IDENTITY FRAUD REPORT 2025-2026

From democratization to sophistication: millions of fraud attempts, but each one stronger

A comprehensive, data-driven report on identity fraud trends and prevention techniques from industry experts

Introduction

In last year's Identity Fraud Report, we identified the Democratization of Fraud: the rapid rise of fraud-as-a-service platforms and ready-made toolkits that lowered the barrier to entry for identity crime. That trend hasn't disappeared. If anything, it has become embedded in the fraud ecosystem, keeping identity fraud widespread and accessible, with millions of attempts recorded on our platform every year.

But while the volume of attacks remains staggering, the nature of fraud is shifting. The "low-effort" schemes of yesterday, such as sloppy document forgeries and crude copy-paste jobs, are increasingly filtered out by more sophisticated verification systems. Yet fraudsters have adapted, repurposing the same democratized tools into smarter, more professionalized operations. Today, deepfake-enabled liveness bypasses, synthetic identity rings, and carefully orchestrated post-KYC abuse are far more common.

We refer to this turning point as the Sophistication Shift: a moment when fraud transitions from high-volume noise to fewer, sharper, and more damaging attacks. This matters because stable percentages can create a false sense of security. In reality, every successful fraud attempt now represents greater preparation, higher costs, and longer-term impact for victims and institutions alike.

That's why taking a step back and looking at the bigger picture is critical. In our Identity Fraud Report 2024, we saw how new technologies and fraud-as-a-service marketplaces reshaped the threat landscape. This year's report continues that narrative, showing how those democratized tactics are now maturing into more targeted, professional operations. By analyzing millions of fraud attempts across industries and combining that data with global survey insights, this report offers a comprehensive view of how identity fraud is evolving — and what businesses, regulators, platforms, and service providers must prepare for as we move into 2026 and beyond.

Andrew Sever,
CEO at Sumsub

"We are witnessing a fundamental shift in the nature of fraud. Generative AI has democratized deception, but it has also forced verification to innovate at a pace faster than ever before. What we're witnessing now is not a rise in the levels of fraud, but instead, smarter and more deliberate attacks, with multiple layers of deceit.

The **Sophistication Shift** marks a turning point, as businesses now face challenges related to their velocity and the speed at which they can detect threats and adapt. The next frontier of fraud prevention will belong to those who can unite human insight, data intelligence, and AI precision to build trust at scale. This report captures the evolution of fraud to turn data into foresight for building a safer digital future."

Table of contents

Methodology

The main data sources for the report

This study offers a detailed analysis of identity fraud dynamics worldwide. Identity fraud refers to the theft or fabrication of personal information to carry out fraudulent activities, such as opening accounts or making unauthorized purchases.

4M+
Fraud attempts analyzed

In this report, we compare internal identity verification and user activity data from 2024 and 2025, covering fraud attempts across multiple regions and industries. In certain cases, data from 2023 is also included to highlight longer-term trends.

300+
Fraud and risk professionals surveyed

All insights are based on countries with significant user activity on our platform. To ensure statistical reliability, we only included jurisdictions where we processed more than 15,000 verification attempts during the reporting period. Countries with lower traffic are excluded from this analysis, as their sample sizes may not accurately reflect broader fraud trends.

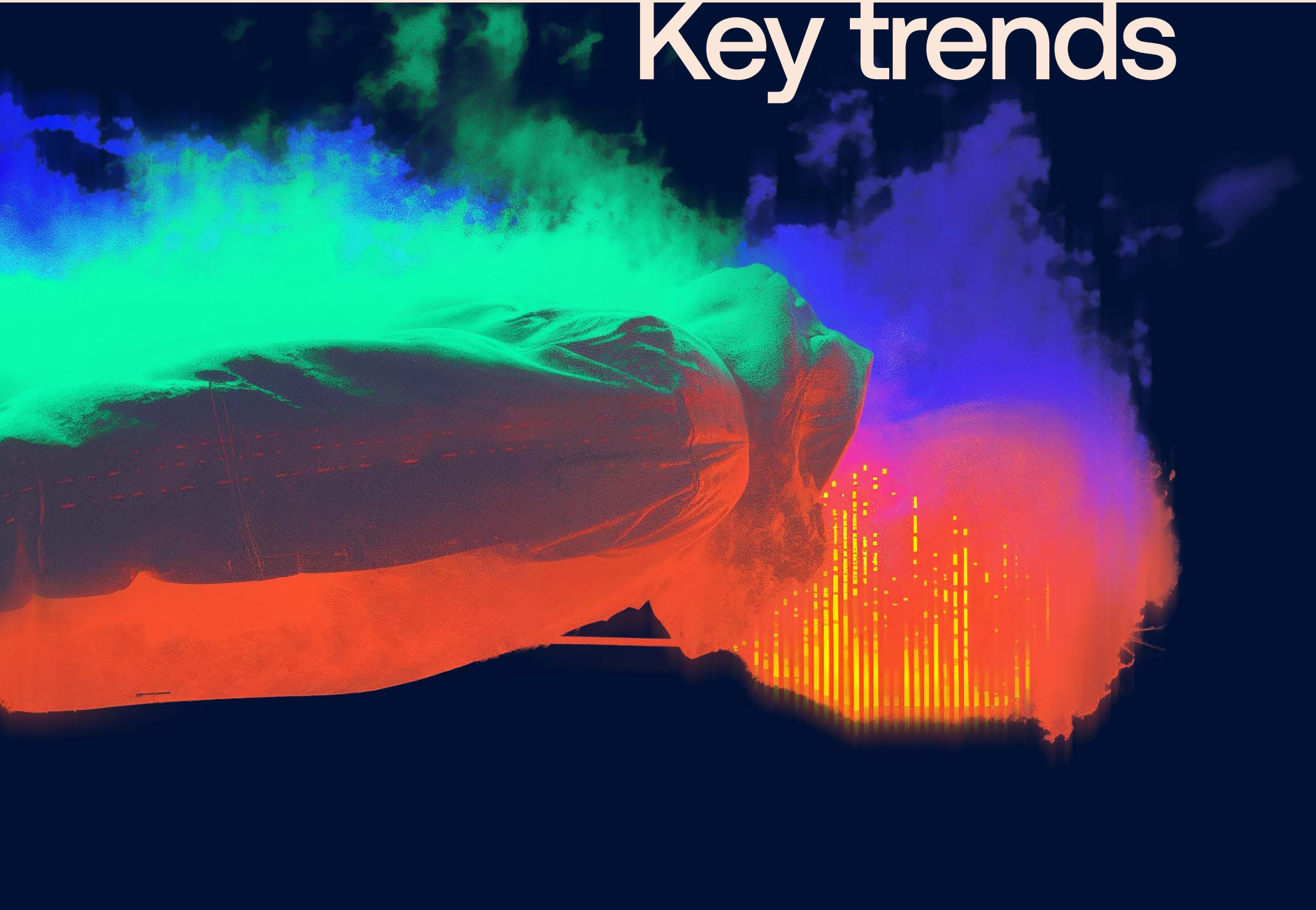
1.2K+
End-users surveyed

To explore the state of identity fraud in greater depth, Sumsub conducted a Fraud Exposure Survey in August 2025, gathering insights from both companies and consumers.
Sumsub's Fraud Exposure Survey 2025 included businesses from diverse sectors such as banking, crypto, payments, e-commerce, trading, and iGaming. Participants shared their experiences with fraud cases in 2025, the impact they faced, and their strategies for combating fraud in 2026.

All graphs and infographics are based on internal statistics compiled from the data of consenting customers. The data has been aggregated and anonymized.

The end users surveyed came from regions across **Latin America, North America, Europe, Asia, Africa, and the Middle East**, including Brazil, Mexico, Canada, the United States, Germany, the United Kingdom, Hong Kong, Indonesia, the Philippines, Singapore, Nigeria, and the United Arab Emirates. They shared the types of identity fraud they experienced, the financial and reputational losses incurred, and their trust levels toward different services.

Key trends



This year's main trend: the Sophistication Shift

What's behind this trend?

1 Less sloppy and low-effort fraud, but more advanced attempts cause greater damage. Compared with 2024, there has been a 180% increase in 'sophisticated fraud' using advanced deception techniques, social engineering, and AI-generated identities.

2 While public awareness and education surrounding fraud improve, keeping up with rapidly evolving technologies remains a significant challenge.

3 Stronger verification platforms have rendered the simplicity of last year's amateur, low-effort, and high-output scams largely fruitless. As a result, creative fraudsters are pivoting to more strategic operations, investing greater time and resources into attacks that can bypass these defenses.

Trend 2: AI industrializes fraud

In previous years, AI has primarily been used by fraudsters as a tool to forge IDs, edit documents, or spoof liveness checks. In 2025, it has evolved into something larger: a sophisticated fraud production ecosystem.

1 **Document forgeries.**
Platforms like OpenAI's advanced image generation tools now create IDs with near-perfect detail — replicating fonts, holograms, and textures that once required specialist skills.

2 **Protection attempts.**
Big Tech companies have attempted to implement protection measures to combat misinformation and plagiarism, including adding watermarks to AI-generated text. However, these watermarks are easily removable, allowing bad actors to pass off their own AI-generated images as genuine or steal them to use the watermark on any of their own AI-generated images.

3 **Synthetic video.**
Next-generation text-to-video systems, such as Google Veo and OpenAI's Sora and Sora 2, can render entire dynamic scenes from short prompts, complete with realistic facial microexpressions, lighting, and depth. These tools enable attackers to stage convincing deepfake liveness checks that mimic the movements and reactions of real people, making visual verification one of the most vulnerable layers of identity defense.

4 **The race to the top.**
As AI swells to its highest adoption with businesses and consumers alike, Big Tech is vying to be the most innovative in this space. After Google's release of Veo 3, OpenAI introduced Sora 2, quickly followed by Google's release of Veo 3.1 — signifying the escalating contest for the most realistic AI tools, thus accelerating the Sophistication Shift.

5 **Automation and scale.**
Fraud-as-a-service providers now bundle these models into ready-made production kits, enabling even low-skilled actors to generate industrial quantities of high-quality forgeries.

This marks the leap from AI as a helper to AI as the engine behind industrialized, scalable fraud. It accelerates both quantity (millions of attempts still flood the system) and quality (more sophisticated, harder-to-detect attacks) — fueling the **Sophistication Shift**.

Trend 3:
AI fraud agents

In 2025, we saw the first appearance of AI fraud agents — autonomous systems that combine generative content, scripting, and behavioral mimicry to execute full verification attempts end-to-end. What began as scattered experiments this year is expected to become a major wave in 2026, as these agents evolve into self-operating fraud bots capable of adjusting their strategies in real-time.

Trend 4: Telemetry tampering becomes the new evasion

As onboarding checks and document forensics improve, fraudsters are increasingly targeting the data pipelines themselves rather than the identity artifacts alone. Instead of only trying to fool the human eye or an AI classifier, they work to manipulate the signals those systems rely on.

1 **SDK and API manipulation.**
Fraudsters script verification flows, replay pre-recorded sessions, or tamper with SDK calls to trick systems into thinking an authentic session occurred.

2 **Device and environment masking.**
Emulator farms, virtual machines, and proxy layers enable attackers to appear as “fresh” users, concealing device fingerprints and location signals that typically expose repeat fraud attempts.

3 **Camera feed interference.**
Fraudsters attempt to override liveness checks by injecting synthetic frames or bypassing camera APIs, feeding prerecorded or AI-generated video into what should be a live capture.

This represents a step change in tactics. Instead of attacking only the **content** (a fake ID or deepfake face), fraudsters are now attacking the **context** (the way verification systems perceive and transmit signals).

Key findings

ID cards

Most vulnerable document type

Iraq ID card

Most forged document, **fraud rate 10.2%**

Maldives

Largest growth in deepfake attacks, **2,100% YoY growth**

Professional services

Consulting, legal, accounting, marketing, and freelance platforms, **232% YoY growth**

Zambia

Country with the highest number of applicants involved in fraud networks, **37% of approved applicants involved in fraud networks**

Nigeria

Country with the biggest share of synthetic documents, **8% of all synthetic documents**

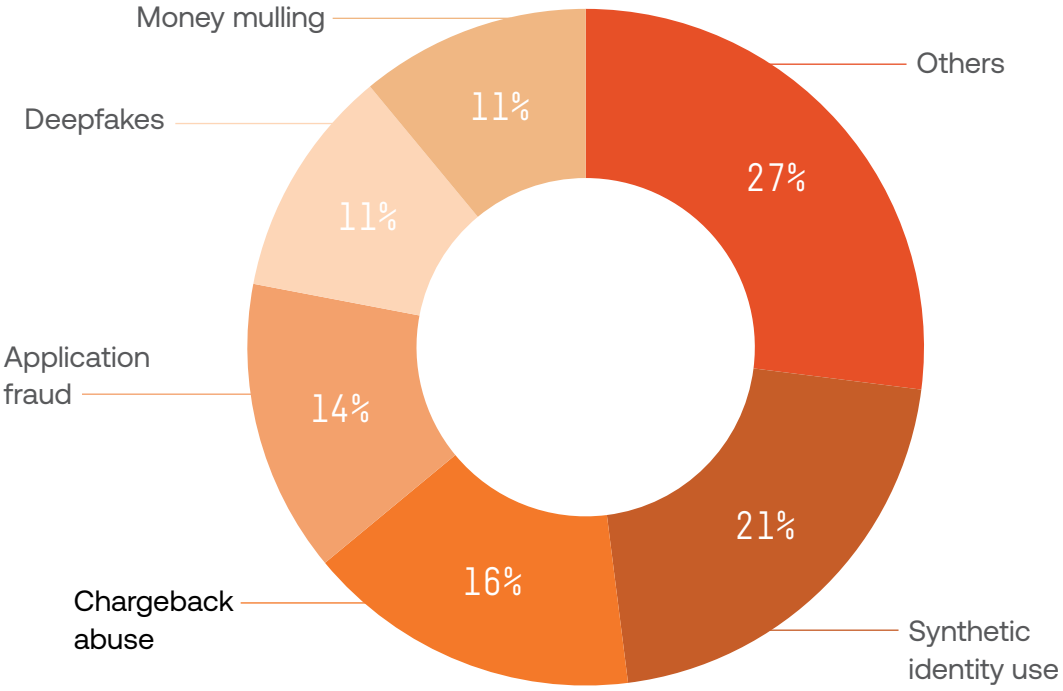
Malaysia

Country with the highest YoY growth in fraud rate, **197% YoY growth**

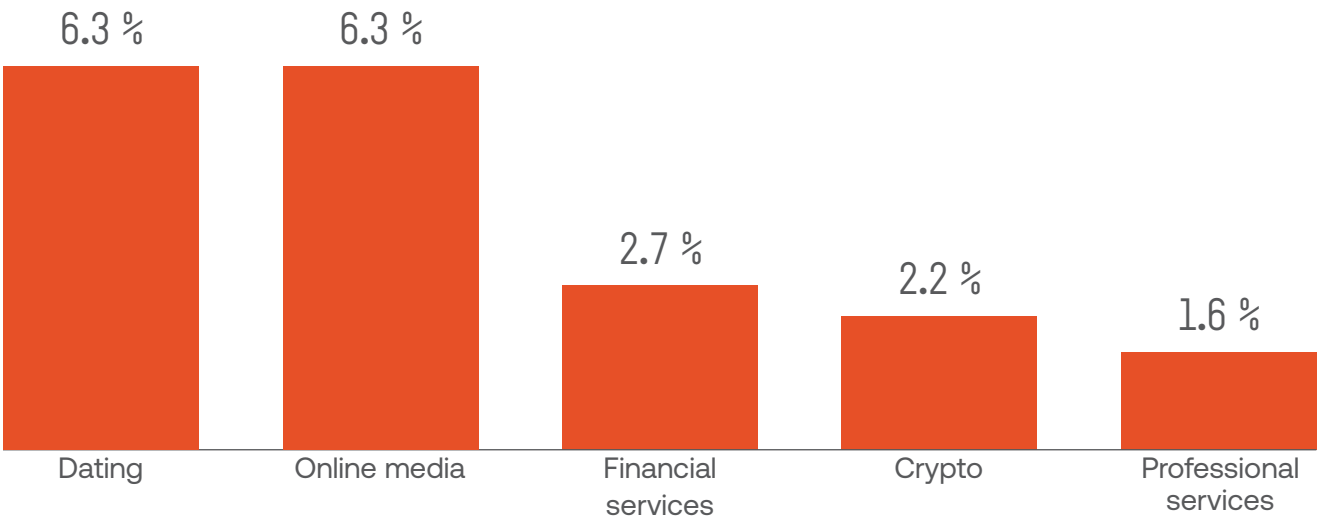
Countries with the highest fraud rates

U.S. & Canada	Middle East	Europe	LATAM & the Caribbean	Africa	APAC
U.S. 1.4%	Iraq 9.7%	Latvia 3.7%	Argentina 3.8%	Tanzania 5.0%	Pakistan 5.9%

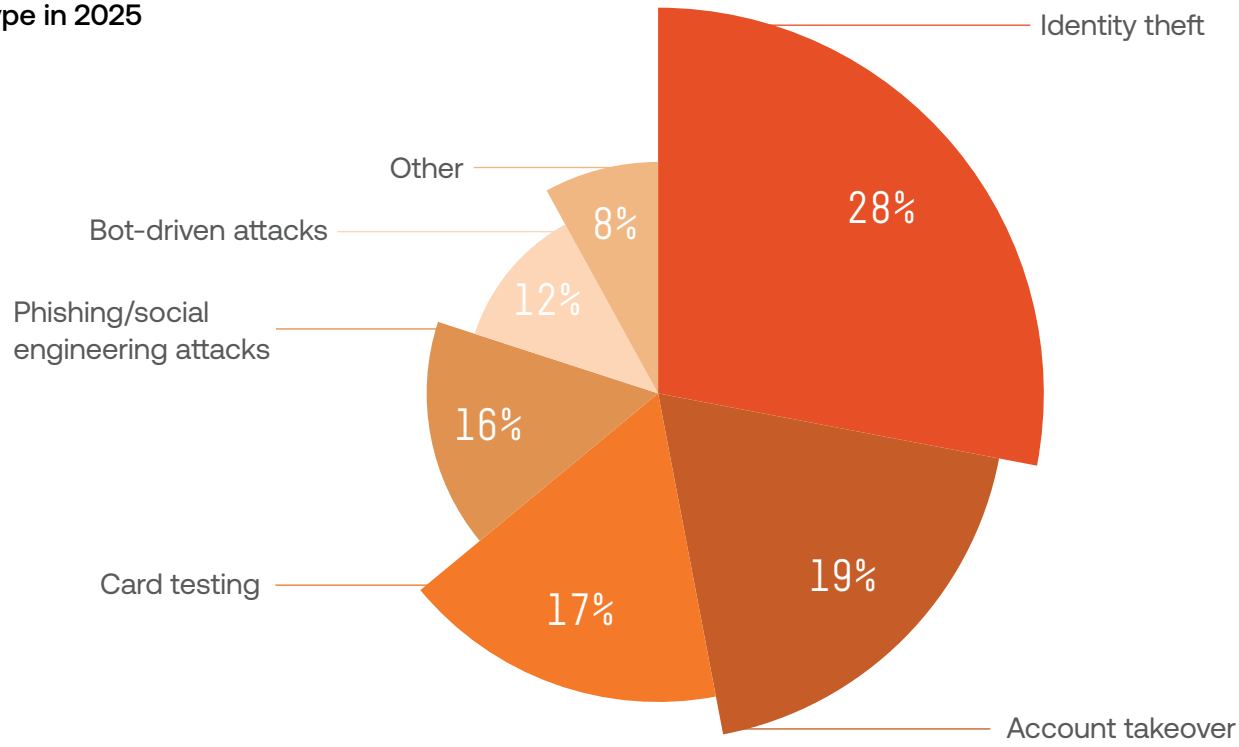
Top-5 first-party fraud type in 2025



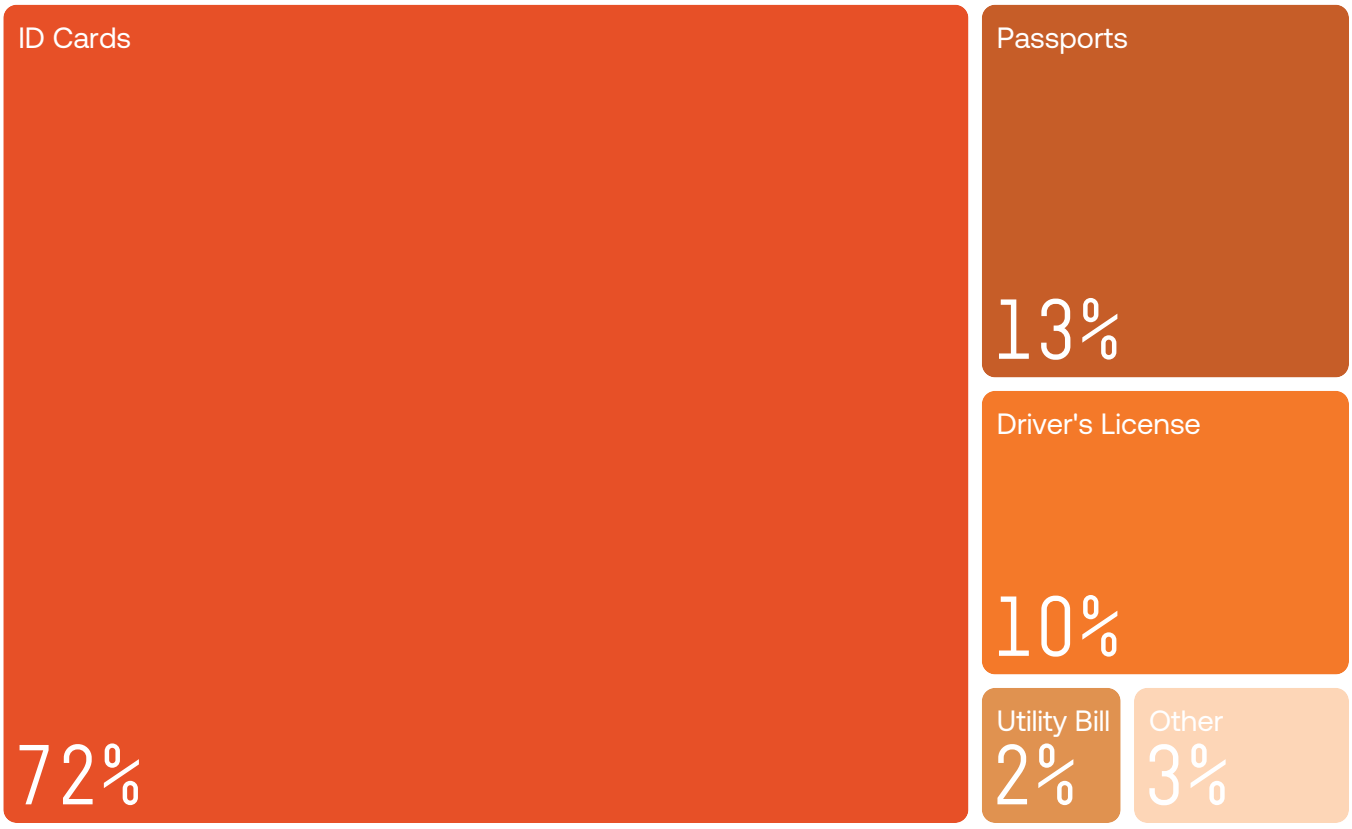
Top-5 industries with the highest fraud rates in 2025



Top-5 third-party fraud type in 2025



Fraud share by ID type, 2025

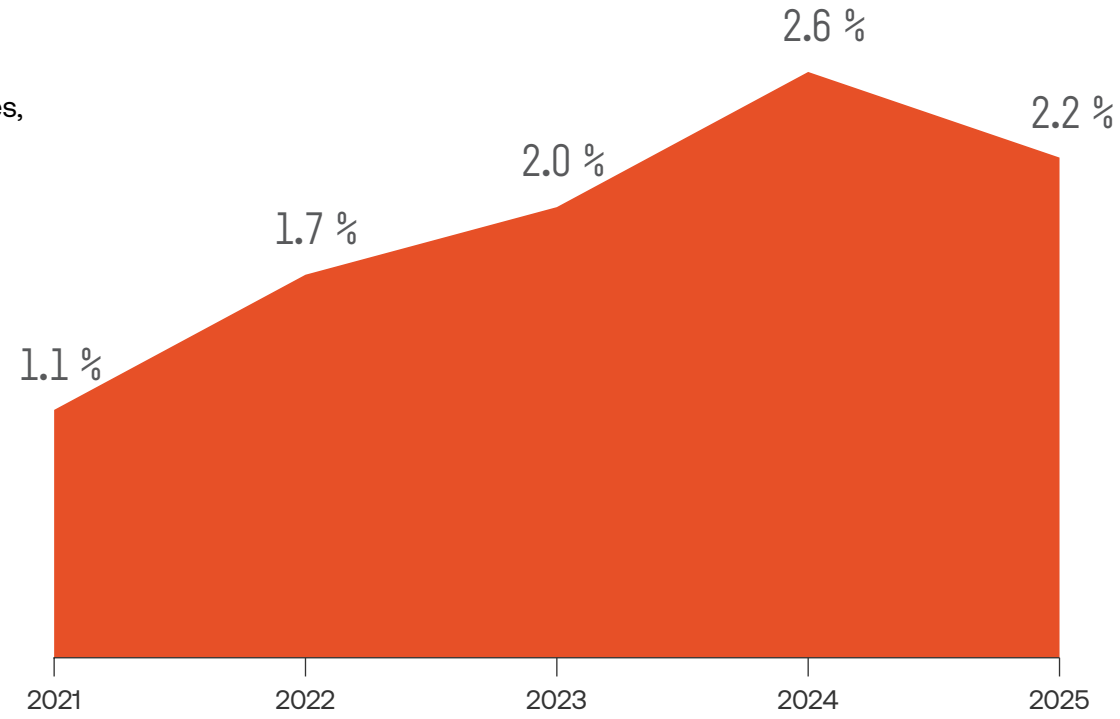


The Sophistication Shift

How fraud is evolving

Global fraud landscape

Chart 1.
Identity fraud rates,
2021-2025



% of fraud in all analyzed verifications worldwide

The global identity fraud rate continues to show a volatile but persistent trend.

1 In **2023**, the fraud rate stood at 2.0%, marking the baseline of the three-year view.

2 In **2024**, it spiked to 2.6%, the highest in recent history. This surge reflected the peak of the Democratization of Fraud, where the accessibility of fraud-as-a-service tools and low barriers to entry drove mass attempts.

3 In **2025**, the rate moderated to 2.2%, a slight decline from the prior year but still well above 2023 levels.

This apparent easing should not be mistaken for relief. Even at **2.2%**, the fraud rate translates to millions of fraudulent attempts across our platform. More importantly, the composition of fraud is shifting:

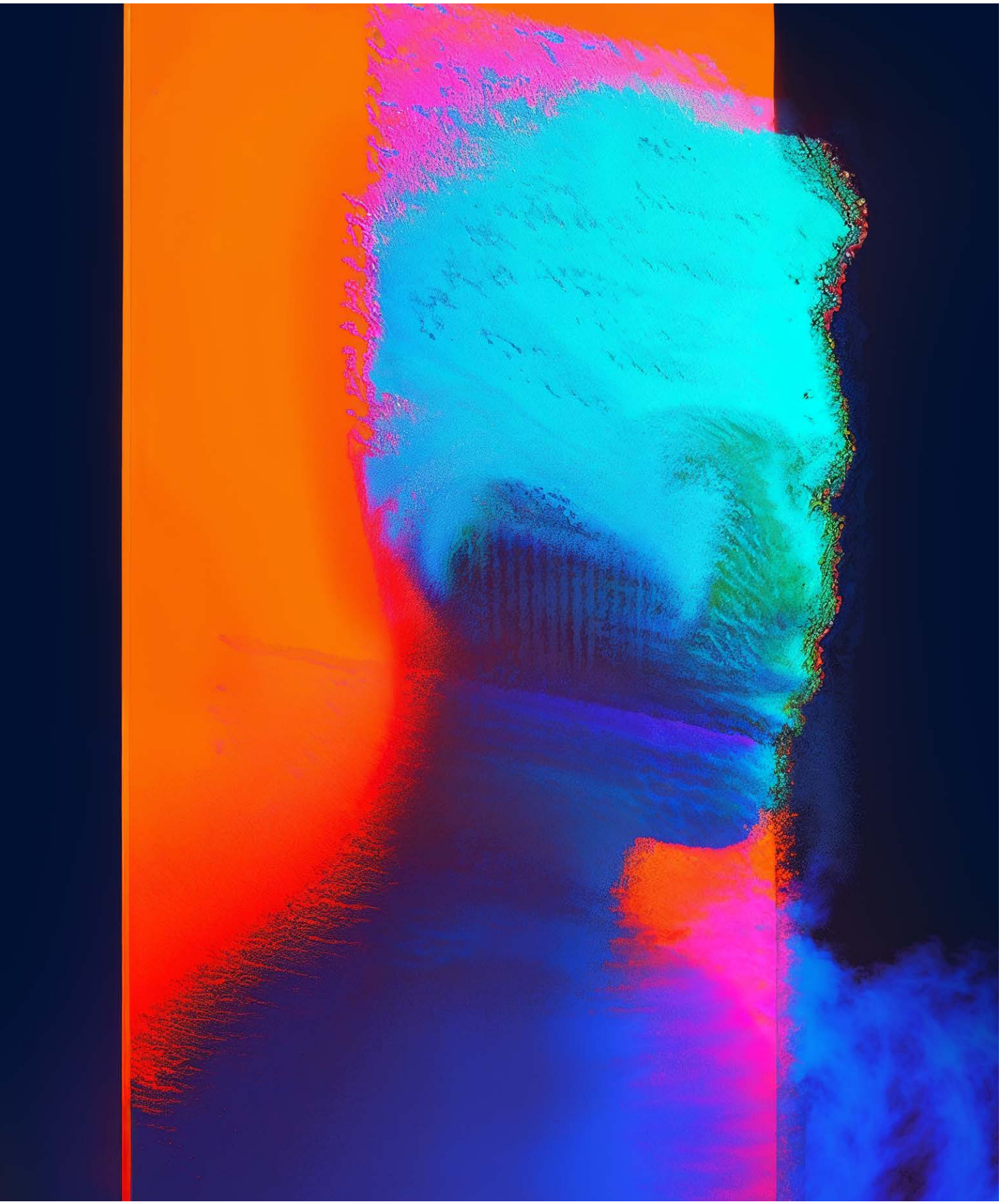
1. **Low-quality:** "easy win" fraud attempts have decreased as defenses have caught up.
2. **High-quality:** AI-augmented and telemetry-tampering attacks are taking their place, meaning fewer but smarter and more damaging incidents.

In 2025, we observed a dramatic 180% year-over-year increase in what we classify as "sophisticated fraud" — attacks that combine multiple coordinated techniques such as synthetic identities, layered social engineering, device or telemetry tampering, and cross-channel manipulation. Unlike single-method attempts, these multi-step schemes require planning, automation, and adaptability, making them far harder to detect and contain.

Deepfakes have been democratized and accessible to anyone with the right tools, but they also play a central role in complex, multi-layered fraud schemes that are increasingly sophisticated and harder to detect.

1. At the **individual** level, savvy teenagers are using deepfakes to bypass age verification in markets such as the UK and Australia.

In 2025, the rate moderated to 2.2%, a slight decline from the prior year but still well above 2023 levels.



2 At the **organized** level, deepfakes are a key component of advanced fraud operations, such as social engineering schemes targeting enterprises, which add further layers of deception through phishing and voice spoofing.

The share of these sophisticated cases within overall fraud has also tripled in just one year:

1 **In 2024, only about 10% of fraud attempts were advanced.**

2 **In 2025, that share has surged to 28%.**

Advanced methods combine multiple coordinated techniques, including higher-quality deepfakes, synthetic identities, multi-step social engineering, and telemetry tampering—evolving beyond the low-effort fraud seen in 2024.

This shift underscores that fraud is no longer dominated by low-effort, copy-paste attacks. Instead, a growing portion of cases are now engineered with precision, requiring more resources to execute, but also causing far greater damage when they succeed.

In other words, while the percentage of fraud attempts among all verifications may appear to stabilize, the threat mix has become far more dangerous. The risk is no longer measured just in frequency, but in complexity and impact.

Now, let's figure out the difference between these "simple" and "sophisticated" types of fraud.

Simple fraud

Low-effort, high-volume attempts that rely on basic deception. These are often cheap to produce, easily available through fraud-as-a-service marketplaces, and relatively easy for verification systems to detect.

Examples

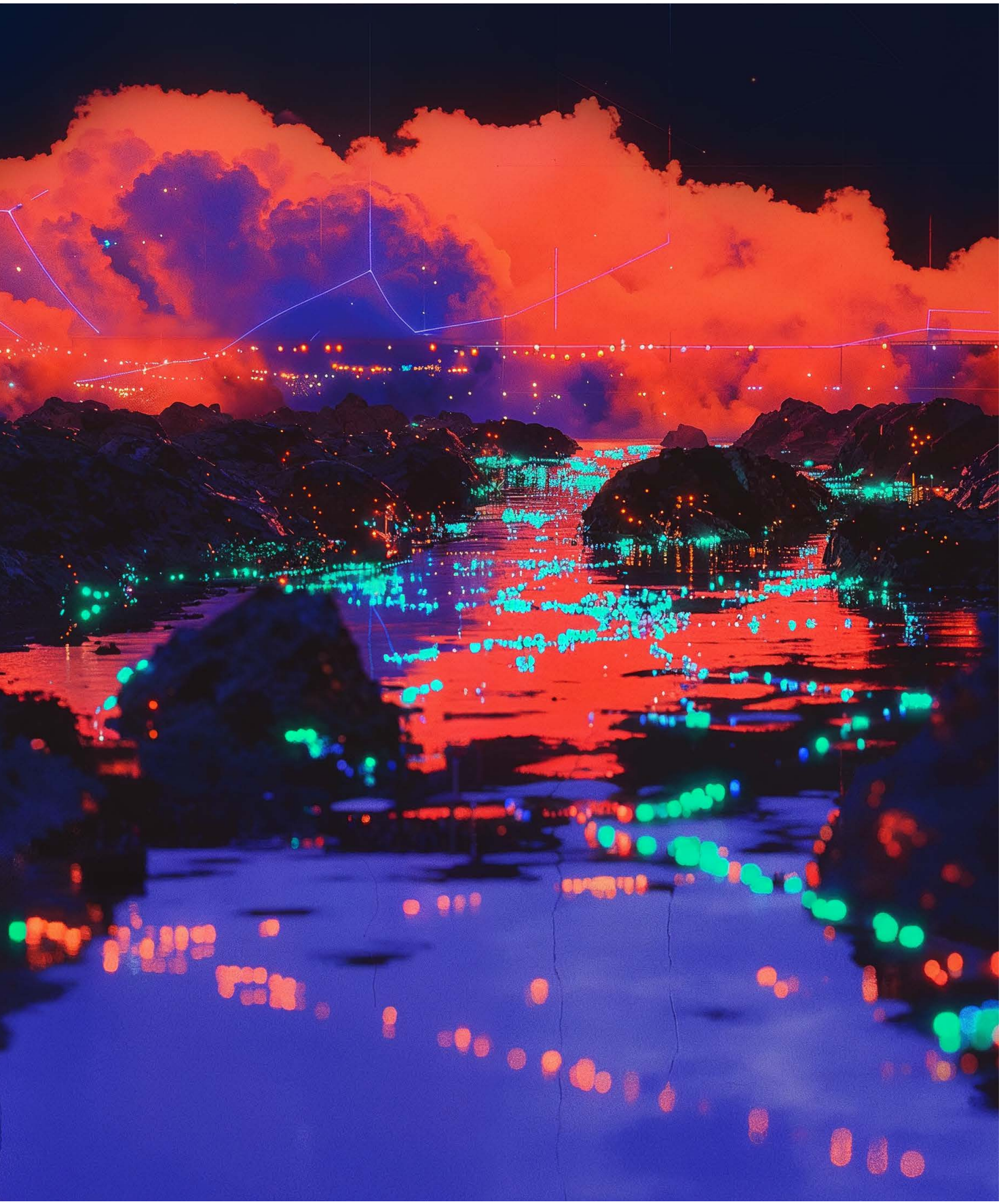
1. Poorly edited or stolen ID scans
2. Basic document template reuse
3. Copy-paste identity details from leaked databases
4. Obvious liveness test bypasses (showing a photo to the camera)
5. Use of “FraudGPT” or similar black-market AI bots to generate phishing emails, fake templates, or scripts for low-skill fraudsters — lowering the entry barrier even further

Simple fraud in real life

Our **Silly Fraud Awards (iGaming edition)** showcased some of these low-effort and poorly made (or just downright silly) attempts made to bypass our verification. Fraud attempts skyrocketed an average of 64% YoY in the online gaming sector, so it’s not surprising to see fraudsters try anything and everything to get past our defenses.

