
THE PROFESSIONALIZATION OF FRAUD:
2027 Identity Fraud Report
New Proprietary Data on Deepfakes, Injection Attacks, and Social Engineering
ENTRUST
SECURING A WORLD IN MOTION

# Foreword

Identity security has always been built around key moments. A customer opens an account, logs in, or makes a payment, and their identity or access is verified. But digital interactions have grown more complex, and establishing trust at one moment doesn't tell us what happens next.

An identity can be legitimate at onboarding and compromised later, and a genuine customer can be manipulated or tricked into approving a fraudulent action. Authentic documents, photos, and videos can all be stolen and reused by someone else. And as AI makes sophisticated fraud tools more accessible, organizations need to consider not only whether an identity is genuine but whether the person using it can still be trusted at that particular moment.

It is more important than ever that trust is built and reinforced at every stage - when the relationship starts, then earned again when the customer comes back, recovers an account, changes a password, or does something higher risk.

This is where the FIDO Alliance's work becomes relevant to the challenges highlighted in this report. FIDO advances identity technologies built around trust and simplicity in the interactions between people, services, and devices. Working together with our members, we create open specifications that make passkeys, online payments, digital credentials, agentic interactions, and edge device provisioning simple, secure, and trustworthy. Our certification programs, recognized around the world, assure enterprises, governments, and consumers that products carrying the FIDO mark meet demanding standards for interoperability, security, and usability.

Strong identity verification at the start of a relationship, and phishing-resistant and biometric authentication throughout, are complementary parts of the same challenge: establishing trust and maintaining it over time. Technology has to keep evolving because, as controls improve, attackers adapt and look for the next opportunity. Identity systems only stay secure without burdening legitimate users when trust and simplicity are built-in from the start and when they are designed to evolve as threats do.

The proprietary data shared in this report gives insight into how fraud is changing, where new risks are emerging, and why trust has to be maintained across the entire identity lifecycle.

The next phase of digital identity will be about establishing trust, maintaining it, and knowing when it needs to be verified again.



**Andrew Shikiar**
**Executive Director & CEO**
**FIDO Alliance**

# Executive Summary

At first glance, the data in this year's report suggest fraud is declining. Document fraud fell to 2.5%, the lowest rate recorded in the eight-year history of this report and a 44% decline over the past two years. But the headline doesn't tell the whole story. While overall fraud rates continue to fall, fraud is becoming more sophisticated. Simple, high-volume attempts are increasingly folded into broader campaigns, while more convincing attacks that require better tools, greater skill, and closer scrutiny take their place.

Then there's the professionalization of fraud. Attackers have more tools and tactics at their disposal, from AI-generated content and injection attacks to social engineering and account takeover. Instead of relying on a single method, they're finding new ways to exploit both technology and trust.

Deepfakes are becoming more common, but generating convincing synthetic content is just one part of the challenge. Injection attacks offer a way to deliver synthetic or stolen media into verification processes, while AI makes it easier to automate, personalize, and scale attacks.

At the same time, social engineering is becoming a much bigger part of the fraud problem. As document and biometric controls improve, attackers have started targeting the people using them. Rather than trying to trick the technology, they may manipulate a legitimate customer or employee into completing the action for them.

Fraud is also happening after onboarding. In industries like banking, payments, and professional services, more fraud is targeting existing accounts than new ones. Once an identity has been verified and an account has built a history of legitimate activity, that established trust can become a target.

Together, these trends identify a broader change in how organizations should think about identity fraud. In addition to establishing trust at onboarding, organizations need to verify and reinforce trust throughout the identity lifecycle. As fraud moves across the identity lifecycle, trust needs to be reinforced during authentication, reverification, account recovery, credential changes, and other high-risk moments. One control cannot address every attack, making multiple signals and layers of protection critical.



## This year's report reveals five key findings:

1

### Fraud Is Professionalizing

A lower fraud rate doesn't mean fraud is disappearing. It just means fewer simple attacks are making it through. Fraudsters are investing more time, resources, and expertise into today's attacks.

2

### AI Is Changing How Fraud Operates

AI-generated content is only one part of the challenge. The methods used to deliver that content are evolving even faster.

3

### Social Engineering Is the Fastest-Growing Vector

As document and biometric controls improve, attackers turn to the people using them.

4

### Fraud Is Happening After Trust Is Established

Banking, payments, and professional services are seeing more fraud against existing accounts than new ones.

5

### Organizations Need Multiple Ways to Verify Trust

No single technology can stop every attack. As fraud diversifies, organizations need a combination of document verification, biometric verification, and attack detection to address risks across the identity lifecycle.

Fraud can happen at any stage of the customer lifecycle. The challenge for organizations will be understanding how fraud is evolving and preparing for it.



### Report Methodology

This year's report draws on proprietary data from September 1, 2025, to August 31, 2026, to highlight how fraud patterns vary around the world.

**20+ Industries | 195 Countries**

The analysis looks at global, regional, and country-level fraud patterns across Europe, the Americas, and Asia Pacific. In some cases, 2026 data is compared with previous years to show how fraud rates, attack methods, and sophistication are changing over time.

The data provides a large-scale, real-world view of how identity fraud is changing, from document fraud and deepfakes to injection attacks, social engineering, and account takeover.

# Table of Contents


| | |
|---|---|
| The State of Identity Fraud | 6 |
| The Impact of AI and Where It's Going | 10 |
| The Rise of Injection Attacks | 13 |
| The Human Layer | 15 |
| Fraud Has Moved Beyond Onboarding | 17 |
| Europe: Higher Trust, Greater Complexity | 19 |
| The Americas: Higher Fraud, Faster Change | 23 |
| Asia Pacific: Digital-First Fraud | 26 |
| The Timing of Fraud | 29 |
| The New Fraud Playbook | 30 |
| What Businesses Should Focus On in 2027 | 32 |
| The Future of Trust | 33 |

CHAPTER 1

# The State of Identity Fraud

## The good news: Fraud rates are falling. The bad news: Fraudulent attacks are becoming more sophisticated.

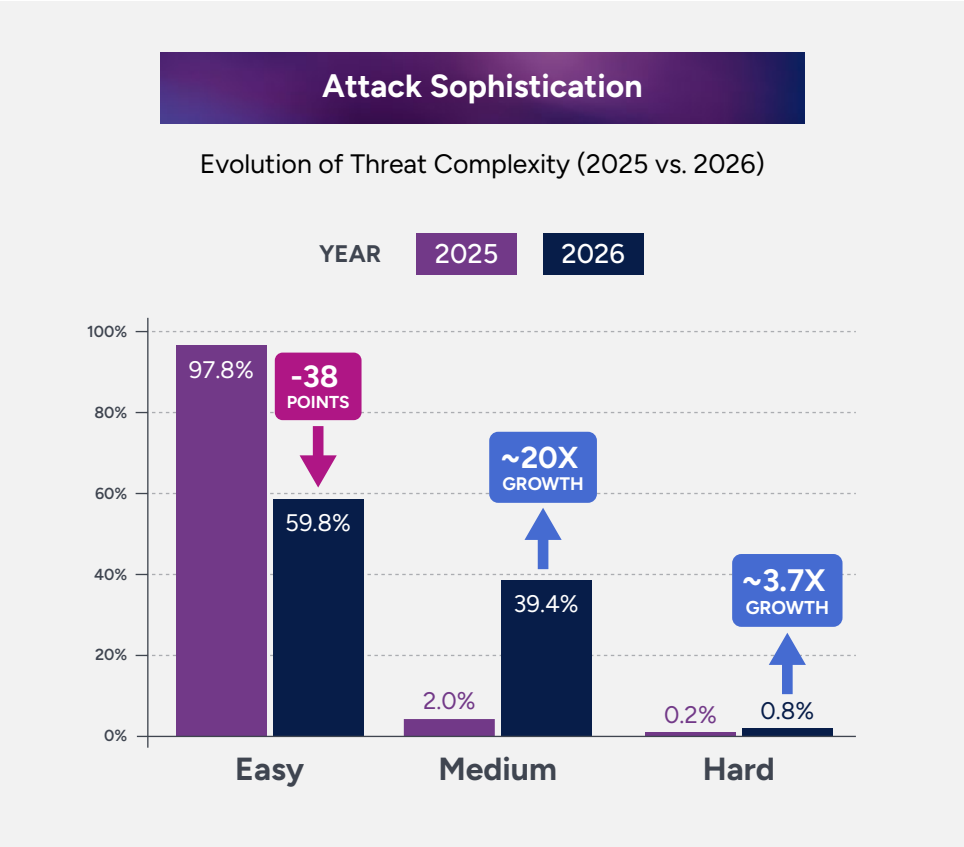
Document fraud fell from 3.1% to 2.5% in 2026. It's the lowest rate recorded in our dataset, down 19% year over year and 58% from the 2021 peak. On the surface, that figure suggests progress. But a closer look shows that the overall fraud rate tells only part of the story. The composition of fraud changed dramatically as more sophisticated attacks accounted for a larger share of activity.

Document fraud is grouped into three levels of sophistication: easy, medium, and hard.

