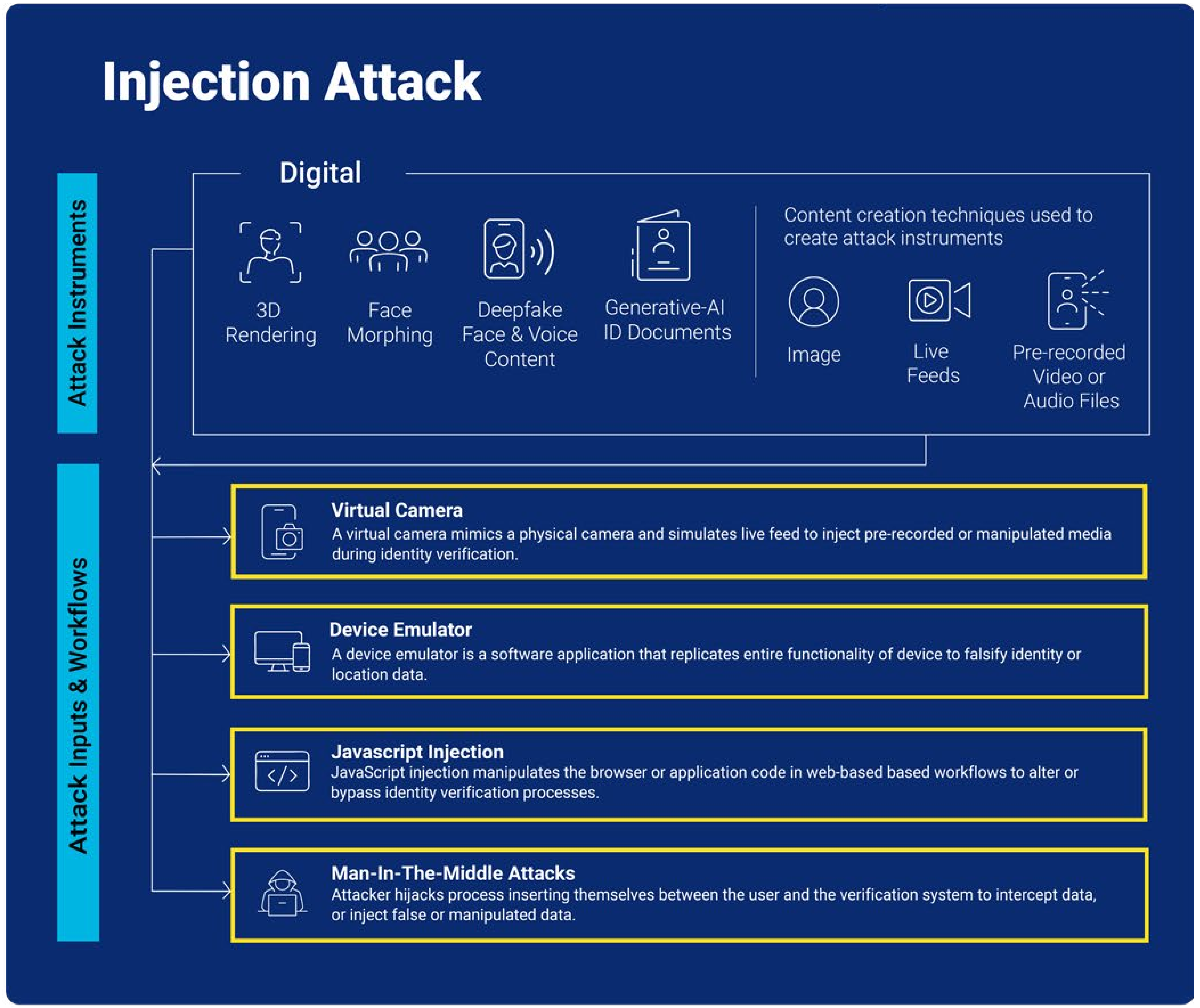
Video Replay

Attack Inputs & Workflows

Camera

Facial Recognition Spoof
Fake or manipulated content presented during biometric authentication prompt.

ID Document Spoof
Fake or manipulated content presented during ID validation step.



Injection Attack

Attack Instruments

Digital

3D Rendering

Face Morphing

Deepfake Face & Voice Content

Generative-AI ID Documents

Content creation techniques used to create attack instruments

Image

Live Feeds

Pre-recorded Video or Audio Files

Attack Inputs & Workflows

Virtual Camera
A virtual camera mimics a physical camera and simulates live feed to inject pre-recorded or manipulated media during identity verification.

Device Emulator
A device emulator is a software application that replicates entire functionality of device to falsify identity or location data.

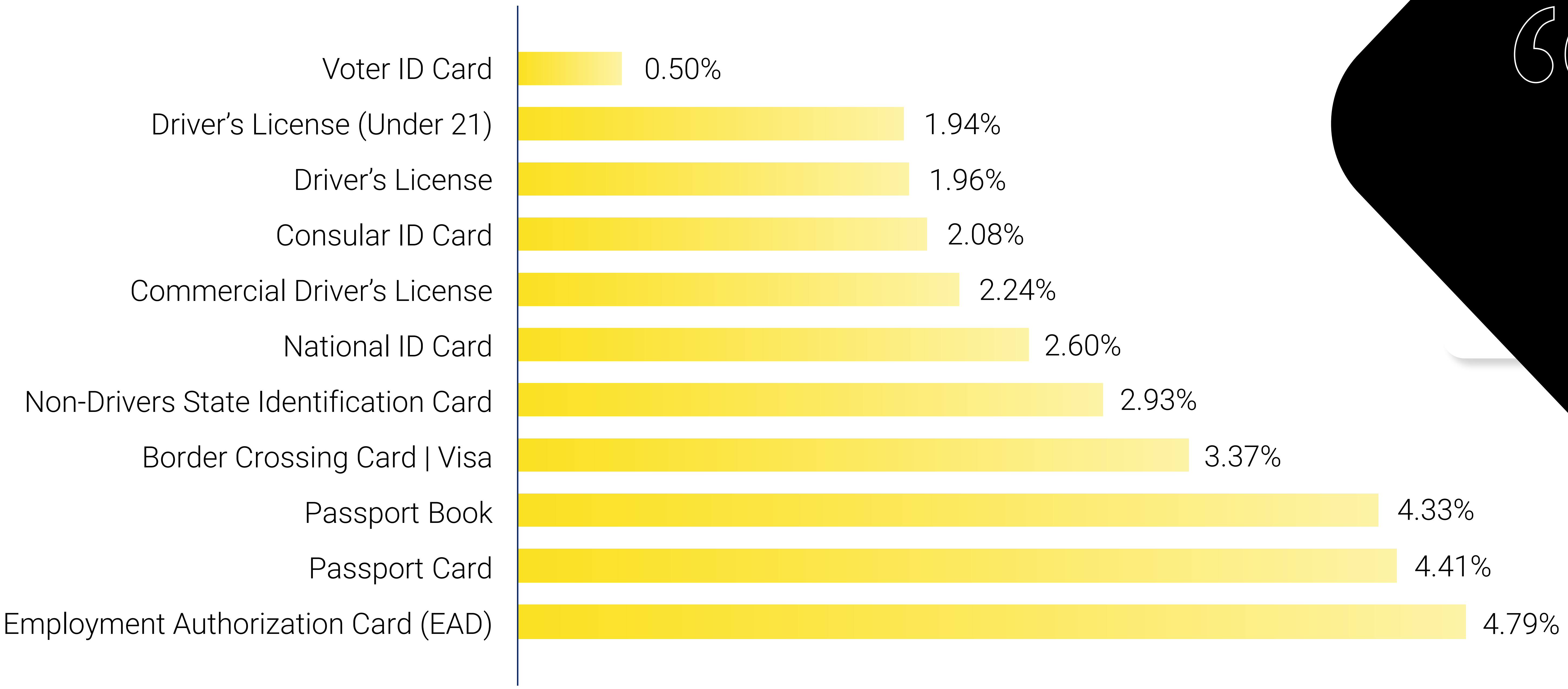
Javascript Injection
JavaScript injection manipulates the browser or application code in web-based based workflows to alter or bypass identity verification processes.

Man-In-The-Middle Attacks
Attacker hijacks process inserting themselves between the user and the verification system to intercept data, or inject false or manipulated data.

FORGED IDENTITY DOCUMENTS

In 2024, AuthenticID detected **42% more fake IDs** and suspicious biometric transactions processed through its verification system year-over-year. The platform conducts over **500 forensic checks** during each verification. Passports surpassed driver's licenses in triggering fraud-related events, while EAD or work permit cards emerged as the most frequently flagged document type for fraud.

Fraud Rate By Document Type*

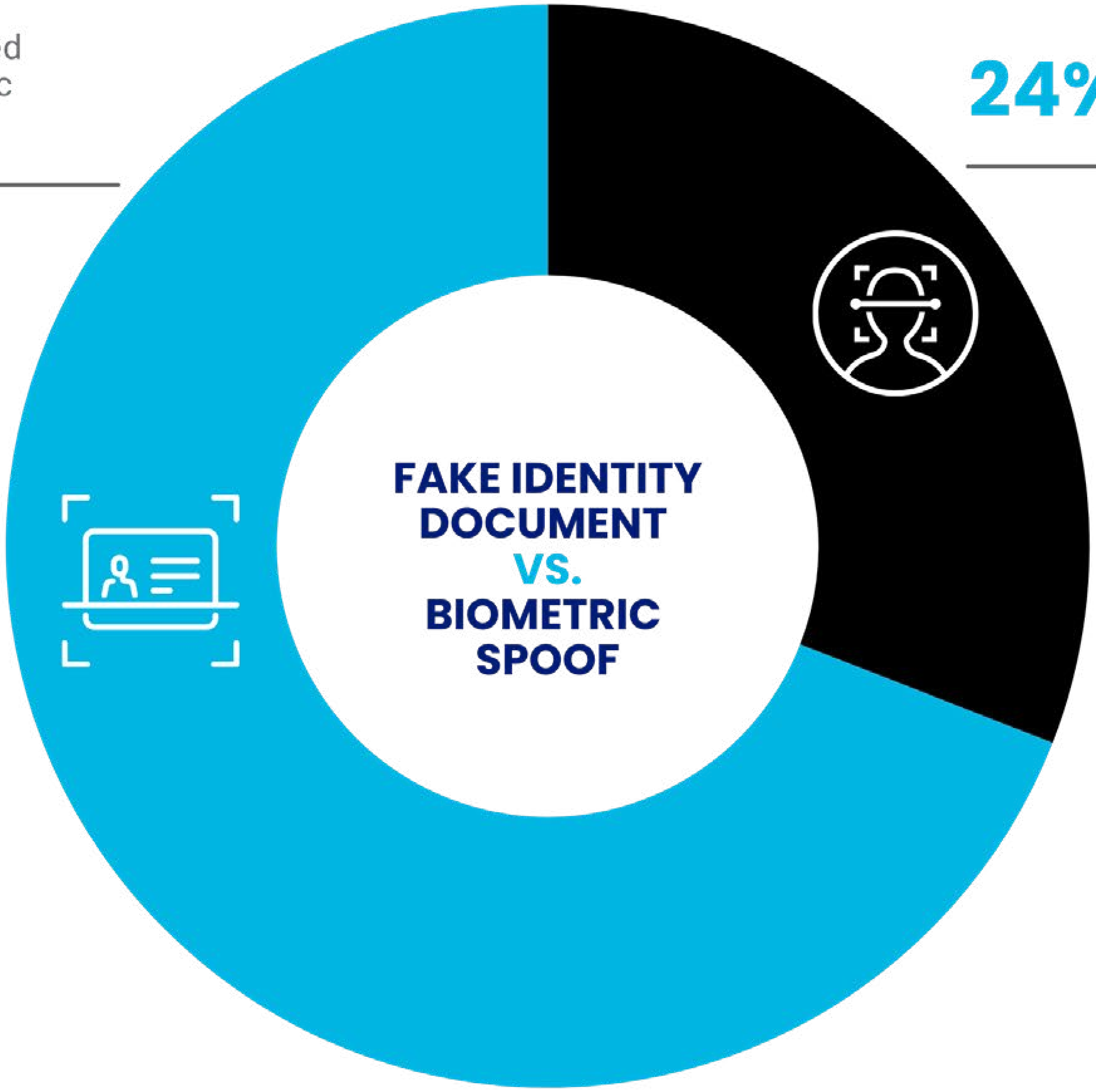


*AuthenticID Internal Data Fraud Analysis from 2024.