From picking on their pets to waving their hands, these fraudsters stood out for their simple fraud attempts.


Type
P
Country Code
EGY
Passport No
A17756024
Full Name
RAMESSES II
Date Of Birth
1303 BC
Place Of Birth
Nationality
EGYPTIAN
Sex
M
Date of issue
09/03/2014
Date of Expiry
09/03/2024
P<DUNN<RAMESSES<<<<<<<<<<<<<<<<
A17734243EGY681440M02<<<<<<<<
HAWAII
DRIVER LICENSE
NUMBER 06-18-1214
DOB 01/01/1991
EXP 06/03/2018
HT 5-10
WT 150
HAIR BRO
EYES BRO
SEX M
CTY 0
ISSUE DATE 01/18/2015
CLASS 3
RESTR
ENDORSE
McLowen
486 HOOMANAO ST
HONOLULU, HI 96706
McLowen



Sophisticated (hard to detect) fraud

High-effort schemes are designed to combine multiple advanced techniques into one complex and coordinated attack. These attempts require planning, technical resources, and often team coordination, making them harder to detect and much more damaging when successful. Increasingly, we see fraud actors combining different methods, creating hybrid attacks that bypass single-layer defenses.

Examples

1. Pairing high-fidelity AI-generated ID documents with deepfake video liveness checks
2. Using synthetic identities that later transition into mule accounts for laundering
3. Combining telemetry tampering (e.g., emulator use) with forged documents to mask repeated attacks
4. Orchestrating fraud rings where multiple synthetic and stolen identities interact, reinforcing each other's legitimacy

With deepfakes creation software becoming more accessible, businesses and their users must now, more than ever, be able to detect them. According to GOV UK, a projected 8 million deepfakes will be shared in 2025 (rising from 500,000 in 2023).

In our 2024 Identity Fraud Report, we referenced an Arup employee who transferred US$25 million following instructions from senior management, only to discover that they had transferred this sum to criminals after falling victim to a sophisticated deepfake. Since then, their Chief Information Officer has addressed the rise of sophisticated cyberattacks at the World Economic Forum, stating, "if cyberattacks were bullets, we would all be crawling around on the floor because they would be coming through the window, thousands of rounds a second."

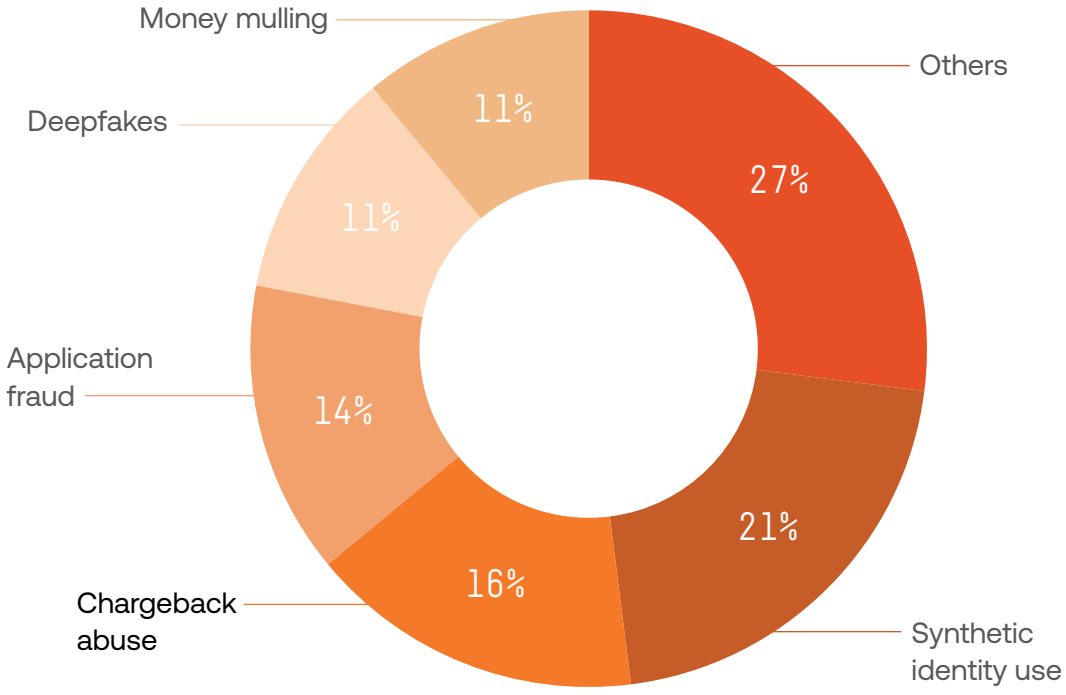
Identity fraud rate dynamics

Fraud types: a dual landscape

In previous editions, we presented a single Top-5 list of fraud types. But in 2025, the picture has become too complex and diverse for a single ranking.

Fraud now spans two very different categories: first-party fraud, where the perpetrator is the verified user themselves, and third-party fraud, where external attackers exploit or impersonate victims.

Chart 2.
Top-5 first-party fraud type in 2025



The following responses are defined by Sumsub's Fraud Exposure Survey 2025

First-party fraud

First-party fraud refers to attempts in which the individual behind the verification is the fraud actor. These are not outsiders impersonating someone else but applicants who present their own (real or fabricated) data with the intent to deceive or abuse the system.

Synthetic identity use (21%)

Fraudsters create composite identities that blend real and fabricated data, then use them to open accounts, access credit, or launder money. Expect synthetics to become more networked. Instead of single fake profiles, we will see clusters of synthetic identities interacting with each other, reinforcing credibility. AI-generated documents and videos will make these identities look more authentic than ever.

Chargeback abuse (16%)

Customers reverse payments after receiving goods or services, exploiting merchant protections. With global e-commerce still growing, chargeback abuse is likely to remain a persistent cost driver. Fraudsters are likely to automate claims at scale or combine chargebacks with other schemes (e.g., loyalty abuse), turning a “small” fraud type into a systemic drain.

Application fraud (14%)

Submitting false or manipulated information to gain financial products or benefits. Application fraud is likely to shift toward targeted, high-value products (loans, credit lines, BNPL). As credit tightening makes approvals more difficult, fraudsters will intensify their efforts with highly polished fake applications, backed by synthetic and fabricated employment data.

Deepfakes (11%)

AI-generated images or videos are used to pass liveness checks or impersonate legitimate users. Deepfakes will move from single-use fakes to adaptive, real-time tools. Expect fraudsters to deploy interactive avatars that can respond during liveness checks, not just replay pre-recorded clips. As detection improves, the focus on fraud will shift from quality alone to tampering with capture pipelines.

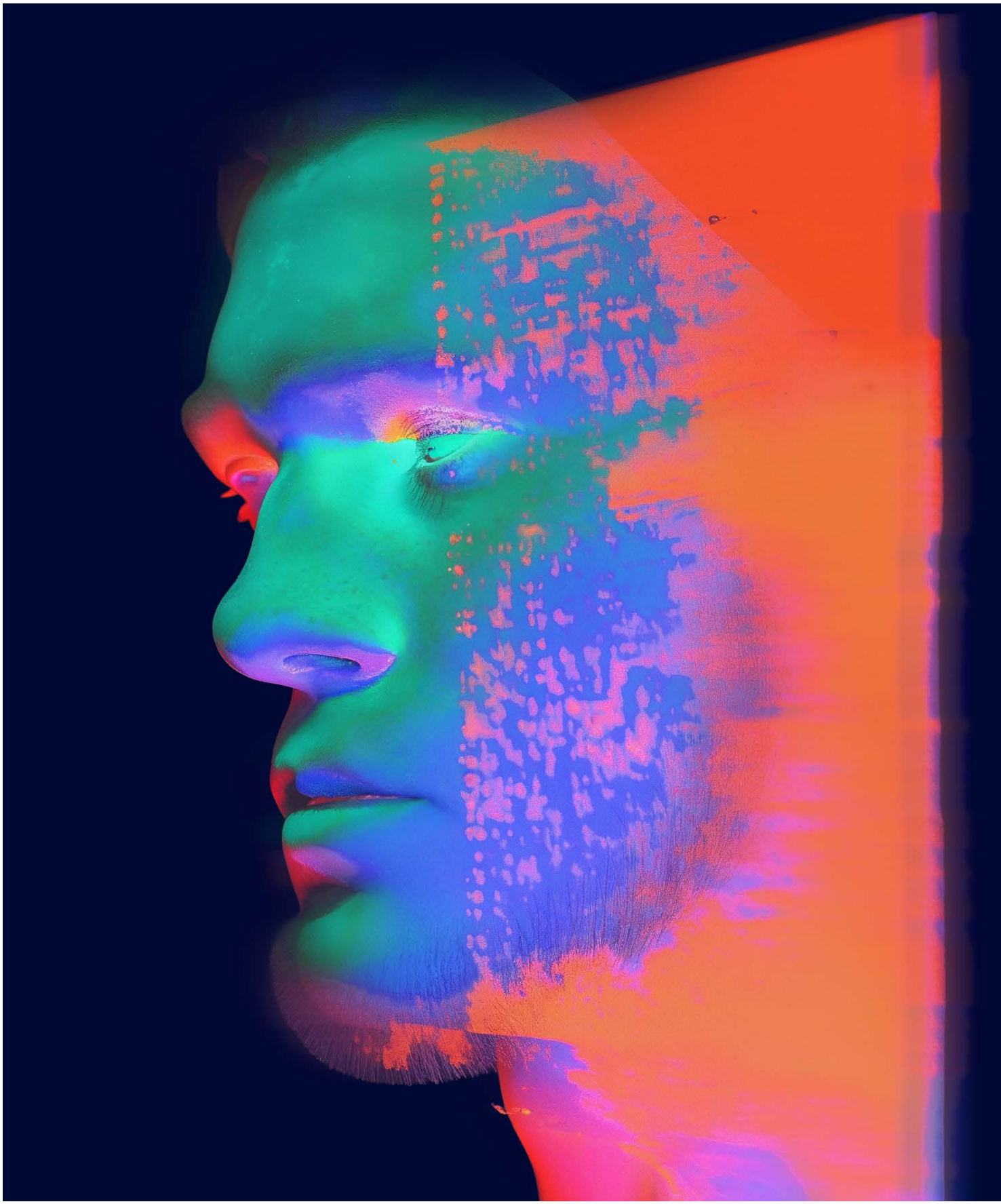
Money muling (11%)

Accounts operated to move illicit funds on behalf of fraud networks. Money mule activity will become more organized and professionalized, with entire mule networks linked together across regions. Fraud actors will increasingly blend synthetic identities with mule accounts, making it more difficult to distinguish between “front-end fraud” and “back-end laundering.”

Based on our research, the average price of one account ranges from US$40 to US$100.

Other (27%)

Smaller but still diverse categories, such as bonus abuse or fake employment documents.



Third-party fraud

Third-party fraud involves external attackers who impersonate or compromise genuine users. These schemes often rely on stolen credentials, social engineering, or automation.

Identity theft (28%)

Using stolen or fabricated personal data to impersonate victims and open accounts. Identity theft will increasingly use AI-generated replicas of stolen data. Instead of simply reusing breached records, fraudsters will enrich and adapt stolen identities with generative tools, making them blend seamlessly into some KYC processes.

Account takeover (19%)

Hijacking legitimate accounts through credential stuffing, phishing, or SIM swaps. ATO will evolve toward real-time, AI-assisted attacks, where fraudsters will use bots and deepfake voice/video to bypass multi-step authentication or social-engineer call centers, making recovery more challenging. Expect ATO-as-a-service kits to proliferate across industries like financial services, iGaming, and crypto.

Card testing (17%)

Using stolen payment cards to run small trial transactions before larger fraud. While card testing is not new, its scale is likely to explode with automation. Bot farms will push thousands of micro-transactions across multiple merchants in seconds, overwhelming defenses. New payment rails (real-time payments, digital wallets) will be tested the same way.

Phishing and social engineering attacks (16%)

Tricking victims into sharing sensitive data or authorizing fraudulent transactions. Social engineering will be supercharged by AI-generated content, from realistic deepfake voices of "family members" to phishing emails tailored in real-time. The line between "phishing" and "identity theft" will blur as fraudsters blend stolen data with AI-generated personas.

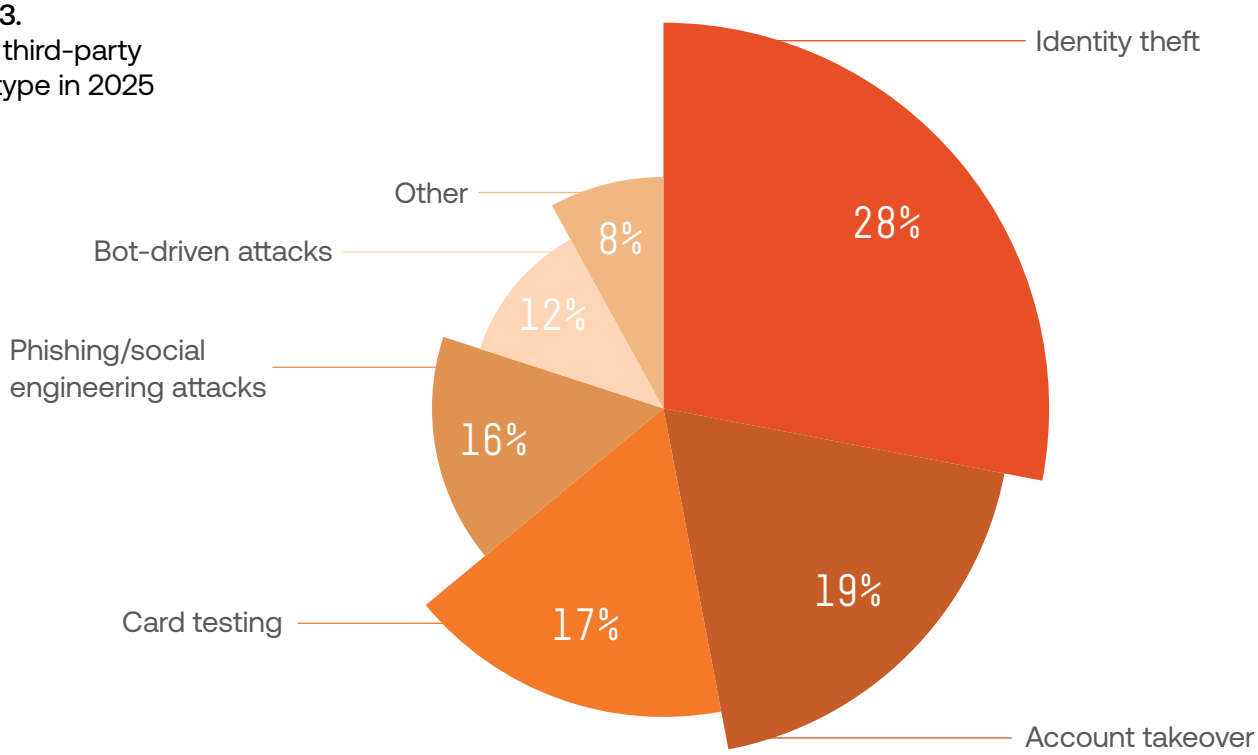
Bot-driven attacks (12%)

Automated scripts that flood verification or login systems with high-volume attempts. Bots will get more human-like by integrating language models to mimic real user flows and bypass behavioral detection. Expect fraud bot marketplaces to offer ready-made "human-in-the-loop" automation kits that alternate between bots and live operators to evade detection.

Other (8%)

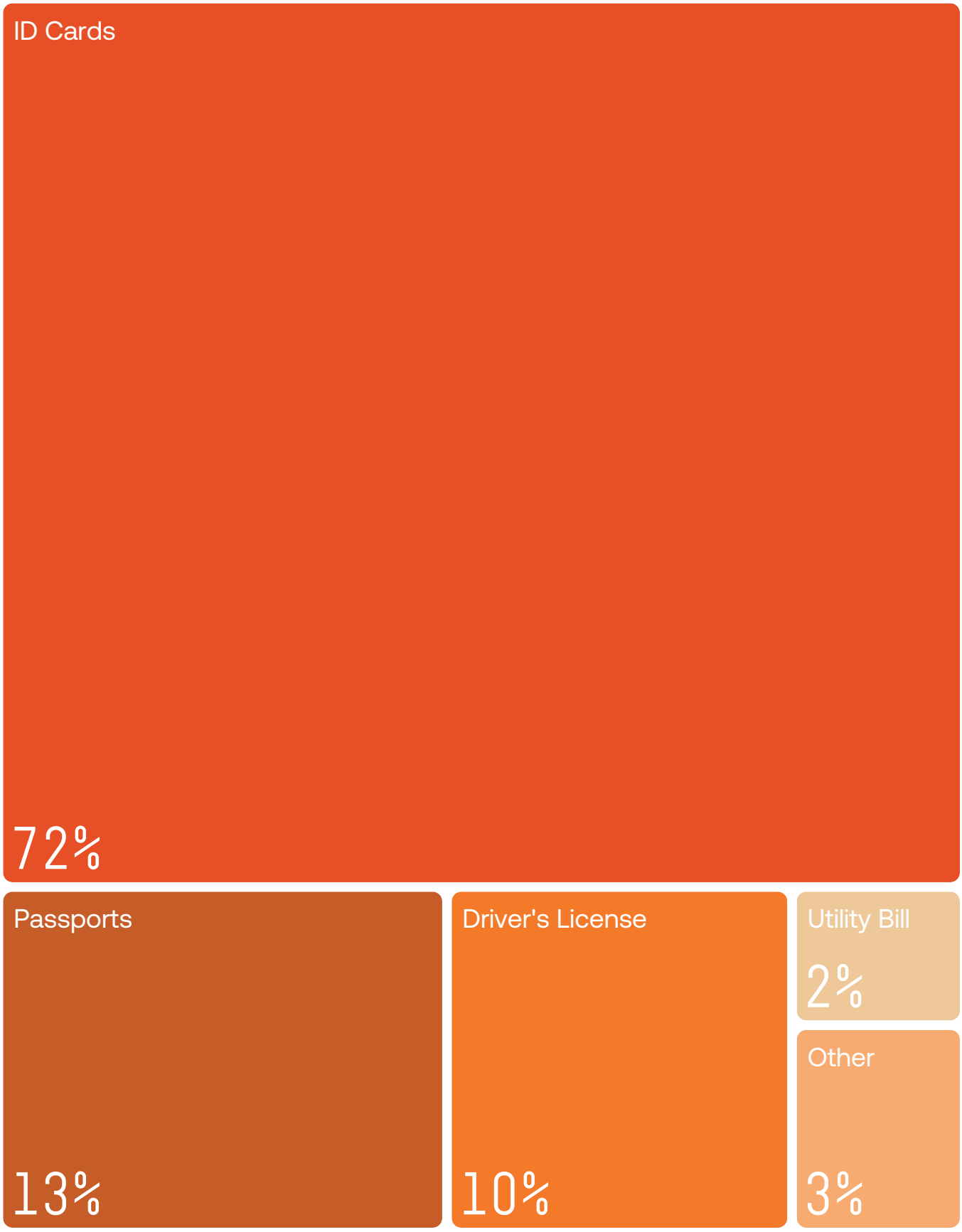
A range of smaller but growing schemes, including synthetic social profiles and referral fraud.

Chart 3.
Top-5 third-party fraud type in 2025



The following responses are defined by Sumsub's Fraud Exposure Survey 2025

Chart 4.
Fraud share by ID type,
2025



Fake documents

While fraud types differ in execution, from account takeovers to chargeback abuse, most of them still rely on one common enabler: fake documents. Whether the goal is to open a synthetic identity, pass an application with false information, or set up mule accounts, forged documents remain the primary entry point into digital ecosystems.

Fraud attempts continue to cluster around a small set of document types, but important shifts are underway.

ID cards remain the most frequently targeted artifact, accounting for 72% of all fraudulent documents detected in 2025. Their ubiquity and ease of access make them the perennial favorite for fraudsters seeking a quick entry point.

Passports (13%) and **driver's licenses (10%)** follow, reflecting their critical role in cross-border mobility and financial access. These documents are often targeted in higher-value schemes that require stronger credentials.

Utility bills (2%) and **other documents (3%)** represent a smaller share, but remain part of synthetic identity and address-verification fraud chains.

Payment methods now show the highest fraud rate across all artifact types at 6.6%.

6.6%

While ID cards dominate in volume, the biggest story of 2025 lies elsewhere: **payment methods now show the highest fraud rate across all artifact types at 6.6%.**

This signals a strategic pivot by fraud actors:

1. ID cards and other identity documents are often the entry point.

2. But payment methods are where the money is, allowing direct monetization through stolen card data, fake funding sources, or manipulated account credentials.

3. With fraud-as-a-service kits offering pre-packaged payment data and scripts, this layer has become the most lucrative and efficient target for cybercriminals.

In previous years, ID cards were the top target, showing the highest fraud rates in our dataset. In 2025, that balance has shifted. Payment methods now take the lead, with a 6.6% fraud rate — the highest among all document types.

This reflects fraudsters' changing priorities. As onboarding controls get stronger, attackers are moving downstream into financial rails: manipulating card details, payment credentials, and funding sources. Payment method fraud is attractive because it combines instant monetization with broader reuse potential across multiple platforms.

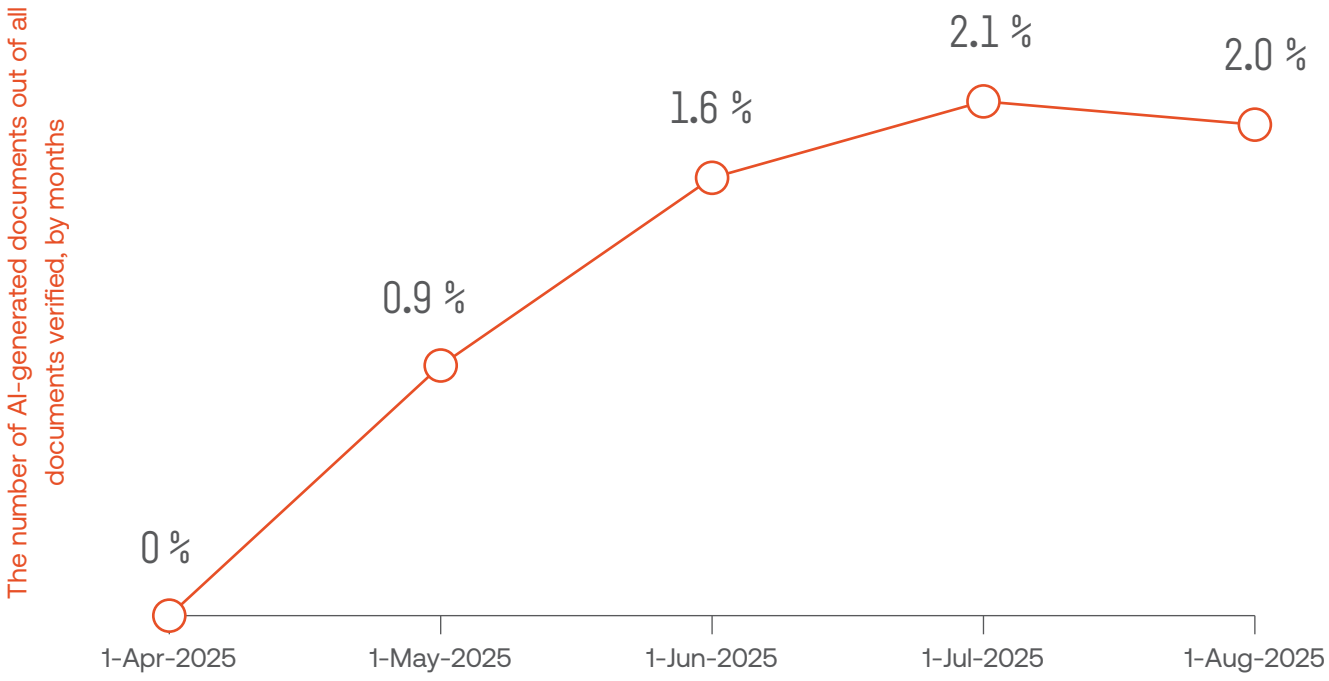
The result: organizations face growing pressure not only to validate who the user is, but also to verify the trustworthiness of how they pay.

AI-generated documents on the rise

A new phenomenon is shaping the fraud landscape in 2025: large-scale AI-assisted document forgery. **Our data indicate that 2% of all fake documents detected this year were generated using tools such as ChatGPT, Grok, and Gemini.** While this may appear to be a small share today, the trajectory is clear—and concerning.

The chart below illustrates this growth, starting in April 2025 (when the first verified ChatGPT-forged documents appeared on our platform) and continuing through August 2025. The trend line rises steadily, peaking in July before experiencing a slight dip in August, but remains well above the initial baseline.

Chart 5.
Growth in AI-generated documents




FACTURE
12 octobre 2025
pk12
Designation
Montant
Fourniture de gaz (10 m³)
45,00 €
Transport et pose
15,00 €
Sous-total
60,00 €
TVA (20%)
12,00 €
Total
72,00 €
Mode de paiement
Virement bancaire
Merci de votre confiance.
CARTE NATIONALE D'IDENTITE BURKINABE
BURKINA FASO
Nom:
Prénoms:
Né(e) le: 29/11/2001 A KIKIGOGO
Sexe: M
Profession: ELEVE
Délivrée le: 01/06/2021
Expire le: 31/05/2031
Taille: 176 cm
Signature du titulaire
Signature de l'autorité
Trạng thái
Thành công
Thời gian
20:40 - 02/10/2025
Mã giao dịch
Tài khoản/thẻ
Tổng phí
Miễn phí
Danh mục
Hóa đơn
Nhà cung cấp
Mã khách hàng
Tên khách hàng
Địa chỉ
THÀNH PHỐ HỒ CHÍ MINH
Kỳ thanh toán
Tiền điện 9/25
Thanh toán tự động
ELECTRICITY BILL- NOTICE
Dt:03/10/2025 Time:11:07
SC No.
USC No.
Name:
Address:
Cat:10(ii) DOMESTIC
Contracted Load 1.00
1.00 KW
MtrNo. (IR)
MF 1.00
Ph1
Days 30
Cat:10(ii) DOMESTIC 1197.16
Previous 0/09/25 25.90
Customer Charges 100.38
Electricity Duty 1.38
Interest on ED 0.42
Surcharge 25.00
FSA/FCA Charges 0.00
Subsidy 0.00
Adjustment 0.00
Interest on CD 8.56
Bill Amount 1362.00
AUSTRALIA
PROOF OF RESIDENT IDENTITY
Name
Date of birth
Sex COM
M
Date of issue
01 JAN 2024
Date of expiry
31 JAN 2034
Signature
Card number
Signature

Despite efforts by Big Tech to control the misuse of AI, including the use of watermarks and investments in new technology to detect AI-generated content, these measures can still be bypassed by professional scammers with the right malware.

What this means:

Accessibility Fraudsters no longer need Photoshop expertise. With AI tools like ChatGPT (and other image-generation extensions), creating a convincing fake ID or utility bill can be accomplished with just a few prompts.

Speed The velocity of attempts is accelerating—fraud actors can generate multiple versions of the same document in just minutes, flooding verification systems.

Quality Early versions were crude and easily detectable, but by mid-2025, the forged documents displayed fonts, layouts, and seals that mimicked authentic templates.

Generative AI is enabling the creation of inexpensive, repeatable, and increasingly realistic fakes—effectively industrializing what was once a skilled, niche activity.

This development connects directly to the Sophistication Shift: even as the overall percentage of fraud attempts appears to stabilize, the composition of fraud is evolving. The accessibility of AI has led to an increase in poor-quality, quick wins for amateur fraudsters, while also advancing the multi-layered, sophisticated scams often used to target high-profile individuals or enterprises.

AI and digital fraud

AI has always been part of the fraud conversation. In earlier reports, we spoke about deepfakes and generative tools as new weapons in the fraudster's toolkit.

But in 2025, the story is no longer about a disjointed tool here or there; it's about a whole ecosystem of AI that industrializes fraud. Models that create documents, voices, or videos are now paired with automation and fraud-as-a-service marketplaces.

The result is a step change: fewer but far more engineered attacks, designed to blind verification pipelines and slip downstream into payments and post-KYC abuse. This evolution means that organizations can no longer rely on static checks. The future of defense lies in understanding behavior — specifically, how fraudsters act over time, how they manipulate signals, and how their patterns differ from those of legitimate users.

While documents and videos can be forged, behavior leaves a trace. Mouse dynamics, typing rhythms, app navigation patterns, transaction timing, and device handoffs all reveal whether an identity behaves like a genuine user or a fraud actor.

In 2025, the most significant progress comes from multi-layer behavioral models:

Onboarding flows	Identifying scripted interactions, suspiciously fast form fills, or inconsistencies between typing and pasted data.
Transaction journeys	Monitoring purchase amounts, geolocation jumps, and payment method switching to flag mule or chargeback abuse.
Cross-section signals	Detecting when “different” users actually share the same behavioral fingerprint, exposing fraud rings.

Behavioral AI shifts the focus from what the document looks like to how the user behaves over time. This approach is critical against combination attacks, where fraudsters mix multiple techniques — for example, presenting a synthetic ID, bypassing liveness with a deepfake, and laundering funds through mule behavior. Even so, documents remain the gateway. Generative AI now produces IDs with fonts, holograms, and watermarks nearly indistinguishable from real ones. To counter this, providers are deploying structure-aware natural language models that check logical consistency within documents. Does the MRZ checksum match? Do issuing authorities align with known policies? Are place names or date formats authentic for that jurisdiction? These checks look beyond the pixels to uncover linguistic and structural seams that betray AI-generated content.

Fraudsters also weaponize AI video tools, such as Google Veo, to generate convincing liveness clips. The countermeasure is multi-modal verification, combining vision (micro-expressions, skin texture, physiological cues), audio (voice cadence, ambient sound), and device telemetry (camera attestation, timestamp integrity). Fraudsters can fake one channel, sometimes two — but maintaining perfect consistency across all three is far harder.

The rise of AI fraud agents

The latest development in 2025 is the emergence of AI fraud agents — autonomous systems capable of executing entire fraud operations with minimal human intervention. Unlike traditional bots or scripts, these agents combine generative AI, automation frameworks, and reinforcement learning, enabling them to:

1. **Generate fake identities and supporting documents on demand.**

2. **Interact with verification interfaces in real time — answering prompts, adjusting behavior mid-process, and mimicking human responses.**

3. **Learn from failed attempts to refine their next approach, achieving adaptive persistence across platforms.**

In practice, this means a single AI fraud agent can orchestrate a comprehensive attack chain, including creating a synthetic persona, submitting a deepfake video, tampering with device telemetry, and reattempting verification with minor variations until it succeeds. Today, these agents are in their infancy — limited to black-market forums and closed research circles — but by 2026, analysts expect a boom in AI-driven autonomous fraud, where coordinated fleets of agents conduct high-speed, multi-step attacks at scale.

This trend is no longer theoretical. In late 2025, Anthropic researchers uncovered an espionage campaign in which autonomous AI agents were deployed by a state-linked actor to conduct cyber operations, including reconnaissance, phishing, and network infiltration — without direct human control.

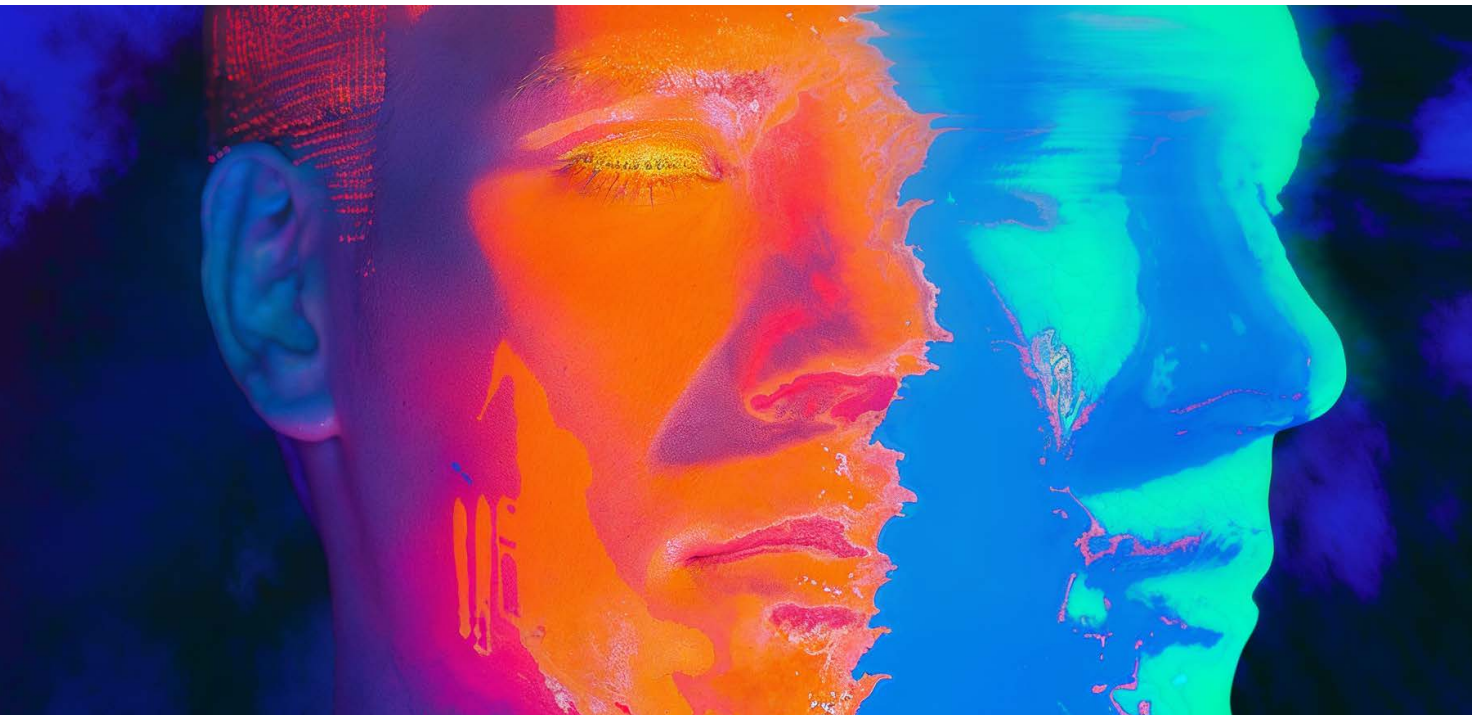
This example underscores how rapidly agentic AI has evolved from a lab curiosity to an operational threat model. While the case involved espionage, the same technology stack — self-directed LLMs coupled with task automation — can be repurposed for financial or identity fraud.