- **Easy:** Low-effort attacks with obvious signs of fraud, such as basic templates, incorrect fonts, screenshots of screenshots, or simple document edits.
- **Medium:** More convincing attacks that require greater skill, tools, or closer inspection to detect, such as higher-quality document alterations or more realistic counterfeits.
- **Hard:** The most sophisticated attacks, such as highly convincing counterfeits or advanced document manipulation that can pass more advanced verification checks.

Nearly 2 in 5 (39%) document fraud attacks are now medium sophistication in 2026, up from 1 in 50 (~2%) a year ago. Hard sophistication fraud also increased 3.7 times year over year, while easy fraud fell from 97.8% of attacks to 59.8%.

The falling fraud rate and rising sophistication of fraud are two sides of the same story. The lower fraud rate is evidence of progress. It measures the volume of attacks, but it's not evidence that the threat is disappearing. Instead, attackers are adapting, changing the techniques they use, and the ways they target organizations.



# Old Attacks, New Tactics

Fraud is becoming more sophisticated but not in the way many people expect. Deepfakes, injection attacks, social engineering, and biometric attacks are growing quickly, yet traditional document fraud is still the largest attack category in the dataset. Within document fraud, however, more sophisticated attacks are becoming more common.

A common assumption is that fraud is moving from physical attacks to digital ones, but the 2026 data suggests the reality is more complex. Digital attacks are growing, but they aren't replacing physical fraud methods. Fraudsters are using both, and often together.

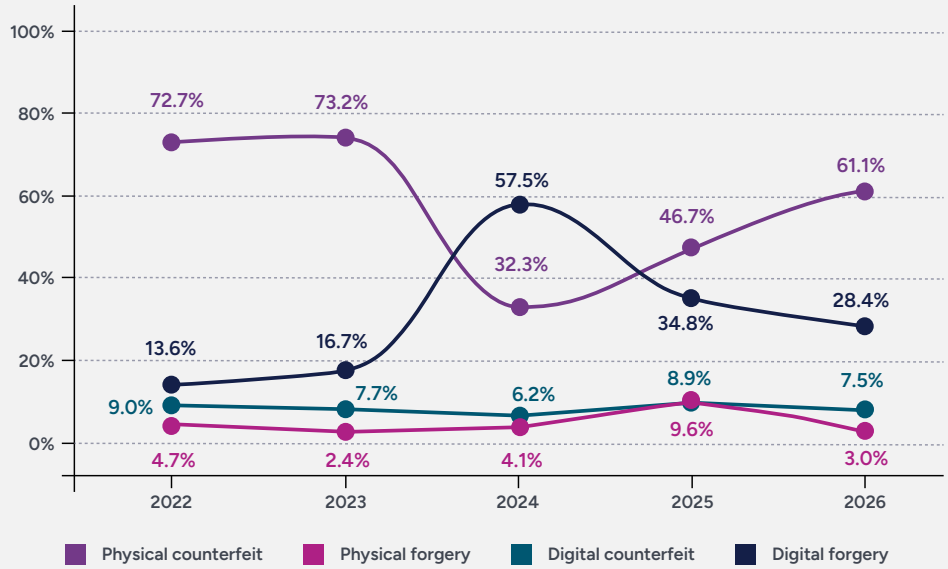
Physical counterfeits make up 61.1% of all document fraud, a 32.3% jump in two years. The reason is simple: High-quality fakes are effective, scalable, and profitable. Organized print operations continue to produce fraudulent credentials that can withstand basic inspection.

Fraudsters often combine physical and digital tactics, using whichever approach has the best chance of success. For instance, a physical counterfeit document may be paired with social engineering, or a stolen identity may be used alongside a deepfake or injection attack.

This is why organizations need more than one way to verify trust. Deepfake detection alone won't stop physical counterfeits. Likewise, strong document controls won't stop social engineering, and neither will passwords or device intelligence, location, and behavioral signals. Each has its limits. No single signal can cover every type of attack.

## Physical and Digital Fraud Over Time

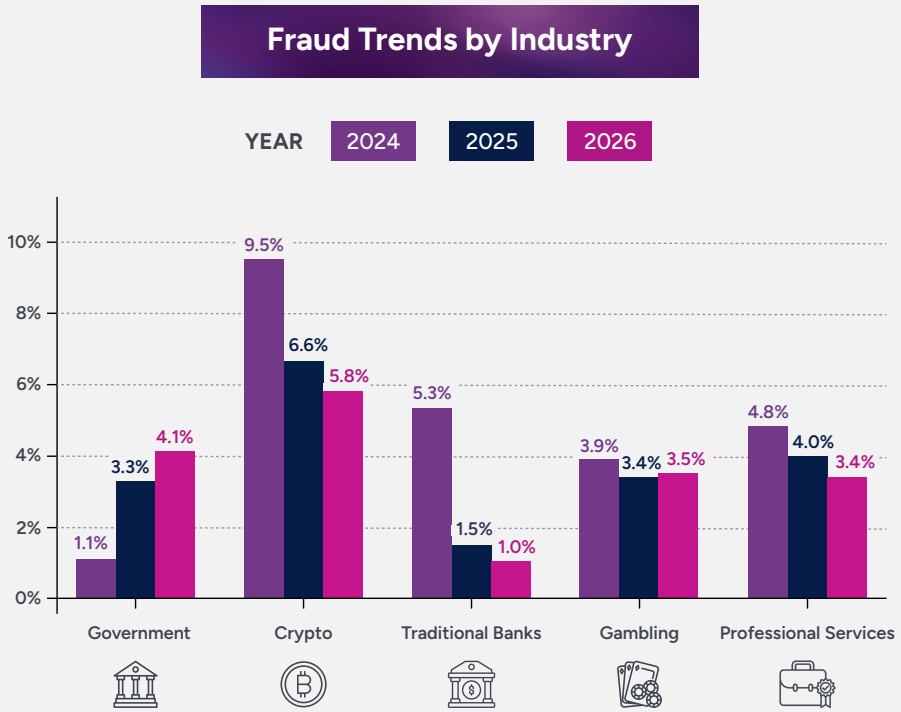
Percentage of Fraud Type by Year (2022–2026)




Attackers aren't replacing old tactics with new ones. They're using both – whichever has the best chance of succeeding.

# Fraudsters Follow Value

Fraudsters will always follow opportunity, especially in sectors where a verified identity unlocks valuable services or accounts.




Government was the fastest growing sector in 2026, with fraud rates increasing 3.7 times over the past two years.

As public services continue their digital transformation, verified identities provide access to benefits, licensing programs, tax systems, healthcare services, and other high-value government resources. These services are also facing growing pressure from attackers: Verizon's 2026 Public Sector Data Breach Investigations Report found that social engineering accounted for 17% of public sector incidents.

Not every sector moved in the same direction, however. Traditional banks tell a different story.

Fraud rates among traditional banks declined 81% compared with 2024 levels, indicating what sustained investment in identity verification and fraud prevention measures can achieve over time. This isn't to say that banks are no longer targeted. Rather, it shows that fraud prevention programs can materially reduce exposure when controls are consistently strengthened and maintained.

Other high-value industries continue to attract significant fraud activity. Crypto remains the most heavily targeted industry at 5.8%. The appeal is straightforward – a successfully verified crypto account provides immediate access to assets that can be transferred quickly and, in many cases, are difficult to recover once stolen. The decline from 9.5% in 2024 to 5.8% in 2026 indicates that stronger fraud controls in the industry may be having an impact, but the risk profile of the sector is still unusually attractive to attackers.

Crypto also is a testing ground for many of the techniques discussed in this report. Deepfakes, injection attacks, and account takeover attempts often appear first in crypto environments, where financial rewards are immediate and barriers to monetization are low.

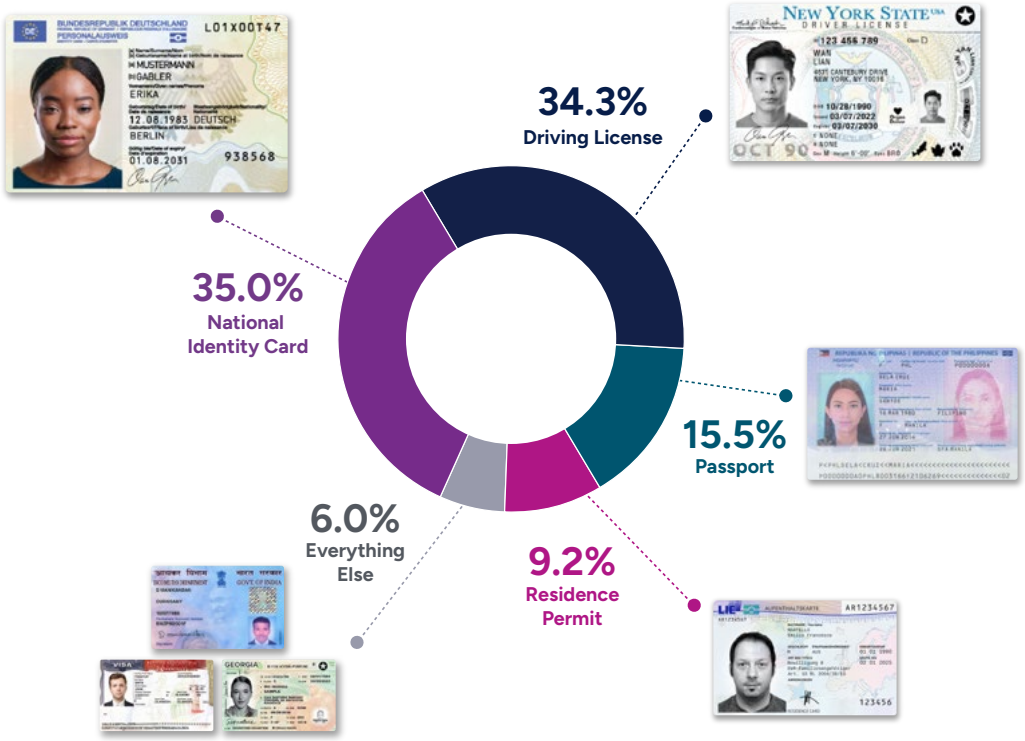
## The Most Targeted Documents

Just four document types account for 94% of global document fraud.