> *SYFRR continues to see significant increases in identity fraud, identity theft, and first-person fraud in both online and in-person lending and account opening processes. Application, data security, and* ***multiple layers of anti-fraud systems*** *continue to be SYFRR's largest expense.*
>
> – Scott Goessling, CEO
> SYFRR

HYBRID FRAUD ATTACKS

Fraudsters know organizations have better security protocols and consumers are increasingly wary of scams, so a simple fake email may not work in a phishing attack. Bad actors can combine tactics and tools into a single attack or a "long con." For example, scammers can use fake support emails, and texts can be used to connect you with an imposter claiming to be from the Social Security Administration to convince you that your account has been compromised. In other instances, scammers can use deepfakes paired with social engineering techniques making authorized push payment (APP) fraud scams more likely to get a victim to wire funds.



76% Fraud Flagged During ID Doc Verification*

Fraud Signal Triggered During:

41% Material Analysis
44% Visual Analysis
15% Barcode and Behavioral Analysis

24% Fraud Flagged During Biometric Authentication*

Fraud Signal Triggered During:

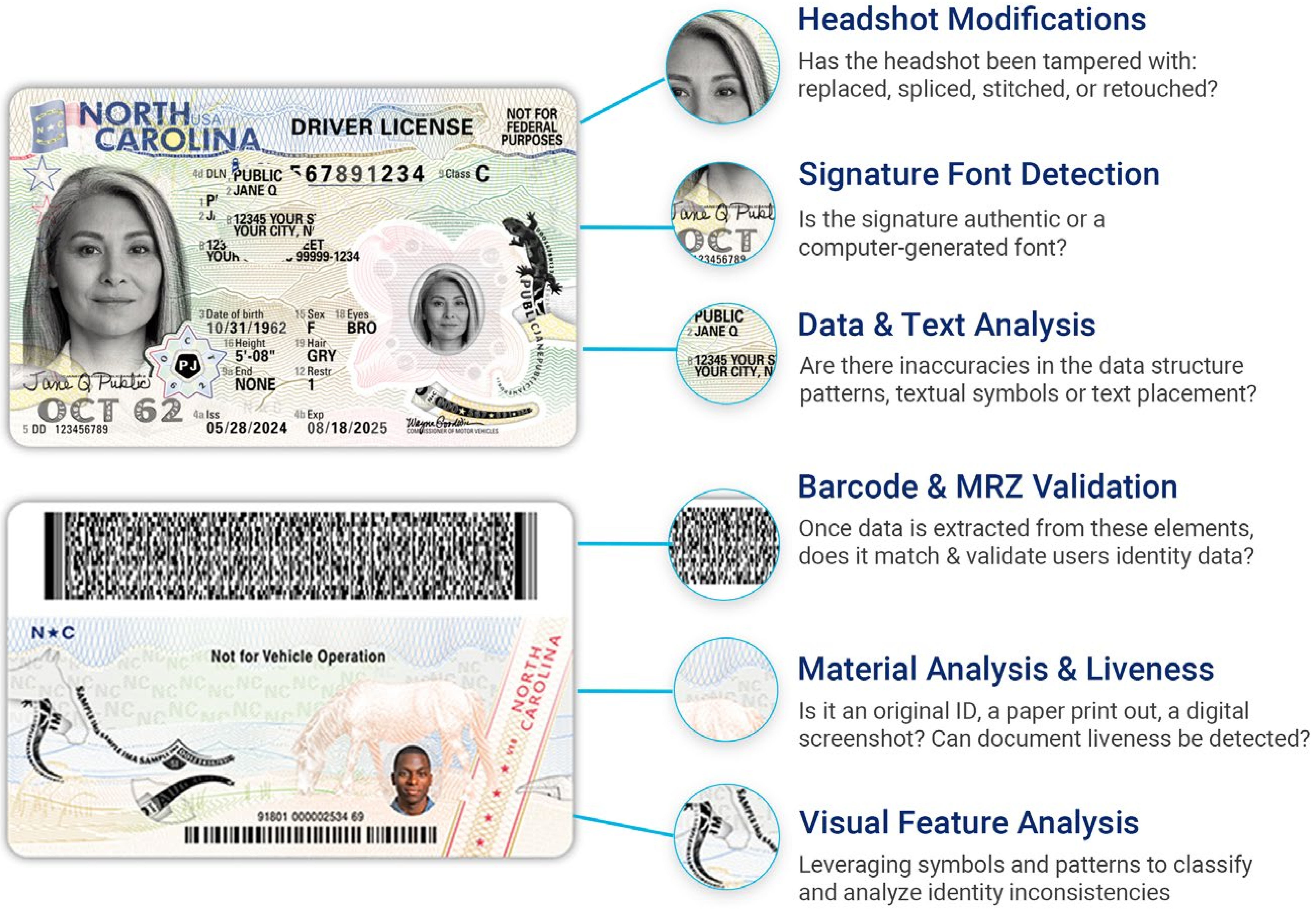
46% Bad Actor Biometric Watchlist Check
43% Selfie Liveness
11% Face Match

*AuthenticID Internal Data Fraud Analysis from 2024.

INNOVATIONS ON IDENTITY DOCUMENTS: TIGHTEN SECURITY

With the rise in forged identity documents, robust security features are critical to stopping fraudsters. In 2024, the **North Carolina Division of Motor Vehicles** introduced redesigned driver licenses, permits, and identification cards incorporating cutting-edge security elements to combat fraud. These new designs include over 50 advanced security features to support law enforcement in detecting and deterring fraudulent activity.

At AuthenticID, we analyze numerous characteristics of identity documents to ensure their authenticity, some of which are highlighted in the diagram shown.



Headshot Modifications

Has the headshot been tampered with: replaced, spliced, stitched, or retouched?

Signature Font Detection

Is the signature authentic or a computer-generated font?

Data & Text Analysis

Are there inaccuracies in the data structure patterns, textual symbols or text placement?

Barcode & MRZ Validation

Once data is extracted from these elements, does it match & validate users identity data?

Material Analysis & Liveness

Is it an original ID, a paper print out, a digital screenshot? Can document liveness be detected?

Visual Feature Analysis

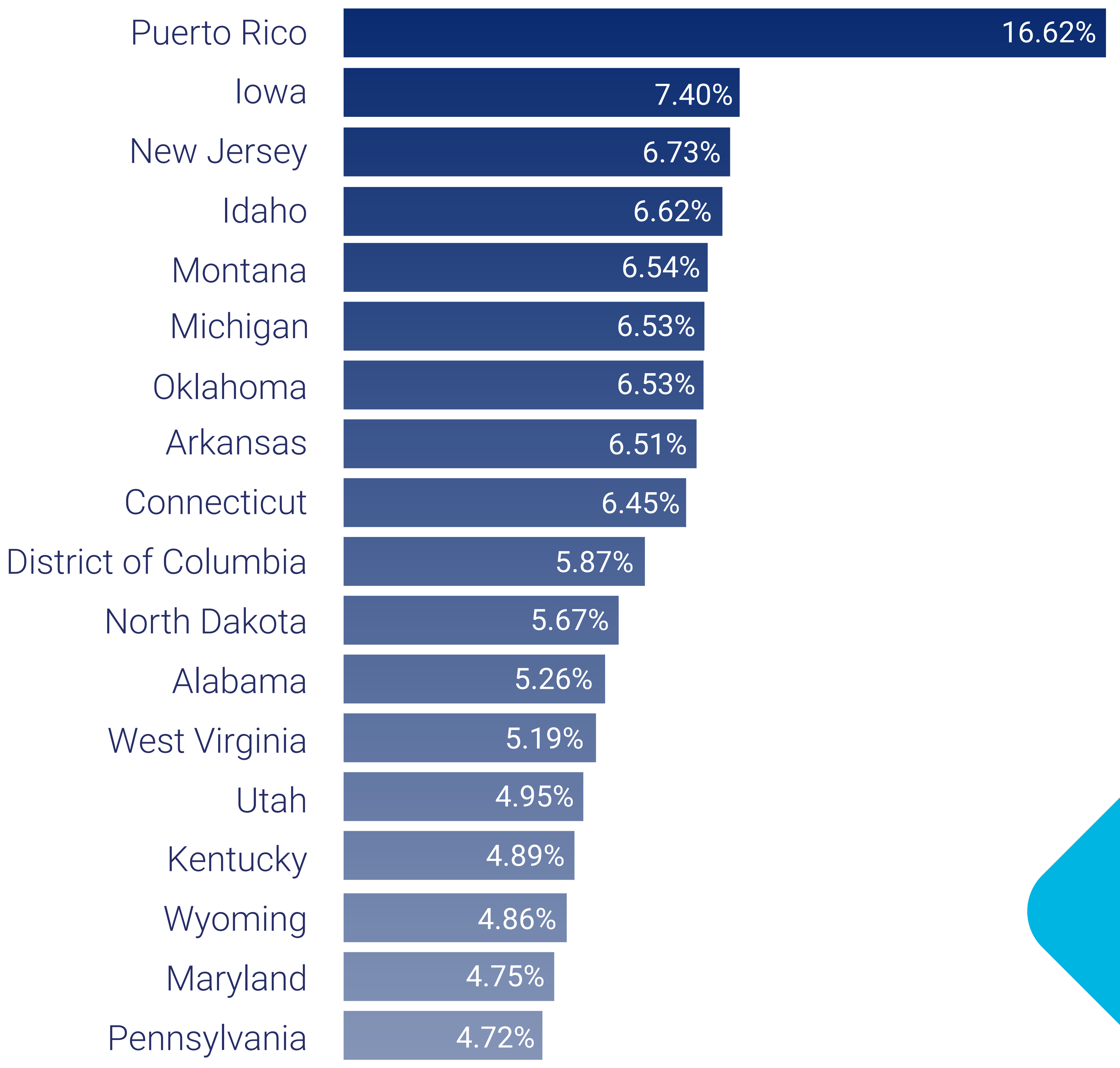
Leveraging symbols and patterns to classify and analyze identity inconsistencies

ID Images courtesy of N.C. Department of Motor Vehicles.