This is the moment when AI stops simply enabling fraud and starts operating it. For organizations, the implication is clear: future defenses must be able to detect not just what is fake, but who or what is behind it — distinguishing between a human fraudster and an intelligent automation system acting on their behalf.

Bypassing Age Verification

With the UK Government introducing mandatory online age verification with the Online Safety Act, necessary for checks on social media, adult sites, and gaming sites, AI has been used to bypass identity checks. From creating synthetic identities with fake IDs to deepfakes of real people, it has become a tool to bypass biometric face scans. While in Australia, Meta announced it would begin testing AI on users under 16, attempting to bypass the social media ban by listing their account as being for users over 18 years old.

In July, the European Commission announced that it is working towards a harmonized approach to age verification, offering a blueprint age verification solution named the 'mini wallet'. The second version of this blueprint was introduced in October, with additional features for passports and ID cards, in addition to eIDs required as proof of age.



How global regulators are responding to the rise of AI-generated fraud

1 The EU Artificial Intelligence Act will impose obligations on high-risk AI, including those related to identity verification.

2 The EU Digital Identity Wallet (piloting in 2025) embeds stricter cross-border document validation.

3 The upcoming PSD3/PSR framework strengthens payment fraud prevention, while in the U.S., NIST SP 800-63-4 updates authentication and anti-spoofing standards.

4 Law enforcement, through initiatives such as INTERPOL's Project SynthWave, is also training officers to recognize and respond to deepfake evidence.

Together, these efforts form the policy backbone for the coming years.

Pavel Goldman-Kalaydin,
Head of AI/ML at Sumsub

"AI is transforming identity verification from both sides of the battlefield. On one hand, it's empowering fraudsters to create deepfakes, synthetic IDs, and even autonomous fraud agents that behave like humans. On the other, it's giving defenders unprecedented visibility — allowing us to model user behavior, detect anomalies in milliseconds, and build self-learning systems that adapt to new threats. The next frontier is verification of AI agents themselves — confirming not just who you are, but who acts on your behalf."

Telemetry tampering becomes the new evasion

As verification systems grow more sophisticated, fraudsters are shifting their attention from what identity data shows to how it's collected and transmitted. Attackers now focus on the telemetry layer, including the SDKs, APIs, and device signals that underpin digital verification. This marks a significant shift in the way fraud operates, from content manipulation to context manipulation.

The rise of device and signal spoofing

In 2025, telemetry tampering surged across industries, accounting for a growing share of blocked verification attempts. The most common masking methods include:

Developer tools (44%)	Used to simulate device behavior, modify network requests, or test verification SDKs in controlled conditions that mimic legitimate environments.
Incognito mode (22%)	Increasingly weaponized to hide browsing fingerprints and session continuity during multi-account creation.
Privacy or hardened browser settings (12%)	Interfering with device fingerprinting or preventing telemetry capture.

Virtual machines (10%)	Enabling fraudsters to scale automation and appear as “fresh” devices with every run.
Remote control software (5%)	Allowing social engineers or fraud-ring operators to complete onboarding flows on behalf of victims.
Other methods (7%)	Including bots, sensor data spoofing, proxy rotation, and device clock manipulation.

Why it matters

Telemetry tampering represents the next frontier of evasion. It allows attackers to interfere not just with visual data, but also with the integrity of behavioral and environmental signals — the very elements that modern anti-fraud systems depend on. A fraudster who controls how a verification SDK perceives device model, geolocation, or camera input can bypass multiple safeguards simultaneously, even when the visual data appears legitimate.

Chart 6.
Top-5 tools and methods used for telemetry masking, 2025

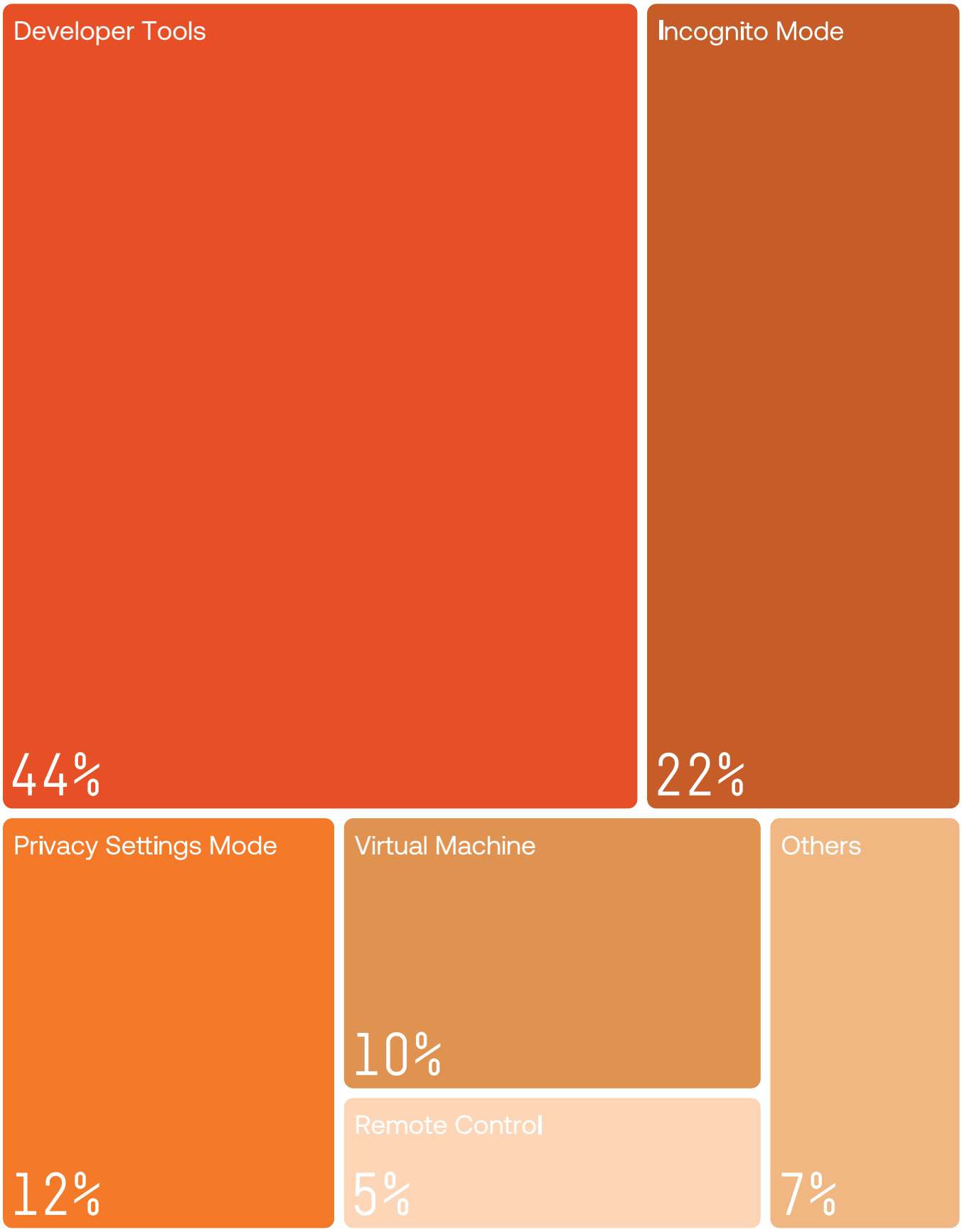
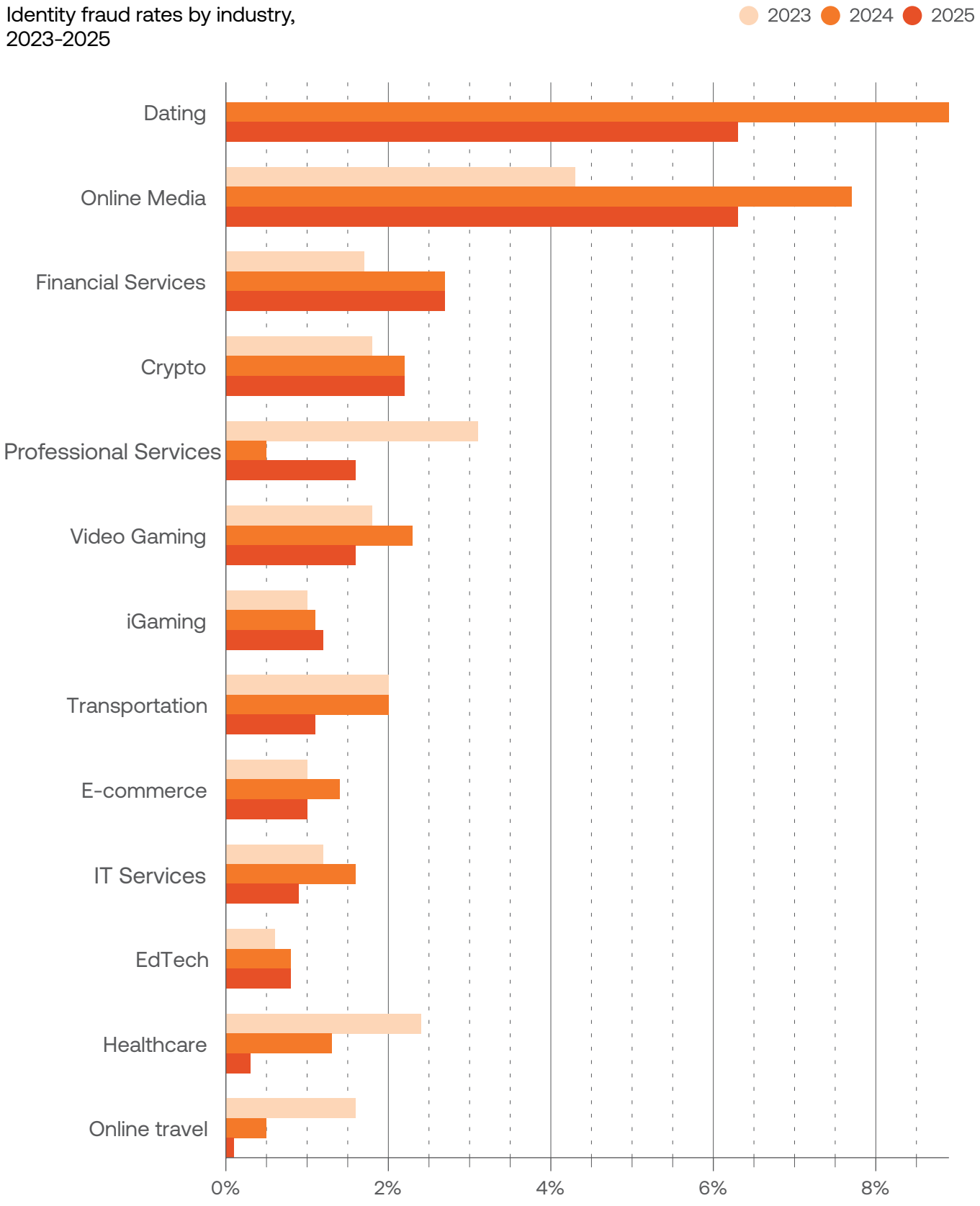


Chart 7.
Identity fraud rates by industry,
2023-2025



Identity fraud by industry

Fraud pressure in 2025 appears very different across industries. While some verticals show sharp declines after years of elevated risk, others remain hotspots where fraudsters continue to invest in new schemes.

Online Media – still at the top, but cooling slightly

Fraud in the online media sector remained high at 6.3%, though slightly down year-over-year. The majority of attacks stem from fake account creation, social-engineering-driven impersonations, and monetization scams targeting ad revenue systems. In March 2025, a boiler-room scam operating out of Tbilisi, Georgia, used deepfake videos and fake promotions on social media to trick over 6,000 victims into losing £27m. This illustrates how online media manipulation contributes to large-scale fraud.

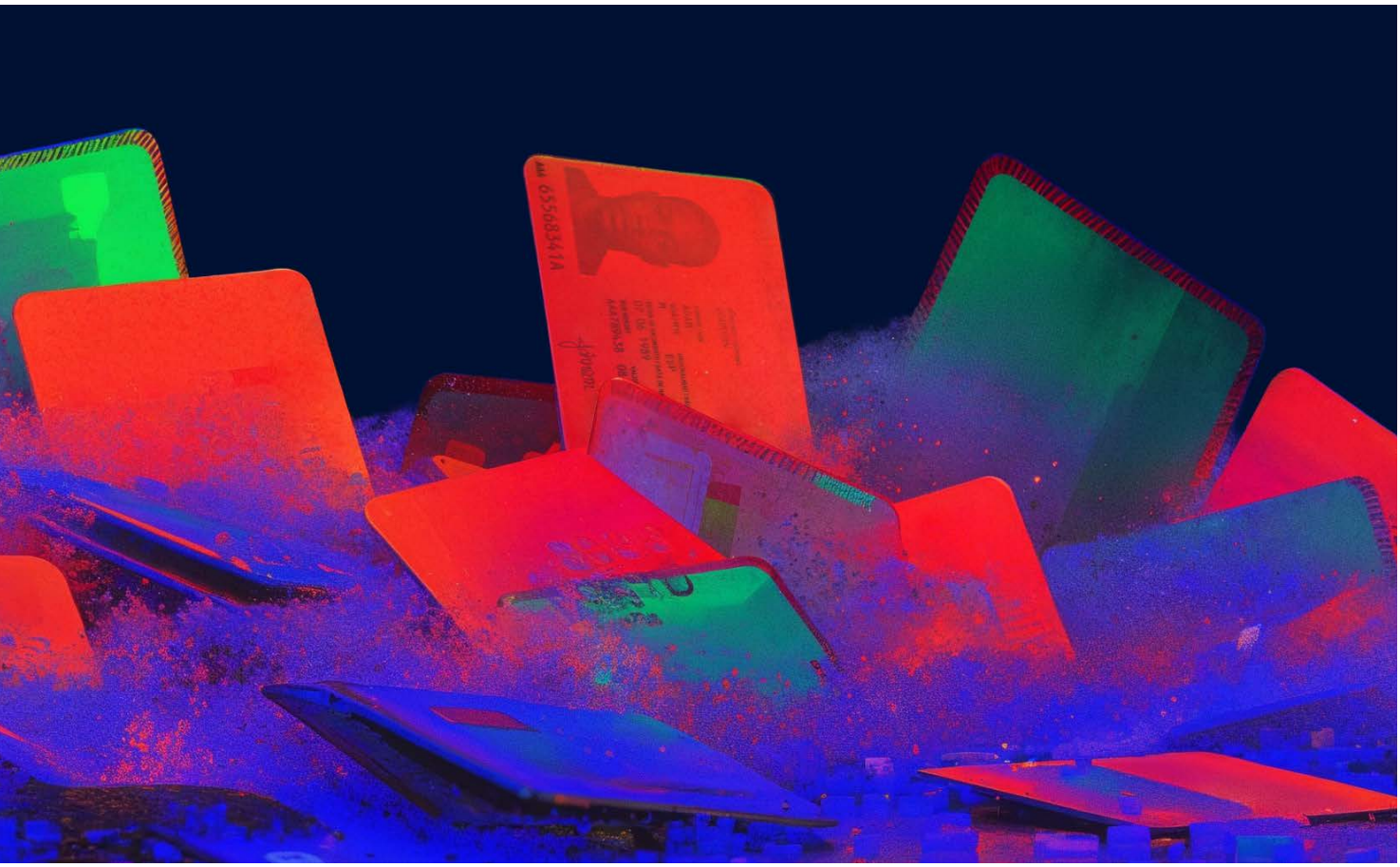
Dating - where AI meets emotional manipulation

Also at 6.3%, the dating industry continues to face one of the most emotionally manipulative forms of fraud: romance scams. Attackers now rely on AI-generated personas and deepfake selfies to build trust quickly, then move victims toward off-platform communication or financial requests. Beyond financial loss, dating fraud drives reputational and psychological harm—highlighting the growing overlap between social engineering, emotional manipulation, and synthetic identity use.

Financial Services – synthetic identities mature

Financial services fraud reached 2.7%, a 2% decrease YoY, but the sector remains one of the most strategically targeted. The real story is not in percentages, but in the sophistication of fraud: synthetic identities that slowly build credibility before executing large cash-outs, and chargeback abuse that exploits consumer protections.

In April 2025, the Boston Fed warned that generative AI is accelerating synthetic identity fraud, citing that it blends real and fake data to create highly convincing applicants.



Sam Boboev,
Founder at
Fintech Wrap Up

"I think we'll see a major shift toward AI-native fraud prevention. Instead of just using AI as a layer, more providers will start designing systems where AI runs detection, decisioning, and learning loops autonomously. This will be crucial as fraudsters also leverage generative AI for synthetic identities and deepfake-based attacks.

The most surprising trend is the remarkable speed at which generative AI has been adopted by fraudsters. Deepfakes and AI-generated documents are now being used at scale, making traditional document checks far less reliable. It's accelerating the industry's shift toward behavioral biometrics and continuous verification."

Dina Mainville,
Independent Director
at Kraken;
Founder & President
at Collisionless

"By 2026, identity verification will shift from static, document-based checks to continuous, intelligence-driven identity assurance. The biggest trend will be the fusion of behavioral biometrics, device intelligence, and on-chain reputation data, where verification becomes dynamic and adaptive rather than transactional. As AI-generated identities blur the line between human and synthetic actors, trust frameworks will evolve toward real-time, context-aware identity scoring that continuously validates 'who you are' based on how you behave, not just what you present.

The most surprising shift over the past year has been how quickly fraud has become collaborative. We're no longer seeing lone actors exploiting weak controls. We're seeing highly organized, AI-enabled fraud ecosystems where identities, playbooks, and infrastructure are traded like assets. Deepfake-as-a-service, voice spoofing kits, and cross-platform social engineering rings have industrialized deception. The real story isn't just about smarter fraudsters, it's about a rapidly collapsing asymmetry between legitimate and illicit innovation. Compliance and intelligence teams are being forced to adopt the same level of coordination and automation as the criminals themselves."

Crypto – a steady cash-out channel

Crypto fraud held at 2.2% (+2% YoY). Attackers use crypto accounts to launder funds from scams, exploiting platforms with weaker KYC. While raw volumes are lower than in 2021–22, crypto remains deeply embedded as a cash-out and laundering rail. In June, Europol reported on a cryptocurrency investment fraud ring in Spain that laundered €460 million. The ring utilized global associates to establish multiple accounts on various exchanges, enabling them to receive, store, and transfer illicit funds.

Scammers are employing sophisticated phishing and vishing tactics to deceive their victims. A police force in North Wales issued warnings to cryptocurrency holders after a victim lost £2.1 million in Bitcoin to a scammer impersonating a police officer. Scammers posed as the presidential inaugural committee and collected donations for the Trump-Vance inauguration through false email addresses, collecting over 250,300 in USDT stablecoin.

The FCA reported almost 5,000 fake FCA scams in the first half of 2025, with one of the most common methods involving crypto wallets. The scam claimed a wallet was opened illegally in the individual's name.

Sean O’Malley,
Research Director at
Chartis Research

“We see the use of IDV expanding, especially with respect to digital identity. This is based partially on eIDAS 2.0 regulations in the European Union, as well as the use of certain technologies (e.g., blockchain) to support a decentralized IDV and management process, and the expanding use of artificial intelligence and machine learning to detect identity fraud – especially fraud perpetrated using AI tools. The most significant trend is the move toward using digital identity to replace other document types that have typically been used as evidence of identity (e.g., government-issued papers). The digitization and security of identity will have a significant impact on the future development of IDV solutions.”

Professional Services – a sharp rebound

After plunging in 2024, fraud in professional services rebounded by 232% in 2025 to 1.6%. This category covers B2B sectors such as consulting, legal, accounting, marketing, and freelance platforms — industries that rely heavily on digital credentials, remote verification, and document exchange. Fraudsters exploit firms that rely on document uploads for onboarding or contracts, inserting fake credentials, invoices, or legal documents to siphon funds. Authorities across Europe flagged invoice and credential forgery scams targeting consultancies and law firms in 2025, often using AI-generated templates to bypass checks.

Earlier this year, Ford sued multiple law firms after an investigation revealed inauthentic documents and fictitious bills from attorneys and law firms, totaling an estimated US$100 million.

Video Gaming – fraud normalizes, but persists

Fraud in video gaming fell to 1.6% (–27% YoY). Yet the industry remains exposed to account takeover, bot-driven item farming, and payment abuse. AI-powered bots now simulate human behavior, making it increasingly difficult to distinguish between real players and fraudulent rings.

From an entire video game being stolen to luring people to scam centers via online video games, this industry is ripe for sophisticated scam artists to prey on, including vulnerable teens seeking jobs abroad.

E-commerce – improvements were visible

E-commerce fraud dropped to 1.0% (–28% YoY). Stronger device fingerprinting and payment validation appear to be paying off. Still, chargeback abuse and refund fraud remain core problems.

Thailand's Electronic Transactions Development Agency (ETDA) reported that 27,332 complaints were filed in the first eight months of 2025, including scams involving fake products and online loan fraud. In September, OpenAI announced its moves towards agentic commerce with instant checkout via ChatGPT. The upside: faster shopping for its 700 million users, from product discovery to payment. The catch: as payment providers power this flow, security and consumer protection have to be non-negotiable. Fraudsters will target any weak link. Malicious agents could impersonate legitimate ones or inject prompts that alter model behavior, making robust audit trails and fraud-prevention controls even more essential.

iGaming – deepfakes redefine risk

Fraud in the iGaming industry rose modestly but transformed fundamentally (1.2%; +8% YoY). Deepfake-linked fraud types represent over half of all cases, reflecting the rise of AI-generated player identities used to bypass age or bonus restrictions. Synthetics grew sharply (+329%), while old-school photo fraud collapsed. Template-based and repeat-actor frauds increased, showing the influence of fraud-as-a-service kits built to automate casino or sportsbook abuse.

Outlook 2026: Expect deepfake liveness attacks to become routine, forcing operators to adopt multi-modal verification and cross-session behavioral tracking.

Customer trust

In our Fraud Exposure Survey 2025, we asked respondents to estimate the level of trust in various industries, ranging from 1 to 100, with 100 indicating complete trust, to gauge which sectors have the highest and lowest levels of consumer trust.

Despite continued exposure to fraud, the banking and financial services sector retains the highest level of customer trust, **scoring 70 points out of 100** in Sumsub's Fraud Exposure Survey 2025. Consumers continue to view banks and financial institutions as the most capable of safeguarding personal information and preventing fraud, reflecting the sector's long-standing commitment to security and compliance.

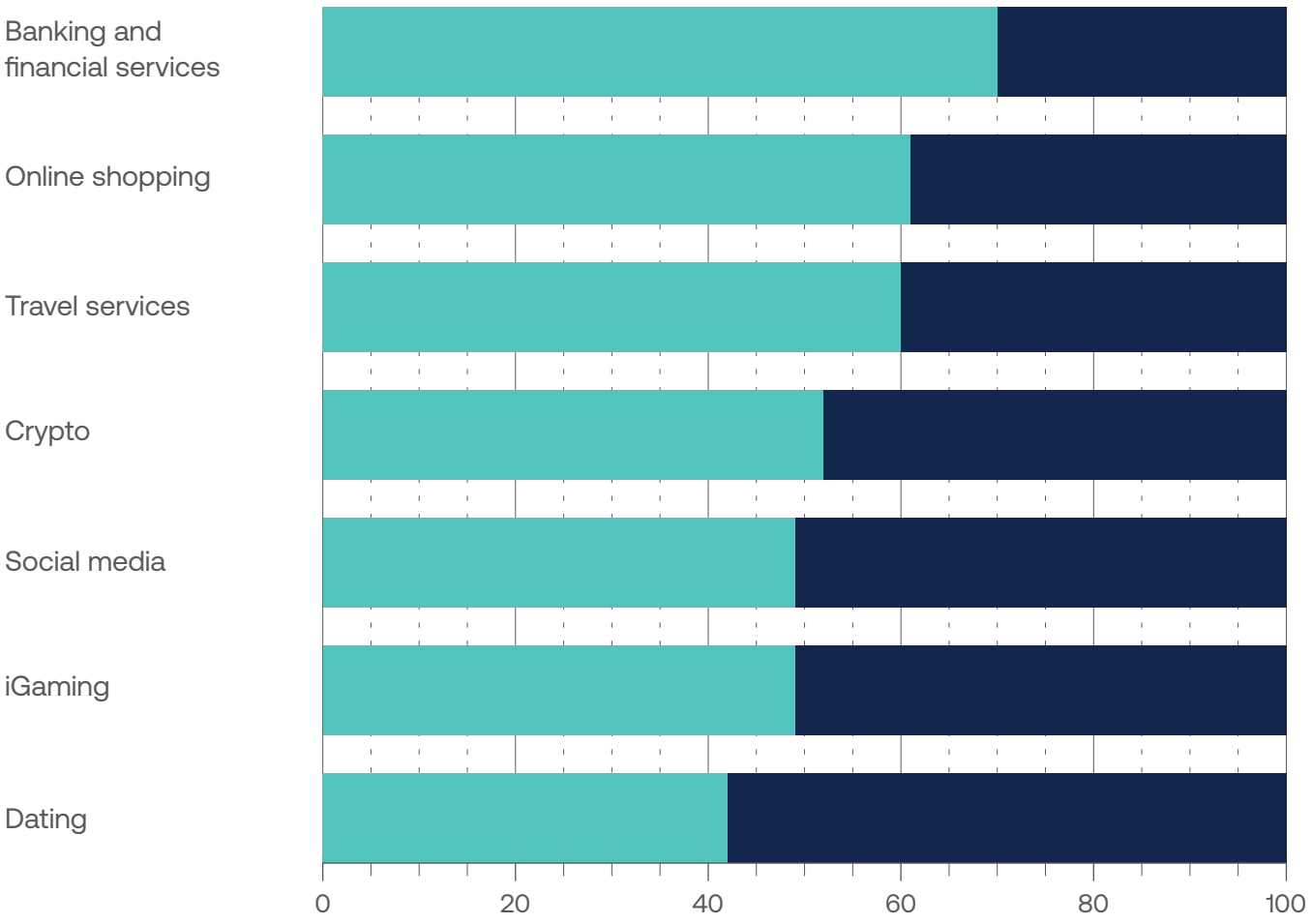
To preserve and strengthen this trust, providers will need to keep advancing detection methods and adapt to emerging AI-driven threats.

In contrast, trust in online shopping (61 points) and travel services (60 points) is moderate. These sectors benefit from familiarity and convenience, but users remain cautious given the persistent risks of payment fraud, refund abuse, and account takeovers. For merchants and travel providers, improving customer trust will require linking strong identity verification with transparent, user-friendly fraud prevention.

Lower down the spectrum, crypto (52 points), social media (49 points), and iGaming (49 points) all cluster around the "trust deficit" zone. Consumers remain skeptical of these industries' ability to protect them, especially as scams, account compromises, and bonus abuse continue to make headlines.

At the bottom, dating platforms score just 42 points, underscoring their vulnerability to scams and impersonation. With romance fraud and deepfake-enabled social engineering on the rise, this sector faces an urgent need to address user concerns through stronger verification and safety mechanisms.

Chart 8.
Identity trust in various industries to protect personal information and prevent fraud



Sumsub's Fraud Exposure Survey 2025: Consumers

Chart 9.
Average YoY fraud rate growth
by region, 2025

Regional breakdowns

Our data reveal an uneven rise in fraud worldwide, with some regions experiencing higher year-on-year growth, notably the Middle East, which saw the highest growth of 19.8%, while others have declined since 2024.

The second edition of our Global Fraud Index reinforces this picture. With fraud activity declining, Europe captured 11 out of the 15 countries with the most protection from fraud. In contrast, rising fraud rates in APAC and Africa pushed many countries from those regions towards the least protected end of the index.

This index evaluates the susceptibility of 112 countries to fraud, with a focus on government intervention, resource accessibility, and economic health. By examining these influential factors, the Global Fraud Index aims to enhance transparency for regulators, businesses, and individuals by identifying where fraud risks exist and supporting digital inclusion globally.

Source: Sumsub 2025 Global Fraud Index

Top 15 countries most protected against fraud

1	Luxembourg
2	Denmark
3	Finland
4	Norway
5	Netherlands
6	Switzerland
7	New Zealand
8	Sweden
9	Austria
10	Singapore
11	Slovenia
12	Israel
13	Malta
14	Lithuania
15	Australia

Source: Sumsub 2025 Global Fraud Index

Top 15 countries least protected against fraud

1	Pakistan
2	Indonesia
3	Nigeria
4	India
5	Tanzania
6	Uganda
7	Bangladesh
8	Rwanda
9	Azerbaijan
10	Sri Lanka
11	Ethiopia
12	Brazil
13	Armenia
14	Kenya
15	Colombia

Regional Insights

The following regional insights are based on countries with significant user activity on our platform. To ensure statistical reliability, we only included jurisdictions where we processed more than 15,000 verification attempts during the reporting period. Countries with lower traffic are excluded from this analysis, as their sample sizes may not accurately reflect broader fraud trends.

Africa

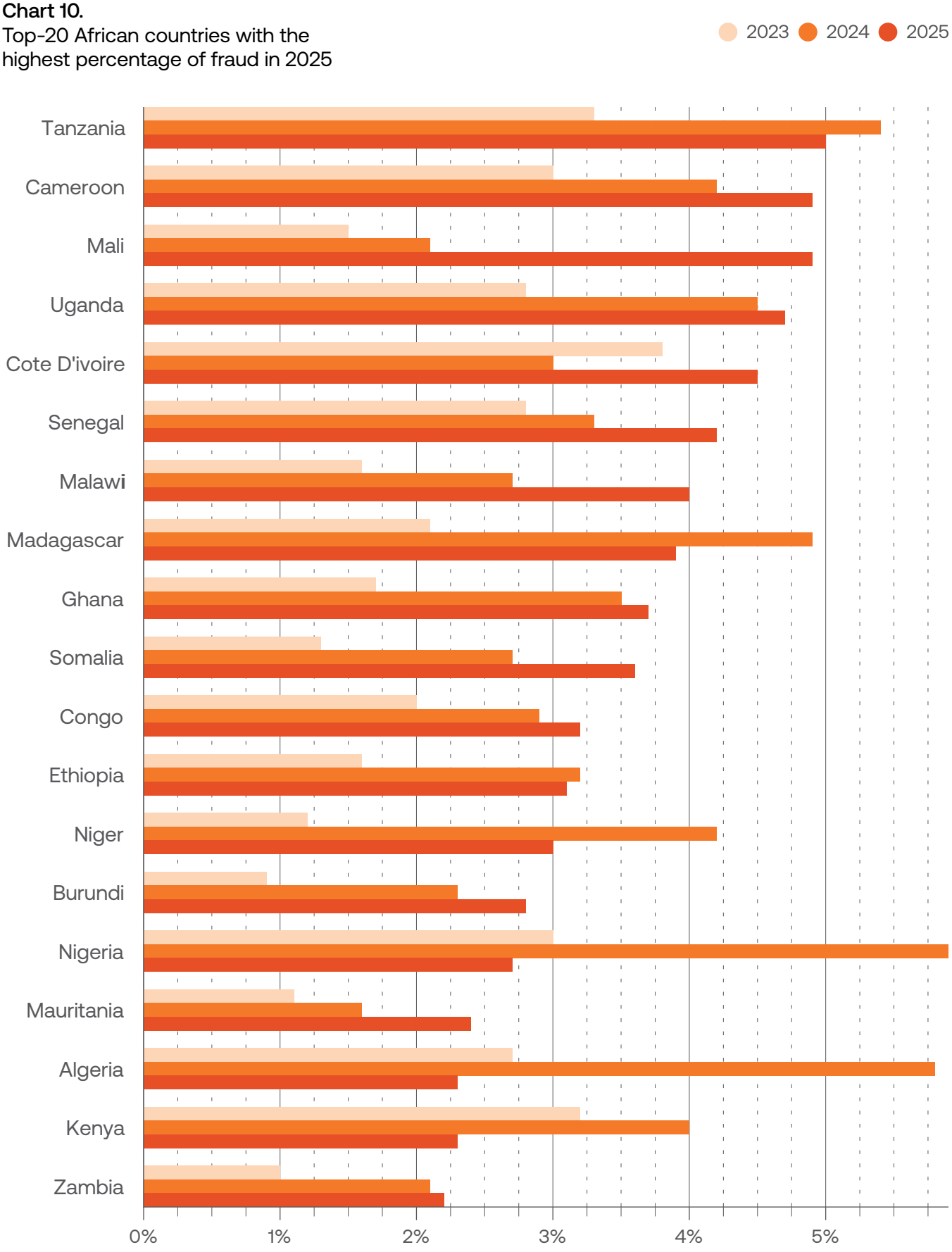
Africa's digital economy is expanding at speed, with mobile money, fintech, and e-government services driving financial inclusion. Yet this rapid transformation has also made the region one of the most dynamic battlegrounds for identity fraud.

In 2025, African markets illustrate the Sophistication Shift: with fewer low-effort, easier-to-spot scams and a pivot to more complex scams, such as deepfakes, synthetic identities, and network-driven fraud. The result is a patchwork of rising and falling fraud rates across the continent, closely tied to local regulation, digital adoption, and organized fraud hubs.

Selfie fraud and deepfakes: the new frontline

The continent's most visible change lies in selfie-based fraud, which surged across markets. Fraud categories involving mismatched or manipulated facial images grew dramatically in 2025, supported by a parallel spike in deepfake activity.