Fraudsters concentrate where the return on investment is highest, focusing on the credentials most commonly used to establish trust, access services, and open accounts.

A small number of credentials dominate global targeting. U.S. driver's licenses take the top three positions, while European national identity cards and residence permits make up much of the rest of the global top 10. France is the only country with three different credentials in the ranking.

**Knowing which credentials are targeted most often helps organizations focus their identity verification and fraud prevention efforts.**




### Top 10 Most Targeted Identity Documents

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **13.7%** US Texas Driving License | **10.8%** US California Driving License | **10.8%** US Florida Driving License | **6.7%** Portugal National Identity Card | **4.8%** Germany Residence Permit | **4.6%** France Residence Permit | **4.1%** France National Identity Card | **3.9%** France Passport | **3.1%** Spain National Identity Card | **3.1%** Italy National Identity Card |

CHAPTER 2

# The Impact of AI and Where It's Going

## Deepfakes are growing, but delivery is becoming the bigger story.

Deepfake detections rose 165% year over year, averaging one detected deepfake every three minutes in 2026. They get the coverage because they're the most visible – and perhaps most unsettling – form of AI-enabled fraud. But AI-enabled fraud is becoming more organized, scalable, and easier to automate, and creating fraudulent content is only one part of the attack.

Generating synthetic identities, deepfakes, fraudulent documents, and convincing scam communications once took specialist skills, significant manual effort, or professional editing tools. Now these attacks can be personalized, automated, and produced at scale, so fraudsters can launch more of them, faster, and at a lower cost.

Deepfakes cause harm in many ways, from eroding trust and spreading misinformation to impersonation scams and identity theft. In the context of identity verification, however, generating a deepfake is only one step in the attack. The synthetic image or video must still be presented during a verification process and successfully pass security checks before it can be used to commit fraud.

This is where injection attacks enter the picture. Deepfakes and injection attacks are often discussed as separate threats, but they're part of the same attack chain. Deepfakes create the fraudulent content, while injection attacks deliver that content into a verification workflow. One creates the asset; the other puts it to use.




A deepfake was detected every three minutes on average in 2026.

# Delivery Determines Whether the Attack Succeeds

Injection attack volume grew 224% in 2026, much faster than deepfake growth. Organizations therefore need visibility beyond the content itself and into how it reaches the verification process. Injection attacks can deliver synthetic media, but they can also deliver genuine photos and videos stolen from real people. In both cases, the media itself may appear authentic.

If your defense against AI-enabled fraud relies on media forensics – analyzing an image for signs that it's been generated or manipulated – you're only addressing part of the problem. A significant share of injected traffic isn't synthetic at all. It's genuine photos, videos, or documents replayed into a verification process by someone who shouldn't have access to them. Because the media itself is genuine, forensics alone may not catch the fraud. You also need to know where the content came from and how it entered the verification process.

And there is no shortage of legitimate content for attackers to work with. Verizon's 2026 Data Breach Investigations Report found stolen credentials were involved in 39% of breaches, which shows how much stolen identity data keeps circulating and getting reused. Fraudsters can repurpose compromised information, credentials, and media under their own control, rather than creating fake identities.

This is where device intelligence becomes important. Signals like whether the user is on a genuine camera, a legitimate device, and an authentic session show how identity, credentials, and media are being presented. Device intelligence-detected fraud rates rose 42% year over year.

Media forensics asks whether the content is real, while device intelligence tells you about the session it came from. You need visibility into both.



As fraudsters gain access to more genuine identity data, understanding where content came from can be just as important as understanding the content itself.

## Financial Services Remain the Primary Target

Deepfake attacks aren't distributed evenly across the economy. They concentrate overwhelmingly in financial services.

Crypto platforms and digital-first banks carried the largest share of that activity. Financial services accounted for 93.5% of all deepfakes detected in 2026, while attacks on digital-first banks increased 714% in a single year (more than eightfold), making them one of the fastest-growing targets in the dataset.

The reason isn't simply "because that's where the money is." It's because financial institutions issue trusted accounts, and these verified accounts are valuable long after onboarding. They can be used to steal funds, support money laundering, facilitate mule activity, and open doors to downstream fraud. Undetected, the account effectively becomes reusable infrastructure.

This helps explain why attackers are so willing to invest in sophisticated techniques like deepfakes, synthetic identities, injection attacks, and stolen genuine media. The more valuable the account, the more sophisticated the attack becomes.

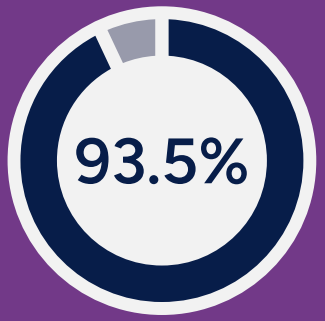
## What This Means for Identity Teams

Three lessons stand out from the 2026 data:

1. **Detect the delivery, not just the content:** Fraudulent content reaches verification workflows via virtual cameras, emulators, and API-level tampering. Media forensics analysis alone doesn't address the delivery mechanism.

2. **Assume the media may be genuine:** Some of the fastest-growing attacks involve authentic documents, images, and videos being used fraudulently. Authenticity checks won't identify content that's real but in the wrong hands.

3. **Expect attackers to follow value:** Financial services is the primary target today because trusted accounts can be reused across multiple fraud schemes. As digital identities become more valuable, attackers will pursue them with the same intensity.




**Financial services** accounted for 93.5% of all deepfakes detected in 2026



CHAPTER 3

# The Rise of Injection Attacks

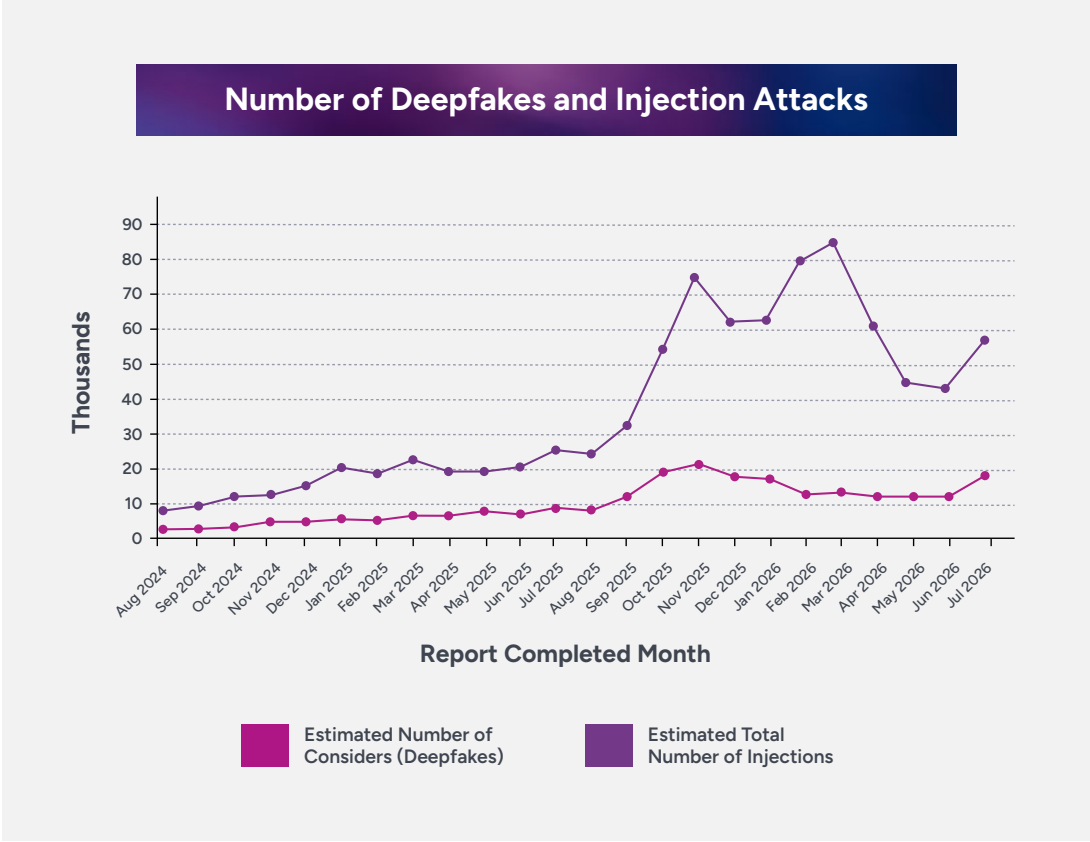
## A fast-growing threat that many organizations aren't measuring.