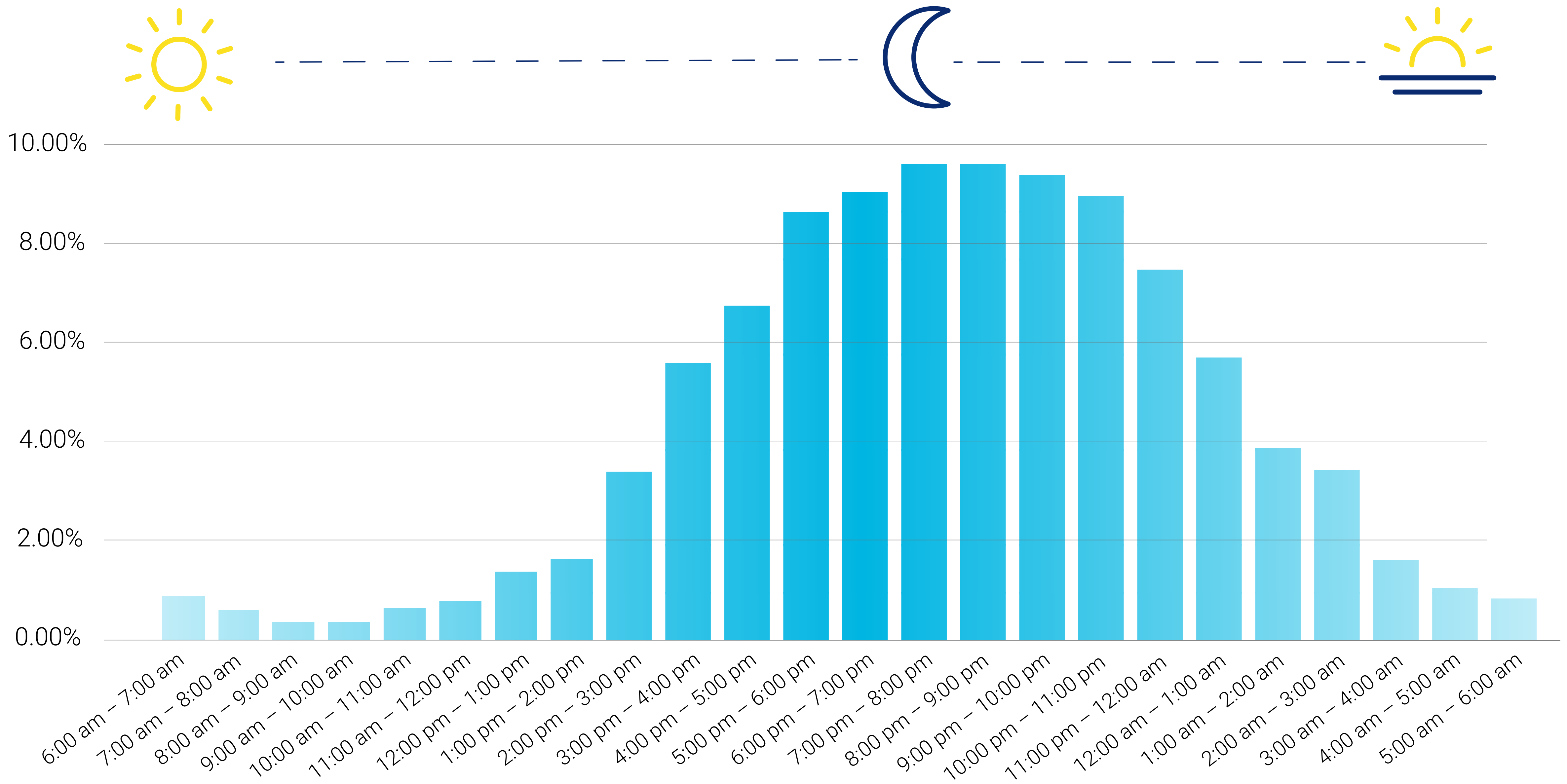
03

When & Where Fraudsters Attack

Fraud Rate per State Transaction Location*

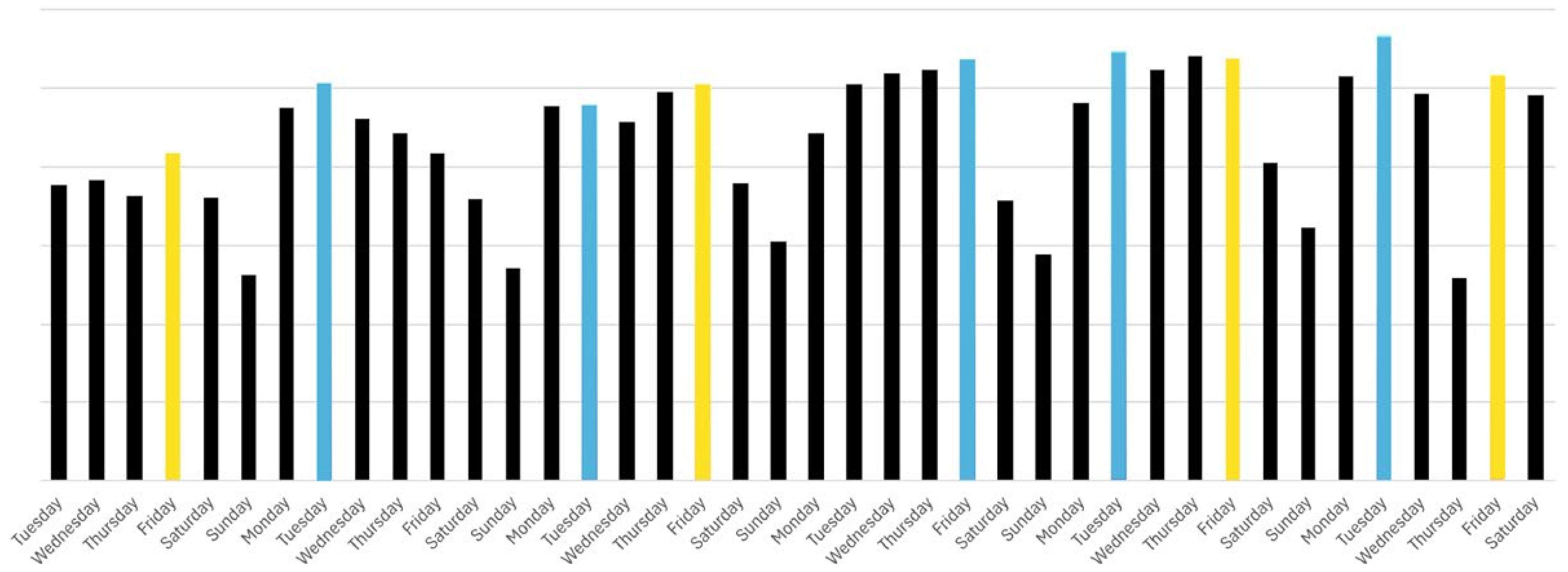


Percentage of Fraud by Time of Day*



*AuthenticID Internal Data Fraud Analysis from 2024.

Days of the Week When Fraudsters Hit Most*



🟨 Tuesdays

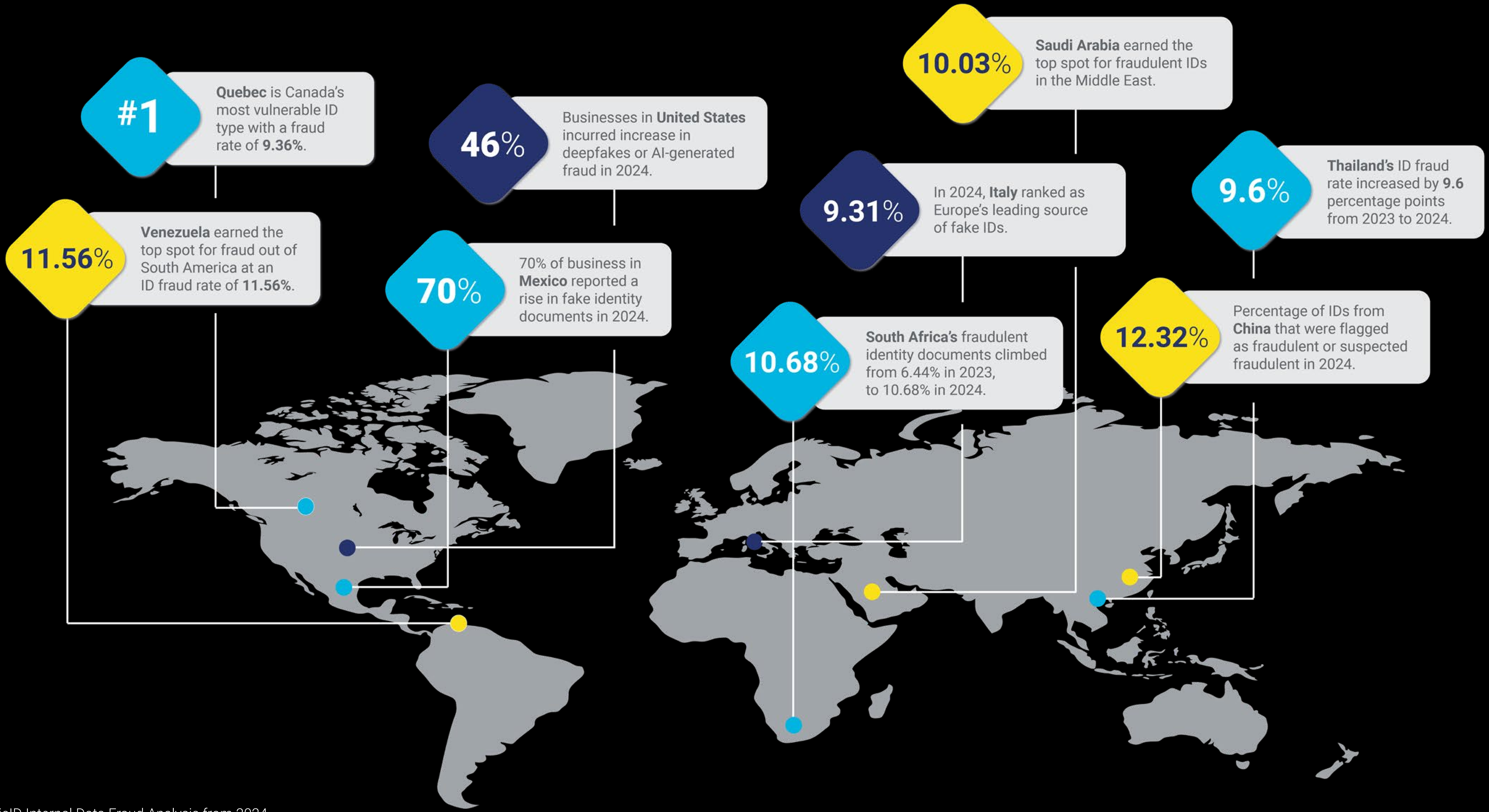
🟦 Fridays

Peak days for fraud activity

In 2024, we observed not only trends in the days of the week when fraud was most commonly committed but also clear seasonality patterns. Significant spikes occurred in April during tax season, in July with the kickoff to summer, and in December during the holiday season.