Chart 10.
Top-20 African countries with the highest percentage of fraud in 2025



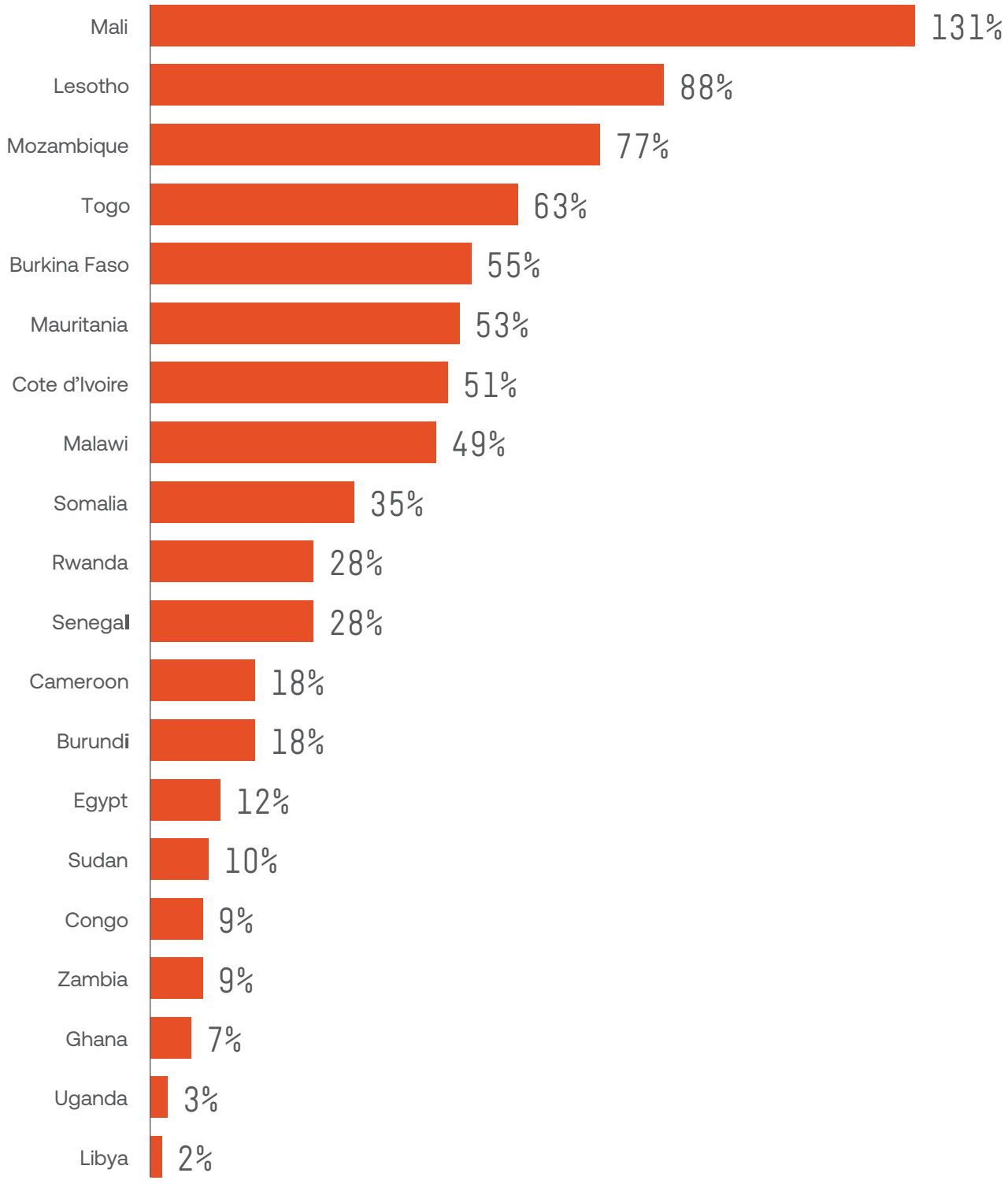
% of fraud in all analyzed verifications by country

The data shows just how sharply this technology is being weaponized:

1. In the **Democratic Republic of the Congo**, deepfake-related attempts rose by +367% YoY.
2. **Malawi** saw a +325% increase.
3. **Tanzania recorded** +317% growth, with deepfakes now part of 0.71% of all attempts.
4. Some countries, like **Kenya**, are even more exposed: while fraud rates fell overall, deepfakes already account for nearly 10% of fraud attempts.

The implication is clear: deepfakes are no longer rare experiments reserved for the tech-savvy. They are integrated into everyday fraud playbooks, often surfacing inside mismatch categories rather than being cleanly labeled, because their realism increasingly confuses detection systems.

Chart 11.
Top-20 African countries with the largest YoY fraud growth (2025 over 2024)



Country-level dynamics

Fraud rates in 2025 vary widely across Africa.

Rising hotspots

1 **Mali (+131% YoY, 4.9% fraud rate):**
A sharp surge tied to rapid mobile-money growth outpacing fraud controls. Cross-border West African fraud networks exploit weaker oversight in Mali to test synthetic IDs and deepfakes.

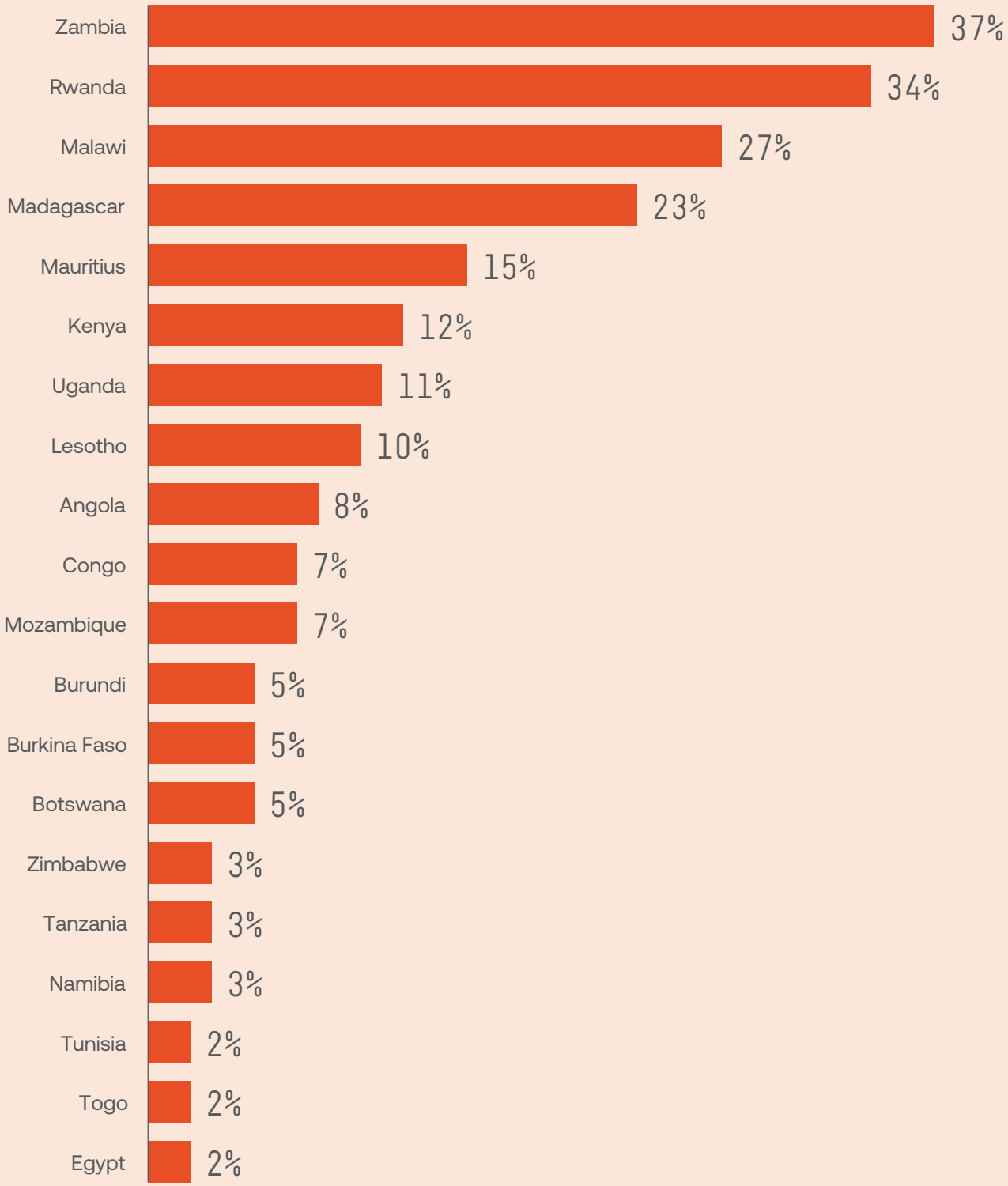
2 **Côte d'Ivoire (+51% YoY, 4.5%) and Senegal (+28% YoY, 4.2%):**
Longstanding scam hubs, including romance fraud, crypto scams, and mule networks, are increasingly powered by AI-generated content, explaining their steep rise.

3 **Cameroon (+18% YoY, 4.9%) and Malawi (+49% YoY, 4.0%):**
Both saw expanding mobile-finance ecosystems with patchy KYC enforcement, creating openings for onboarding fraud.

4 **Uganda (+3% YoY, 4.7%):**
Fraud network activity has soared 9.2% as the region has emerged as a growing hotspot for romance scams, blackmail, and forgery.

5 **Zambia (+9% YoY, 2.2%):**
Recorded the highest ratio of approved applicants linked to fraud networks (37%), signaling a high concentration of potential future fraudsters.

Chart 12.
Top-20 jurisdictions with the highest ratio of approved applicants involved in fraud networks



76.5% of African respondents in Sumsub's Fraud Exposure Survey 2025 are aware of "money muling," but most underestimate its seriousness.

1 in 4 have been personally targeted, confirming that mule recruitment is an active regional problem.

Question:
Have you heard of "money muling" - letting someone move stolen money through your bank account?

Sumsub's Fraud Exposure Survey 2025, Africa: Consumers

This gap between awareness and understanding reveals a critical weakness: people recognize the term but fail to identify mule schemes when approached, often mistaking them for legitimate job or payment opportunities.

Declining markets

1 **Nigeria (–54% YoY, 2.7%):**
The most dramatic fall, reflecting the enforcement of NIN–SIM linkage and sustained cybercrime crackdowns. Fraud rates halved as attackers faced higher costs. While fraud rates have fallen, the AML rate of fraud in Nigeria is 4%, which is 2-8 times higher than that of its African counterparts, placing Nigeria as Africa's worst-performer in the Global Fraud Index 2025.

2 **South Africa (–31% YoY, 1.4%):**
A standout example of regulatory maturity. Strengthened AML/CFT frameworks, enhanced verification across major banks, and the rollout of biometric-based eKYC standards have all contributed to a sharp drop in overall fraud. However, deepfake incidents increased by more than 269% YoY, showing that while traditional document and selfie fraud are effectively mitigated, AI-enabled impersonation is quickly emerging as the next frontier in South Africa's digital identity landscape.

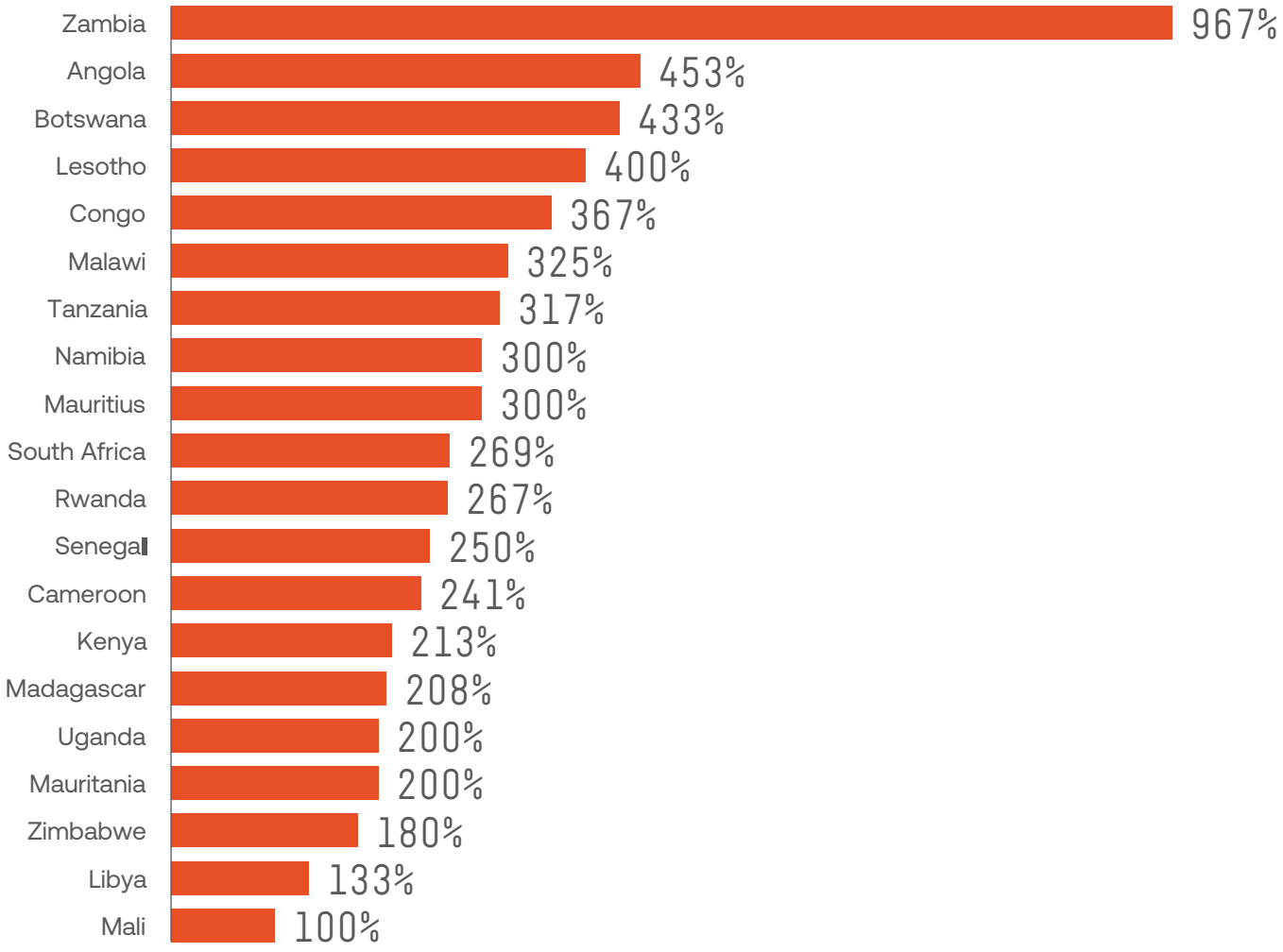
3 **Algeria (–60% YoY, 2.3%) and Kenya (–42% YoY, 2.3%):**
Both benefited from stronger KYC regimes in banking and telecom. Yet, Kenya's deepfake share indicates that while crude fraud is declining, sophisticated fraud is rising rapidly.

4 **Madagascar (–21% YoY, 3.9%) and Niger (–29% YoY, 3.0%):**
The declines likely reflect fraudsters shifting their focus to larger or more lucrative markets rather than systemic improvements.

Why deepfakes matter here more than elsewhere

Deepfake penetration in Africa reveals both opportunity and vulnerability. In high-adoption markets like Kenya and Nigeria, the fraud rate has decreased, but deepfakes already account for a significant share of what remains. This suggests that AI-enhanced fraudsters are targeting the strongest defenses, betting that deepfakes can succeed where crude forgeries no longer work.

Chart 13.
Top-20 African countries with the largest YoY deepfakes growth (2025 over 2024)



Meanwhile, in emerging fintech markets such as Malawi, Tanzania, and the Democratic Republic of the Congo, the overall share of deepfakes remains small, but growth rates exceeding 300% indicate how rapidly they are being adopted by fraud networks.

Question:
Which of these best describes your experience with deepfake videos or audio?

Sumsub's Fraud Exposure Survey 2025
All responses represent the personal experiences of all survey participants.

Deepfake exposure over the region is nearly universal (91%), and 1 in 5 people have been directly targeted.

The inability of **24% of respondents to distinguish deepfakes** indicates major risks for **fraud, misinformation, and impersonation attacks.**

91%

What to expect next

Africa's fraud ecosystem is split. In some countries, stronger policies and SIM–ID linkages are helping to reduce fraud rates. In others, fintech growth without matching controls is fueling double- and triple-digit increases. Overlaying all of this is the rise of deepfakes, which have shifted from novelty to mainstream in just one year.

Looking ahead, two paths are clear:

1. Countries that enforce structural protections (national ID integration, cross-border data-sharing, AI detection investments) will see fraud pressure stabilize.

2. Those that lag will remain testing grounds for synthetic IDs, deepfakes, and fraud networks seeking the path of least resistance.

The Sophistication Shift is already underway in Africa. Fraudsters are leaving behind the blurry photo era and moving into one where AI and deepfakes are the default weapon.

Purity Gakuru,
Compliance Specialist
(KYC), Wallet

“**2025: Fraud Got Smarter, Faster, and Borderless**
Over the past year, identity fraud has shifted into a post-KYC challenge, with most attacks now targeting verified accounts after onboarding. The rise of AI-powered fraud-as-a-service has unleashed pro-level deepfakes, synthetic identities, and forged documents, which have changed the risk landscape. Emerging markets such as Africa and Southeast Asia have seen sharp increases in fraud, emphasizing the need for region-specific verification intelligence. At the same time, organisations are merging fraud, AML, and cybersecurity functions to counter multi-channel threats, while regulators are demanding measurable fraud-loss prevention over box-ticking compliance

.

2026: Identity Verification Levels Up
Identity verification is expected to evolve past one-time KYC into continuous, intelligence-driven assurance, monitoring behaviour and transactions to detect emerging risks throughout the customer lifecycle. As AI-powered fraud and deepfakes grow more sophisticated, providers will be pushed to adopt smarter liveness checks and synthetic ID detection. The rise of identity orchestration platforms will unify key fraud signals into a single risk framework for AML and fraud teams. With fraud rates surging in emerging markets like Africa and Southeast Asia, 2026 will mark a shift toward region-specific verification intelligence. Finally, regulators will demand measurable fraud-loss prevention as reusable, privacy-first identities move into the mainstream.”

Global challenge, local realities

Fraud is a universal reality, but its impact varies from one location to another. Using data from Sumsub's Fraud Exposure Survey 2025, we can analyze how fraud patterns evolve in different regions and gain a better understanding of the shared challenges posed by the global threat of fraud.

Companies

53%

African businesses have fallen victim to fraud in 2025

Consumers

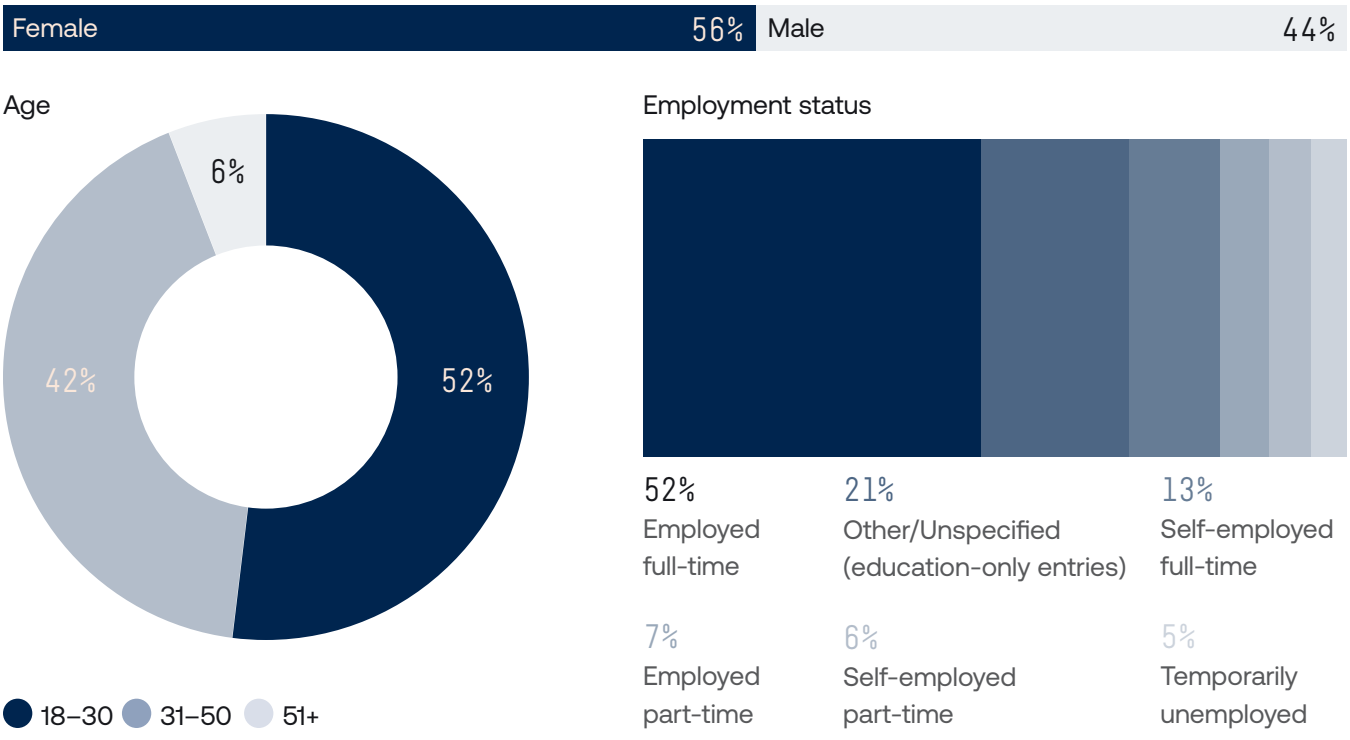
47%

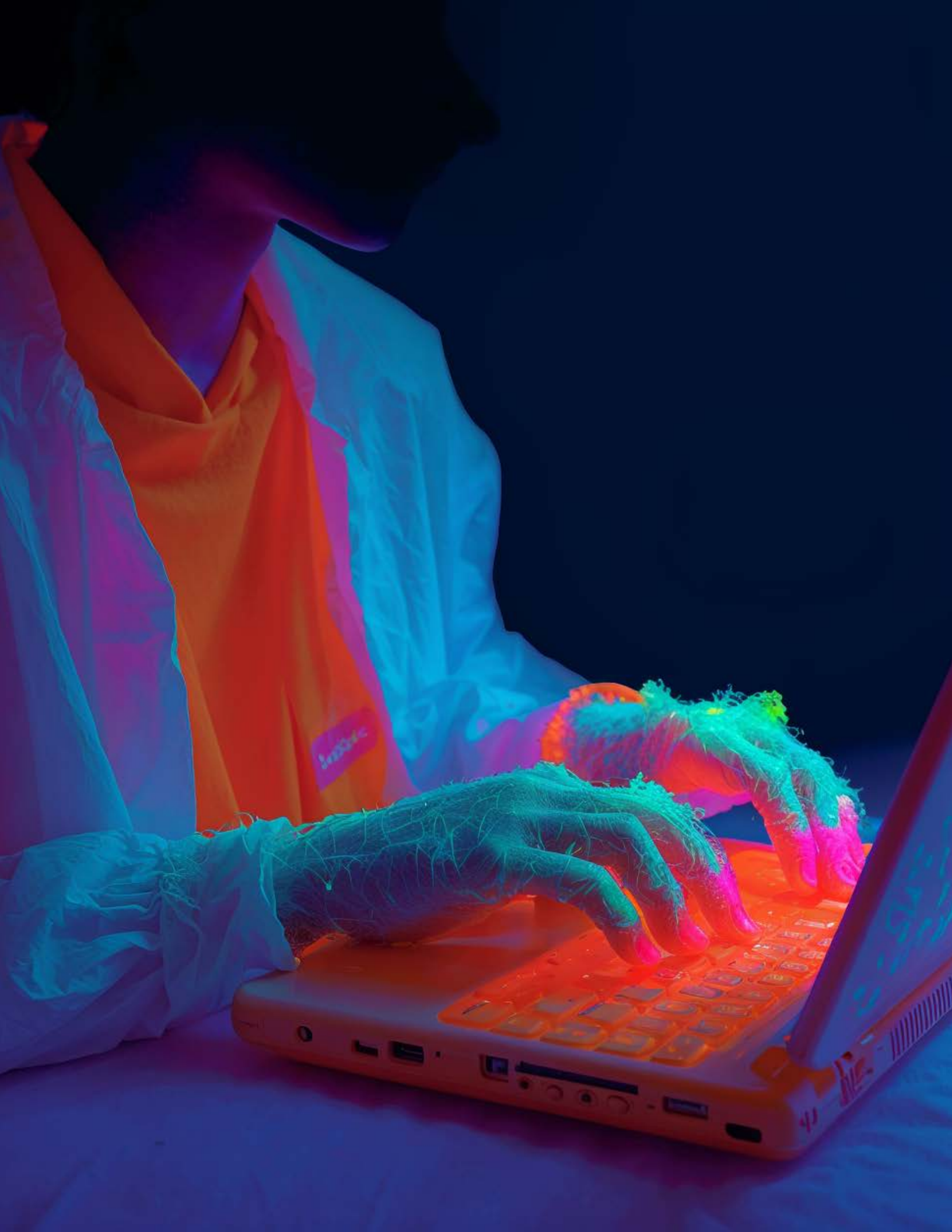
End users in Africa have fallen victim to fraud at least once in 2025

Consumer fraud findings in Africa

Take a closer look at Africa-based respondents, from their age to employment status.

Chart 14.

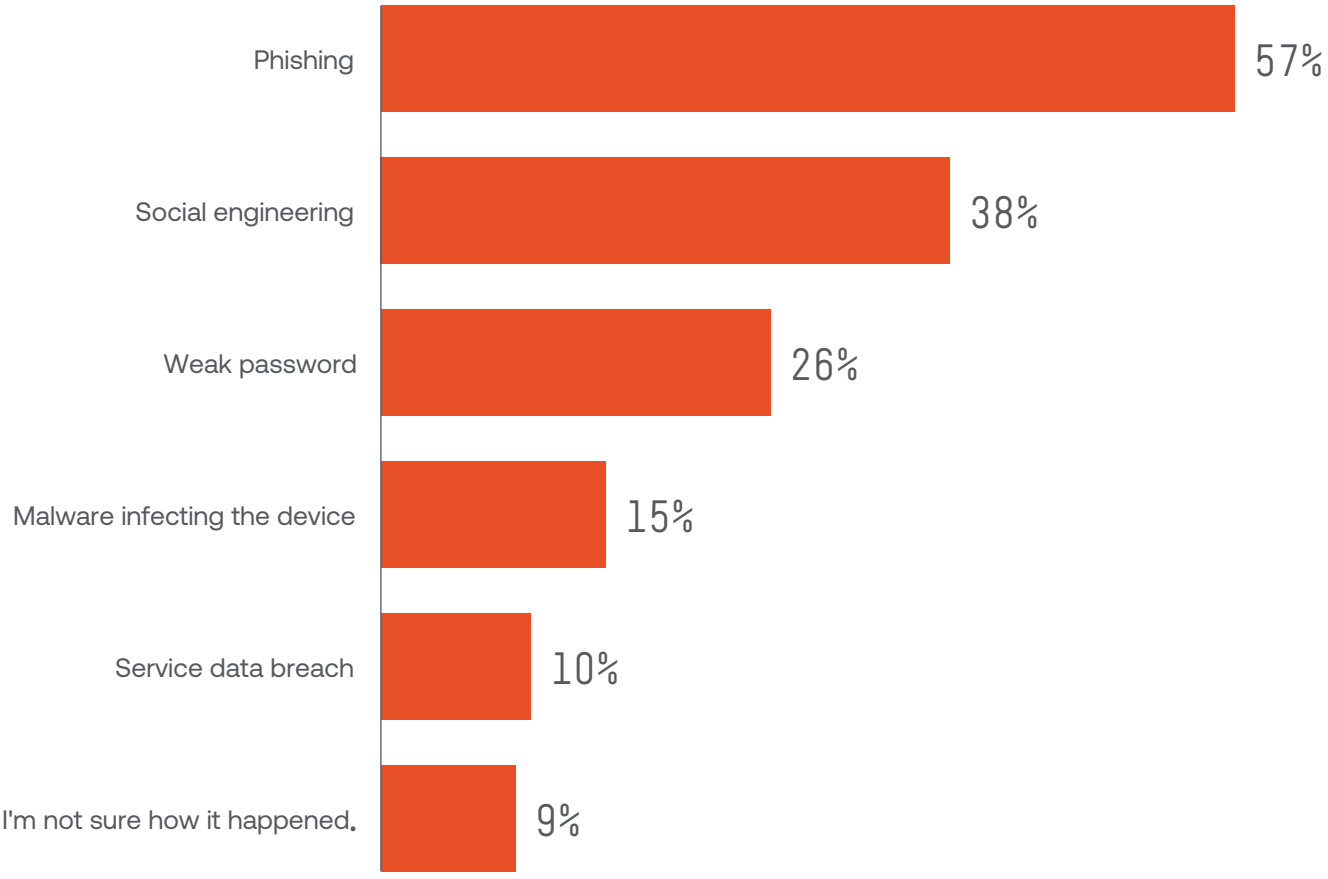




Main attack vectors

The main attack vectors reported were phishing (57%) and social engineering (38%), followed by weak passwords (26%), malware infections (15%), and service data breaches (10%), highlighting that most fraud incidents still originate from human-targeted deception rather than technical exploitation.

Chart 15.
Question:
What do you think was the cause of the fraud incident?

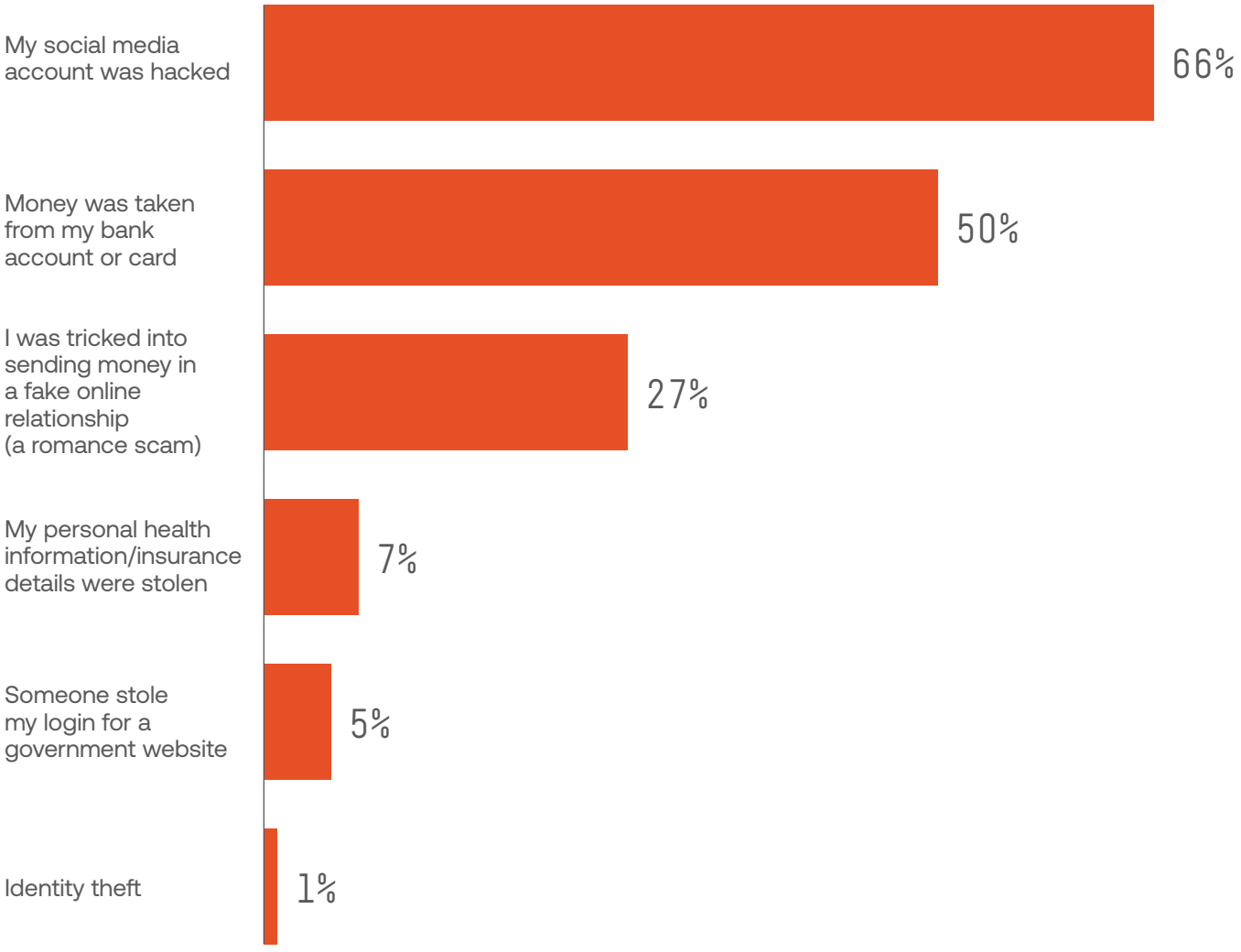


Sumsub's Fraud Exposure Survey 2025, Africa: Consumers

Main fraud outcome

The main fraud outcomes included social media account hacks (66%) and money theft (50%) as the most common consequences, while smaller but notable shares reported having personal health or insurance information stolen (7%), being tricked into sending money (27%), or having their government service accounts compromised (5%), indicating that both financial and identity-related damages are widespread.

Chart 16.
Question:
What type of identity fraud did you experience?



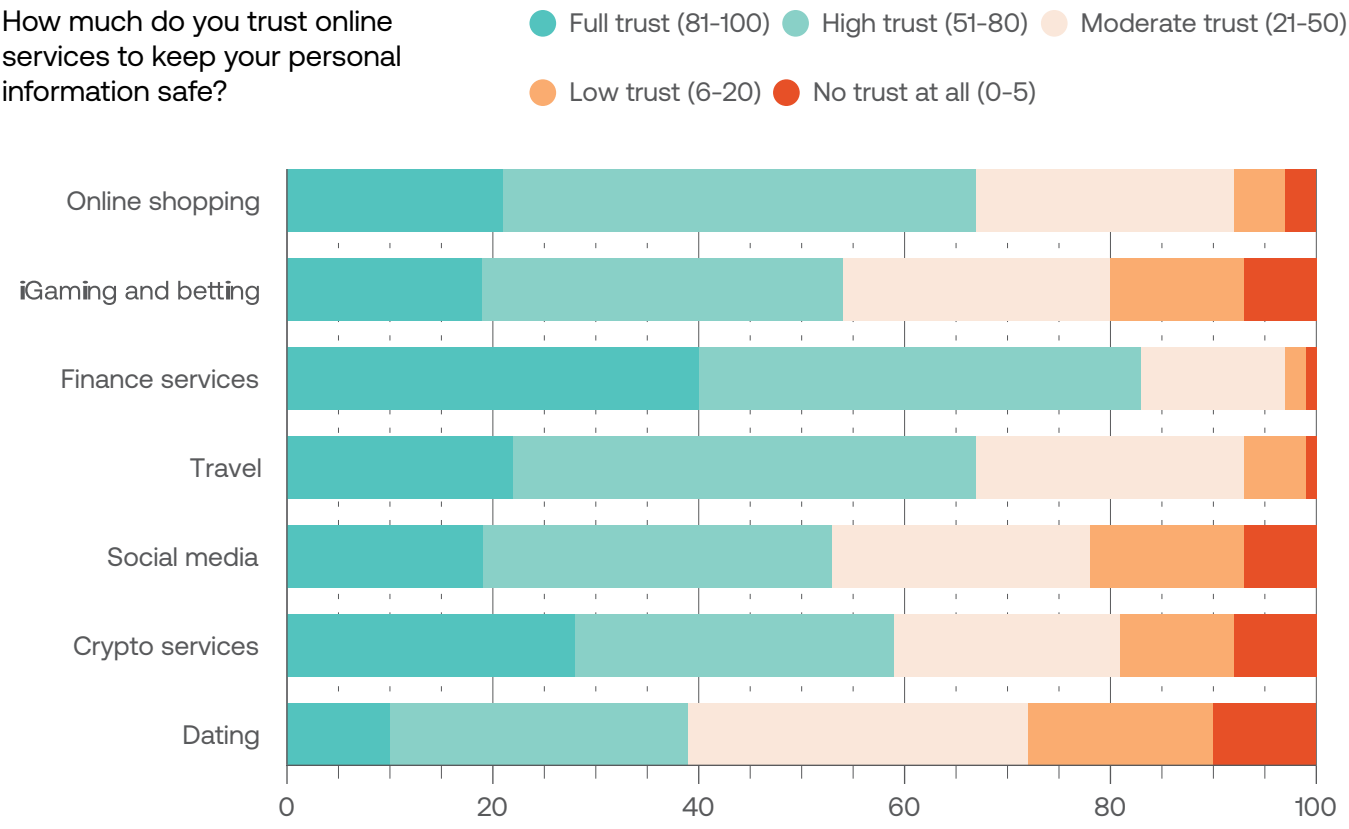
Sumsub's Fraud Exposure Survey 2025, Africa: Consumers

Digital trust in Africa

Trust in data security varies widely across industries. Finance (84%) remains the most trusted sector, followed by travel and online shopping (68% each).