As we saw in the previous chapter, injection attacks can introduce synthetic or genuine media directly into a verification process. But to understand why these attacks can be difficult to detect, it helps to look more closely at how that injection actually happens.

An injection attack involves sending fraudulent, AI-generated, or stolen genuine images or video directly into the verification process, bypassing the device's camera. The person you think you're looking at may never have been present during the verification process. Instead, the media reaching the verification check has been inserted into the workflow.

Unlike SQL injection, code injection, and other application-layer attacks that target systems or infrastructure, injection attacks target the integrity of the verification process itself by "injecting" the attack into an actual workflow. From the application's point of view, the media may look legitimate and be processed normally. Many traditional fraud controls may not recognize that an attack is taking place, even though the content didn't originate from the live capture process.

This helps explain why injection attacks are growing so quickly, with rates up 40% year over year and more than doubling since 2024. As organizations improve their ability to detect document fraud and deepfakes, fraudsters are focusing on how content reaches the verification process rather than just the content itself.



## The Four Delivery Methods

While the techniques vary, all injection attacks share the same objective of replacing a live camera capture with attacker-controlled content. The intent is that the application believes it's receiving a live feed, so the verification process would continue normally.

**1 Virtual cameras:**
Software that appears to be a legitimate camera while playing prerecorded or AI-generated video.

**2 Emulators and virtual devices:**
Software that simulates a mobile device on a computer. Instead of using a real camera, the emulator feeds stored images or video directly into the verification process in an attempt to trick the system.

**3 API-level submission:**
Sending images or video directly to a verification endpoint rather than capturing through the application's camera workflow. In these cases, the media is uploaded without proving how it was originally captured.

**4 Hardware interception:**
Replacing or manipulating the video signal between a real camera and the device using capture cards, modified hardware, or other equipment like signal splitters. This method is less common because it requires more expertise and equipment.

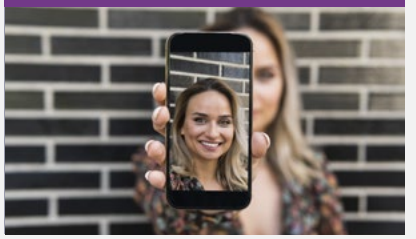
In all four techniques, the attacker controls the content reaching the verification process.

## The Hidden Side of AI Fraud

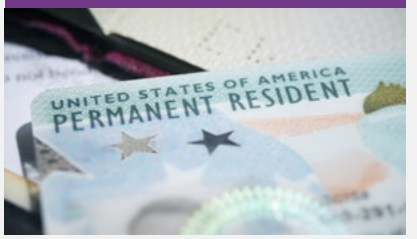
Injection attacks are one of the primary ways fraudulent content is delivered into the verification process. In these cases, the fraud isn't in the content itself but in how that content is being used. As more attacks involve genuine media, organizations need to understand not only what they're seeing but how it reached the verification process.

### Real Doesn't Always Mean Safe

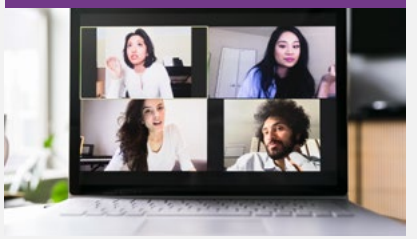
A Genuine Image



A Genuine Document




A Genuine Video



**These can all be fraudulent.**

CHAPTER 4

# The Human Layer

## As fraud prevention improves, attackers turn to people.

Most identity fraud attempts to fool or bypass verification controls. Social engineering moves the focus to the person instead, manipulating a legitimate user into completing an action themselves.

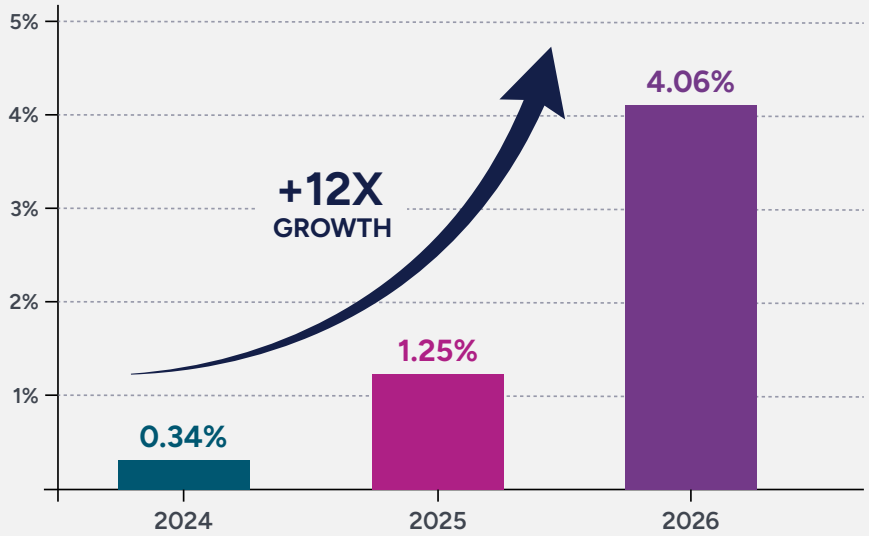
This makes social engineering particularly difficult to detect. The person may be genuine, the credentials may be legitimate, and the verification process may work exactly as intended. But unlike injection attacks, the fraud comes from the legitimate user being persuaded or deceived into facilitating the fraud.

Social engineering can take many forms. Attackers may impersonate a bank, government agency, employer, or other trusted organization to persuade a victim to transfer money, reveal credentials, recover an account, or complete a verification process. In other cases, a fraudster may build trust with the victim over time before asking them to take action.

It's also the fastest-growing attack. Reports of social engineering attacks rose 520% year over year and are running 75 times higher than two years ago, while its share of all reports climbed from 0.34% to 4.06%, a twelvefold increase. While social engineering represents a relatively small share of total fraud activity, its growth rate far exceeds any other attack type in the dataset. Activity peaks in November and December, when holiday spending and scam campaigns create more opportunities for manipulation.

**Social Engineering Increases**

Nearly 12x growth in two years – with one being detected every eight minutes



## Why It's Growing Fast

The professionalization story in Chapter 1 explains the surge here.

As document verification, liveness detection, and injection detection improved, simple attacks became harder to carry out. Fraudsters adapt when attacks become more difficult or more expensive. When technical routes become less effective, the easiest path to a verified identity is often the person who already owns one. And once attackers turn to people, scale becomes the next advantage.

Manipulation is easier to scale than document forgery. Threat actors can send a convincing story to thousands of people at once and use generative AI to make those stories fluent, personalized, and available in any language at negligible cost. The same AI capability that produces a synthetic face can produce the script that persuades a real person to use their own identity.

## How Social Engineering Works

Social engineering succeeds because it exploits trust rather than technology.

**In authorized fraud**, victims willingly transfer funds or approve transactions after being manipulated by a fraudster. Because the legitimate account holder performs the action, traditional fraud detection systems often struggle to distinguish the activity from a genuine transaction.

**Customer coaching schemes** are similar. Attackers prepare victims to answer security questions, explain suspicious activity, or respond to reassurance checks in ways that help the attack succeed.

**Employee manipulation** follows the same pattern, targeting help desks, customer service teams, HR teams, and internal support functions that can reset credentials, override controls, remove security flags, or grant access.

One tricked employee can affect many parts of the organization, from hiring processes to account recovery workflows. As a result, social engineering becomes an operational risk across the organization.

These attacks are supported by highly organized scam ecosystems. Different criminal groups specialize in specific parts of the fraud lifecycle, including lead generation, victim manipulation, account takeover, credential theft, and money movement. The result is a more coordinated and scalable form of fraud than many organizations are prepared for.

## The Defensive Problem

Social engineering presents a unique challenge because it involves genuine users knowingly or unknowingly facilitating the attack. There are fewer signals of fraud available for the system to flag. Organizations can instead look for signals around the event and request reverification at high-risk moments, such as unusual behavior, remote access software running during a session, and activity patterns that suggest coaching.



CHAPTER 5

# Fraud Has Moved Beyond Onboarding

## Fraudsters are targeting trusted accounts – not just new ones.

Most identity verification happens at onboarding. A customer proves who they are once, and that trust carries forward into every future interaction. But today, attackers are focused on compromising accounts that have already been established, and this year's data shows where that change is happening.