*AuthenticID Internal Data Fraud Analysis from 2024.

The Global Impact Of Identity Fraud*



#1 **Quebec** is Canada's most vulnerable ID type with a fraud rate of **9.36%**.

11.56% **Venezuela** earned the top spot for fraud out of South America at an ID fraud rate of **11.56%**.

46% Businesses in **United States** incurred increase in deepfakes or AI-generated fraud in 2024.

70% 70% of business in **Mexico** reported a rise in fake identity documents in 2024.

10.68% **South Africa's** fraudulent identity documents climbed from 6.44% in 2023, to 10.68% in 2024.

9.31% In 2024, **Italy** ranked as Europe's leading source of fake IDs.

10.03% **Saudi Arabia** earned the top spot for fraudulent IDs in the Middle East.

12.32% Percentage of IDs from **China** that were flagged as fraudulent or suspected fraudulent in 2024.

9.6% **Thailand's** ID fraud rate increased by **9.6** percentage points from 2023 to 2024.

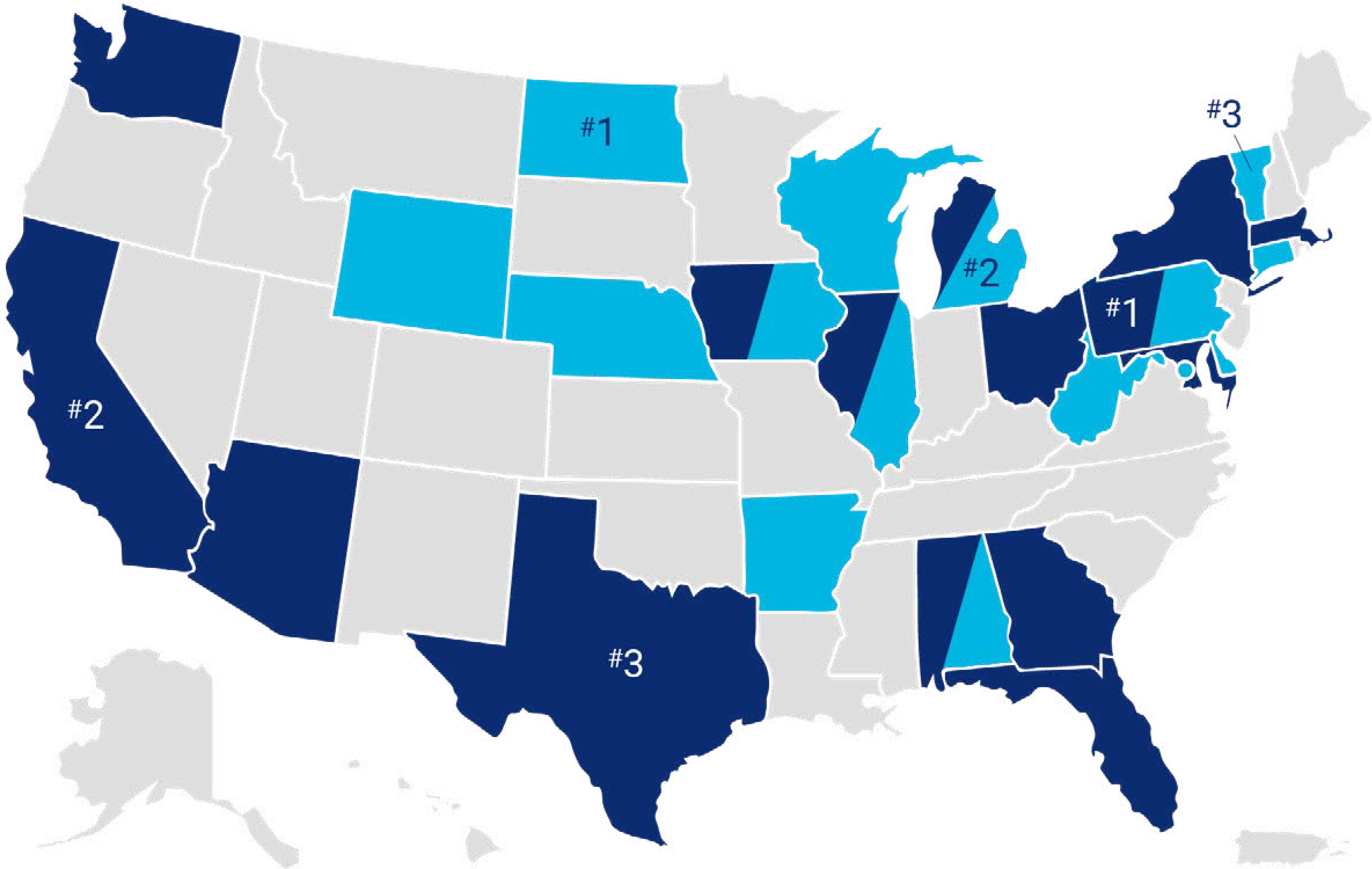
*AuthenticID Internal Data Fraud Analysis from 2024.

State-Issued IDs with the Most Red Flags*

Top States based on Transaction Volume

These numbers naturally correlate with population and customer footprint.

1 Pennsylvania
2 California
3 Texas
4 Florida
5 New York
6 Michigan
7 Ohio
8 Illinois
9 Georgia
10 New Jersey
11 Arizona
12 Massachusetts
13 Washington
14 Iowa
15 Alabama



Top States based on Fraud Rate

These numbers may indicate perceived vulnerability of state ID security features or accessibility of IDs by fraudsters.

1 North Dakota
2 Michigan
3 Vermont
4 Pennsylvania
5 Iowa
6 Delaware
7 Nebraska
8 Wisconsin
9 Wyoming
10 West Virginia
11 Arkansas
12 District of Columbia
13 Connecticut
14 Illinois
15 Alabama

*AuthenticID Internal Data Fraud Analysis from 2024.

04

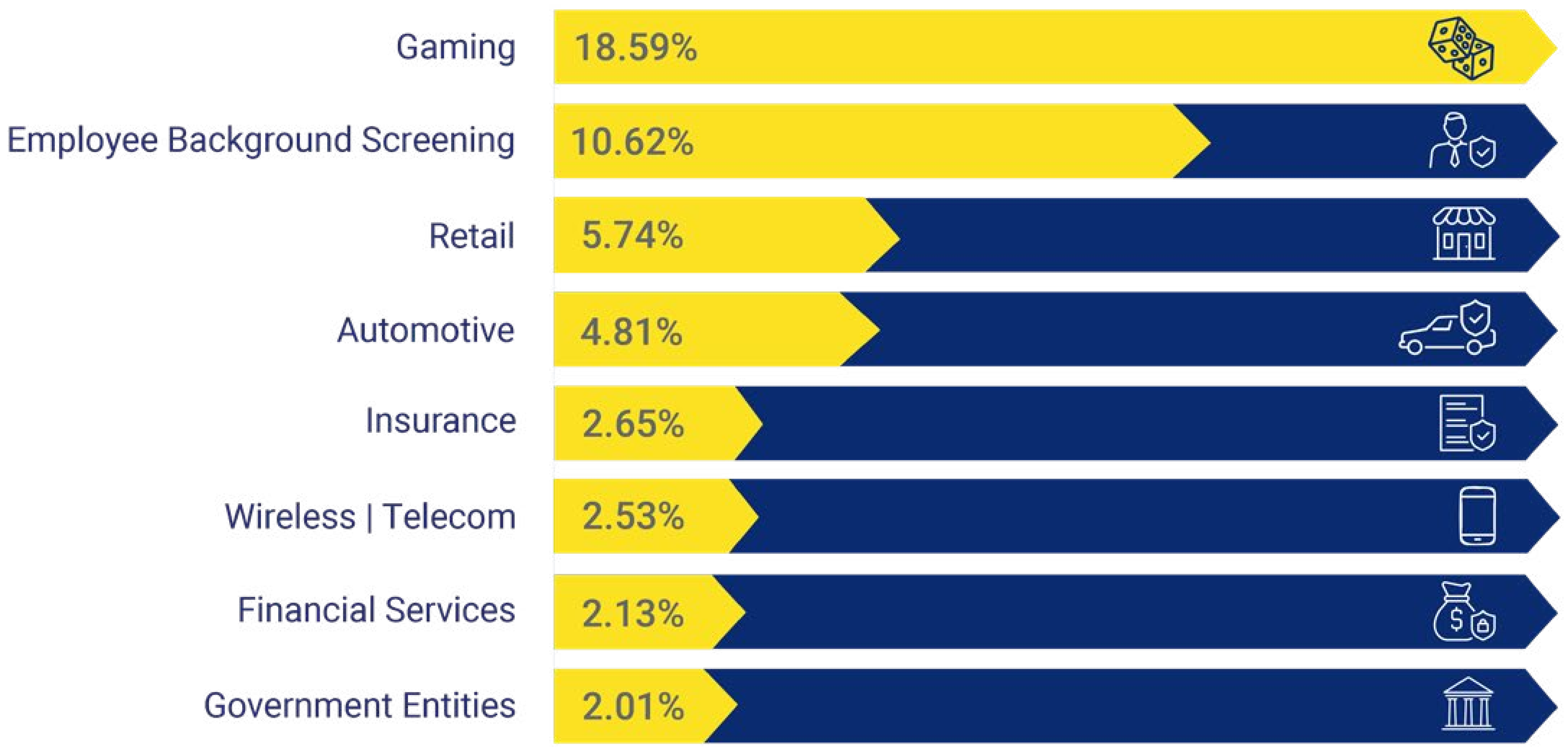
At a Glance: How Fraud Hits Industries

Identity fraud attacks all industries, but several industries are at a higher risk for the evolving, sophisticated identity fraud we've observed in 2024. Fraudsters are developing and enhancing new strategies to exploit vulnerabilities across distinct points in the customer journey.

Among AuthenticID customers, fraud rates are highest in the gaming and employee background screening industries. Importantly, these rates are impacted by organizations' risk tolerances and thresholds, and their use cases may also affect their fraud rate. Within verticals, there are also further nuances and differences: for instance, AuthenticID lender customers see a higher fraud rate than other financial institutions including neobanks and traditional banks, coming in at 8%.

Across channels, fraud rates vary significantly, ranging from 4.6% digital fraud rate in financial services and 7.2% in gaming, as reported by TransUnion.[15] The chart below represents fraud for all channels combined.

Fraud Rate By Industry*



GAMING

EMPLOYEE BACKGROUND SCREENING

NOTABLY ON THE RISE

[15] TransUnion, "State of Omnichannel Fraud," H2 2024 Update.
*AuthenticID Internal Data Fraud Analysis from 2024.