At the other end of the spectrum, iGaming (55%), social media (54%), and dating platforms (40%) still struggle with user skepticism due to frequent data leaks, scams, and unclear accountability. Crypto (61%) sits in between — trusted by active users, but still viewed as risky by the broader public. The pattern is clear: the more transparent and regulated the industry, the higher the user trust.

Chart 17.
Question:
How much do you trust online services to keep your personal information safe?



Sumsub's Fraud Exposure Survey 2025, Africa: Consumers


1234 4567 1234 5678
VALID THRU 12/30
KOFI ABARA

92% of respondents would choose a service provider only if they have strong anti-fraud measures in place

92%

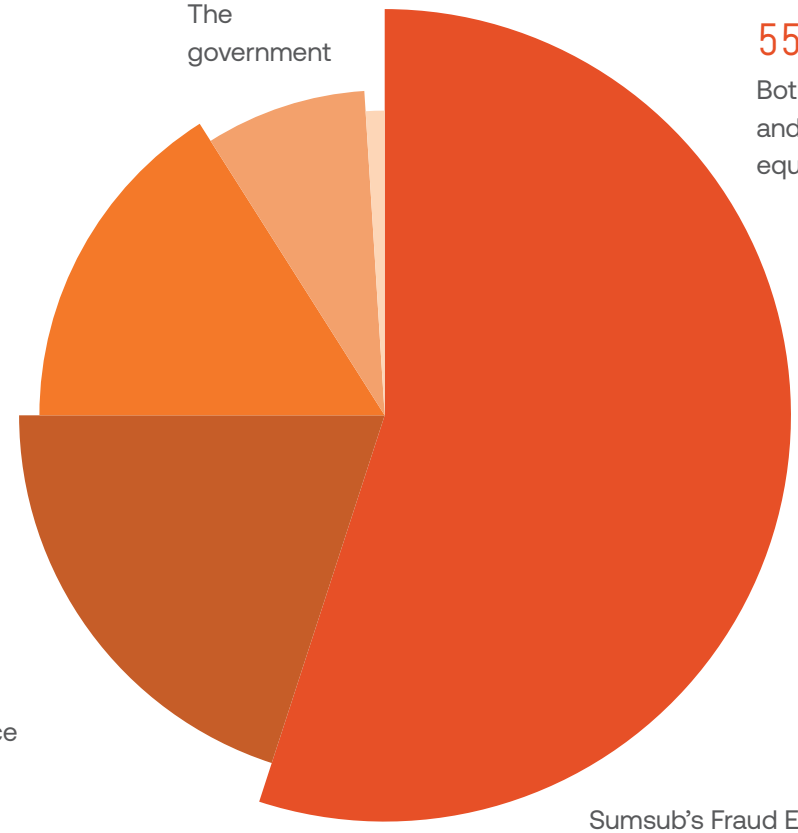
7 in 10 respondents use virtual/disposable cards, confirming widespread adoption and awareness of online payment security.

Question:
Who do you think should take the lead in keeping people safe from fraud?

Responsibility for fraud prevention

The majority (55%) support a joint responsibility model for combating and preventing fraud, while 20% trust companies to lead, and 16% emphasize the importance of individual awareness. Very few (8%) believe governments alone can ensure safety, indicating a clear understanding that effective fraud prevention requires shared effort across all stakeholders.

Chart 18.
Question:
Who do you think should take the lead in keeping people safe from fraud?



Sumsub's Fraud Exposure Survey 2025, Africa: Consumers

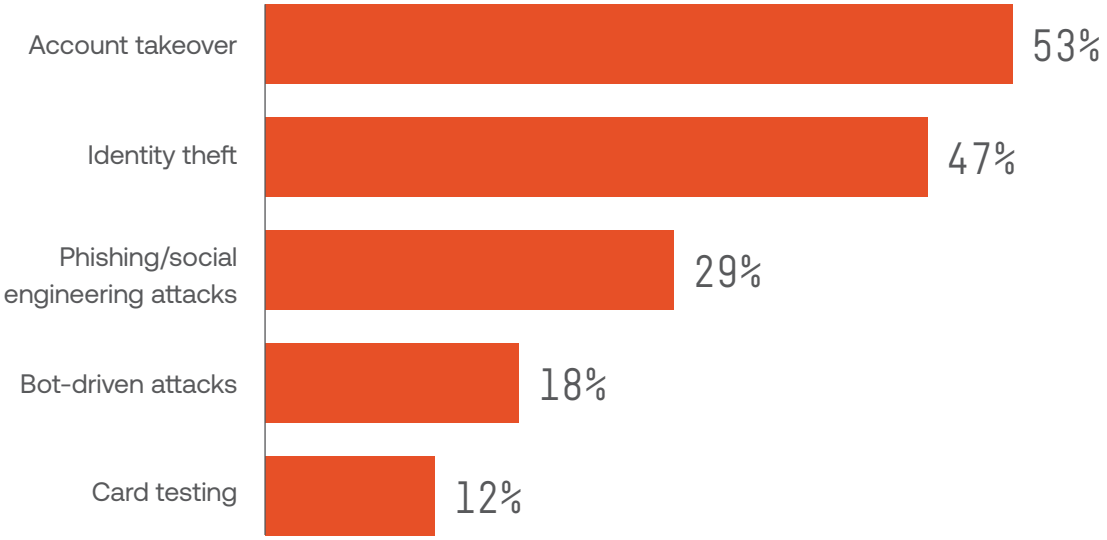
Company fraud findings in Africa

Top 3 types of fraud faced by companies in Africa

1. Account takeover (53%)
2. Identity theft (47%)
3. Phishing/social engineering attacks (29%)

At the same time, they had to manage first-party fraud from their customers, who used synthetic identity (71%) and deepfakes (18%) and conducted application and chargeback abuse (35% and 29% of cases, respectively).

Chart 19.
Question:
What kind of third-party fraud has your business faced?



Sumsub's Fraud Exposure Survey 2025, Africa: Companies

Nearly 9 in 10 respondents (87.5%) agree that fraud attempts are becoming increasingly sophisticated due to the use of AI and deepfake tools. This aligns with the global pattern, confirming that AI-enabled fraud is now considered the leading emerging threat.

Top 3 consequences companies have experienced as a result of fraud attacks:

1. Financial losses (76%)
2. Operational disruption (71%)
3. Reputational damage (47%)

How African companies manage fraud

To manage fraud, Africa shows a strong preference for in-house control (47%), with manual processes (41%) still heavily used. The region prioritizes direct oversight and local control over outsourced automation.

In Africa, most businesses report identity fraud to financial institutions (67%) and regulators (62%), while fewer than half report it to the police (48%).

Fraud is handled primarily within the financial and regulatory ecosystem, with law enforcement playing a secondary role.

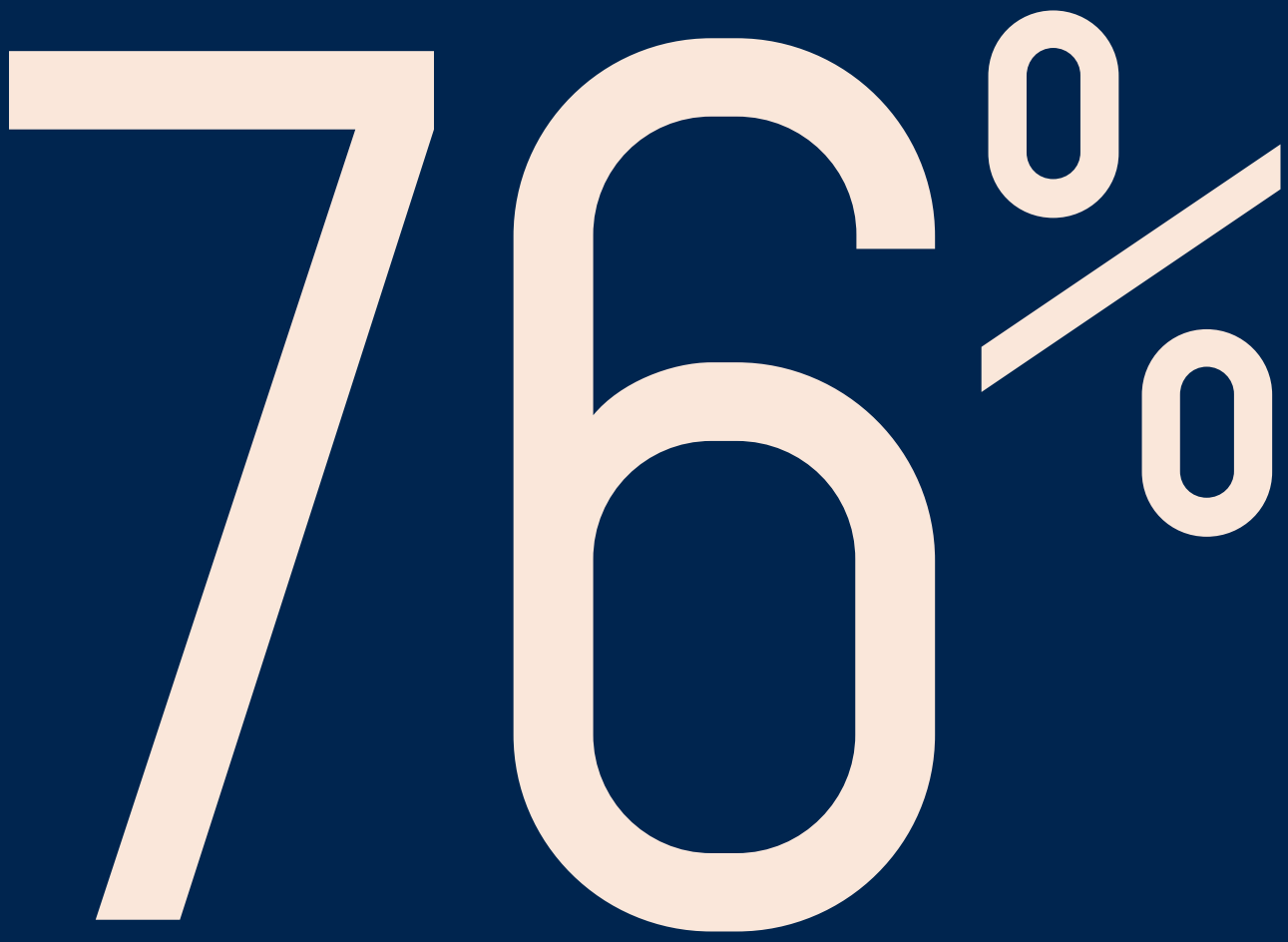
90% support stricter regulations, even if operations become more complex.

Predictions for the future

AI will be the main driver of next-generation fraud:

- → 78% expect more sophisticated attacks using AI.
- → 72% predict deepfake-based scams and 59% expect AI-generated fake documents/profiles.
- → 75% believe businesses will increase cybersecurity investment.
- → 59% foresee more organized digital crime.
- → 59% predict stricter regulations to combat fraud.
- → 50% expect more spoofing and biometric fraud.

76% report that organized fraud attempts have become more frequent. At the same time, 24% see no change, indicating that not every sector has observed escalation.



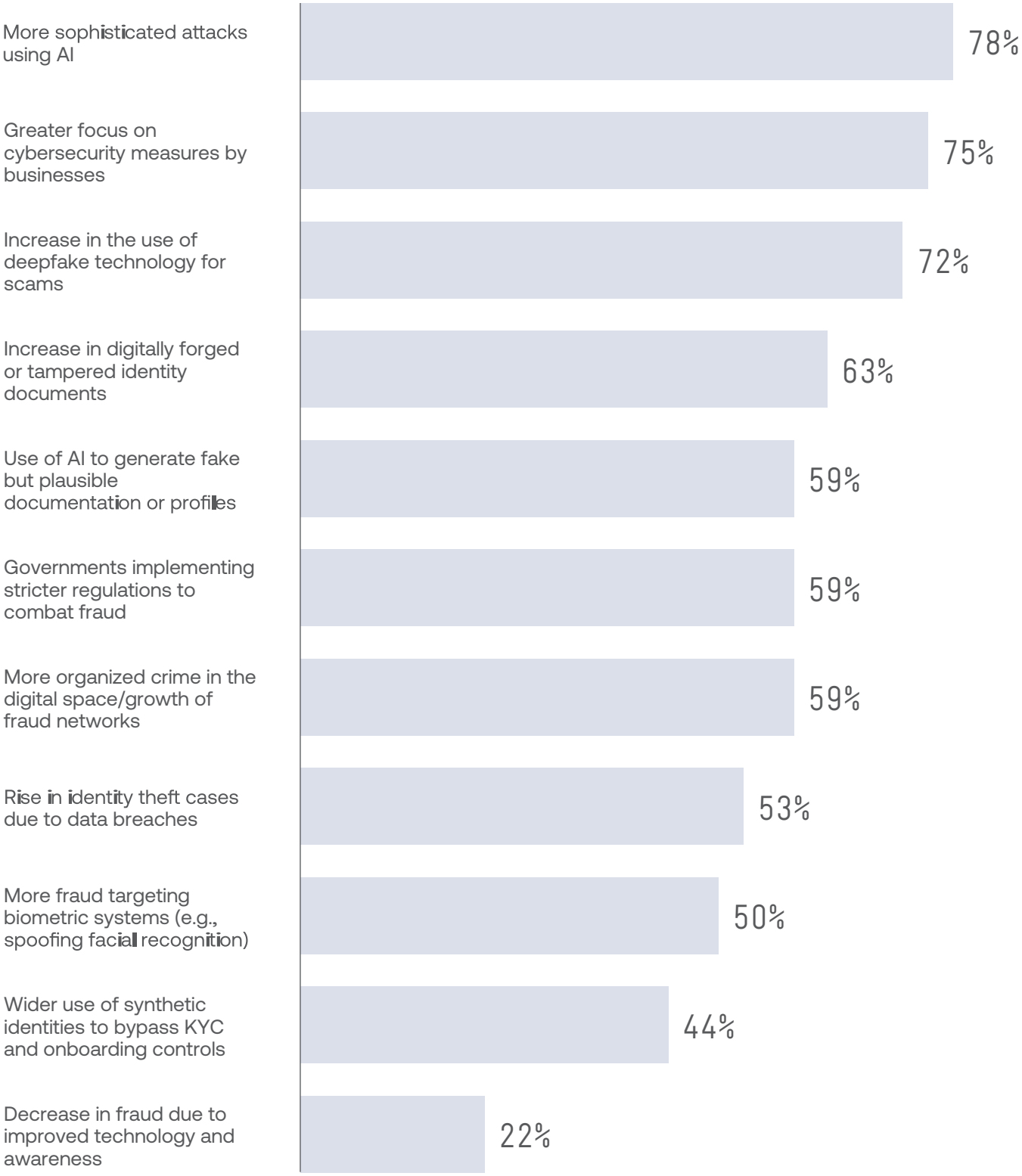


Chart 20.
Question:
What are your predictions for the future of the fraud landscape?

Sumsub's Fraud Exposure Survey 2025, Africa: Companies

Regional case studies of fraud up close

The following case studies spotlight real-world fraud incidents that occurred in Africa in 2025.

1 **Mozambique's Former Finance Minister sentenced to US$2 billion in fraud schemes**
In January 2025, Manuel Chang was sentenced by a US court to eight and a half years in prison for orchestrating a US$2 billion loan fraud disguised as a maritime development project. Chang accepted bribes and diverted around US$200 million for personal gain, triggering one of Africa's largest corruption scandals. The case involved cross-border cooperation among South Africa, the U.S., the UK, Switzerland, Spain, and Portugal, marking a significant step toward accountability in transnational corruption cases.

2 **INTERPOL operation 'Serengeti 2.0' dismantles Africa-wide cyber fraud networks**
In August 2025, INTERPOL coordinated Operation Serengeti, leading to 1,209 arrests across 18 countries and the recovery of US$97.4 million in stolen funds. Over 11,400 malicious cyber infrastructures, including phishing servers and illicit crypto-mining farms, were dismantled as part of this Africa-wide operation, which was the largest of its kind. This sweep highlights the scale and diversity of fraud schemes, as well as the capacity of African agencies to collaborate in addressing them.

3 **Human trafficking scam centers expand into Africa**
In June 2025, INTERPOL reported warnings of the global spread of scam call-centers run through human trafficking, migrating from Southeast Asia to West Africa. Victims are lured by fake job ads and then forced to conduct romance scams, crypto-investment fraud, and other online schemes. Using AI-generated photos, deepfake videos, and automated chatbots, their social engineering schemes appear more convincing.

Regulatory shifts redefining identity protection

As fraud becomes increasingly sophisticated, local governments are stepping up with more stringent compliance frameworks and enhanced enforcement. Here are some of the latest developments in Africa.

Kenya

SIM registration regulations

In 2025, Kenya issued the Registration of Telecommunications Service Subscribers Regulations (Legal Notice No. 90), tightening SIM card registration requirements. The rules mandate verification of subscriber identity against government databases, restrict proxy registrations except for minors, and limit who can register SIMs, aiming to reduce identity fraud in telecom and mobile money services.

Mauritius

Second national risk assessment

In May 2025, Mauritius published its Second National Risk Assessment on money laundering and terrorist financing, covering data through December 2024. The report identified fraud and illegal betting as internal threats and highlighted banking, trust and company services, leasing, gambling, real estate, notaries, and jewelry as high-exposure sectors. The overall money laundering risk was rated “medium-high.”

FCC guidelines for legal persons

On 14 July 2025, the Financial Crimes Commission issued new guidelines under the Financial Crimes Commission Act requiring corporate entities to implement risk assessments, internal controls, top-level oversight, monitoring, enforcement, and training to prevent fraud, corruption, and money laundering.

Nigeria	**Draft standards for automated AML solutions** On 20 May 2025, the Central Bank of Nigeria released draft baseline standards requiring banks, wallet providers, and other financial institutions to implement real-time transaction alerts. The alerts must cover high-risk activity such as large cash deposits, cross-border transfers, and crypto-related transactions. **CBN directive on settlement accounts** In January 2025, the Central Bank directed the Nigeria Inter-Bank Settlement System to debit the settlement accounts of commercial banks that receive proceeds of fraudulent transactions if they fail to detect or prevent them. The rule increases liability for banks and fintechs and strengthens expectations around monitoring and KYC.
South Africa	**Draft AML/CFT amendment bill** In December 2024, the Treasury released a draft amendment bill to align the Financial Intelligence Center Act, the Companies Act, and the Non-Profit Organizations Act. The proposals introduce enhanced due diligence for high-risk clients, stricter beneficial ownership disclosure requirements (≥25%), shorter deadlines for suspicious transaction reports, and more severe penalties for non-compliance. **SARB directive on EFT credit payments** In 2024, the South African Reserve Bank issued Directive No. 2, requiring issuers of EFT credit payments, including those using screen scraping, to register with the central bank. The measure addresses fraud risks linked to weak consent, misuse of banking credentials, bypassing clearing systems, and exposure to cyberattacks and APP fraud.

Hannes Bezuidenhout,
VP Business Development
Africa at Sumsub

"Africa is undergoing one of the fastest digital transformations in the world. Every year, millions of people gain access to financial services, digital identity systems, and e-government platforms for the very first time. This progress is creating opportunity on an unprecedented scale — but it also means that fraudsters are watching closely, evolving just as fast as innovation itself.

In 2025, we are witnessing a new reality: the continent is no longer fighting isolated scams or low-effort impersonation attempts. We are confronting organized, AI-powered operations — deepfakes, synthetic identities, and cross-border fraud rings that move with precision and speed. These are not random acts; they are structured systems that exploit gaps between markets, regulations, and technologies.

At the same time, the response from Africa's public and private sectors is accelerating. We see governments tightening SIM–ID registration, fintechs investing in behavioral analytics, and regulators prioritizing cross-border cooperation. The progress is uneven but unmistakable. Africa is no longer playing catch-up — it is setting its own path toward resilient, intelligent verification ecosystems built for its unique context.

Our mission at Sumsub is to support that transformation. While the risks are growing, so is the collective capacity to mitigate them. Africa's story is not only about exposure — it is about resilience, innovation, and a shared commitment to building digital trust from the ground up."

Asia & Pacific

The Asia-Pacific (APAC) region is one of the most dynamic fraud environments globally. Home to both high-trust digital leaders, such as Singapore and Japan, and fraud-heavy ecosystems, such as Pakistan and Indonesia, the APAC region reflects the full spectrum of the global Sophistication Shift.

What makes the APAC region unique is its rapid transition. In just three years, the types of fraud have swung sharply away from crude, low-effort forgeries toward AI-driven deepfakes, synthetic identities, and persistence-based schemes. At the same time, overall fraud rates diverge widely: while some economies reduce their exposure through stronger regulations, others experience double- or triple-digit growth. This tension defines the region: falling percentages in mature markets, surging AI-driven fraud in emerging ones.

Fraud type evolution: deepfakes and synthetics rising

The fraud-type distribution in APAC shows a dramatic shift compared to 2024.

Selfie-driven fraud takes center stage.
In 2025, fraud involving inconsistencies between a user's selfie and their ID photo represents 35.4% of all fraud, after growing by +73% YoY and gaining +6.8 percentage points of share. This category highlights how deepfake video attacks increasingly masquerade as ordinary mismatches, confusing systems that were designed for low-quality spoofing.

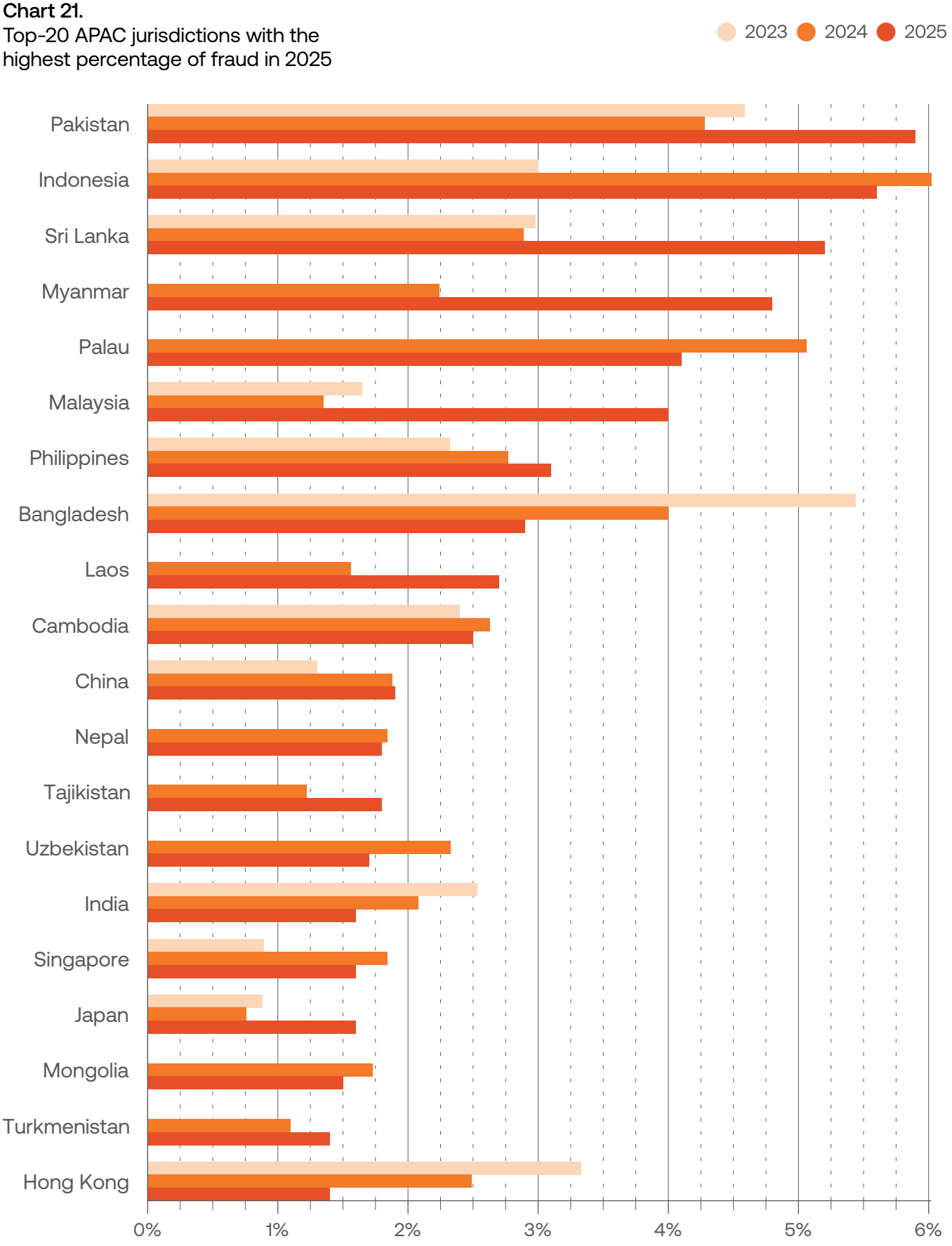
Stolen is out, synthetic is in.
Synthetic personal data grew +142% YoY, lifting its share to 15.7% of all fraud. Here, we see fraudsters creating entire synthetic identities — including names, addresses, and dates of birth — often generated with AI and paired with high-quality deepfake selfies. For banks, trading apps, and e-commerce platforms, this means that fraud no longer comes solely from stolen IDs, but from fabricated digital identities that may initially pass checks and only reveal their fraudulent nature much later.

Old tricks are fading.
Categories like blacklist violations (–50% YoY; –9.1 pp share) and forged IDs (–11% YoY; –4.1 pp) are in retreat. Blurry photos, copy-paste edits, and crude forgeries are simply no longer effective. This decline frees up capacity for verification teams but also signals where attackers are reallocating their energy.

Persistence as a tactic.
Duplicate submissions nearly quadrupled (+388% YoY), while liveness bypass attempts also rose. These patterns suggest fraudsters are investing not only in quality (deepfakes, synthetics) but also in volume and resilience, hammering systems with repeated attempts until one slips through.

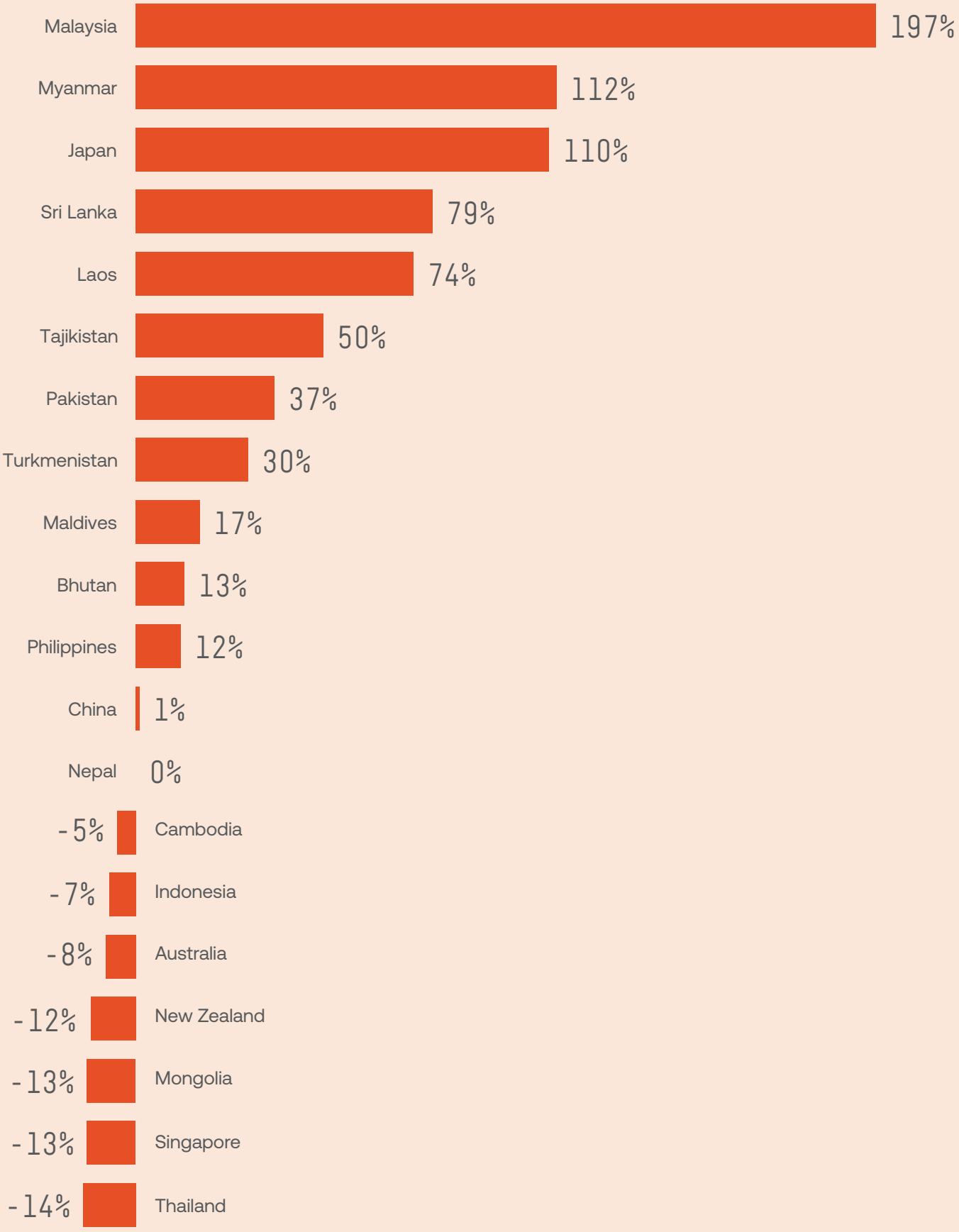
Taken together, APAC's fraud-type data provides a snapshot of fraud's evolution in real time: crude forgeries are shrinking, AI-generated forgeries are exploding, and persistence tactics are filling in the gaps.

Chart 21.
Top-20 APAC jurisdictions with the highest percentage of fraud in 2025



% of fraud in all analyzed verifications by jurisdiction

Chart 22.
Top-20 APAC jurisdictions with the largest fraud growth (2025 over 2024)



Country-level dynamics

Beneath these aggregate trends lies a fragmented regional landscape.

High-growth fraud markets

1 **Malaysia (4.0%, +197% YoY):**
The fraud rate in Malaysia experienced the highest year-on-year increase, with cybercriminals targeting online transactions using money mules, as well as investment fraud aimed at expatriates, retirees, and young professionals.

2 **Pakistan (5.9%, +37% YoY):**
Fraud surged despite moderate regulation. Mobile wallets and informal financial channels remain vulnerable, with weak KYC enforcement giving fraudsters space to scale. The fraud rate in Pakistan is one of the highest globally, with its fraud during AML checks being 1.5 times higher than in any other country. One in ten Pakistani applicants was found to have triggered fraud during their AML checks.

3 **Sri Lanka (5.2%, +79% YoY):**
A standout riser. The spike is tied to rapid fintech and e-commerce expansion, where onboarding checks have not kept pace with fraud sophistication.

4 **Myanmar (4.8%, +112% YoY) and Laos (2.7%, +74% YoY):**
Both of these smaller markets are vulnerable to exploitation by fraudsters due to gaps in newly digitizing systems. These countries illustrate how attackers actively seek out the weakest links in APAC's ecosystem.

Stable but high-risk

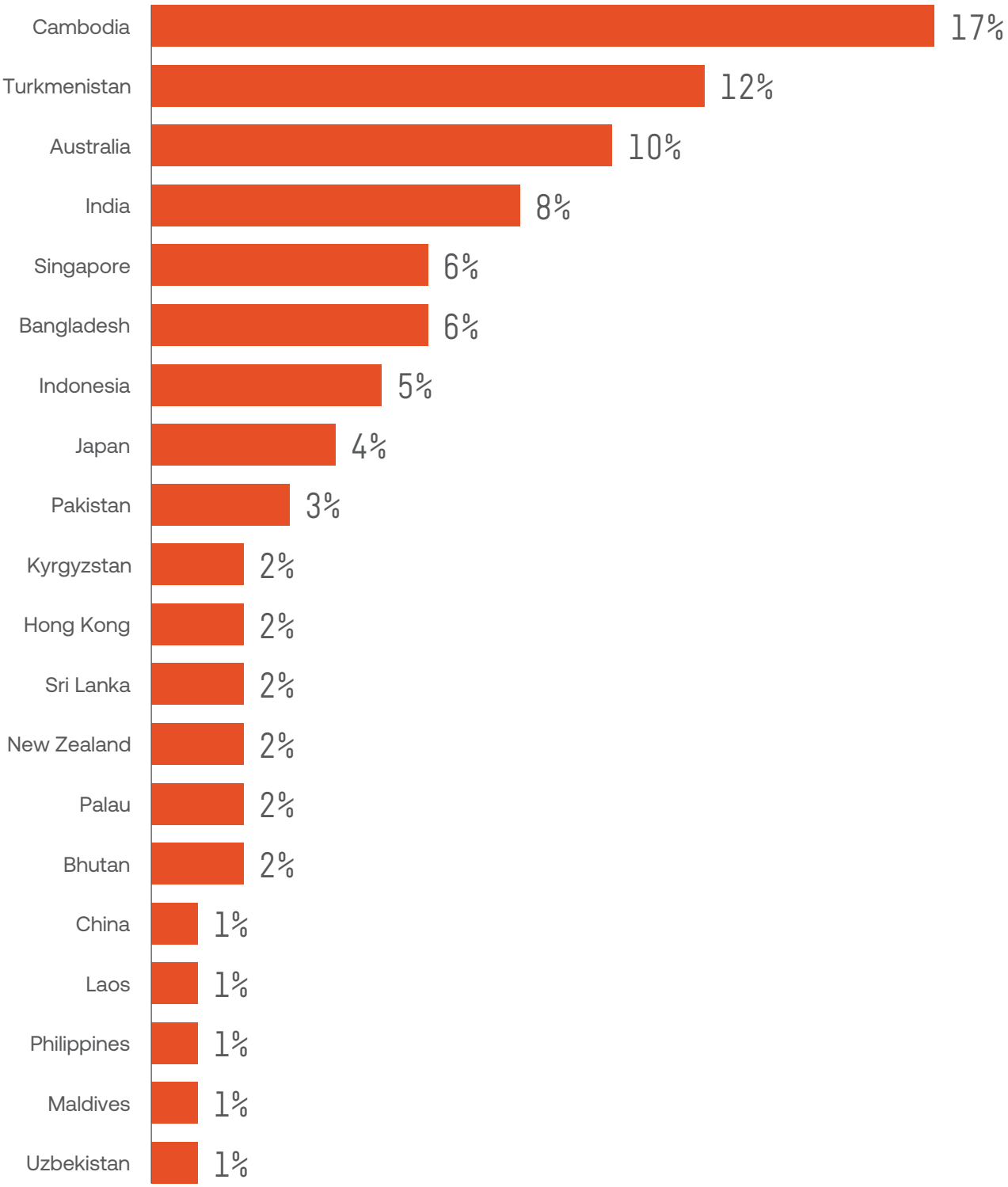
1 **Indonesia (5.6%, –7% YoY):**
Despite a slight drop, Indonesia remains among the highest-risk countries. Its vast e-commerce and super-app ecosystems create constant exposure. Deepfakes already account for 5% of fraud attempts, making Indonesia a proving ground for AI-driven onboarding fraud.