In banking, **account takeover** now accounts for 52% of fraud, compared with 48% for new account fraud. The biggest challenge for banks is protecting trusted accounts after KYC checks and onboarding. Payments follow the same pattern, with 56% of fraud taking place after onboarding, compared with 44% for new account fraud. Professional services shows a similar split. Fraud is increasingly focused on compromising trusted identities.

A takeover of an established account is often more valuable than a fraudulent new one. The account has a history, established patterns of activity, and a foundation of trust built by the genuine account holder before the takeover occurred.

This is why reverification is becoming so important. The highest-risk moments in the customer journey are increasingly at moments when a user recovers an account, changes a device, updates contact information, or initiates a high-value transaction. These events occur at predictable points in the customer journey, making them attractive targets for attackers. At those moments, trust needs to be reverified, not assumed.



## The Highest Risk Moments in the Lifecycle

The highest-risk moments usually occur when organizations need to reestablish trust after onboarding. Many of these events are designed for customer convenience over identity security:

> **Account recovery:** A user locked out has, by definition, lost the credential they normally rely on. Recovery flows are frequently the weakest identity check a business operates, and attackers know they can use them to bypass stronger controls.
>
> **Step-up authentication:** High-value actions trigger additional verification, creating a predictable checkpoint that attackers can prepare for.
>
> **Reverification:** Periodic identity refresh, regulatory or otherwise, often relies on lighter controls than the original onboarding process.
>
> **Profile and contact changes:** Updating a phone number or email is frequently the first move in a takeover, because it redirects every subsequent security signal to the attacker.

What these events have in common is that they occur after trust has already been established. Because they're designed for user convenience, they are attractive targets for attackers.

## Trust Isn't Permanent

As digital relationships become longer and more valuable, attackers are moving their focus from creating fraudulent identities to compromising trusted accounts. Banking is simply the clearest example of that trend today. The same principle applies across organizations wherever a trusted identity can be exploited, including bank accounts, help desk interactions, and internal systems.

Reverification is becoming a critical control because trust changes over time. High-risk events and large transactions often require stronger identity assurance than routine account activity. Organizations are increasingly combining biometrics, authentication, device intelligence, and step-up verification to confirm that the person behind a trusted account is still the legitimate account holder.

The same principle applies beyond customer accounts. Employee identities, help desk interactions, and internal access requests can all become targets when trust is assumed rather than continuously verified.

Organizations that focus only on onboarding are leaving some of the highest-risk moments unprotected.

The documents fraudsters target also vary by market. National identity cards account for 35% of document fraud globally, but the mix changes by region depending on the credentials people use to prove their identity. The regional chapters that follow look more closely at those differences.

**Trust Has to Be Verified Across the Identity Lifecycle**



CHAPTER 6

# Europe: Higher Trust, Greater Complexity

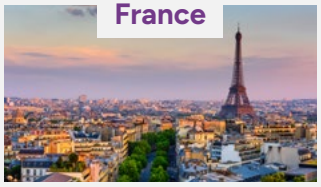
## Regulation, digital identity, and fraud are evolving together.

Europe has the lowest document fraud rate globally, but some of the most sophisticated fraud measured. Markets such as the UK are moving toward medium sophistication fraud, while parts of continental Europe remain dominated by lower-complexity attacks. In many ways, this reflects Europe's more mature identity and regulatory environment, where stronger trust frameworks are raising the bar for both businesses and attackers.

Europe sees fewer fraud attempts, but the ones it does see are more advanced. Medium sophistication fraud now accounts for 42.7% of document fraud in the region, while hard sophistication attacks represent 1.0% of cases – 2.6 times the Asia Pacific rate. Europe's document fraud rate is comparatively low at 1.7%.

### Five Markets With Five Fraud Stories

**France**



**Deepfake hotspot:** Three core French credentials are listed in the top 10 most targeted documents.

**Romania**



**Industry-specific pressure:** Gaming and gambling record with an 8.9% fraud rate overall.

**Italy**



**Digital forgery inches ahead:** Digital forgeries make up 50% of document fraud versus 49% for physical counterfeits.

**Spain**



**Physical counterfeits dominate:** Physical counterfeits account for 82% of document fraud.

**UK**



**Sophistication is rising:** Medium sophistication fraud exceeds easy fraud, 53% to 47%.

Europe is also the deepfake epicenter, with the largest regional share of deepfake attacks and 462% year-over-year growth.

The region also sees the highest concentration of social engineering activity, with social engineering being the highest of the three regions, at 4.90%.

Physical counterfeits account for 64.2% of document fraud in Europe, while digital forgeries represent 26.4%. Despite the growth of AI-enabled attacks, traditional document fraud is still the dominant attack method across the region.

National identity cards are the most commonly targeted credential in Europe, accounting for 38.6% of fraud activity. Driving licenses follow at 23.9%, passports at 17.9%, and residence permits at 12.7%, compared with 9.2% globally. National identity cards and residence permits are targeted more often in Europe, where national identity cards are widely used in much of the region and residence permits play an important role in cross-border movement.

Most European markets remain dominated by easy sophistication fraud, including France (83%), Romania (90%), Italy (86%), and Spain (70%). The UK is an exception, with medium sophistication attacks accounting for 53% of fraud activity. These attacks persist because they're profitable. As stronger identity checks make basic fraud harder, attackers move toward more sophisticated techniques such as deepfakes, injection attacks, and account takeover.

Spain highlights an important theme: Despite growing attention on AI-enabled fraud, traditional document fraud is still highly effective in this region. Physical counterfeits and national identity cards continue to play a central role in Europe's fraud activity.

## EUROPE AT A GLANCE

### Key Fraud Trends - What We're Seeing in Europe



# When Compliance Becomes Fraud Prevention

Europe is adapting its regulatory approach as fraud evolves. As fraud becomes more advanced, governments, regulators, and businesses are strengthening the systems used to establish and maintain digital trust. The same trends driving growth in deepfakes, social engineering, and other forms of identity fraud are also driving investment in stronger identity proofing, trust services, and digital identity programs.

European Union initiatives such as eIDAS 2.0, AMLR, and ETSI's revised identity-proofing requirements are both standardizing digital identity and raising the technical bar for how identity is established and verified remotely.

Article 22(6)(b) of AMLR specifically recognizes electronic identification at "substantial" or "high" assurance levels, along with relevant qualified trust services, as a way of verifying customer identity.

The eIDAS Regulation takes a similar approach for qualified trust services. Article 24(1)c requires identity to be verified before a qualified certification or qualified electronic attestation of attributes is issued. It allows several routes, including the European Digital Identity (EUDI) Wallet or notified electronic identification at a high assurance level, as well as other identification methods that provide a high level of confidence and are confirmed through conformity assessment.

The ETSI technical standard 119 461 v2.1.1 revision reflects the reality across Europe: Fraud is becoming more sophisticated, and identity standards are increasing requirements in response. The new requirements strengthen remote identity proofing, identity assurance, and presentation of attack detection, helping organizations address threats such as deepfakes and injection attacks. As these threats are becoming ever more common, proving identity remotely requires greater confidence and assurance than it did just a few years ago.

AMLR is also becoming more prescriptive about how customer due diligence should work in practice. AMLA's September 2026 final draft Regulatory Technical Standards under Article 28(1) set out requirements for standard, simplified, and enhanced customer due diligence and address the reliable and independent sources of information that may be used to verify identity under AMLR Article 22(6) and (7).

As a result, identity proofing and fraud prevention are becoming more closely connected in Europe. Organizations are being asked both to verify identities and demonstrate how those identities were verified, and what level of trust supports them. Document verification, biometric verification, identity proofing, and presentation attack detection (PAD) are becoming part of the trust foundation for compliant digital onboarding.

## Europe's Trust Framework Expectations

European Regulation – What You Can Expect

### eIDAS 2.0

Every EU Member State must offer at least one European Digital Identity (EUDI) Wallet by the end of 2026. Regulated sectors such as banking, payments, and telecommunications must be able to accept those wallets by December 2027.

### AMLR

Beginning in 2027, non-face-to-face customer due diligence will increasingly rely on stronger digital identity and trust-service requirements, tying compliance more closely to high-assurance identity verification.