FINANCIAL Institutions

Financial institutions continue to be a prime target for bad actors; in 2025, this trend will most likely grow, driven by increased consumer need for fast, digital options for payments, purchases, and banks, and the proliferation of synthetic identity fraud.

Consumers are split on whether institutions are doing enough: 49% of consumers are confident their financial institution has the right security in place to protect their identities–but 51% are unsure or doubtful.

Financial organizations, like many businesses that operate apps or services digitally, face a balancing act of fraud protection vs. customer experience. And for consumers, security ranks the highest: our data shows that **67% of people** put security features as the factors that matter most to them during new account opening.

> *Identity fraud with all of the current technology and the ability to use the dark web to create fake identities will continue to escalate and require subject matter experts and appropriate training and technology to thwart attacks.*
>
> – Garry W.G. Clement, CAMS, CFE, CFCS, FIS, CCI
> Chief Anti-Money Laundering Officer at Versa Bank

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	5.74%	24.95%	33.86%	20.59%	14.85%
Frictionless access to online accounts and account recovery (forgot login info)	3.20%	14.71%	34.54%	28.14%	19.40%
Strong security measures to ensure unauthorized access to my account	2.34%	5.10%	15.71%	22.51%	54.35%
Trusted adherence to privacy and compliance regulation to keep my personal data safe	1.96%	4.79%	14.16%	23.75%	55.34%

*AuthenticID State of Identity Fraud Surveys, 2024.

FINANCIAL **INSTITUTIONS:** Traditional Banks

What to Watch

Scams are becoming increasingly sophisticated and are hitting traditional banks hard. Because AI has made identity scams, phishing, and other methods more difficult to detect, banks will need to double down on their use of ML/AI as well as risk factors and flags during all customer touchpoints to stop fraud before losses escalate. Scams are often more difficult for banks to manage than ATO attacks, meaning banks must continue efforts to combine data sources and leverage centralized consortiums to fight fraud effectively.

Rising Fear

For years, synthetic identities have been building credit–and now they're poised to do real damage to the financial system. Check fraud also continues to grow despite a parallel growth in digital payments, meaning banks face fraud from multiple angles.

Stat to Know

ID fraud may account for 50% of bank-reported fraud by 2025.[16]

50%

OF BANK-REPORTED FRAUD = ID FRAUD

WHAT YOU DON'T KNOW CAN HURT YOU: While all financial institutions probably experience fake/modified documents, only a fraction of that number report that they have knowledge of this issue. The reason? Organizations can't report what they don't see, with some businesses nearly blind to this type of fraud, due to poor/no monitoring mechanisms or a lack of identity verification processes.

76% **Fintech** businesses that experienced fake or modified documents.*

66% **Financial Services** businesses that experienced fake or modified documents.*

[16] "ID fraud may account for 50% of all bank-reported fraud by 2025," Retail Banker International, March 11, 2024.
*Regula's 2024 Deepfake Trends Study.

LENDING

FINANCIAL **INSTITUTIONS:** Lending

What to Watch

Lenders are increasingly at risk of losses from identity scams, especially those using synthetic identities. From auto loans to bank credit cards to personal loans, synthetic identities are now a pressing threat and are being used for credit washing, which occurs when bad actors use synthetic identities to remove negative information from a credit history by filing a false identity fraud claim.

Rising Fear

Auto lending is an appealing fraud target, as dealers often offer sales incentives for financing deals–a potentially dangerous combination in an industry that has struggled with proof of income and traditional identity fraud.

Stat to Know

A record high of $3.2B in fraud hit the lending market in 2024.[17]

3.2 BILLION

PAYMENT PROCESSORS

FINANCIAL **INSTITUTIONS:** Payment Processors

What to Watch

Text message scams are increasing, and while they often target traditional banks, they're a headache for payment processors. Payment processing is also plagued by unauthorized transactions and transaction disputes, including chargebacks and friendly fraud. But those tactics often are secondary in the face of escalating social engineering tactics that mean money changes hands faster than organizations can flag.

Rising Fear

Some payment processors may be missing out on deploying robust technology, including screening tools like fraud scores that harness large datasets to slow fraud losses. What's more, payment processors often have lower rates of implementation of anti-fraud systems.[18]

What to Know

In the US, there have been changes to NACHA's ACH rules that are meant to streamline payment processing. But with these efficiencies come new vulnerabilities, as fraud systems must respond quickly to identify any bad actors or suspicious activities.

[17] TransUnion, "State of Omnichannel Fraud" H2 2024 Update.

[18] PYMNTS, The State of Fraud and Financial Crime in the US 2024: What FIs Need to Know. November 2024.

TELECOMMUNICATIONS

Industry

What to Watch:

Imposter scams and investment frauds are growing in telecommunications, as the industry was hit hard by organized cybercrime in 2024. In addition, **SIM swapping, subscription fraud, IRSF (International Revenue Sharing Fraud), and phishing** continue to escalate. As these tactics continue to rise, some are changing: subscription fraud is a huge target with post-paid plans that allow bad actors to get pricey phones without paying anything up front. By using a quick application process with weak security and sophisticated social engineering, these scams are increasingly successful.

What to Know:

$1.55 Million = **$5.5 Billion**

Counterfeit IDs Stopped in 2024 for Telecom Customers*

Savings in Estimated Fraud Loss Based on Average Cost Per Incident*

5G

RISING FEAR

Developing markets and new 5G networks are top targets for bad actors. Often, 5G has opened weak spots in organizations' security protocols, with billions of devices connecting and all-software network providing plenty of vulnerabilities.

*AuthenticID Internal Data Fraud Analysis from 2024.

TRUST Marketplaces

While each type of marketplace and service is unique, they share core identity fraud concerns: the reciprocal trust that the person or entity you're transacting with is legitimate.

Gig Economy

A third of Americans who use gig economy platforms have fallen victim to identity fraud. The millennial generation is the primary user of these accounts, so they're the most targeted victims.[19] The use of new payment methods has also opened new opportunities for fraudsters, compounding issues seen in payments and fintechs as fraudsters exploit gaps created by convenience.

Sharing Economy

Counterfeit listings on vacation rentals as well as fraud in online food ordering—when bad actors can sign on as supposed legitimate delivery people—mean that these platforms need higher standards for authenticating identity, including biometrics.

81%

81% of people surveyed view biometric authentication as a way to strengthen trust and security in marketplaces.*

Marketplaces

Identity Fraud is surging in marketplaces, which lose billions to fraud each year. With both buyer and seller to exploit, these marketplaces are plagued by high rates of ATO: for buyer accounts, bad actors can test cards and assess any account balances. For seller accounts, they can take seller profits, changing account information, or even create separate fake accounts to further scam both sellers and buyers.

54%

Consumers are looking for more security*

54% of people say biometrics would definitely or probably make them feel more comfortable using these platforms.

[19] TransUnion, 2024 US Gig Economy Semi-Annual Study.
*AuthenticID State of Identity Fraud Surveys, 2024.

RETAIL & eCommerce

What to Watch

Powered by AI and ML, retail fraud rings are growing rapidly, operating much like businesses themselves as they get increasingly efficient at fraud. By using both stolen and synthetic identities, these groups are constantly looking for new revenue streams. A frequent target for these fraudsters is first-party fraud, such as false order damage claims, nonpayment fraud, unauthorized reselling, and more. In addition, they'll place fraudulent orders and use manipulated addresses as they attempt to outsmart protocols that look for previously flagged addresses. Both consumers and retailers are victims of these fraud schemes, with credit card credentials the highest prize of many bad actors.

Rising Fear

Credential phishing has escalated, and with new tactics, it's easier than ever. Both enhanced social engineering and sophisticated malware mean that enhanced identity fraud is helping bad actors obtain more sensitive information than ever. In addition, affiliate fraud has become more common, as criminals take advantage of affiliate marketing programs aimed at delivering sales opportunities to the brand.

What to Know

eCommerce Fraud is expected to exceed $107 billion by 2029.[20] Tracking user behavior and fraudulent websites is crucial to minimizing the impact as fraudulent activity increases.

107 BILLION

[20] Juniper Research, Global Merchant Fraud Prevention Market 2024-2029. October 2024.

WORKFORCE:
EMPLOYEE BACKGROUND SCREENING

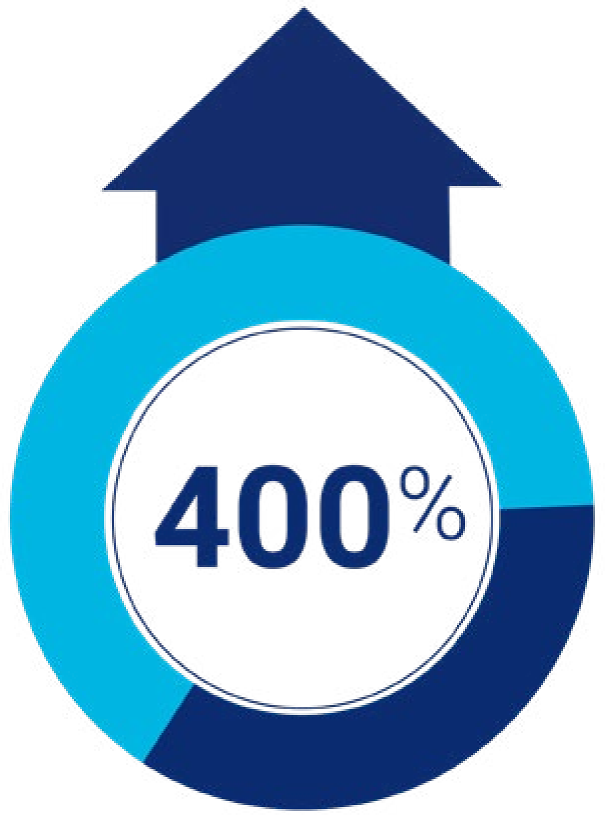
What to Watch

With the increase in remote and hybrid work, distinguishing between fraud and misrepresentation in **workforce credentials** has become critical.

Fraud involves intentional deception, such as using fake documents or stolen identities to secure employment. This can include creating entirely fictitious qualifications or using deepfake technology in interviews. Misrepresentation, while still problematic, may involve exaggerating qualifications or omitting negative information, rather than outright fabrication.

Even the most security-forward companies can be duped by new methods. KnowBe4, the world's largest security awareness training platform, unknowingly hired a threat actor to their IT team in 2024. While the employee was vetted and interviewed, the moment this employee's workstation was received, it started to load malware. Luckily, before the person was granted access to the company's network, they were discovered. This person had used AI-enhanced headshots with a valid but stolen US identity.[21] The sophistication of threats is growing, making enhanced screening a necessity.

Alarming Stats



Fake job offers and task scams **surged by 400%**, according to the FTC.[22]

Scammers can post jobs that don't actually exist or are not as they are depicted to steal your money and personally identifiable information (PII). Work-from-home job scams involving cashing suspicious checks are also on the rise. With **162,000** potential "Ghost" employers with **$1.7B** in estimated tax liability being investigated by the IRS, it's no surprise that the number one recommendation by the Treasury Inspector General is to improve verification processes for employers.[23]

162,000 "GHOST" EMPLOYERS = 1.7 billion ESTIMATED TAX LIABILITY

[21] ”How a North Korean Fake IT Worker Tried to Infiltrate Us," KnowBe4 Security Awareness Training Blog, 23 July 2024.