2 **Philippines (3.1%, +12% YoY):**
Pressure persists, largely driven by remittance platforms, gaming accounts, and social media-linked onboarding, all of which are frequent targets of fraud.

Markets with declining fraud rates

India (1.6%, –23%), Bangladesh (2.9%, –26%), Hong Kong (1.4%, –43%), Singapore (1.0%, –12%), South Korea (0.8%, –22%), Cambodia (2.5%, –5%), and Australia (1.1%, –8%) all recorded declines.
These reductions reflect stronger regulation, including India's RBI-mandated KYC tightening, Hong Kong's financial regulator's push for new anti-fraud rules, and Singapore's strengthened anti-scam and e-payment frameworks introduced by MAS.
Yet, the paradox persists: while overall percentages have fallen, the share of deepfake-related fraud continues to climb. In Singapore, deepfake incidents rose by +158% YoY, with impersonation scams and fraudulent e-wallet registrations emerging as the main drivers. This reinforces the trend seen across advanced APAC markets — falling fraud volumes but rising sophistication.

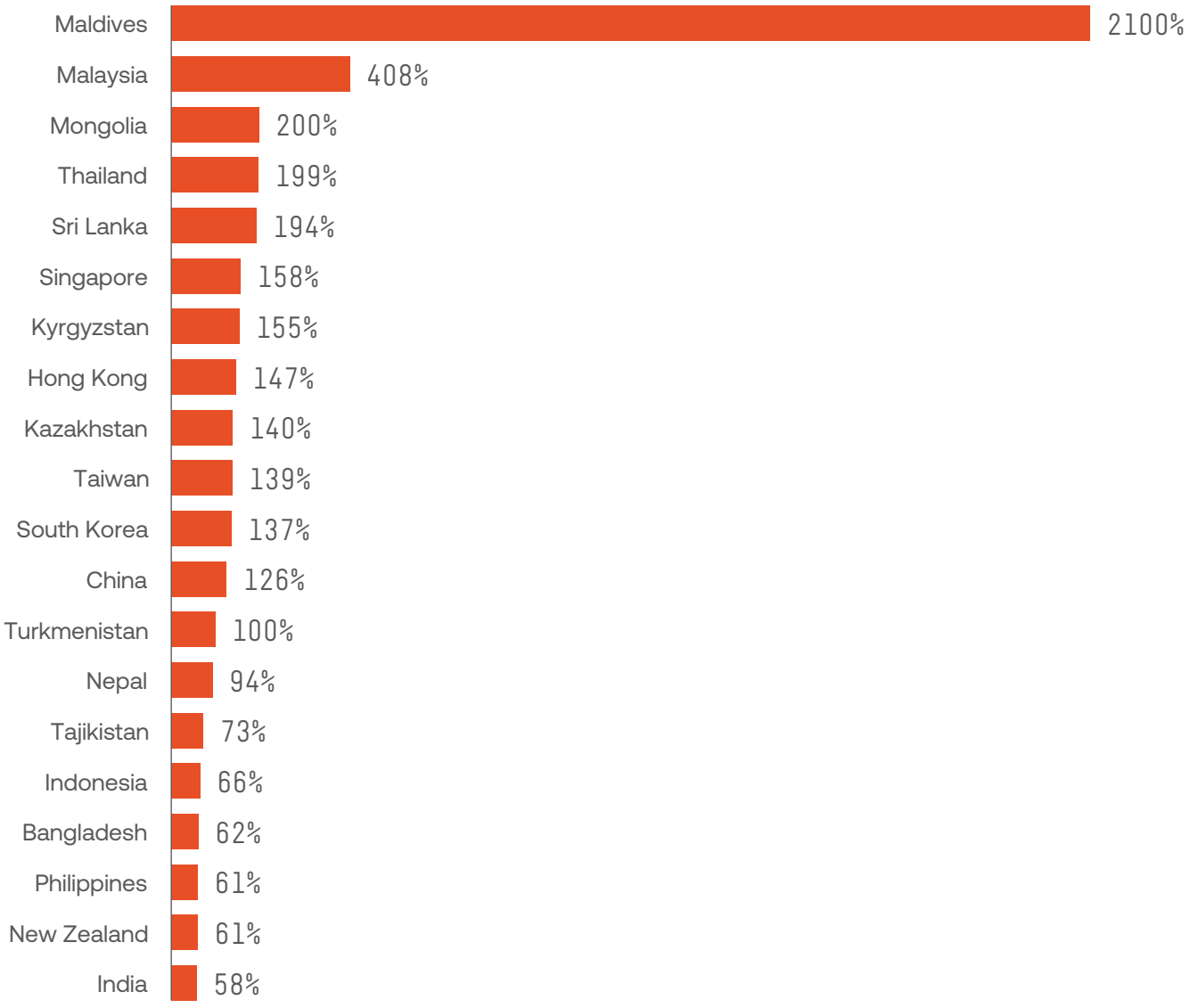
Chart 23.
Top-20 jurisdictions with the highest ratio of approved applicants involved in fraud networks



Deepfakes

The diverging fraud trajectories across APAC highlight how much outcomes depend on policy enforcement, digital adoption speed, and attacker strategy. These numbers show that the quality of fraud is rising faster than its quantity is falling.

Chart 24.
Top-20 APAC jurisdictions with the largest YoY deepfakes growth (2025 over 2024)



In large economies such as India and Bangladesh, stronger regulation has helped reduce crude fraud attempts. Central banks and regulators have forced fintechs and mobile money operators to adopt stricter KYC and biometric checks, making it harder for low-effort fraud to succeed. Yet these markets also illustrate a paradox: while overall percentages have fallen, the remaining fraud is increasingly sophisticated, with deepfakes and synthetic identities carving out a growing share of the market.

Hong Kong and South Korea show a similar story. Both benefit from mature financial infrastructures and coordinated enforcement efforts, which dampen the overall volume of fraud. But sophisticated actors continue to target them, especially through cross-border corridors, meaning that while casual scams decline, complex synthetic and deepfake-based attacks are becoming the main challenge.

By contrast, countries such as Pakistan, Sri Lanka, and Myanmar moved in the opposite direction. Their rapidly expanding digital ecosystems, particularly in wallets, payments, and e-commerce, still lack consistent onboarding standards. Fraudsters exploit these gaps, often recycling the same synthetic identities and deepfake kits across borders. Sri Lanka's sharp rise, for example, reflects the appeal of a growing e-commerce market combined with relatively light-touch controls.

Indonesia stands out as a stable but persistently high-risk environment. Its sprawling super-app ecosystems create a wide attack surface, where one compromised identity can unlock multiple services. Fraudsters continue to prize this environment even when crude fraud attempts are curbed, because the potential payoff of each breach remains exceptionally high.

The lessons

1. Fraud declined in markets where regulation and infrastructure forced fraudsters to abandon easy wins, but the fraud that persists is sharper, harder to detect, and costlier per case.

2. Fraud rose in markets where adoption outpaced control, making them fertile ground for fraud rings and synthetic identity kits that thrive in loosely regulated ecosystems.

Pasi Koistinen,
Chief Information Security Officer at Coinhako

"In 2026, AI-driven compliance, fraud prevention, and security platforms will dominate. Their predictive capabilities will allow industries to act before cyberattacks or fraud occur. Advanced liveness detection and multimodal biometrics will counter sophisticated KYC fraud, while NFC reading of passports and IDs becomes routine. Behavioral indicators such as typing rhythm, scrolling patterns, and navigation habits will further strengthen identity verification.

Digital identity ecosystems will continue to merge. Private identity providers will increasingly integrate with government verification systems, enabling seamless, high-assurance authentication across services. Blockchain may later secure document integrity within these frameworks. Continuous identity monitoring and adaptive anti-fraud systems will replace the old "check once, trust forever" model, reshaping compliance into a dynamic, ongoing process.

From 2025 trends, it is clear that criminals have embraced AI even faster than regulators or enterprises. Large language models now power global waves of fraud, from impersonation and phishing to elaborate scams—employment, romance, investment, and "pig butchering." Combined with data from constant breaches, AI-driven phishing tactics routinely bypass 2FA and identity checks. Fraud losses have reached record highs, proving that the very technologies meant to defend digital systems are being turned against them, forcing an urgent evolution in defense strategies."

What to expect next

Looking forward to 2026, APAC is poised to become the testbed for global fraud innovation. Several trends stand out:

Deepfake normalization

Fraudsters are investing in generative AI not as an experiment but as the default method of attack. Expect deepfakes to expand into multi-modal fraud, combining video, voice, and tampered telemetry to overwhelm liveness and behavioral checks.

According to Sumsub's Fraud Exposure Survey 2025, 32% in APAC have come across deepfakes online, while another 24% are unsure, showing that synthetic media is now so convincing that many users can't tell real from fake.

17% have seen friends or coworkers share deepfakes, suggesting these manipulated videos are spreading organically through social networks. Even more concerning, 14% of respondents have been personally targeted or fooled — whether through fake scam calls, emails, or synthetic impersonations — confirming that deepfakes are already being weaponized for fraud and social engineering.

Only 12% report never encountering a deepfake, and a small but telling 2% have created one, highlighting the increasing accessibility of generative tools.

Cross-border fraud rings

South Asia is emerging as a hub for synthetic identity rings. Kits and stolen data circulate freely across Pakistan, Sri Lanka, and Bangladesh, allowing fraudsters to attack multiple markets with the same playbooks. For defenders, this means that fraud cannot be solved in isolation; collaboration and intelligence-sharing are essential.

Shift to high-value targets

As crude onboarding scams decline, attackers are pivoting toward credit products, trading platforms, and high-limit financial accounts. Each successful synthetic identity now aims for a larger payout, raising the stakes for institutions.

Regulatory response is catching up

1. India is pushing biometric requirements for fintechs.
2. Singapore is preparing AI-governance rules that will affect fraud detection.
3. Japan is expanding digital identity pilots but faces new risks as fraudsters target previously low-risk markets.

So what's the big picture?

APAC's fraud battle will not be won by lowering percentages alone. By 2026, even "safer" markets will face their highest-ever risk of fraud sophistication, while smaller, fast-growing economies will remain magnets for high-volume fraud rings. Success will depend on pairing advanced detection technologies (behavioral analytics, multi-modal AI checks, federated fraud intelligence) with regional regulatory alignment to close gaps that fraudsters exploit.

Global challenge, local realities

Discover APAC's performance in Sumsub's Fraud Exposure Survey 2025.

Companies

69%

Businesses in Asia & the Pacific have fallen victim to fraud in 2025

Consumers

53%

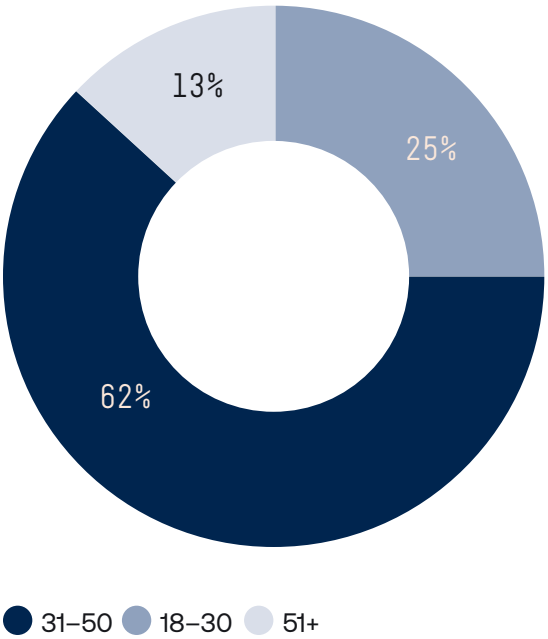
End users in Asia & the Pacific have fallen victim to fraud at least once in 2025

Consumer fraud findings in APAC

Take a closer look at who our APAC-based consumers are, from their age to employment status.

Chart 25.

Age



31–50 18–30 51+

Employment status

81% Employed full-time

9% Employed part-time

6% Self-employed full-time

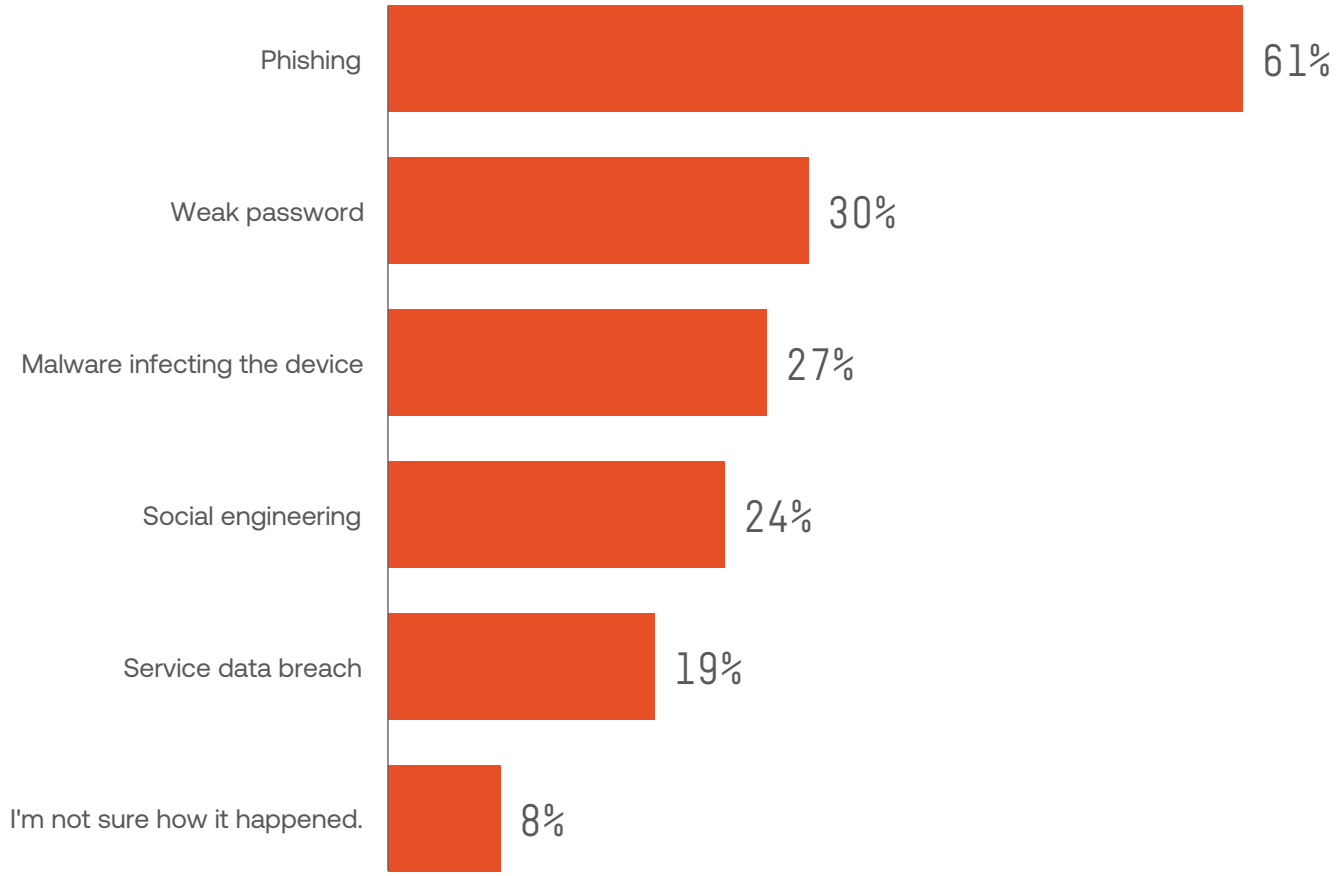
3% Temporarily unemployed

2% Self-employed part-time

Main attack vectors

The data reveals a clear pattern: most attacks still start with people, not systems. With phishing (61%) and weak passwords (30%) leading the list, human error and low digital hygiene remain the most exploitable weaknesses.

Chart 26.
Question:
What do you think was the cause of the fraud incident?



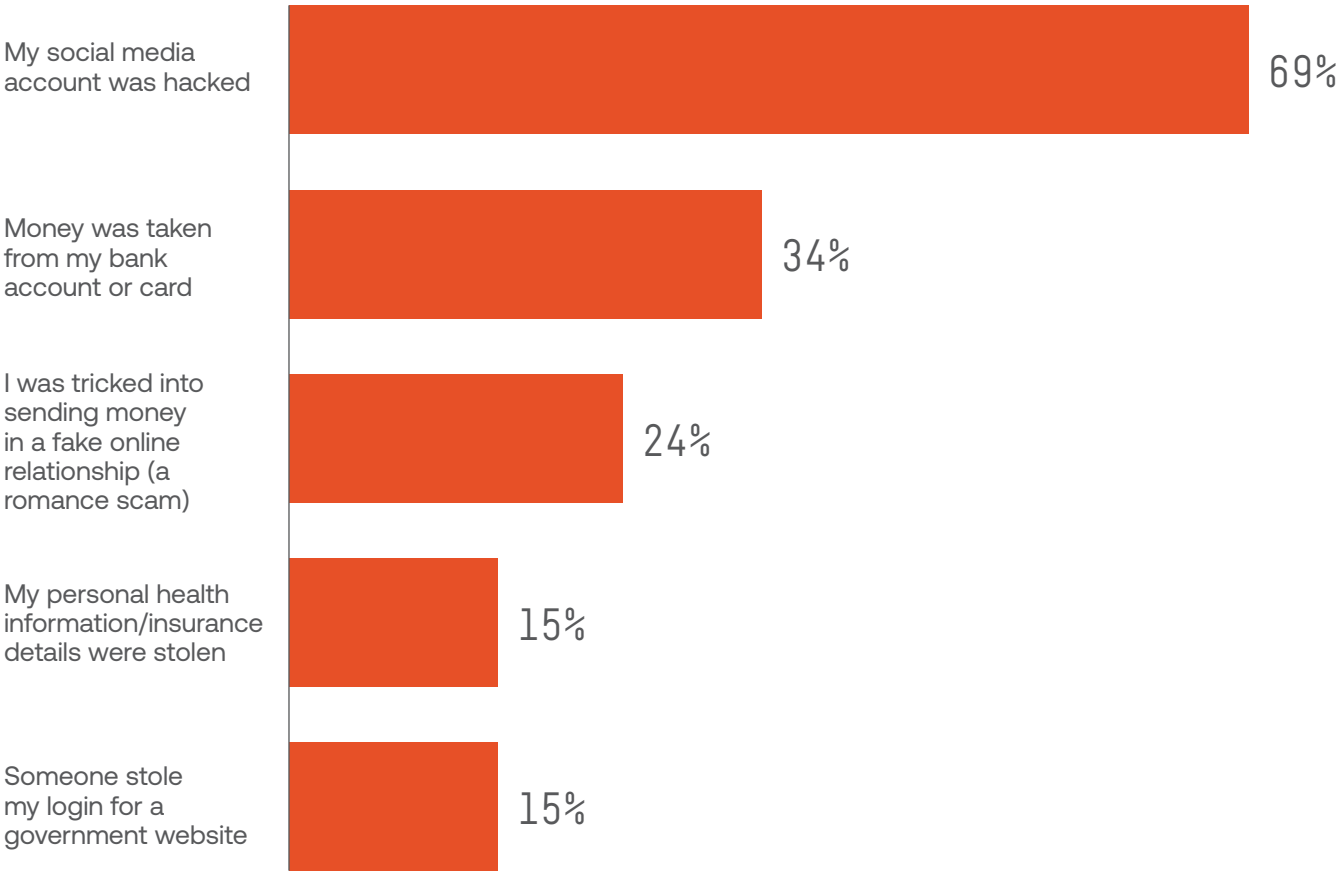
Sumsub's Fraud Exposure Survey 2025, APAC: Consumers

Main fraud outcome

The dominant fraud outcome - social media (69%) and government portal (15%) account takeovers - underscores a shift in attacker priorities: rather than targeting money directly, fraudsters increasingly seek to control identities and gain digital access.

At the same time, financial loss remains significant, with 34% reporting that funds were stolen and 24% tricked into sending money.

Chart 27.
Question:
What type of identity fraud did you experience?



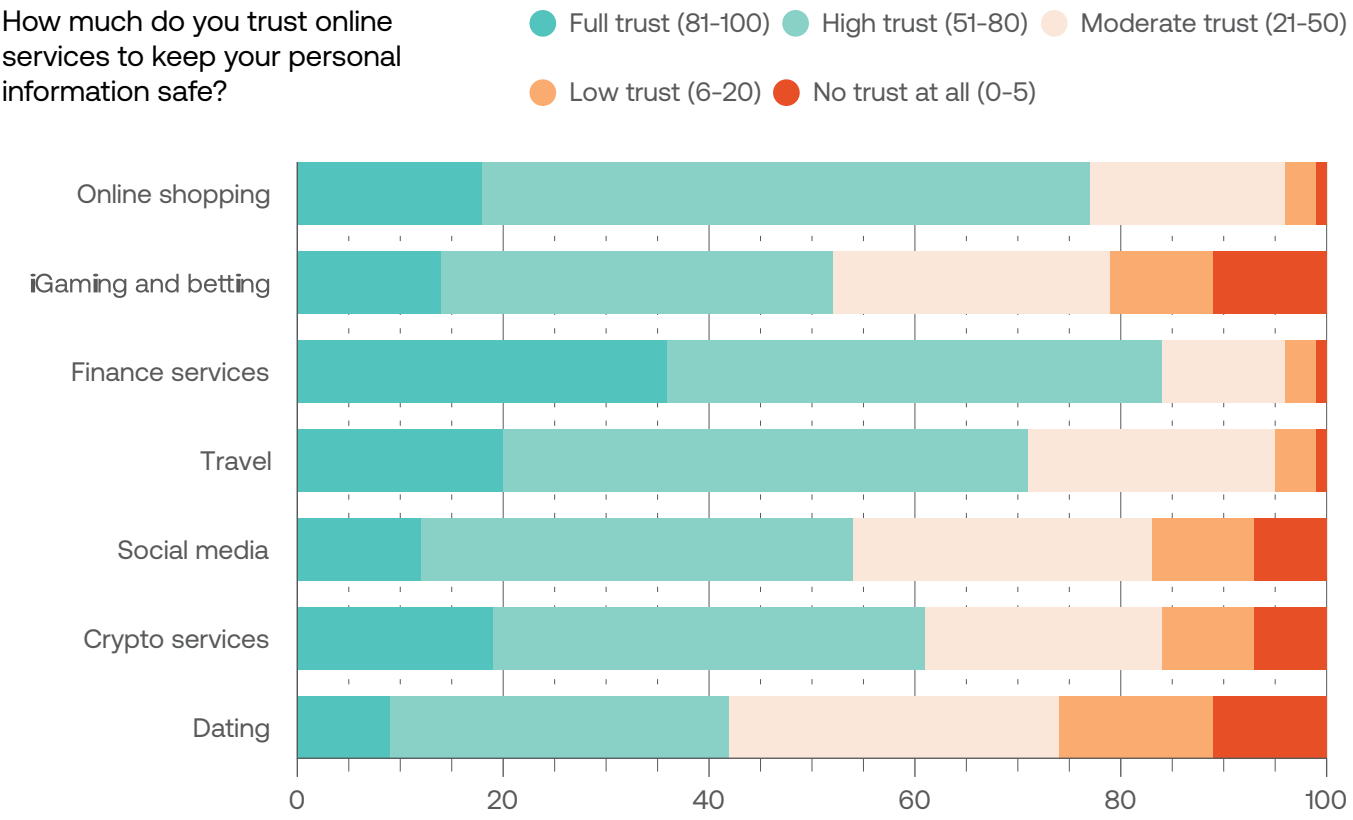
Sumsub's Fraud Exposure Survey 2025, APAC: Consumers

Digital trust in APAC

Overall, respondents show stronger confidence in traditional and regulated sectors, with finance (85%), online shopping (77%), and travel (71%), earning the highest combined high or full trust scores. This reflects consistent exposure, clear regulation, and visible consumer protection mechanisms.

However, trust sharply declines in higher-risk or socially sensitive sectors — crypto services (61%), social media (55%), and dating (42%) — where user data is more exposed to manipulation, leaks, or misuse. These industries face a persistent perception challenge: users engage heavily with them but doubt their ability to protect privacy.

Chart 28.
Question:
How much do you trust online services to keep your personal information safe?



Sumsub's Fraud Exposure Survey 2025, APAC: Consumers

89% of respondents would choose a service provider only if they have strong anti-fraud measures in place.

Responsibility for fraud prevention

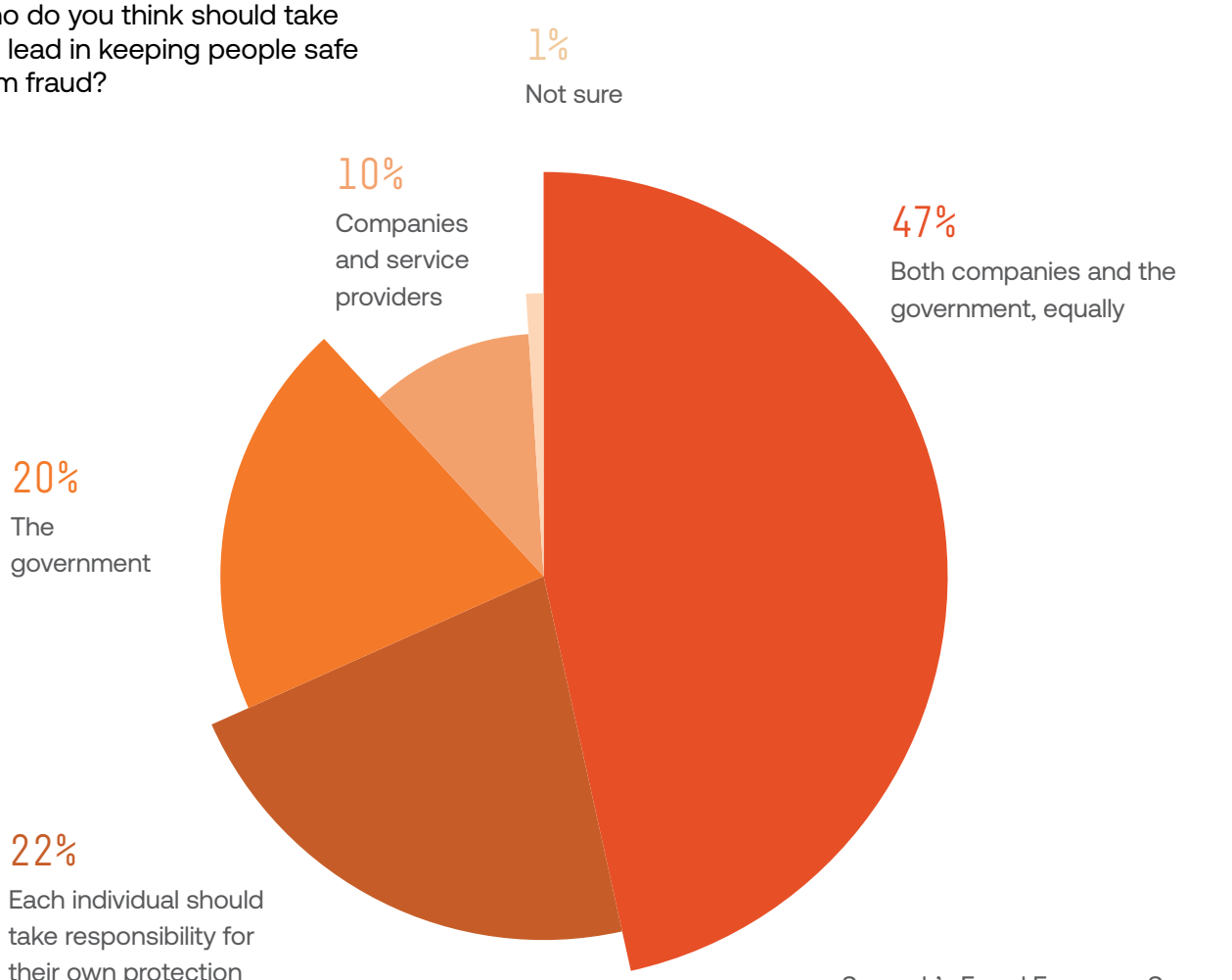
47% of respondents believe companies and the government should share responsibility for fraud protection equally.

Higher expectation of individual responsibility in APAC - 22% believe each person should protect themselves.

20% put the burden on the government alone, which is higher than in Europe (15%) and in Latin America (8%).

Only 10% think companies should take the lead.

Chart 29.
Question:
Who do you think should take the lead in keeping people safe from fraud?



Sumsub's Fraud Exposure Survey 2025, APAC: Consumers

Growing adoption of virtual cards

Over 60% of APAC users already leverage virtual or disposable cards at least occasionally. This indicates a growing awareness of payment fraud risks and a willingness to adopt preventive measures.

However, the 40% who rarely or never use such cards point to a persistent trust and accessibility gap — especially among users who rely on traditional banking channels or lack exposure to fintech-driven solutions.

Question:
Do you use disposable or virtual cards for online payments?

Sumsub's Fraud Exposure Survey 2025, APAC: Consumers

Money muling remains a hidden threat

While nearly 80% of respondents recognize the term "money muling", the majority lack a clear understanding of its legal and financial consequences — revealing a dangerous gap between awareness and comprehension.

Even more alarming, **1 in 4 individuals have been personally targeted for mule activity,** suggesting that **criminal recruitment is active and widespread** in the region. This highlights how fraud networks are scaling social engineering tactics to exploit financially vulnerable or unaware users.

Question:
Have you heard of "money muling" - letting someone move stolen money through your bank account?

Sumsub's Fraud Exposure Survey 2025, APAC: Consumers

88% of respondents are highly convinced that fraud is becoming more sophisticated and AI-driven.

This confirms that companies are aware of deepfake risks, synthetic identities, and AI-driven forgeries, and are looking for next-generation fraud prevention solutions.

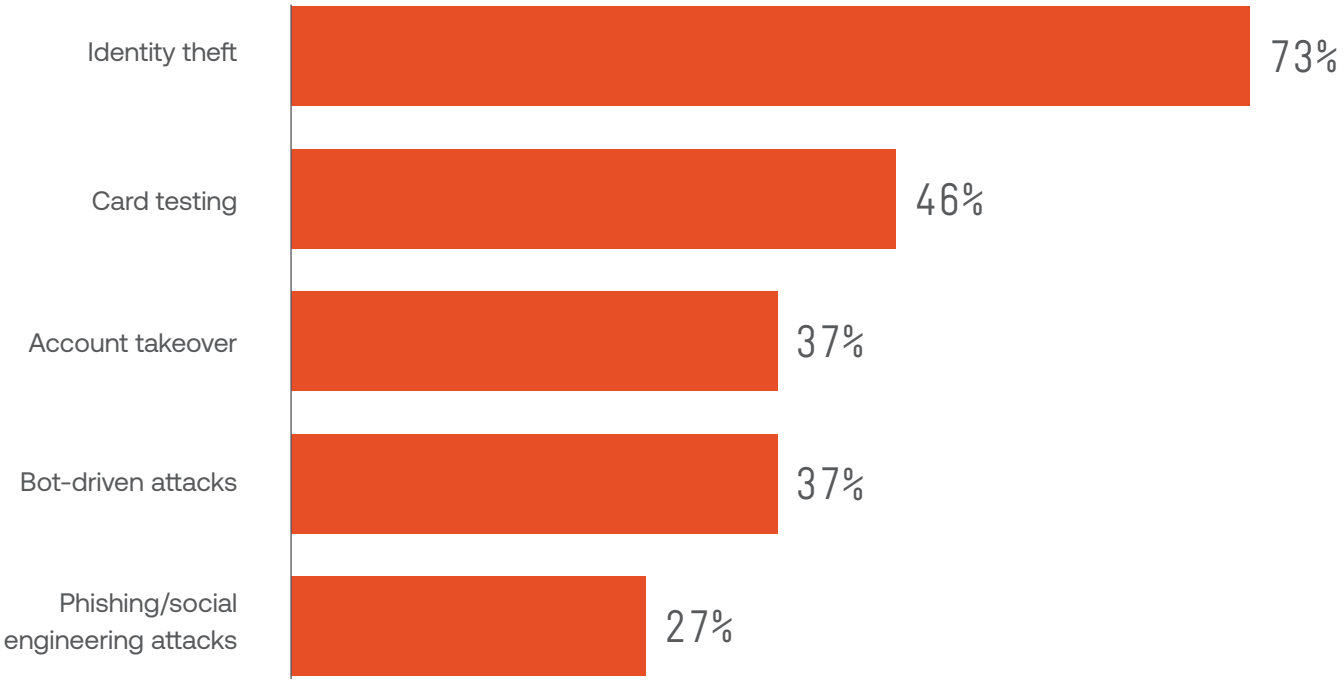
Company fraud findings in APAC

Top 3 types of fraud faced by companies in Asia & the Pacific

1. Identity theft (73%)
2. Card testing (46%)
3. Account takeover & bot-driven attacks (37% respectively)

At the same time, they had to manage first-party fraud from their customers, who used synthetic identity (64%) and deepfakes (46%), and conducted application (46%) and chargeback abuse (64%).

Chart 30.
Question:
What kind of third-party fraud has your business faced?



Sumsub's Fraud Exposure Survey 2025, APAC: Companies

55% report that organized fraud attempts have become more frequent. At the same time, 27% see no change, indicating that not every sector has observed escalation.

Major consequences companies have experienced as a result of fraud attacks:

1. Financial losses (64%)
2. Customer churn (55%)

How companies in Asia & the Pacific manage fraud

Most companies today rely on a hybrid approach to fraud prevention — 69% combine in-house expertise with external solutions, blending internal control with advanced vendor technologies for stronger detection and compliance coverage.