### ETSI TS 119 461 v2.1.1

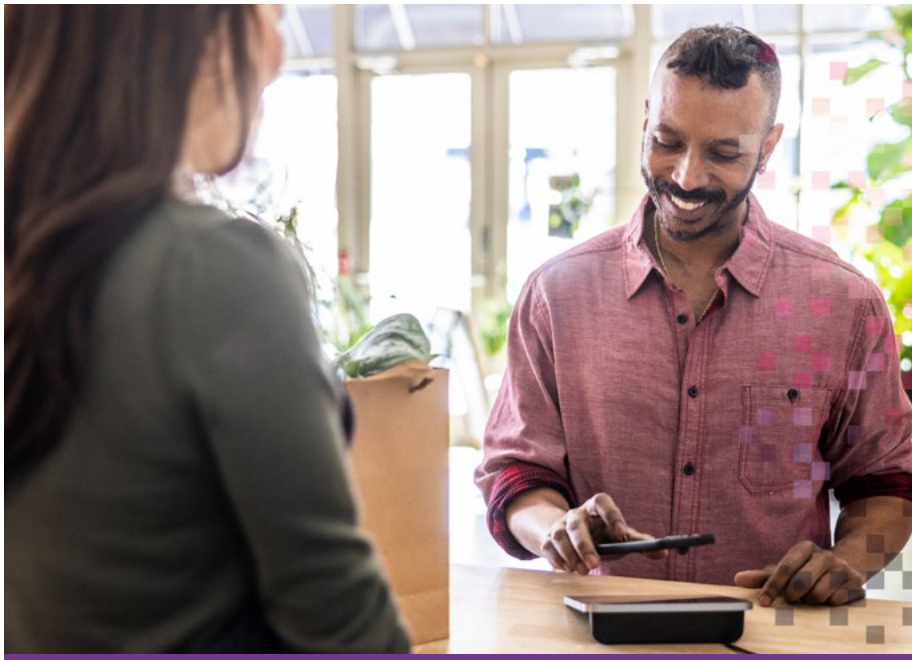
Establishes a higher technical standard for remote identity proofing, strengthening identity assurance and attack detection requirements. The standard becomes a key reference point for Europe's digital trust framework from August 2027.

## What Digital Wallets Change and What They Don't

Those same trust frameworks are laying the foundation for Europe's next phase of digital identity: the EUDI Wallet ecosystem. Europe is moving toward government-backed digital identities that are harder to fake and easier to verify. Wallets can eliminate some types of fraud, but they don't eliminate fraud itself. Fraudsters will simply shift their attention to whichever part of the identity journey is easiest to exploit. For example:

> **Binding:** A wallet credential proves an attribute was issued to a person. It doesn't, by itself, prove the person presenting it today is that person. Biometric binding is still needed to confirm the credential belongs to the person presenting it.
>
> **Enrollment:** Before a wallet can be used, it has to be linked to a real identity, creating many of the same risks found in traditional identity verification. Fraud doesn't disappear. It shifts to the enrollment process, making strong identity proofing important from the beginning.
>
> **Social engineering:** A customer who has been manipulated can present a genuine wallet credential and still complete a fraudulent transaction. The credential is valid, but the intent behind its use isn't.
>
> **Coverage:** Adoption will be uneven across sectors and borders for years. Organizations will need to support both wallet-based and document-based identity journeys, and fraudsters will target whichever option is easier to exploit.

This is particularly important in Europe, where physical counterfeits still dominate fraud activity in several markets, including France (60%) and Romania (59%). National identity cards are the most frequently targeted document type across the region, meaning traditional identity proofing will continue to play an important role even as wallet adoption grows.



While they don't eliminate fraud, digital wallets do represent a significant step forward. During Europe's transition to digital identities, organizations will need to protect both wallet-based and traditional identity journeys, because attackers will target whichever path is weaker.

CHAPTER 7

# The Americas: Higher Fraud, Faster Change

## Where document and biometric fraud meet.

The Americas is the global document fraud hotspot. At 5.7%, the regional document fraud rate is more than three times higher than Europe's and the highest of any region in this report. Physical counterfeits account for 67.6% of document fraud in the region, the highest share globally, while digital forgeries represent just 13.4%.

But the more important story sits beneath the region's high fraud rate. The Americas records the highest share of medium sophistication fraud in the dataset, with medium attacks accounting for 45.3% of document fraud, compared with 54.3% classified as easy, and 0.37% as hard. Social engineering activity is also high at 4.65%, just slightly below Europe.

High volume, low-effort fraud and more sophisticated attacks can exist side by side. Simple attacks remain common, while more sophisticated techniques are becoming a larger part of the fraud mix.

The region is also experiencing the fastest growth in deepfake activity, with attacks increasing 2,200% year over year. Growth in biometric and video-based attacks is putting pressure on both sides of the identity verification process.

**The combination of high document fraud rates and rapid deepfake growth is what makes the Americas unique. Organizations need to protect traditional identity documents while also addressing AI-enabled attacks against biometric systems. Whatever is driving the increase, the data shows that organizations in the Americas need to contend with both document and biometric fraud.**

## AMERICAS AT A GLANCE

### Key Fraud Trends - What We're Seeing in the Americas

**Deepfakes**
Deepfakes are growing faster than in any other region studied.

**Account Takeover**
Banking fraud has moved from an onboarding-only concern to include account takeover.

**Trusted Accounts**
Payments and professional services show the same post-onboarding fraud trend.

**AI-Enabled Fraud**
Deepfakes, injection attacks, and stolen genuine media accounts are becoming more common as AI-usage increases.

**Identity Challenge**
Verifying trust after onboarding is becoming as important as onboarding itself.

# The Limits of Document-Centric Verification

Driver's licenses are by far the most targeted credential type in the Americas, accounting for nearly two-thirds (64.4%) of document fraud. National identity cards account for 20.6%, while passports represent 9.0%. Because driver's licenses are the primary identity credential for many North Americans, they are one of the most valuable targets for fraudsters.

In the U.S., licenses are issued by more than 50 jurisdictions with different designs, security features, and verification standards. Unlike countries with centralized identity systems, the U.S. relies on purpose-built verification services, such as DMV-based driver's license checks and Social Security verification, to help validate identity information.

That means verification systems must recognize and validate 50+ variations of legitimate documents while simultaneously detecting fraudulent versions of those same credentials. REAL ID is bringing greater standardization through minimum security requirements for state-issued driver's licenses and identification cards, but the documents themselves are still issued at the state level. That creates more opportunities for fraudsters to exploit gaps in verification.

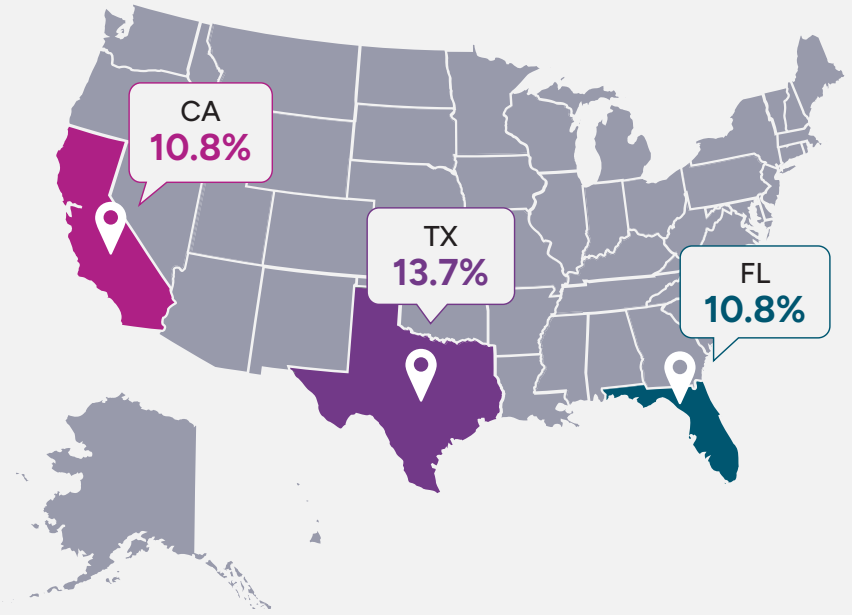
For many years, identity verification in the U.S. relied heavily on credit-header data such as name, address history, date of birth, and Social Security number. Repeated large-scale breaches have significantly reduced the value of those attributes as trusted identity signals.

Knowledge of that information no longer proves identity because, in many cases, attackers have access to the same data as legitimate users. This helps explain why document verification has become so important. It also shows why organizations are pairing it with biometric verification.

Deepfake attacks are growing faster in the Americas than in any other region, which is why document and biometric verification need to work together. Document verification helps confirm that identity credentials are legitimate, while biometric verification helps confirm that the person presenting them is real and physically present. As deepfake and biometric attacks become more common, organizations need both controls working together.

## Most-Targeted Documents in the U.S.

As the global Top 10 earlier in this report shows, the three most-targeted credentials in the dataset are driver's licenses from Texas, California, and Florida.



# The Transition to Digital Credentials

Mobile driver's licenses (mDLs) are being issued in a growing number of U.S. states using ISO/IEC 18013-5 standards. These credentials are an important step forward, providing a more secure and verifiable alternative to traditional driver's licenses.

Unlike Europe, which is moving toward a more unified digital identity framework, the U.S. transition is being driven by individual states, creating a more fragmented adoption path.

Regulatory support in the U.S. also is growing. In September 2026, FinCEN and federal banking regulators confirmed that state-issued mDLs and other government-issued digital credentials can be used for documentary identity verification, including remote verification scenarios. However, adoption remains uneven and varies significantly across states, agencies, financial institutions, and technology platforms. The transition will be gradual, with physical and digital credentials existing side by side rather than one replacing the other.

## Fraud Patterns Across the Americas

North America and Latin America share a high concentration of physical counterfeit fraud, but the credentials targeted and sophistication of those attacks differ.

Canada's profile is closely tied to driver's licenses and physical counterfeits. Its fraud mix is almost evenly split between easy and medium sophistication, with hard attacks accounting for 1.1%.