[22] ”New FTC Data Show Skyrocketing Consumer Reports About Game-Like Online Job Scams," FTC Release, Published December 12, 2024.

[23] Treasury Inspector General For Tax Ad.ministration, Criminal Investigation Had Success With Ghost Employers, While Civil Enforcement Efforts Can Be Improved. April 12, 2024

WORKFORCE:

EMPLOYEE BACKGROUND SCREENING cont’d

A university in India was charged with issuing a shocking **43,409 fake degrees**, with many degree holders secured government jobs.[24]

43,409

FAKE DEGREES ISSUED

6 out of **10** Resume Fraudsters were able to land a job in 2024.[25]

> *"Verifiable credentials are the new digital passport for workforce security. In an era of sophisticated identity fraud, our solution transforms credential verification from a challenge into a strategic advantage, ensuring organizations hire authentic talent with confidence."*
>
> **Dan Giurescu**, Chief Executive Officer, Credivera

Fighting Back

Verifiable credentials can offer a means to combat both fraud and misrepresentation:

Secure, Real-time Authentications
Ensures a secure, open exchange for verifiable credentials, enabling employers to instantly verify the authenticity of an applicant's qualifications with the most up-to-date data.

Holistic View of Applicants
Verifiable credentials paired with background checks, education verification, and professional certification provide the most holistic view of an employee's identity to determine authenticity.

Digital Identity Protection
Verifiable credentials ensure the integrity and immutability of credential data, making it near impossible for bad actors to manipulate or falsify information.

Streamlined Compliance
For industries with strict regulatory requirements, helps maintain compliance by ensuring all employee credentials are current and verifiable.

[24]"Rajasthan university under police radar for issuing over 40,000 fake degrees," The Economy Times. Published July 12, 2024.
[25]"Resume.org Survey Shows 6 in 10 Resume Fraudsters Landed a Job in 2024," Resume.Org. Published October 25, 2024.

05

Digital Identity: Change is Ahead, Change Is Here

The global issue of physical and digital credentials being forged is growing. Often, the process for organizations to verify the authenticity of credentials is slow, time-consuming, and expensive. But the shift of identity from physical to digital is creating a new reality for consumers, fraudsters, and businesses globally- here are the trends that will continue to shake identity in 2025.

REUSABLE IDENTITY: ENABLING NEW FRONTIERS

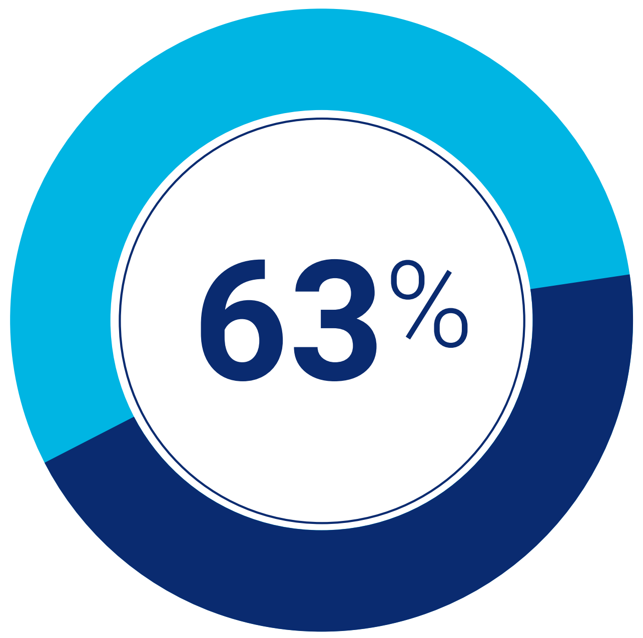
Globally, the concept of reusable identity is changing how both consumers and organizations can verify identity safely and efficiently while complying with regulatory standards. That's why shareable, reusable identity is taking hold. While initially demonstrating its value in travel, reusable identity has a potentially large number of use cases by offering a simpler sign-in process, increased convenience, standardization of data, and enhanced customer experience. Globally, several governments have launched these strategies to enhance citizen access to services, like India and Estonia. And in the European Union, plans for an interoperable European Digital Identity Wallet (EUDI) are progressing as the adoption of this technology evolves.

Reusable identity is a single, standardized, secure, and portable digital identity that multiple platforms and/or services can access for identity details. User-friendly with robust verification capabilities, reusable identity allows for verification once, reuse anywhere, or where accepted system. In a reusable identity system, a trusted authority verifies these credentials and users can access multiple systems without the need for a single-sign on system (SSO). As consumer-centric verification solutions gain steam, the demand for interoperable identity verification is rising.

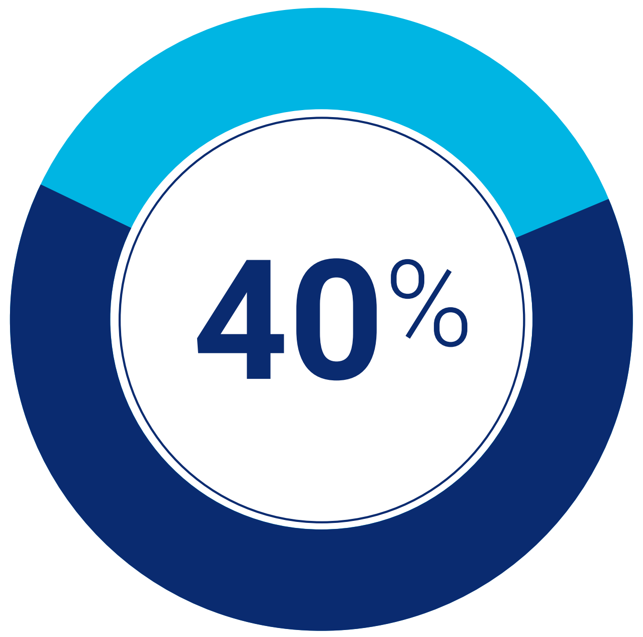
As we'll explore below, the continued evolution of digital identity means that organizations must stay vigilant: evaluating new technology that fits customer preference with the needs and risks they face in doing business online and in person.

Challenges remain ahead: As part of the digital identity evolution, the use of biometrics is moving full steam ahead, with a growing number of businesses adopting this method and consumers becoming comfortable with its use. As biometrics are incorporated into more sophisticated security mechanisms and digital identity methods, they're facing growing regulatory and consumer scrutiny. For example: in 2024, four states enacted legislation regulating the collection and use of biometric information, one state has active legislation, and ten states saw these bills rejected.[1]

63% of consumers* would go completely **passwordless** and access their accounts solely through biometrics if they had the option–and biometrics are the preferred authentication method of nearly **40% of consumers**.*



Consumers who would go completely passwordless.



Consumers who prefer biometrics as the preferred authentication method.

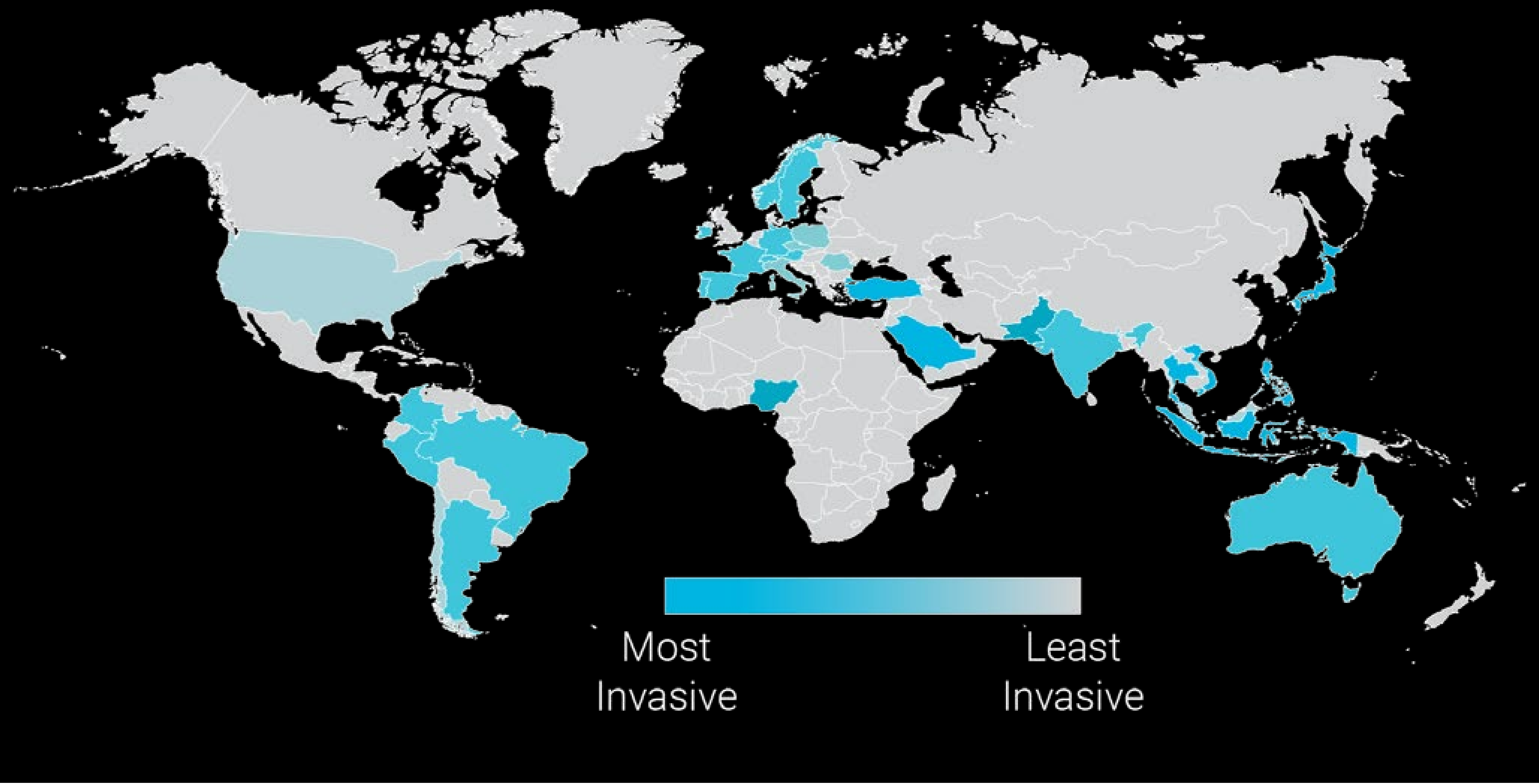
*AuthenticID State of Identity Fraud Surveys, 2024.

Digital Identities and mDLS

With a growing shift toward digital identity, digital IDs and mDLs are gaining momentum. Although the U.S. does not have a national digital ID, numerous states have adopted them. As of late 2024, twelve states have active mDL programs with interoperability across operating systems. Aside from the early adopters, there are over two dozen other states across the country that are pursuing pilot mDL programs or are currently implementing interoperability.