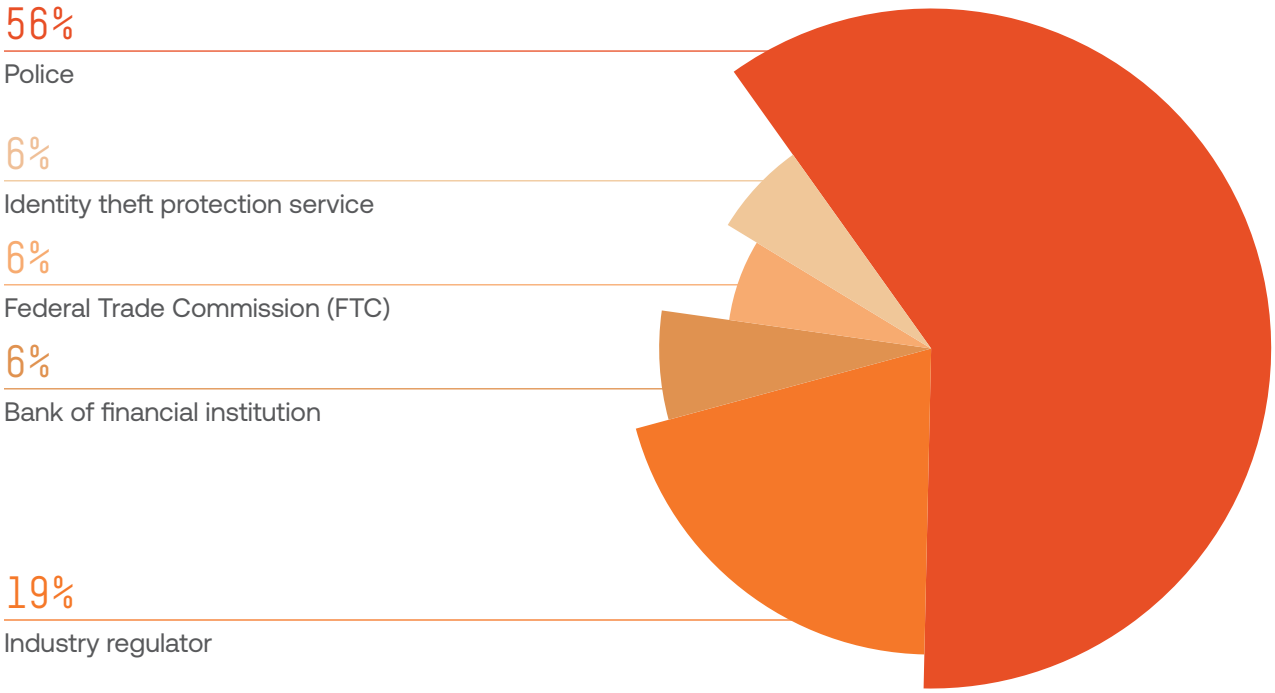
However, **manual reviews remain common (44%)**, showing that many teams still face workflow silos, repetitive checks, and slow case handling.

Nearly 60% of respondents reported fraud incidents to the police for investigation.

Unlike in Europe, APAC businesses tend to treat fraud as a criminal investigation issue first.

63% support stricter regulations, even if operations become more complex.

Chart 31.
Question:
Did your business report incidents of identity fraud to authorities or institutions



Sumsub's Fraud Exposure Survey
2025, APAC: Companies

Predictions for the future

AI-driven fraud will dominate

- → 88% expect more deepfake scams
- → 81% predict more sophisticated AI-driven attacks.

Multiple risks seen as equally likely (63% each)

- → Greater business focus on cybersecurity.
- → AI-generated fake documentation & profiles.
- → Stricter regulations by governments.
- → More fraud targeting biometric systems (e.g., spoofing face recognition).
- → Wider use of synthetic identities to bypass KYC/onboarding.

88%

More deepfake scams

81%

More sophisticated AI-driven attacks.

56%

Growing organized fraud & identity theft

50%

More digitally forged/tampered IDs

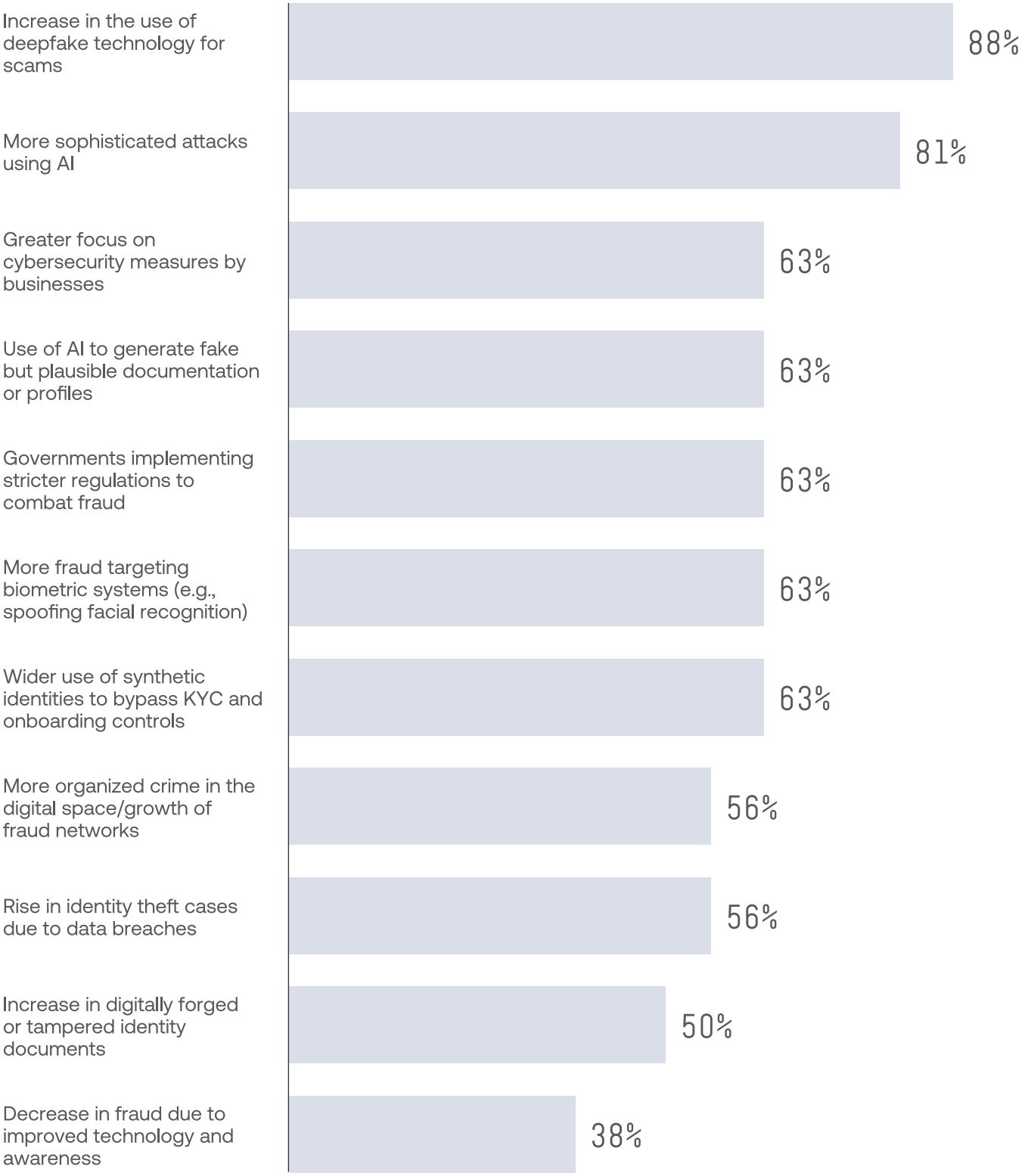


Chart 32.
Question:
What are your predictions for the future of the fraud landscape?

Sumsub's Fraud Exposure Survey 2025, APAC: Companies

Regulatory shifts redefining identity protection

As fraud grows more sophisticated, APAC regulators are tightening oversight through stronger digital identity rules, cross-border data controls, and coordinated enforcement. Here are some of the latest developments across the Asia-Pacific region.

Australia

AML/CTF Amendment Act

On 29 November 2024, Parliament passed the Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2024, expanding the AML/CTF regime to cover new "designated services." These include real-estate professionals, dealers in precious metals, lawyers, accountants, and trust and company service providers, all now brought under AUSTRAC supervision. The reforms also modernize requirements for digital currency and virtual asset service providers, strengthen risk assessment obligations, and tighten governance for reporting entities—closing loopholes often exploited for shell companies, layering schemes, and crypto-enabled fraud.

Scams Prevention Framework Bill

On 21 February 2025, the Scams Prevention Framework Bill came into force, creating a statutory regime that requires banks, telecom operators, and digital platforms to prevent, detect, disrupt, report, and respond to scams. The framework embeds the SPF Principles—Governance, Prevent, Detect, Report, Disrupt, Respond—into law, with sector-specific codes of conduct, governance structures, and accountability metrics. This shifts scam prevention from a voluntary duty to a mandatory compliance obligation, holding service providers directly responsible for proactively blocking scam activity.

ASIC guidance on share sale fraud

In June 2025, ASIC updated its guidance (INFO 237) to help Australian Financial Services licensees respond to rising share sale fraud, where criminals impersonate legitimate clients to sell or transfer shares or divert proceeds. The guidance emphasizes stronger client onboarding and identity verification, closer monitoring of unusual trading patterns, and stricter verification of changes to personal or bank accounts. It stresses that account detail updates should not be actioned on minimal checks alone.

Telecom and Messaging fraud controls

Between 2024 and 2025, ACMA intensified enforcement against phone and SMS fraud. Telcos reported blocking more than 2.6 billion scam calls since December 2020 and nearly 937 million scam SMS since July 2022. Providers have faced penalties for non-compliance with anti-spam and telecom fraud rules, and new compliance alerts have been issued. A key measure in development is the SMS Sender ID Register, currently piloted, which will verify message sender identities and block fake headers commonly exploited by scammers to impersonate banks and government agencies.

China

Revised anti-money laundering law

Approved on 8 November 2024 and effective 1 January 2025, China's revised AML Law expanded coverage to fraud proceeds, extended AML/CFT duties to DNFBPs, introduced a UBO filing system, and raised penalties and supervision powers. The key changes:

1 **Broader scope:**
The law now explicitly covers laundering the proceeds of a wide range of “other crimes,” including gains from fraud, telecom/online scams, and syndicated digital crime. This closes critical loopholes and ensures that cross-channel fraud proceeds are actionable for law enforcement and banks.

2 **DNFBP obligations:**
AML/CFT requirements are extended to designated non-financial businesses and professions (DNFBPs)—including real estate, legal, accounting, and notary sectors—which are often used to layer or conceal fraudulent assets. These sectors must now conduct ongoing KYC, monitor for suspicious transactions, and report STRs as rigorously as banks and payments providers.

3 **Beneficial ownership transparency:**
A new UBO/BOI filing system enables authorities to more easily identify and scrutinize shell companies and complex structures that often conceal the proceeds of fraud, thereby helping to unmask key beneficiaries and facilitating asset tracing and asset freezes.

4 **Stronger penalties, enhanced supervision:**
The revised law increases penalties for breaches, enhances regulatory and law enforcement powers to investigate, conduct on-site inspections, mandate screening, and requires the timely submission of STRs for all entities.

Crackdown on insurance fraud

On 3 January 2025, China's Ministry of Public Security and the National Financial Regulatory Administration announced the results of a nationwide crackdown on insurance fraud. More than 1,400 cases were investigated, 300 gangs dismantled, and RMB 1.5 billion in fraud uncovered. Key fraud schemes include:

1. **Luxury car accident fraud:**
   Staged collisions and inflated repair receipts, sometimes involving >RMB 9m.

2. **E-commerce return & freight insurance fraud:**
   Fabricated exchanges exploiting online platform policies.

3. **Employer liability fraud:**
   Fake injury claims, collusion with employers, or embezzlement of employee compensation.

4. **Commission fraud:**
   Brokerage firms manipulating "first-year free" policies to extract commissions (RMB 1.2bn in one case).

5. **Repeated small-claim fraud:**
   Exploiting the lack of insurer data-sharing for multiple accident claims.

6. **Agricultural insurance fraud:**
   Intentionally killing insured livestock and colluding with adjusters.

Anti-Fraud Alliance Proposal

In September 2025, the Ministry of Public Security proposed forming an international alliance to coordinate efforts against telecom and cyber fraud, building on the successes of cross-border enforcement. As part of this, China highlighted its prior collaborative successes, including the repatriation of approximately 68,000 fraud suspects from other countries and the training of thousands of law enforcement officers internationally.

Anti-Unfair Competition Law revisions

Passed on June 27, 2025, and effective October 15, 2025, China's revised AUCL introduced new obligations for platforms to prevent fake reviews, deceptive marketing, data misuse, and algorithm manipulation. The law also raised penalties and introduced personal liability for executives. Platforms are required to monitor and police their merchants and users more actively; personal liability is introduced for legal representatives and executives in certain cases. Fines for violations have been raised to RMB 5 million for entities, with added liability for individuals. The law also applies extraterritorially—that is, conduct outside China that harms the Chinese market may be subject to enforcement. These changes directly target fraud vectors such as fake reviews, deceptive endorsements, algorithmic manipulation, and data misuse—all common in platform fraud and digital deception.

Hong Kong

Stablecoin Ordinance

Effective 1 August 2025, Hong Kong's Stablecoin Ordinance established a licensing regime for fiat-referenced stablecoin issuers. The framework restricts issuance to regulated entities and requires strict reserve, redemption, and identity verification standards to mitigate fraud and consumer risks.

Banking amendment bill on information sharing

In May 2025, the Legislative Council passed the Banking (Amendment) Bill, establishing a voluntary framework supervised by the HKMA that allows authorized institutions to share account and transaction data with each other and law enforcement. The law provides safe harbor protections for good-faith disclosures, enabling faster detection of mule accounts and cross-bank fraud networks.

Anti-Scam Consumer Protection Charter 3.0

On 9 July 2025, the HKMA, together with other regulators and industry players, launched the Anti-Scam Consumer Protection Charter 3.0. The initiative expands cooperation among regulators, telecom operators, social media platforms, and financial institutions to enhance scam ad monitoring, advertiser vetting, the takedown of fraudulent promotions, and consumer reporting channels.

Crackdown on mule accounts

In April 2025, the HKMA, Hong Kong Police, and HKAB launched a coordinated crackdown on mule accounts. Banks were directed to strengthen detection systems, courts imposed tougher sentences on offenders, and a public awareness campaign, "Don't lend/sell your account," was rolled out to highlight the risks.

Indonesia

BI-FAST fraud and cybersecurity enhancements
On 30 June 2025, Bank Indonesia issued PADG No. 14/2025, the second amendment to PADG No. 17/2023, governing the BI-FAST payment system. This amendment requires real-time fraud detection, stronger cybersecurity audits, stricter rules for third parties, and faster incident reporting to close vulnerabilities in fast payment channels.

OJK anti-fraud regulation
Effective 31 October 2024, OJK Regulation No. 12/2024 requires all financial institutions to implement formal anti-fraud programs, conduct annual reporting, and disclose major fraud cases. Non-compliance can result in fines or suspension of activities.

MOL Regulation No. 2/2025 on beneficial ownership
In 2025, Indonesia's Ministry of Law expanded beneficial ownership disclosure to cover all corporate entities, requiring annual updates and immediate reporting of changes. Non-compliance can result in blacklisting and access bans.

Malaysia

E-money exposure draft

In 2025, Bank Negara Malaysia issued an exposure draft for e-money issuers and wallet providers, proposing stronger AML/CFT obligations. These include stricter customer due diligence, mandatory sanctions screening, continuous transaction monitoring, and risk-based controls tied to issuer size and customer risk.

National Registration Amendment Bill

On 27 August 2025, the Dewan Rakyat passed the National Registration (Amendment) Bill, introducing new biometric rules. The law defines biometric data, empowers the minister to regulate its capture and use, and strengthens controls on ID-data usage, storage, and sharing. Key features include:

1. Statutory definition of biometric data (e.g., facial, fingerprint, iris, behavioral traits).
2. Ministerial powers to regulate biometric capture and use of ID-card data, including standards on secure capture, liveness/anti-spoofing, retention, and audits.
3. Expanded controls on ID data usage in onboarding, with implications for OCR, NFC/chip reads, storage, and onward sharing.
4. Interplay with PDPA – Onboarding processes will be subject to both the PDPA and new ID-specific regulations once they come into effect.

Philippines

BSP circular on fraud management systems
In May 2025, BSP issued Circular No. 1213 requiring supervised financial institutions with high transaction volumes to implement real-time fraud management systems. Requirements include velocity checks, geolocation monitoring, anomaly detection, and stronger authentication.

Directive to remove gambling links from e-wallets
In August 2025, BSP issued Memorandum M-2025-029 ordering all financial institutions to remove in-app icons and links to online gambling platforms. The measure aims to mitigate the risks of fraud associated with illegal or scam-related gaming activities.

Enhanced authentication requirements
By June 2026, in accordance with AFASA and BSP Circular No. 1213, all financial institutions must replace SMS and email OTPs for high-risk transactions with secure methods, such as biometrics or app-based authentication, to reduce phishing and SIM-swap risks.

Enhanced due diligence for large cash withdrawals
On 18 September 2025, BSP issued Circular No. 1218 requiring enhanced due diligence for daily cash transactions exceeding PHP 500,000. Such transactions must be conducted through traceable channels unless a legitimate purpose for cash is verified.

Singapore

Protection from Scams Act

In January 2025, Singapore enacted the Protection from Scams Act, granting police and Commercial Affairs officers powers to issue restriction orders that temporarily freeze or limit scam-linked accounts. The act shifts enforcement toward real-time fraud disruption rather than after-the-fact recovery.

MAS Anti-Scam Circular

On 25 October 2024, MAS issued a circular requiring Major Payment Institutions to implement anti-scam controls before raising e-wallet caps. Measures include cooling-off periods for new devices, limits on clickable links in messages, enhanced governance oversight, and stronger incident response.

Amendments to AML/CFT notices and guidelines

On 8 April 2025, MAS proposed amendments to AML/CFT notices for financial institutions and VCCs, with changes finalized on 1 July 2025. Updates include incorporating proliferation financing risks, faster suspicious transaction reporting timelines, stricter Source of Wealth and Source of Funds checks, and greater scrutiny of complex structures.

E-payments guidelines and shared responsibility framework

On 16 December 2024, MAS updated the E-Payments User Protection Guidelines and introduced a Shared Responsibility Framework. The rules allocate fraud-prevention duties between financial institutions and telecommunications companies, requiring the establishment of liability rules, error resolution processes, and enhanced transaction monitoring.

MAS publishes "Cyber Risks Associated With Deepfakes"
In September 2025, following the rise of deepfake attacks on financial institutions, the Monetary Authority of Singapore published an information paper to raise awareness of the emerging risks posed by deepfakes, their potential impact on the financial sector, and recommended steps to address these evolving risks.

U.S. sanctions 3 Singaporeans after ties to one of Asia's largest transnational criminal organizations
In October, three Singaporeans and seventeen Singapore-registered entities were sanctioned by the U.S. due to their ties to a Cambodian scam empire, marking one of the largest financial fraud takedowns in history. This fraud ring consisted of forced labor compounds operating online investment 'pig butchering' scams, where victims were defrauded of billions of dollars, with the U.S. government seizing more than 127,000 bitcoins, valued at approximately US$15 billion.

Thailand

Crypto mule account penalties

Thailand amended its Digital Asset Business Law and Cybercrime Law in 2025 to criminalize the use of mule accounts in crypto scams. Penalties include up to three years' imprisonment, fines up to 300,000 baht, or both.

Royal decree on technological crimes

Effective 13 April 2025, Thailand expanded its technology-crime law, the Royal Decree on Measures for the Prevention and Suppression of Technological Crimes (No. 2), B.E. 2568 (2025), to cover digital asset platforms, telecommunications, and social media. Authorities gained the power to suspend accounts, block scam SMS messages, and impose corporate and personal liability for facilitating fraud.

BOT Digital Fraud Framework

In 2025, the Bank of Thailand issued draft guidelines requiring banks and payment providers to strengthen fraud prevention, mule account detection, and customer support processes. These measures directly tackle APP fraud and mule account laundering, forcing providers to embed proactive fraud controls, transfer monitoring, and stricter KYC/EDD.

Digital Platform Service (DPS) Law

In 2025, Thailand intensified enforcement of its DPS Law, imposing stricter monitoring requirements on platforms linked to scams, impersonation, and counterfeit goods. In 2024 alone, regulators recorded 3,381 fraud complaints and losses exceeding 19 billion baht, underscoring the significant financial harm caused by digital scams. The DPS Law emphasizes the significance of digital platforms as key vectors for fraud, with losses comparable to those from systemic financial crimes.

Penny Chai,
VP of Business Development APAC at Sumsub

"The fraud landscape in APAC has changed faster in the past twelve months than in the previous five years combined. In 2025, we saw fraud rates decline across mature economies, including India, Hong Kong, and South Korea — yet deepfakes and synthetic identities are rising faster than anywhere else in the world. Countries such as Bangladesh and India have seen AI-driven impersonations become the new normal. This shift indicates that the region's success in combating basic scams has prompted attackers to adapt their tactics.

At the same time, emerging markets like Pakistan, Sri Lanka, and Malaysia are experiencing the opposite trend: soaring fraud volumes driven by mobile-first growth and uneven KYC enforcement. Cross-border fraud rings now operate seamlessly between South and Southeast Asia, recycling synthetic identities and liveness-bypass kits across markets. The data tells a clear story — APAC has become the global epicenter of industrialized, AI-powered fraud.

The good news is that the region is also leading the counterattack. Regulators in Singapore and Hong Kong are setting new benchmarks for scam prevention and AI governance, fintechs are deploying behavioral AI at scale, and collaboration between banks, telecoms, and digital platforms is accelerating. APAC isn't just catching up to global standards — it's defining the future of proactive, AI-aware fraud prevention."

Europe

Europe presents a paradox in the global fraud landscape. On one hand, it is home to some of the world's most advanced digital identity programs, strictest regulatory regimes, and mature financial institutions. On the other hand, fraud remains stubbornly resilient, exploiting weaknesses in fragmented national systems and cross-border financial flows.

In 2025, Europe illustrates the Sophistication Shift in two ways:

1. Fraud types are tilting decisively toward AI-powered attacks — deepfakes, synthetic identities, and highly realistic document manipulations.

2. Fraud rates vary across the continent, with some countries experiencing steep increases, while others reduce fraud through enforcement and structural reforms.

Fraud type evolution in Europe

The fraud-type data confirms how fast the picture is changing:

Selfie-driven fraud dominates the landscape.
Fraud involving inconsistencies between a user's selfie and their ID image remains the single largest category, now accounting for 22% of all fraud in Europe, after rising by almost half year-on-year. This category shows that deepfake-based identity spoofing has gone mainstream in Europe.

Synthetic identities surge.
Fake personal data jumped by over 160% year-on-year, increasing its share by nearly 7 percentage points to reach 15% of all fraud. This reflects the growing use of AI-generated personal information — including fabricated names, addresses, and dates of birth — to create convincing yet entirely fake profiles.

Legacy tactics decline.
Blacklist and blocklist violations fell in share, dropping to under 9% of fraud, while crude screenshot fraud also fell. These declines suggest that low-effort attacks are being filtered out early, forcing fraudsters to adapt.

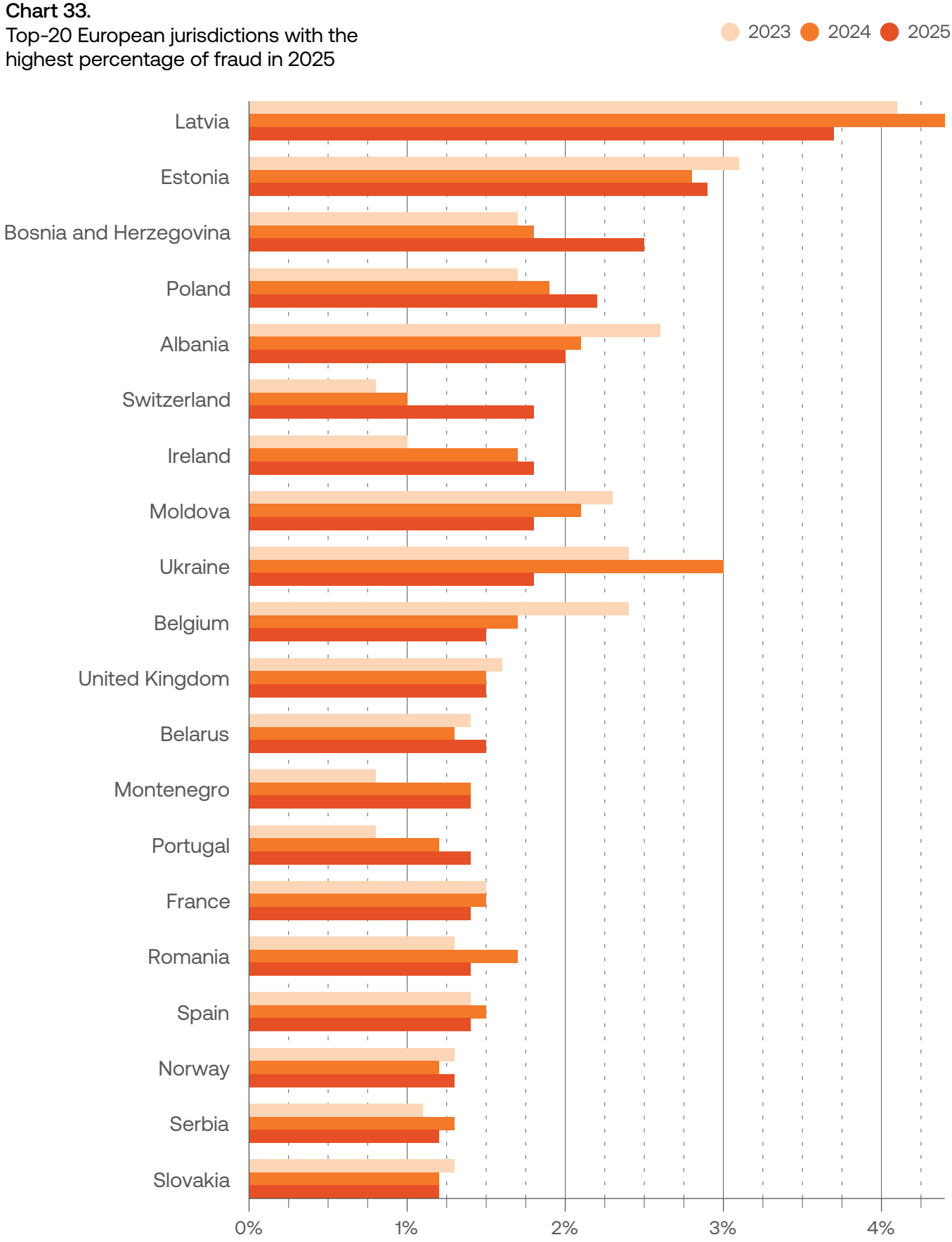
Persistence strategies grow.
Categories like liveness bypass and template-based fraud expanded, reflecting systematic probing by fraud rings that test multiple document sets and exploit weaknesses in liveness workflows.

Document tampering makes a comeback—a uniquely European trend.
Unlike other regions where physical forgeries are steadily declining, Europe saw a resurgence in forged and edited IDs in 2025, together representing over 15% of all fraud cases. This reversal stands out globally. It reflects the continent's highly standardized identity ecosystem—where AI-generated deepfakes now coexist with increasingly sophisticated document edits crafted to bypass automated screening.

In markets with strong digital ID adoption, fraudsters are deliberately returning to classic manipulation tactics, exploiting gaps in optical character recognition and template-based verification. As verification systems focus more on facial biometrics and liveness, attackers have rediscovered that subtle tampering of genuine ID templates—fonts, micro-text, holograms—can still trick AI models trained primarily on synthetic content.

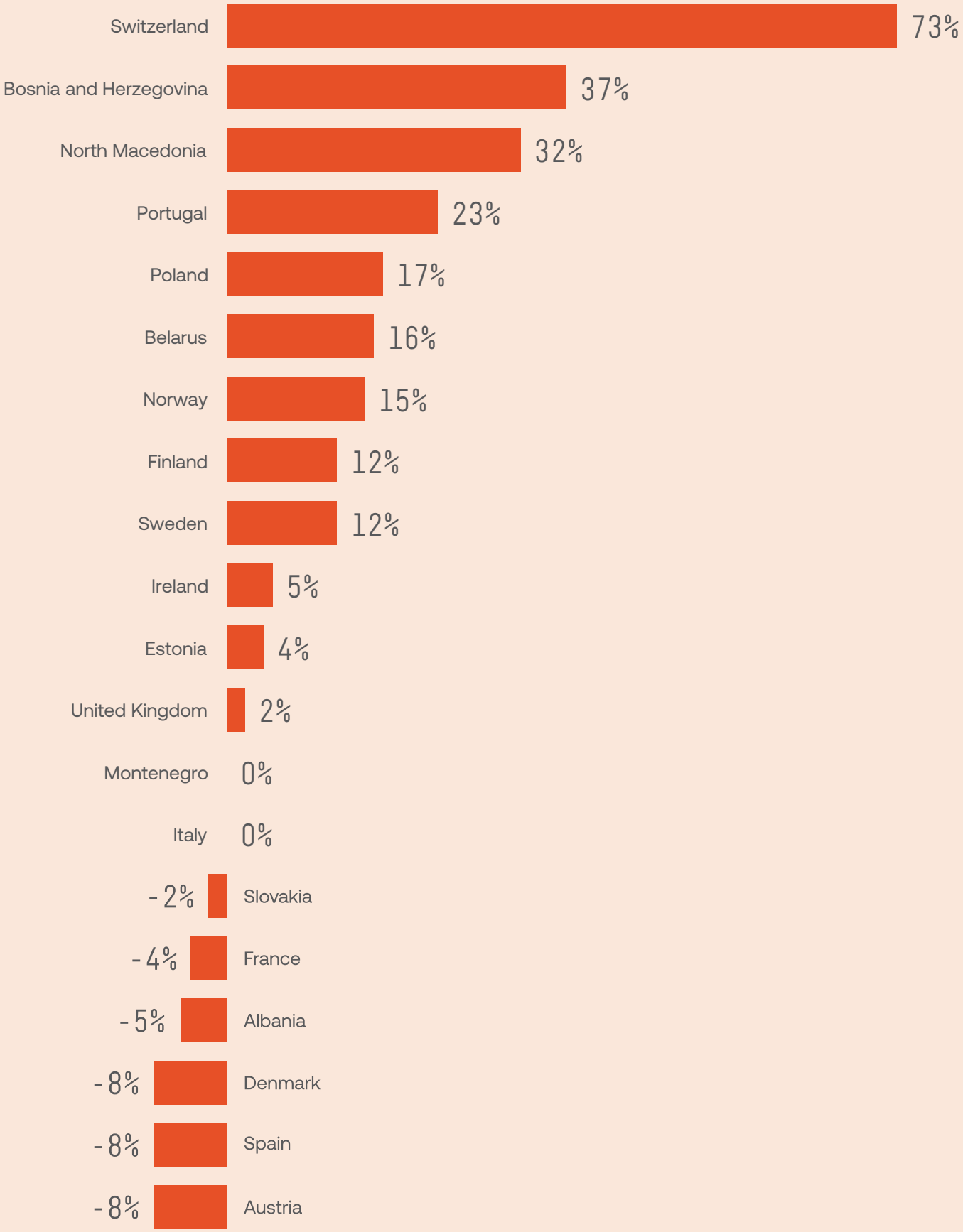
This European pattern underscores a wider truth: even in mature markets, fraud adapts to the dominant control method. As Europe invests in AI-driven detection, fraudsters are countering with higher-quality manual and hybrid document edits designed precisely to slip past machine vision.

Chart 33.
Top-20 European jurisdictions with the highest percentage of fraud in 2025



% of fraud in all analyzed verifications by jurisdiction

Chart 34.
Top-20 European countries with the largest fraud growth (2025 over 2024)



Country-level dynamics

Fraud rates across Europe in 2025 reveal sharp contrasts between rising hotspots and markets pulling rates down through structural defenses.

Rising hotspots

1 **Bosnia & Herzegovina rose to 2.5% (+37% YoY)**, with deepfakes exploding +588% YoY, showing the region's role as a testing ground for fraud kits.

2 **Poland climbed to 2.2% (+17% YoY)**, with deepfakes up +183% — indicating how Central Europe is becoming increasingly exposed to sophisticated identity fraud.

3 **Switzerland**, despite its robust financial system, reported 1.8% fraud rate (+73% YoY), accompanied by a 22% rise in deepfakes, a reminder that high-trust markets are not immune.

Stable but pressured

1 **Estonia** remained stable at 2.9%, a slight +4% YoY, supported by its advanced digital ID system, but still attractive to attackers experimenting with fraud automation.

3 **Ireland, at 1.8% (+5% YoY)**, is another example of a low-fraud-rate market where deepfakes are also creeping in (+2%).

3 **The United Kingdom reported a rate of 1.5% (+2% YoY)**, while deepfake attempts increased by 94%, indicating that while overall fraud remains relatively flat, sophistication is on the rise.

Falling markets

1. **Ukraine dropped to 1.8%**, down 41% year-over-year, as fraud shifted away due to tightened onboarding controls with Diia digital ID. Still, deepfakes grew by +82%, proving attackers are adapting.
2. **Latvia declined to 3.7% (–16% YoY),** while Moldova also fell to 1.8% (–16% YoY). Both declines reflect new supervisory rules in the payments sector.
3. **France remained flat at 1.4% (–4% YoY),** but deepfake attempts nearly doubled (+96%).
4. **Spain's decrease was slight, at 1.4% (–8% YoY)**, although deepfakes grew by 84%, revealing the same paradox: volume declines while sophistication rises.

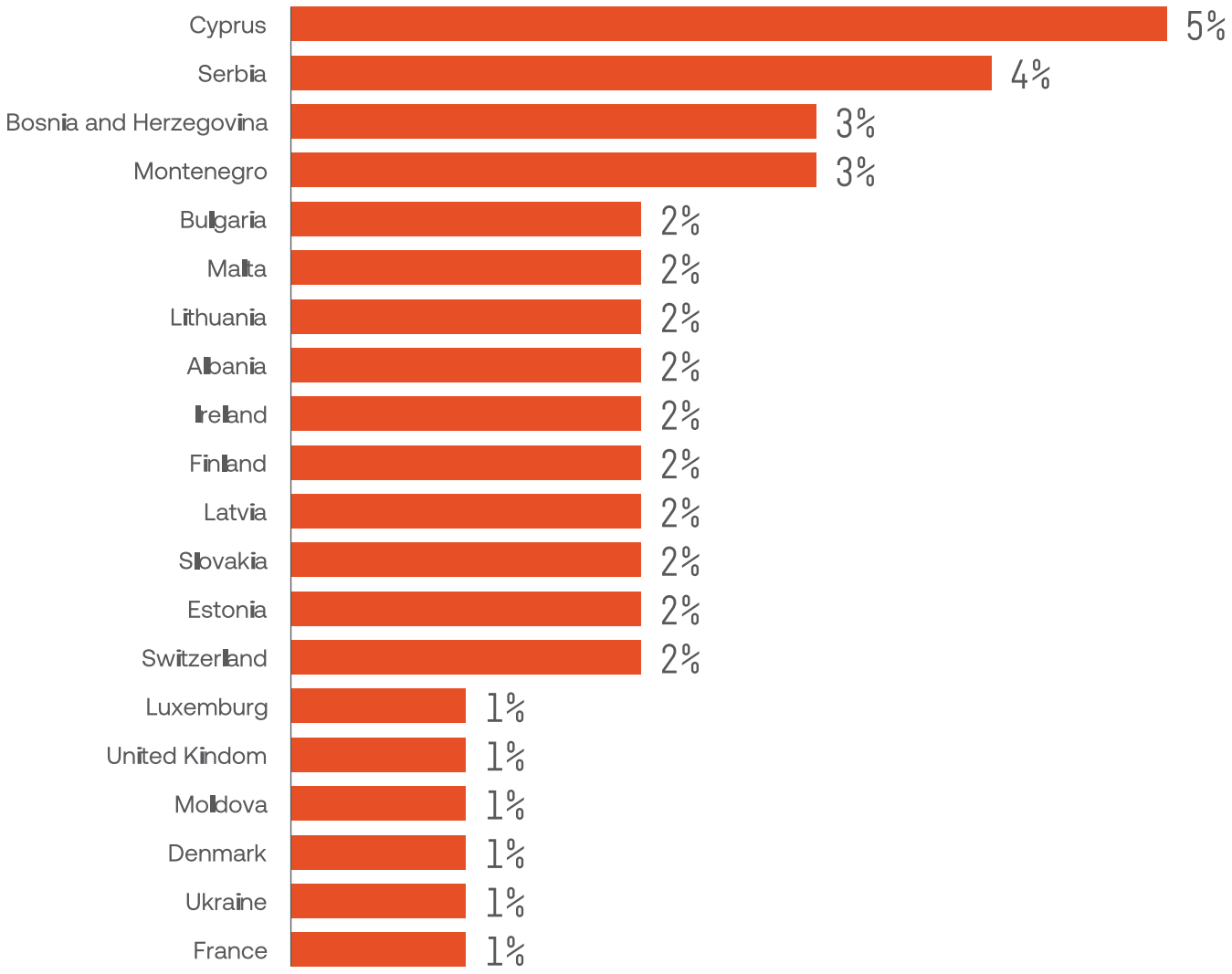
Low-fraud but rising sophistication markets

1. **Belgium fell to 1.5% (–12% YoY)**, with deepfakes up +121%.
2. **Germany fell to 0.9% (–8% YoY)** — one of the lowest rates in Europe — driven by the rollout of stronger AML supervision under the new Federal Office to Combat Financial Crime (BBF) and stricter verification under the EU's AML Package. However, deepfake (+53% YoY growth) and synthetic identity attempts are on the rise, particularly in the crypto and fintech onboarding sectors, signaling that even Europe's most compliant markets are not immune to AI-enabled deception.
3. **Norway stood at 1.3% (+15% YoY),** while deepfakes grew modestly (+17%).