Latin America looks different. National identity cards account for 87% of attacks, followed by voter IDs at 10%. Physical counterfeits account for 76% of document fraud, while medium sophistication attacks represent 67% of activity.

Financial services are a major target in both Canada and Latin America. In Canada, the sector has the highest fraud rate at 10%. Across Latin America, payments face the greatest fraud pressure, followed by credit cards. Within Latin America, Chile's National ID card is the most frequently targeted individual credential.

### CANADA

| Physical Counterfeits | Most-Targeted Document | Easy Sophistication |
|---|---|---|
| 71% |  Driver's Licenses **77.32%** | **51.6%** |

### U.S.

| Physical Counterfeits | Most-Targeted Document | Easy Sophistication |
|---|---|---|
| 63% |  Driver's Licenses **67.58%** | **64%** |

### LATIN AMERICA

| Physical Counterfeits | Most-Targeted Document | Easy Sophistication |
|---|---|---|
| 76% |  National IDs **87%** | **32%** |

CHAPTER 8

# Asia Pacific: Digital-First Fraud

## A fraud environment early in the sophistication cycle.

Much of the document fraud in the Asia Pacific region is straightforward, with 74.0% classified as easy and just 0.38% as hard. Medium sophistication attacks are rising, reaching 25.6%. Deepfakes are also growing, increasing 116% year over year. APAC has the second highest share of deepfake activity across the three regions, with three APAC countries ranking among the top eight markets for deepfakes.

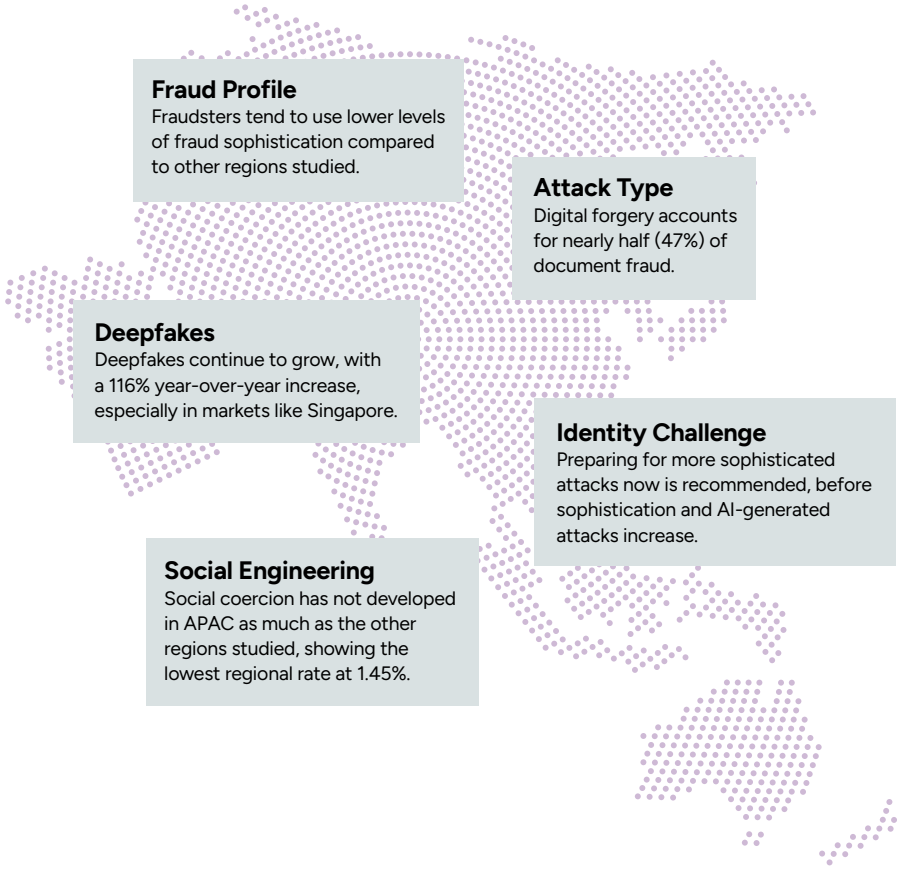
Social engineering remains relatively uncommon, accounting for just 1.45% of attacks. Fraudsters are still finding enough success through technical attacks that they have less need to target people directly. For now, digital forgery remains a more common attack path than large-scale social engineering campaigns.

Asia Pacific is the most digitally native fraud market in the dataset, with digital forgeries accounting for 47.2% of document fraud. Nearly half of the fraudulent documents submitted in the region were never physical documents at all.

When read together, these findings suggest Asia Pacific's attack surface is already digital, even if fraud sophistication remains relatively low. **Fraudsters are more likely to alter document images than create counterfeit physical documents, making Asia Pacific a digital-first fraud environment that's still earlier in the sophistication cycle.**

## ASIA AT A GLANCE

### Key Fraud Trends - What We're Seeing in Asia



## Digital Forgery Leads the Way

Digital forgery accounts for nearly half of all document fraud in our proprietary data analysis. Unlike physical counterfeits, digital forgeries involve altering a genuine document image rather than manufacturing a fake credential.

Asia Pacific has the highest proportion of fully digital, mobile-first onboarding of any region examined for this report. When the document never exists as a physical object in the verification flow and is instead photographed, uploaded, and assessed as an image, there's little advantage to manufacturing a physical card. Editing the image is often easier and more effective than producing a physical counterfeit.

## The Next Phase of Fraud

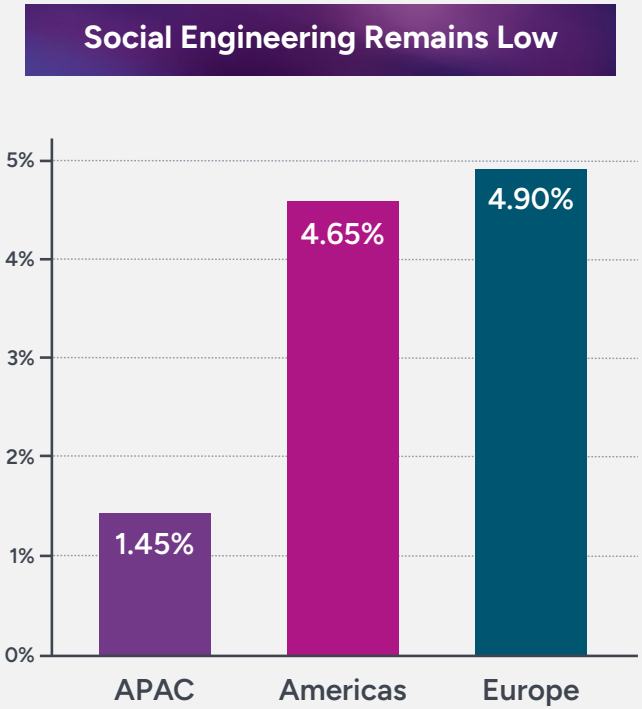
There are two key takeaways:

First, image-level forensics play an especially important role in Asia Pacific because many attacks rely on digital forgery rather than physical counterfeit documents.

Second, today's fraud profile may not be permanent. Europe and the Americas both show what happens when a high-volume, low-effort attack population meets improving automated detection. Easy attacks decline, while more sophisticated attacks become more common.

**Asia Pacific is still earlier in that cycle, creating an opportunity to prepare before more sophisticated attacks become widespread.**

Organizations can use this window to put capabilities like injection attack detection, biometric verification, and cryptographically verifiable credentials in place before the fraud mix changes further.





# Digital Identity Is Moving Forward Fast

Regulation is helping drive identity modernization across the region. Governments and regulators are expanding digital identity programs and updating requirements for remote onboarding and identity verification, giving organizations more reasons to strengthen their identity processes.

This is happening alongside the region's move toward digital-first fraud. As more onboarding and verification activities move online, governments are introducing new frameworks designed to improve trust in digital transactions.

The challenge for organizations operating across the Asia Pacific region is to manage different identity systems, regulations, and verification requirements across multiple markets. Supporting these differences without creating separate onboarding journeys for each country will become more important.

## Regulatory Momentum Across Asia Pacific

Anticipated Regulatory Changes

### Malaysia



eKYC requirements place a strong emphasis on document verification, biometric verification, and liveness detection.

### Philippines



The PhilSys national identity system is playing a growing role in digital onboarding and identity verification, with organizations increasingly relying on national identity data during onboarding.

### Australia



The Digital ID framework is expanding the use of trusted digital identities across public and private services.