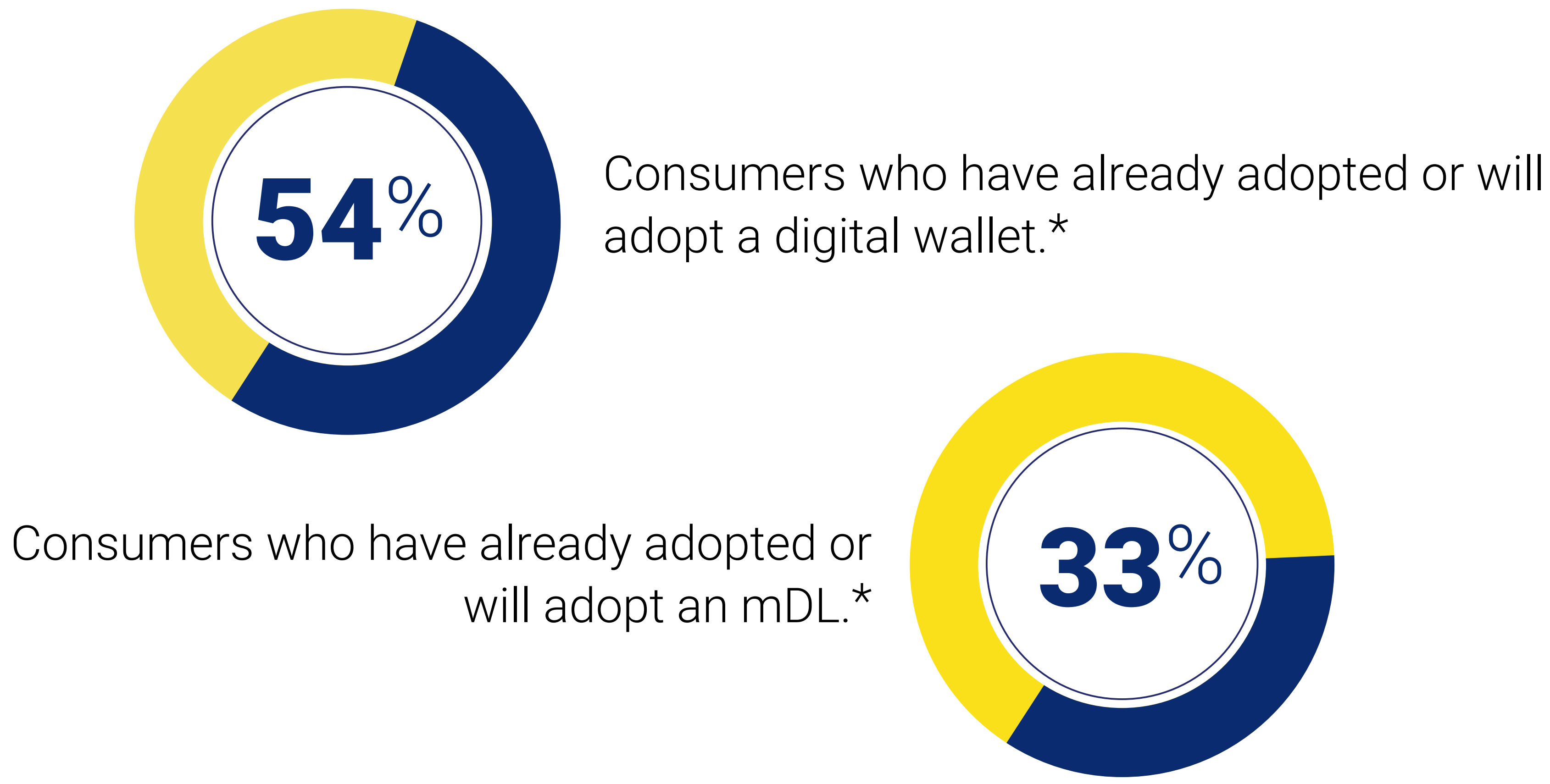
There's been growing momentum to integrate the technology into consumers' lives to streamline access to government services, enhance financial inclusion, and bolster national security. Nations like Estonia, Singapore, India, and Sweden have set benchmarks with advanced systems that integrate biometric authentication, blockchain technology, and privacy-centric frameworks. Estonia's e-Residency program continues to pioneer cross-border digital identity, while India's Aadhaar system provides 1.3 billion residents with unique, verifiable credentials. Singapore's Singpass enables seamless access to government and private services, and Sweden's BankID showcases a highly trusted and widely adopted identity solution.

THE GROWTH OF DIGITAL IDENTITIES GLOBALLY: A VISUAL



WILL CONSUMERS MAKE THE SHIFT?

54% of consumers have already adopted or will adopt digital wallets, but mDLs are a slower process: 33% of surveyed consumers have already or plan to adopt this technology.[27]



VERIFIABLE CREDENTIALS: AN IMMINENT REALITY?

Verifiable credentials are credentials that are both tamper-evident and cryptographically secure, as well as following World Wide Web Consortium (W3C) open standards. Over the past several years, this technology has continued to mature. Issuing organizations can generate fraud-proof digital credentials that verification entities can instantly check and authenticate, making them an attractive method in the shift to digital modes of identity. Recently, nations like Australia have tested verifiable credentials stored in a digital wallet as a method to verify identity.

[27] US Homeland Security Rule, "Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes; Waiver for Mobile Driver's Licenses," Published October 25, 2024.
*AuthenticID State of Identity Fraud Surveys, 2024.

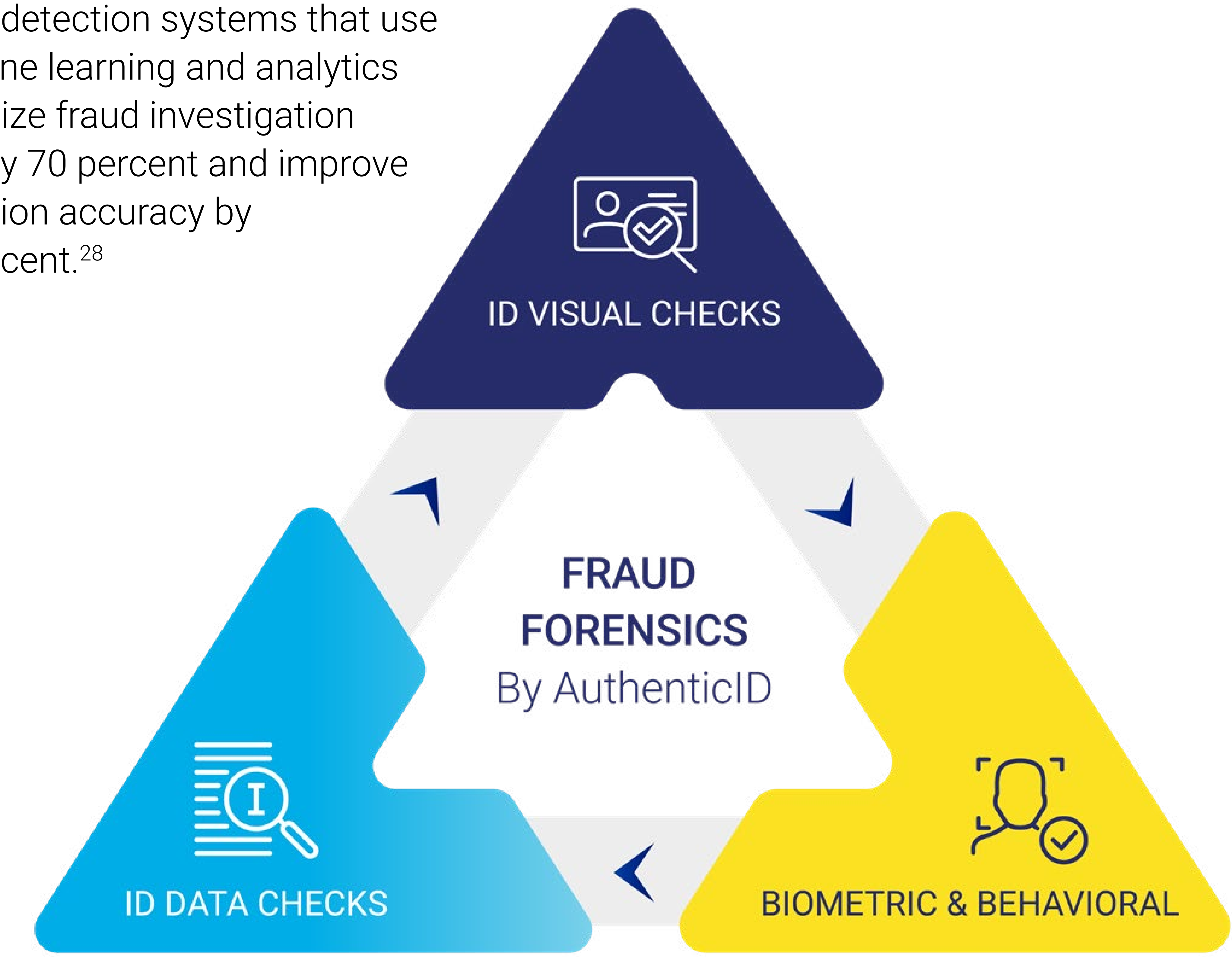
06

Outsmart, Outpace, Outfight: Your Playbook To Fight Identity-based Fraud

FRAUD FORENSICS

Today's cybercriminals continue to develop advanced techniques to bypass even the most robust fraud defenses. AuthenticID moves at the speed of fraud with the use of advanced AI and Machine Learning technology. With robust fraud algorithms, any potential for a fraudster to fake a small piece of a document, biometric, or other identity piece can be detected.

Fraud detection systems that use machine learning and analytics minimize fraud investigation time by 70 percent and improve detection accuracy by 90 percent.[28]



ID VISUAL CHECKS

FRAUD FORENSICS By AuthenticID

ID DATA CHECKS

BIOMETRIC & BEHAVIORAL

VISUAL ID & IMAGE QUALITY ANALYSIS

- Document Liveness
- Headshot Replacement
- Aspect Ratio
- Headshot Photo Tamper
- Headshot Replacement
- Signature Font Detection
- Glare Analysis
- Photo Splice
- Photo Stitch
- Photo Border
- Focus/Blur
- DPI Minimum
- Digital Screen Detection
- Rectification
- Paper Detection

DATA ID ANALYSIS

- Data Structure Patterns
- EXIF Data Check
- XMP Data Check
- Personal # Analysis
- Doc. Discriminator Analysis
- Barcode Integrity
- Document # Analysis
- Height & Weight Analysis
- Hair & Eye Color Analysis
- Data Field Comparisons
- Expired ID
- Date Integrity
- Textual Symbol Errors
- Document Watchlists: Client & AuthenticID

BIOMETRIC & BEHAVIORAL ANALYSIS

- Selfie Liveness Detection
- Face Match
- Face Enrollment
- Re-Authentication
- Biometric Tamper
- Geo-location Checks
- Deepfake Detection

Comprehensive forensic checks of visual elements, identity data, and biometric data ensures secure identity verification by analyzing document authenticity, data integrity, and biometric features like headshot tampering and selfie liveness.