CHAPTER 9

# The Timing of Fraud

## Fraud follows predictable daily and seasonal patterns.

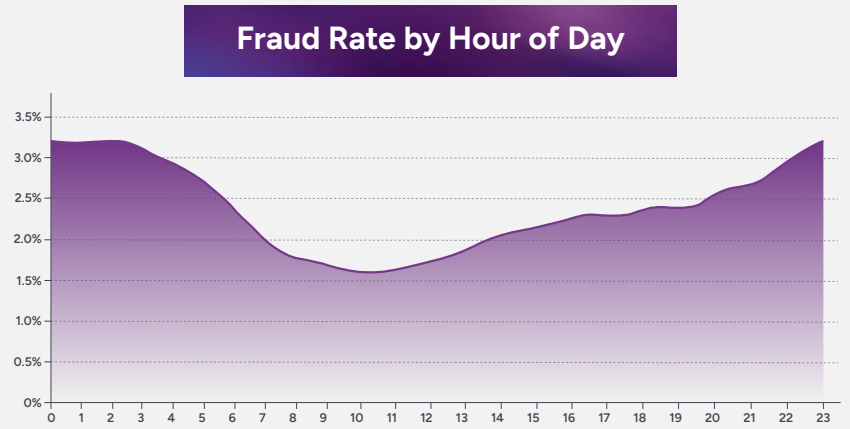
Fraud is more organized than many people realize. Like any business, it has operating hours, busy seasons, and quiet periods.

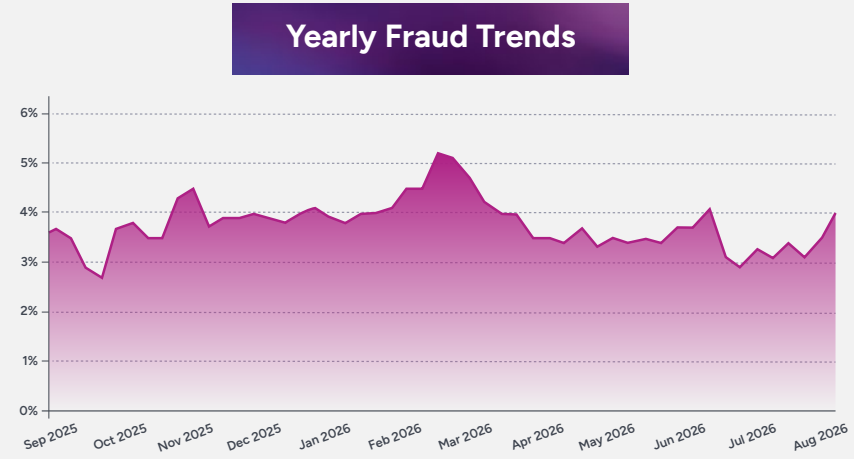
**The daily peak falls between midnight and 3 am UTC.** Fraud rates are roughly twice as high between midnight and 3 am UTC as they are during the lowest-risk hours of the day, when fewer staff are available to review suspicious activity.

**Social engineering peaks in November and December,** tracking holiday spending, seasonal scam campaigns, and a period when unusual financial activity looks ordinary.

**Fraudsters take summer vacations too.** Fraud activity falls by roughly 25% during July compared with winter peaks. The seasonal pattern suggests fraud activity rises and falls at predictable points throughout the year.

Automated detection is especially important when human review is limited. Quieter summer months are a good time for model tuning, testing, and rule updates. By contrast, fraud pressure increases in November and December, when social engineering activity is at its highest. Understanding when fraud is most likely to occur allows organizations to plan staffing, monitoring, and detection strategies with periods of higher risk.



CHAPTER 10

# The New Fraud Playbook

## Fraudsters are combining more attack methods than before.

The individual findings in this report are important, but the bigger story is how they connect.

Counterfeit documents, digital forgeries, deepfakes, injection attacks, social engineering, and account takeover often work together. Fraudsters use whichever tactic best exploits the weakest point in the process.

A typical attack might begin with a genuine document image obtained through a breach and injected through a virtual camera to pass onboarding. If the process escalates to human review, the attacker may even rely on social engineering. Weeks later, once the account has gained credibility, the same attacker may attempt account takeover through an account recovery process.

**Fraudsters may use multiple techniques, but they only need one weak point to succeed, which is why relying on a single control creates unnecessary risk. The challenge isn't stopping one attack technique but making sure each layer can compensate for the weaknesses of another.**



# Layers Win Against Modern Fraud

The most effective fraud prevention strategy uses document verification, biometrics, device intelligence, behavioral signals, and reverification together. Each layer addresses weaknesses that another layer can't.

Many of today's attacks involve genuine documents, people, or accounts being used in fraudulent ways. That's exactly why multiple forms of verification are needed. No single control can reliably detect every type of fraud discussed in this report.

Each control has its strengths and weaknesses. What one control misses, another can often catch. That's why multiple layers of verification work better than any single control alone.





## How Identity Controls Work Together

### Document Authentication

Detects counterfeits, forgeries, and tampering, but a genuine document could still be presented by the wrong person.

### Biometric Matching

Helps detect imposters using someone else's document, while deepfakes of the legitimate holder create a different challenge.

### Liveness Detection

Helps identify static images, replays, and masks, but injected videos can still bypass the camera itself.

### Injection and Device Intelligence

Identifies virtual cameras, emulators, and tampered sessions, while activity from a genuine user on a genuine device requires other signals.

### Behavioral Monitoring

Helps detect coached sessions and anomalous patterns, though a patient attacker may be harder to identify.

### Reverification

Helps address account takeover after initial trust, with compromise at the point of reverification remaining a consideration.

CHAPTER 11

# What Businesses Should Focus On in 2027

The same lessons appear throughout this report: Fraudsters are using more tactics and mixing in more sophisticated attacks. Organizations need more than one way to stop them. **These are five priorities for the year ahead:**

## 1 Defend the document layer harder, not less.

Physical counterfeits account for 61% of document fraud, making them the largest attack category in the dataset. Organizations shouldn't overlook document verification while preparing for newer fraud threats.

## 2 Prepare for AI-enabled fraud at both ends.

Detecting deepfakes is just one part of the challenge. Organizations also need to address how synthetic and stolen media reaches the verification process through injection attacks and other delivery methods.

## 3 Add device intelligence.

Injection attacks show that genuine-looking media, and sometimes genuinely authentic media, can still be used fraudulently. Device and session signals help identify risk that image analysis can't, making device intelligence an important part of identity verification.

## 4 Protect the moments after onboarding.

Fraud often targets account recovery, reverification, credential resets, and high-risk transactions. These moments need the same level of identity assurance as the original onboarding process. Reverification helps organizations confirm that a trusted user is still the right person when risk increases. When used at key moments throughout the identity lifecycle, it helps organizations maintain trust as opposed to establishing it just once.

## 5 Build regional strategies.

Fraud patterns vary significantly by region, which means controls that work well in one market may not work as well in another. Europe needs strong protection against sophisticated fraud and social engineering. The Americas needs resilient document and biometric verification. Asia Pacific needs strong digital forgery detection and preparation for a growing sophistication curve.

**Taken together, these priorities reinforce the central lesson of this year's report: No single technology can stop every attack. Effective fraud prevention requires multiple ways to verify trust.**

CHAPTER 12

# The Future of Trust

## Trust needs to be established and reinforced throughout the identity lifecycle.

The most important finding discovered within this year's proprietary data is the way fraud is changing and the way organizations need to respond.

Today's fraudsters use many different attack methods, often combining them within the same campaign. Fraud can now occur at any point in the customer relationship – not just during onboarding.

Trust needs to be reinforced throughout the identity lifecycle: onboarding, authentication, reverification, account recovery, and high-risk transactions. Doing that requires many layers of protection working together, including identity verification, biometrics, device intelligence, continuous behavioral monitoring, and reverification. No single control can stop every attack, but together, they help organizations build and maintain trust. This is the direction identity security is heading, from a single verification event to continuous trust throughout the identity lifecycle.





## Why Entrust?

Entrust fights fraud and cyber threats with identity-centric security. Our comprehensive solutions help organizations secure every step of the identity lifecycle, from verifying identity at onboarding to securing connections and fighting fraud in everyday transactions. Ongoing monitoring supports compliance and safeguards keys, secrets, and certificates.

Our capabilities include identity verification, biometric verification, ID and card issuance, device intelligence, fraud prevention, authentication, AI trust, and cryptographic security solutions. These capabilities help organizations establish trust during onboarding, reinforce it during authentication and reverification, protect against fraud throughout the customer lifecycle, and secure the systems and data that support digital interactions.

And as fraud evolves, compliance is evolving with it, making trusted identity critical for meeting requirements across regional and global markets where organizations operate.

**Discover how Entrust can help organizations verify identities, prevent fraud, and protect trust across the identity lifecycle.**

Learn more about Entrust Identity Verification

## ABOUT ENTRUST

Entrust fights fraud and cyber threats with identity-centric security that protects people, devices, and data. Our comprehensive solutions help organizations secure every step of the identity lifecycle, from verifying identity at onboarding to securing connections and fighting fraud in everyday transactions. Ongoing monitoring supports compliance and safeguards keys, secrets, and certificates. With a foundation of identity-centric security, our customers can transact and grow with confidence. Entrust has a global partner network and supports customers in over 150 countries.

entrust.com | Toll-Free: 888.690.2424 | International: +1.952.933.1223 | sales@entrust.com

©2026 Entrust Corporation. All rights reserved. Entrust and the hexagon logo are trademarks, registered trademarks, and/or service marks of Entrust Corporation in the U.S. and/or other countries. All other brand or product names are the property of their respective owners. IV27Q3-2027-identity-fraud-report-re

ENTRUST

SECURING A WORLD IN MOTION