[28] Altexsoft, "Fraud Detection: How Machine Learning Systems Help Reveal Scams in Fintech, Healthcare, and eCommerce"

FIGHT FRAUD

By Channel and Stage

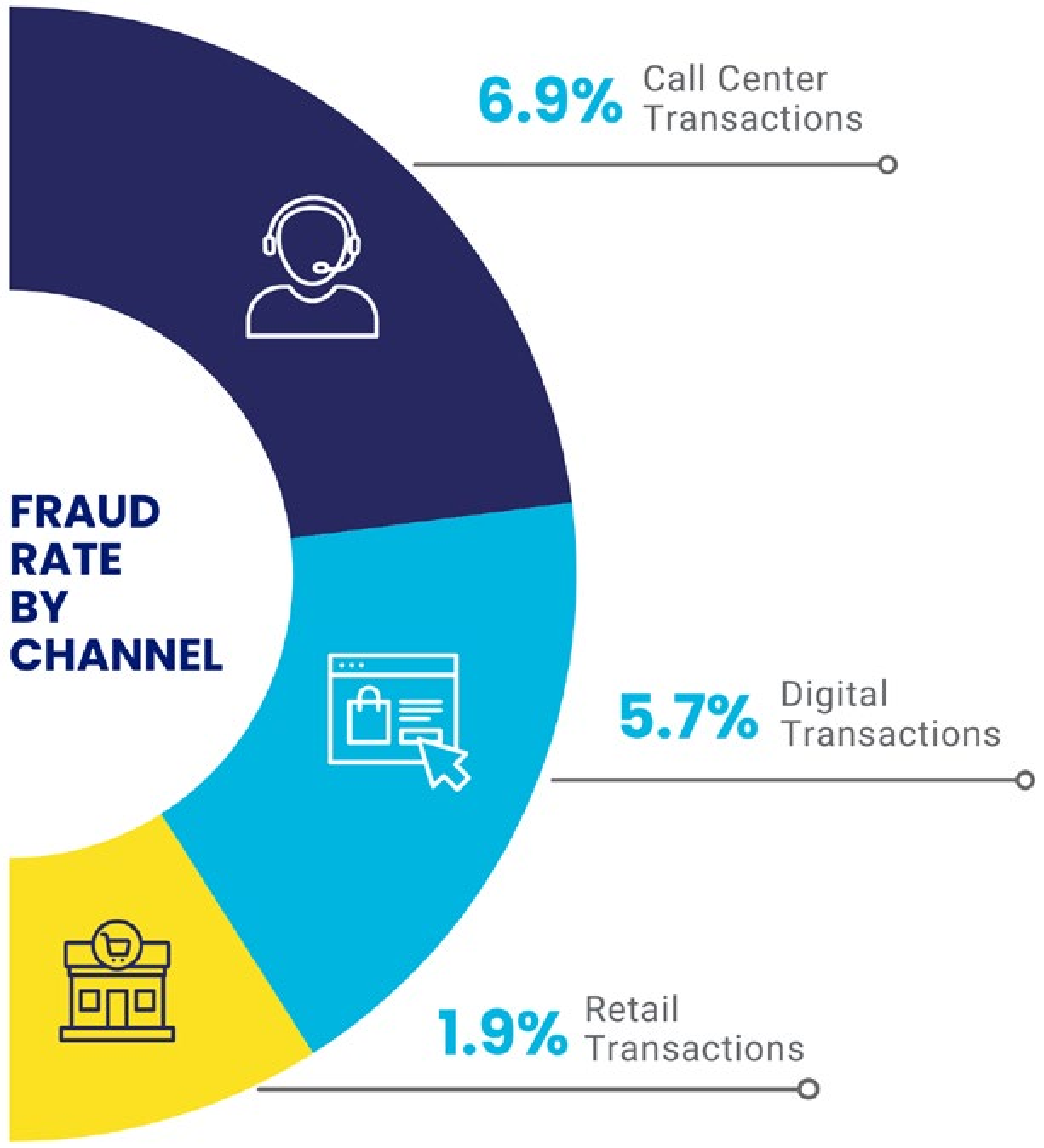
Effectively fighting fraud isn't a one-size-fits-all endeavor. Bad actors will attack your platform, customers, and workforce at each stage of their journey, and through a variety of channels. Staying ahead of identity fraud requires treating and configuring each touchpoint uniquely, while ensuring identity data, fraud flags, and other metrics speaks to each part of your system, with a central repository for the important data that can help you fight fraud.

The steps for success:

- **Customize workflows by channels**: are users in person, digital, using a call center, or using multiple modes to interact with your organization?
- **Adapt workflows by customer journey stages**: for example, account opening, login, transaction, high-security access. At each stage, consider not just the data and verification factors you're using to stay compliant with any necessary regulations, but how fraudsters might attack. Whether it's using signals from device behavior, biometrics, or patterns of login and transactions.
- **Create a unified view for cross-channel analysis** with centralized repository for data that allows for risk signals and actionable data.
- **Continuously analyze, optimize**–and repeat your steps. Bad actors are constantly evolving and changing tactics to avoid detection and exploit weaknesses, meaning evaluation and action is crucial before losses mount.

Businesses surveyed reported an increase in these fraud channels in 2024*:

25%	In Person
66%	Online Stores & Websites
71%	Mobile Apps
37%	Call Center



*AuthenticID State of Identity Fraud Surveys, 2024.

AUTHENTICID
Identity Fraud
Taskforce

THE EXPERTS BEHIND THE TECH:

THE IDENTITY FRAUD TASKFORCE

AuthenticID's Identity Fraud Taskforce's groundbreaking efforts fight fraud, protect identities, and cultivate trust in an evolving digital landscape. It's comprised of over a dozen specialists who bring decades of experience, unique accolades, and diverse expertise to the table. In a world where fraud is both multidimensional and ever changing, this Taskforce equips AuthenticID with the research and knowledge required to detect fraud before it reaches customer systems, equipping both AuthenticID and our clients for the future of fraud.

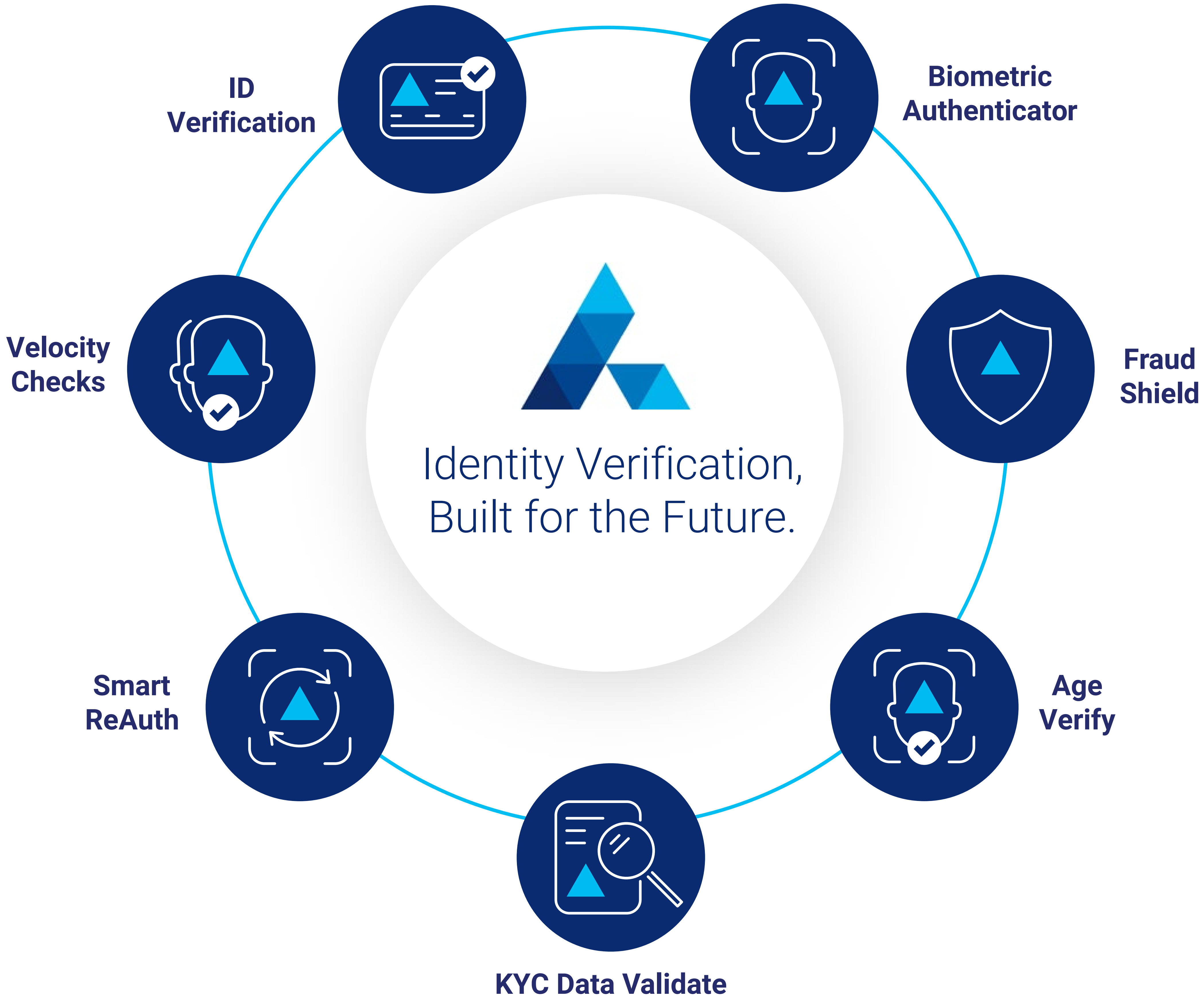
- ✓ **Optical and material lab experimentation**
- ✓ **Systematic literature reviews and code-breaking research**
- ✓ **Machine learning and algorithm development**
- ✓ **Daily testing and evaluations**
- ✓ **Fraud monitoring and reporting**

FAST FACT

In 2024 AuthenticID was awarded a patent for novel tamper detection technology to add another critical tool to detect unauthorized alterations in documents.

COMBAT FRAUD

With a Holistic Solution



There's no silver bullet to fight fraud. That's why **multi-layered fraud protection** is important, ensuring your organization's sensitive data—and your customers—are protected from the breadth and depth of today and tomorrow's sophisticated fraud threats. Fighting fraud and maintaining a positive customer experience is a complicated process, and your business needs a partner that can do both.

AuthenticID360 is a comprehensive platform that can be easily deployed and **scaled quickly to ensure an immediate ROI**. It is optimized for both mid-market and enterprise-level businesses, offering the complete package of speed, accuracy, and security.

AuthenticID360 combines ID verification, biometric authentication, KYC and KYB data checks, and advanced fraud watchlists tools–all within a single platform.

2
Seconds or Less Verifications

99%+
Accuracy in Counterfeit Detection

500
Forensic Checks

98%
First-Time Pass Rates

Learn More.

Book a fraud consultation and demo to explore secure, next-gen identity proofing solutions.

AUTHENTICID

www.authenticid.com