4 **Sweden's rate edged down to 1.1%**, but deepfakes climbed by +75%.

5 **Italy (1.2%, stable), Finland (1.2%, +12%), and Portugal (1.4%, +23%)** show minor shifts but similar underlying patterns: fraud volume is controlled, but deepfakes are quietly expanding.

Chart 35.
Top-20 jurisdictions with the highest ratio of approved applicants involved in fraud networks



Deepfakes in Europe: creeping up

The data also shows how deepfake fraud is scaling rapidly across the continent:

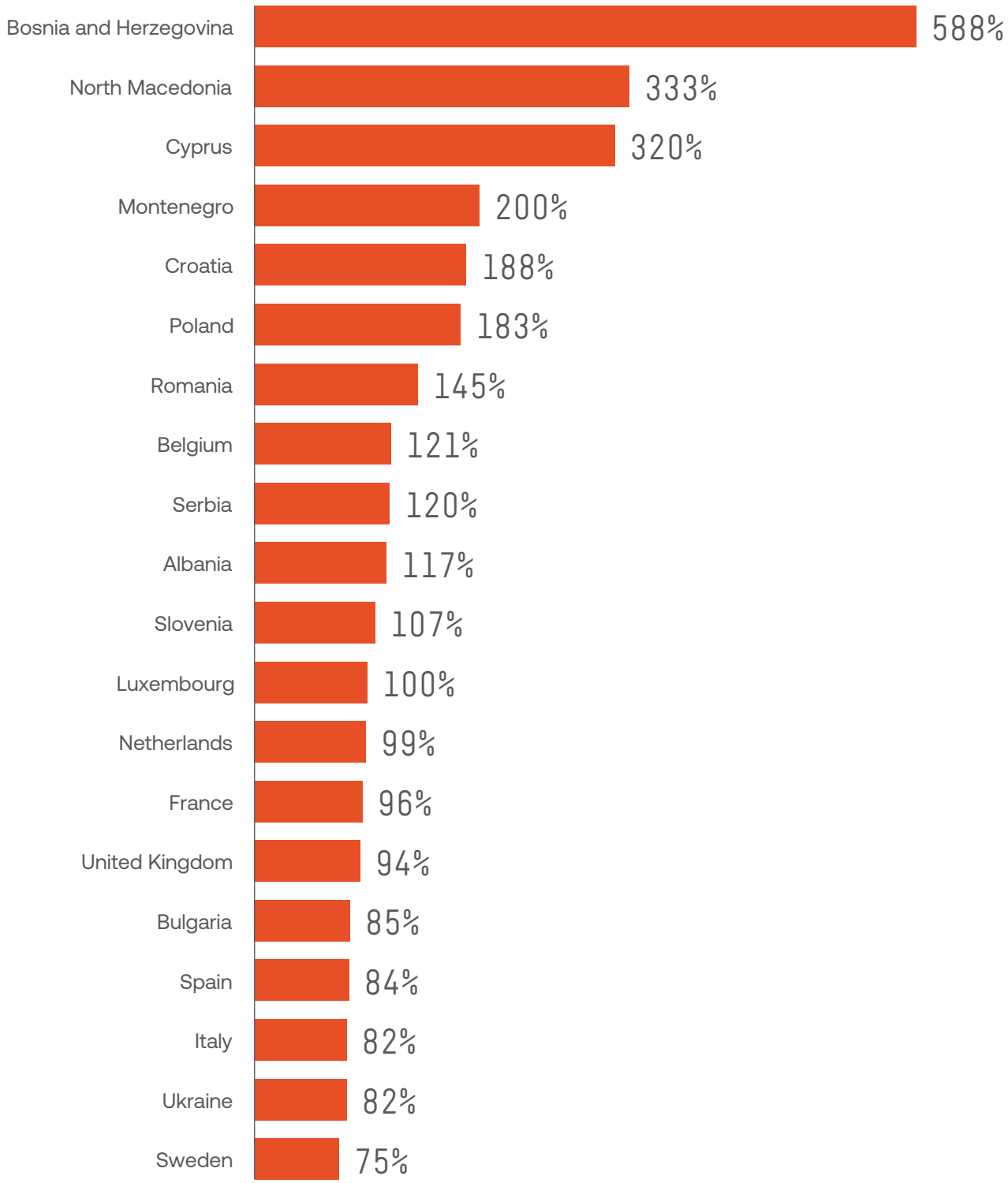
1. **Poland and Albania** both saw triple-digit growth in deepfake attempts.
2. **Bosnia & Herzegovina** recorded a staggering +588% YoY increase in deepfakes, albeit from a small base.
3. **Switzerland**, despite its traditionally low levels of fraud, also saw a significant growth in deepfake usage.

Even in countries with declining overall fraud rates, deepfakes are quietly becoming the weapon of choice, reshaping the risk landscape beneath the surface.

58% have encountered deepfakes, confirming that AI-generated media has become an integral part of everyday online life. Most see it passively — online or shared by others — while only 8% report being directly targeted or deceived, showing that exposure currently outweighs direct harm. Still, the 23% who've never encountered a deepfake — alongside 20% unsure if they have — reveal growing confusion about what's real, not just risk of deception.

Question:
Which of these best describes your experience with deepfake videos or audio?
Sumsub's Fraud Exposure Survey 2025, Europe: Consumers

Chart 36.
Top-20 European countries with the largest YoY deepfakes growth (2025 over 2024)



Why some countries fell while others rose

Europe's divergence primarily stems from differences in regulation and the focus on attackers. Countries with strong digital ID frameworks and harmonized AML/KYC standards (Nordics, France, Spain) succeeded in pushing down fraud volumes. Meanwhile, smaller or transitional economies in Eastern and Southeastern Europe became testing grounds for fraud kits, especially those built around deepfakes and synthetic identities.

Cross-border rings play a decisive role: once stricter regimes close off opportunities in Western Europe, attackers shift to softer markets where controls are weaker. This explains why fraud decreased in some EU markets but increased in neighboring countries just outside the EU's regulatory core.

What to expect next

Looking ahead, Europe will remain a mixed picture:

1. **Deepfakes will shift from the edge to the center.**
   They remain a minority of fraud in most countries, but growth rates of 200–500% in several markets indicate that this trend is changing rapidly.

2. **Synthetic identity fraud will expand.**
   With fake data already accounting for 15% of fraud in the region, it is expected to spread further into financial services, e-commerce, and iGaming.

3. **Fraud rings will keep exploiting gaps.**
   Cross-border coordination, duplicate submissions, and recycled synthetics will continue to be common, especially in smaller markets where verification pipelines are lagging.

4. **Regulation will tighten further.**
   The EU's AI Act and eIDAS 2.0 will introduce stricter requirements for identity verification and AI-generated content; however, fraudsters are likely to adapt more quickly in jurisdictions outside the EU's direct reach.

Aarti Samani,
Founder at Shreem
Growth Partners

"2025 marked the first time AI-enabled operations were openly used as instruments of warfare. Deepfake and generative technologies became tools to weaken financial and critical infrastructure, gather intelligence, and shape public perception. In parallel, fraud networks began experimenting with AI agents to research, craft, and deliver believable narratives for social engineering. These proved alarmingly effective at scale. Beneath it all, economic pressure gave rise to a new vulnerability: identity surrogates. Ordinary citizens, often unaware of the risk, rented their verified credentials to online networks that repurposed them for fraud. Together, these trends show how deeply AI has penetrated the mechanics of cyber attacks. This is now an issue of resilience. How quickly can we strengthen human judgement, organisational readiness, and post-attack recovery.

In 2026, identity verification will evolve across three dimensions. First, identity risk scoring. We will move from binary pass–fail checks to probabilistic trust intelligence that measures how real or synthetic an entity might be. Second, reciprocal identity verification. As AI agents proliferate, both humans and machines will need to prove authenticity before trust is established. Third, the human-layer threat surface. Deepfake technology has turned social engineering into an enterprise. Awareness training, cognitive resilience and DEFCON-style readiness will become part of mainstream threat modelling. The next phase of verification includes faces and documents, but it also includes verification of our AI agents, our biases, and our belief systems."

Global challenge, local realities

Discover Europe's performance in Sumsub's Fraud Exposure Survey 2025.

Companies

51%

European businesses have fallen victim to fraud in 2025

Consumers

58%

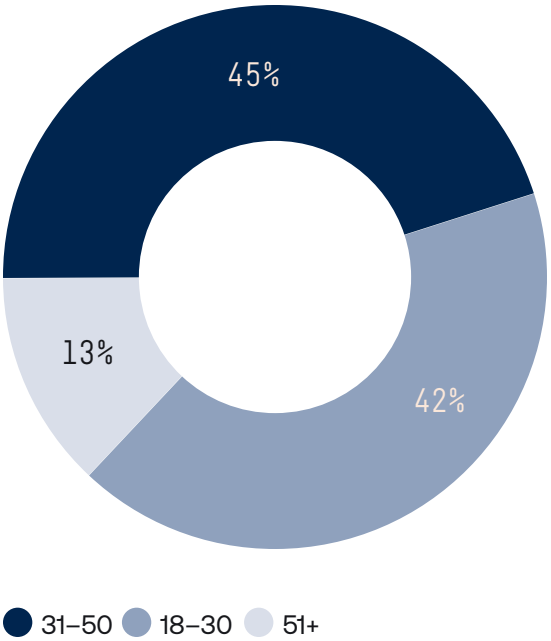
End users in Europe have fallen victim to fraud at least once in 2025

Consumer fraud findings in Europe

Take a closer look at who our Europe-based consumers are, from their age to employment status.

Chart 37.

Age



Employment status

73%
Employed full-time

13%
Employed part-time

7%
Self-employed full-/part time

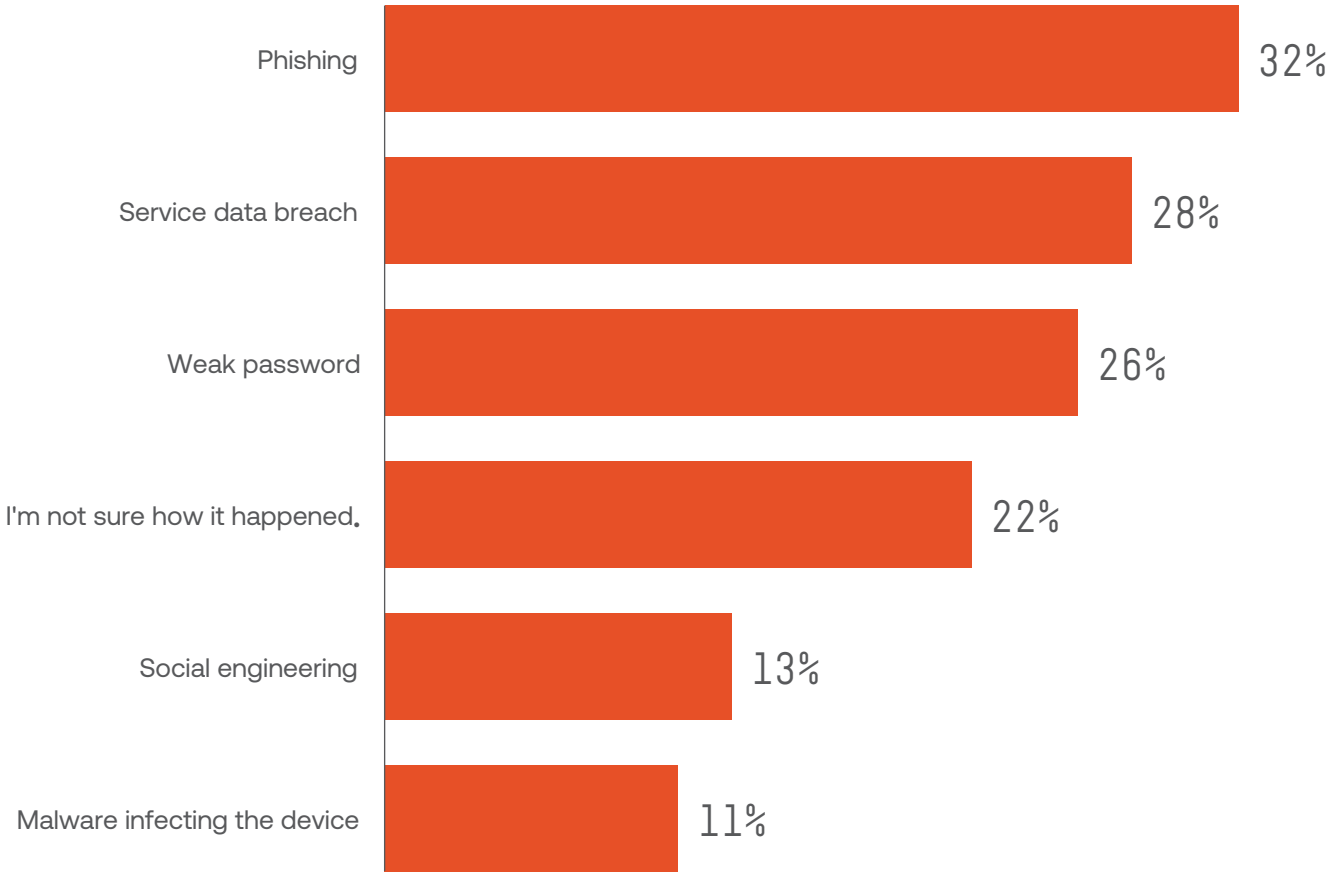
7%
Temporarily unemployed

Main attack vectors

Phishing remains the top attack vector (32%), proving that social manipulation continues to outperform technical exploits. Yet, weak passwords (26%) show that poor credential hygiene still fuels a large share of preventable incidents — a risk entirely within user control.

At the same time, service data breaches (28%) highlight growing systemic exposure, where even cautious users can be affected by platform-level failures. The 22% of respondents unsure how their data was compromised suggests that fraud methods are becoming stealthier, often blending human and technical attack paths.

Chart 38.
Question:
What do you think was the cause of the fraud incident?



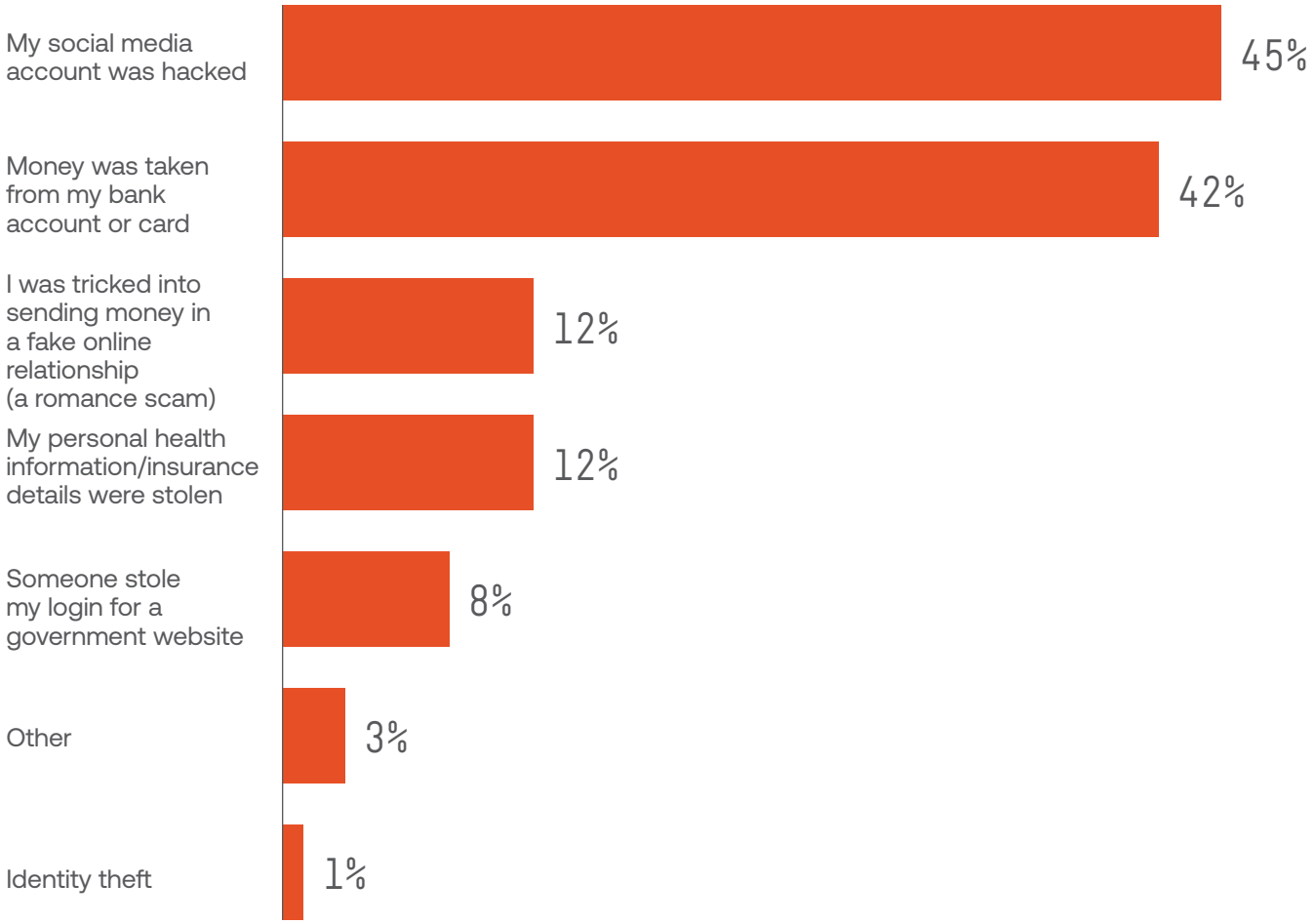
Sumsub's Fraud Exposure Survey 2025, Europe: Consumers

Main fraud outcome

The majority of fraud victims report direct account compromise, with social media (45%) and banking or card theft (42%) being the most common forms.

This suggests that fraudsters are now targeting both the financial services accounts and digital identities of their victims, exploiting personal networks and simultaneously accessing funds.

Chart 39.
Question:
What type of identity fraud did you experience?



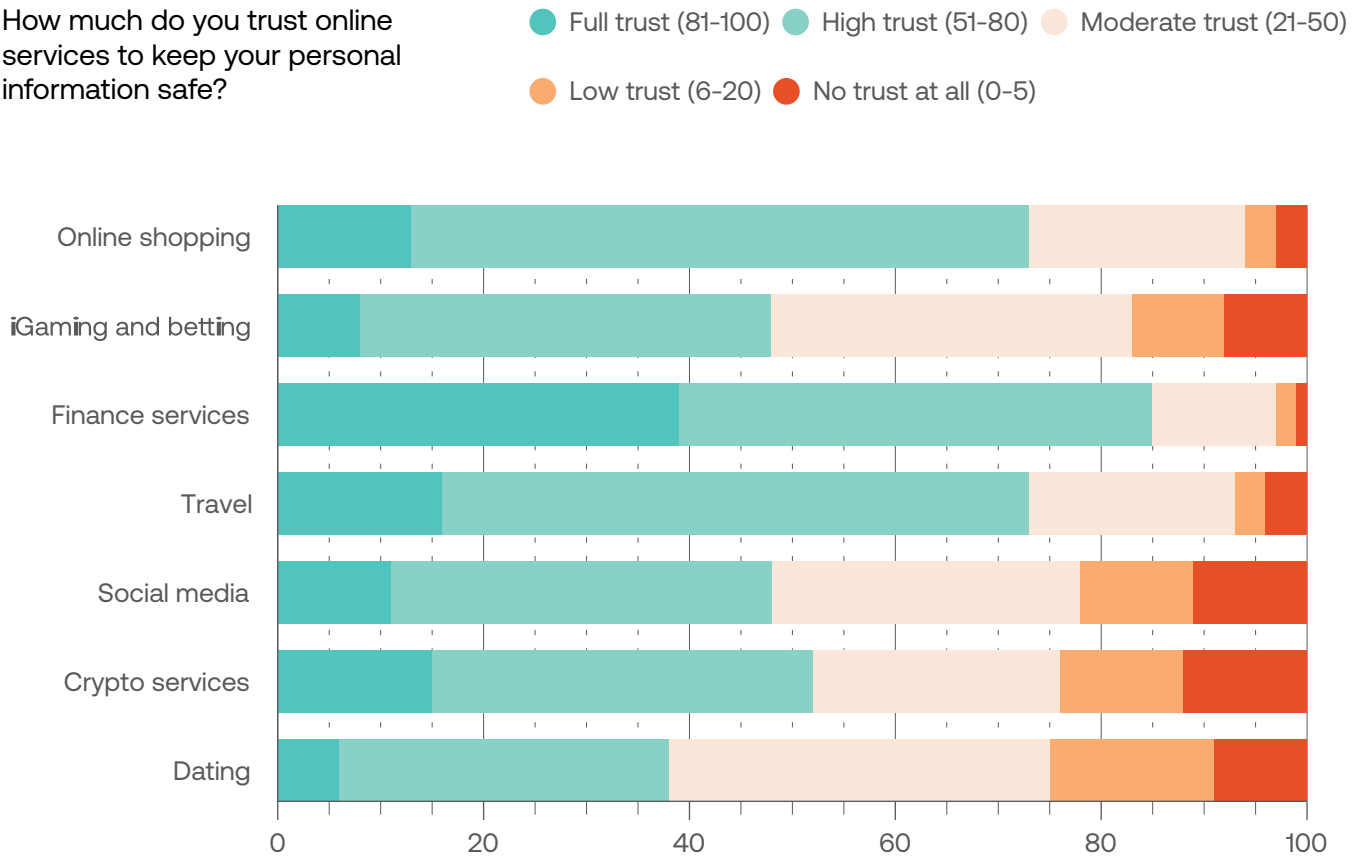
Sumsub's Fraud Exposure Survey 2025, Europe: Consumers

Digital trust in Europe

Finance (87% high or full trust), online shopping and travel services (74% each) remain the most trusted sectors, reflecting strong regulation, recognizable brands, and visible security measures.

In contrast, crypto (52%), social media (49%), and dating platforms (38%) struggle to gain user confidence, with double-digit “no trust” rates signaling ongoing concerns about data misuse, scams, and weak verification controls.

Chart 40.
Question:
How much do you trust online services to keep your personal information safe?



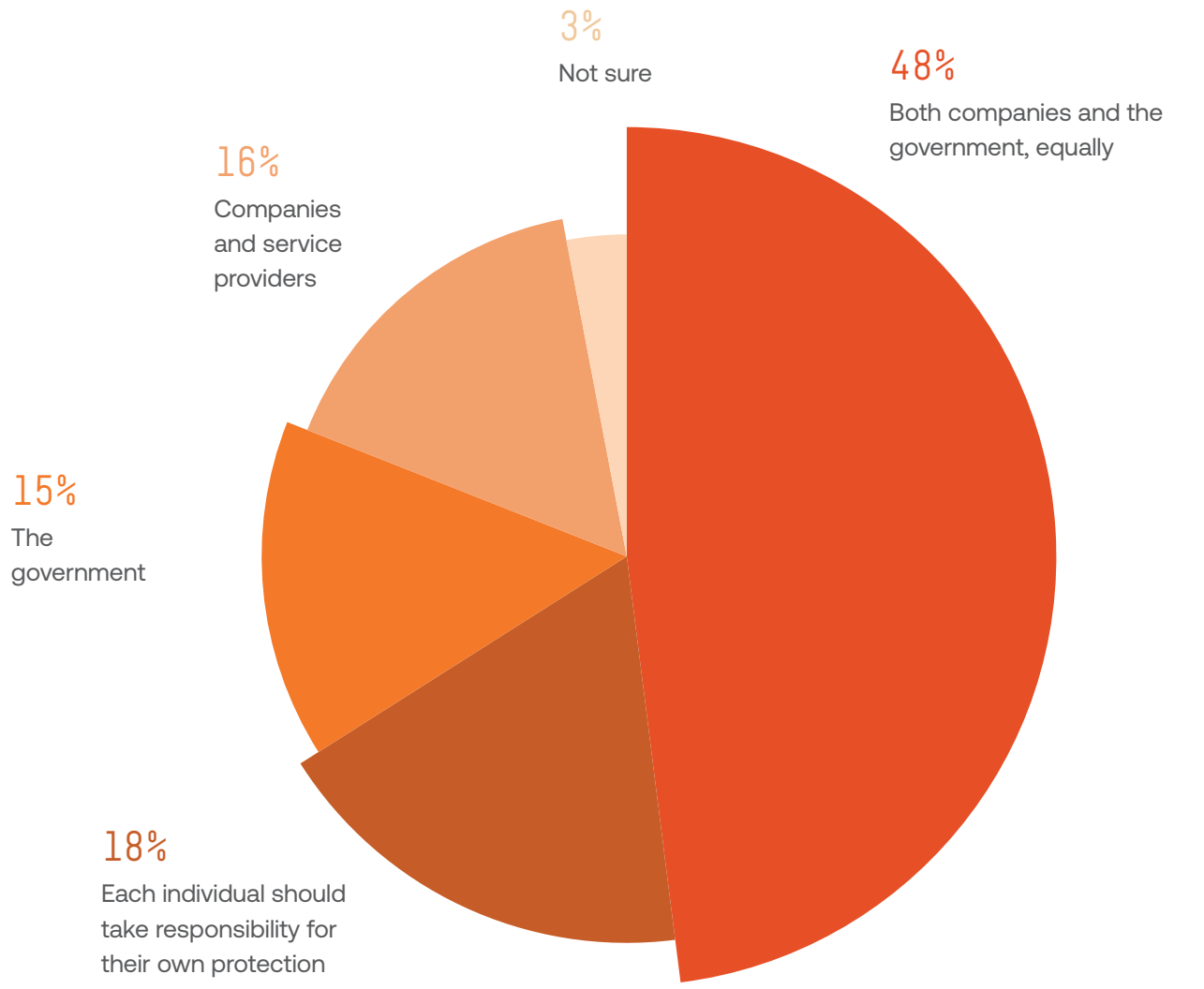
Sumsub’s Fraud Exposure Survey
2025, Europe: Consumers

81% of respondents would choose a service provider only if they have strong anti-fraud measures in place.

Responsibility for fraud prevention

48% of respondents believe companies and the government should share responsibility for fraud protection equally. 18% believe each person should protect themselves and 16% think companies should take the lead. 15% of respondents support this being a government-only responsibility.

Chart 41.
Question:
Who do you think should take the lead in keeping people safe from fraud?



Sumsub's Fraud Exposure Survey 2025, Europe: Consumers

Rising awareness of payment security

Nearly 60% of respondents use disposable or virtual cards at least occasionally, indicating a growing awareness of digital payment security and privacy protection. However, with 24% never using them and another 14% rarely doing so, a large share of consumers still rely on traditional card payments.

Question:
Do you use disposable or virtual cards for online payments?

Sumsub's Fraud Exposure Survey 2025, Europe: Consumers

The gap around money muling

Nearly 9 in 10 respondents either don't know or only vaguely understand what money muling is, showing a major awareness gap in financial crime education. This lack of understanding leaves many users vulnerable to manipulation, particularly through social media or gig-style recruitment scams that masquerade as legitimate work.

At the same time, 13% report being directly targeted, suggesting lower active mule recruitment in Europe compared to others.

Question:
Have you heard of "money muling" - letting someone move stolen money through your bank account?

Sumsub's Fraud Exposure Survey 2025, Europe: Consumers

74% of respondents are highly convinced that fraud is becoming more sophisticated and AI-driven.

This confirms that companies are aware of deepfake risks, synthetic identities, and AI-driven forgeries, and are looking for next-generation fraud prevention solutions.

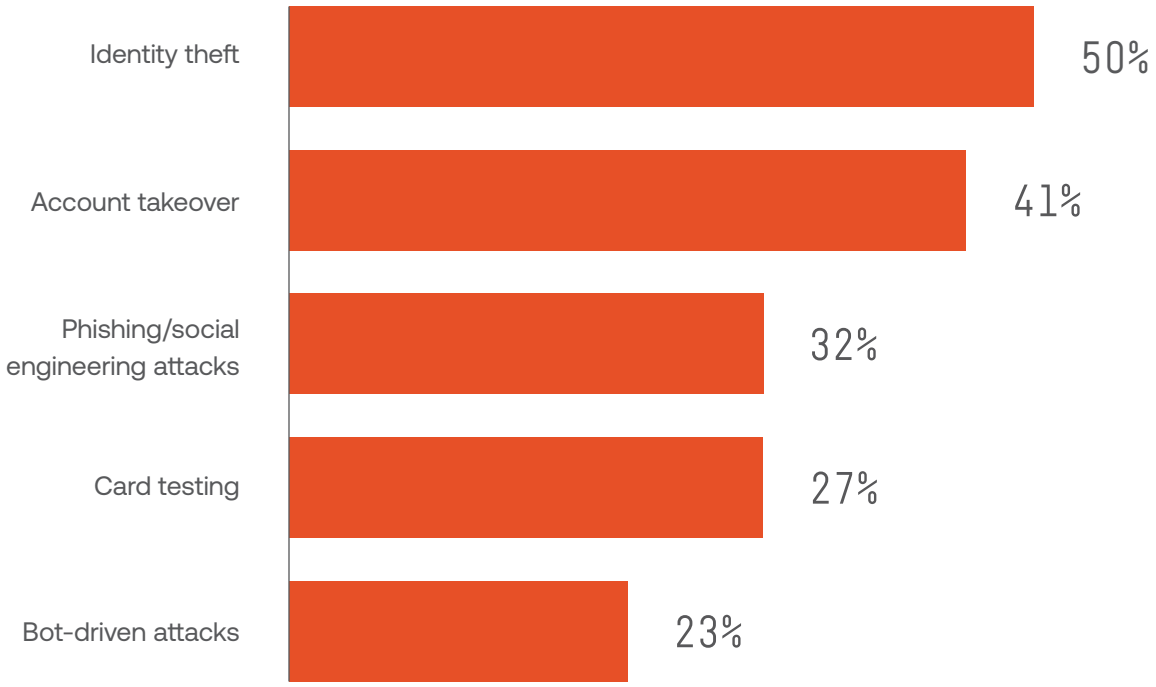
Company fraud findings in Europe

Top 3 types of fraud faced by companies in Europe

1 Identity theft (50%)
2 Account takeover (41%)
3 Phishing/social engineering attacks (32%)

At the same time, they had to manage first-party fraud from their customers, who used synthetic identity (36%) and deepfakes (18%) and conducted application and chargeback abuse (36% of cases, respectively).

Chart 42.
Question:
What kind of third-party fraud has your business faced?



Sumsub's Fraud Exposure Survey 2025, Europe: Companies

55% report that organized fraud attempts have become more frequent.

At the same time, 3% see no change, indicating that not every sector has observed escalation.

Major consequences companies have experienced as a result of fraud attacks:

1. Financial losses (64%)
2. Reputational damage (36%)
3. Operational disruption (36%)

How European companies manage fraud

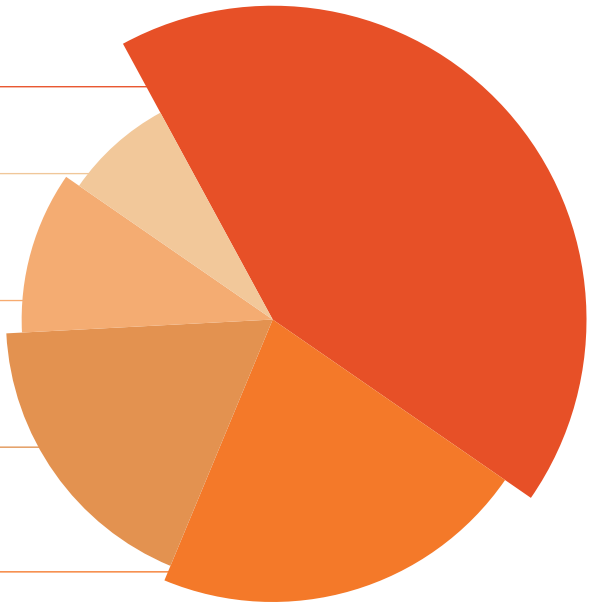
Nearly half of businesses (49%) now employ a hybrid fraud prevention model, combining in-house expertise with external vendor solutions — a sign that organizations are increasingly valuing control and flexibility while leveraging specialized tools for detection and automation. However, **manual processes remain high (37%)**, suggesting many teams still rely on human review and fragmented systems, which can slow response times and increase operational costs.

Meanwhile, only 19% fully rely on in-house technology, and 26% depend entirely on external providers, indicating that most businesses are still searching for the right balance between internal ownership and outsourced efficiency.

57% of respondents reported fraud incidents to industry regulators first, and only 29% contacted the police for investigation. This means that most businesses initially treat fraud as a compliance issue and only consider it a criminal investigation issue second.

6 in 10 support stricter regulations, even if operations become more complex.

Chart 43.
Question:
Did your business report incidents of identity fraud to authorities or institutions



Sumsub's Fraud Exposure Survey 2025, Europe: Companies

Predictions for the future

AI-driven fraud will dominate

- → 72% expect more sophisticated attacks using AI
- → 58% expect increased use of deepfake technology for scams
- → 53% expect AI-generated fake documentation/profiles

Identity-based fraud risks will grow

- → 54% expect a rise in identity theft due to breaches
- → 51% predict wider use of synthetic identities to bypass KYC
- → 37% expect more digitally forged/tampered identity documents
- → 40% expect more fraud targeting biometric systems
- → 47% foresee more organized fraud rings
- → 49% predict businesses will focus more on cybersecurity
- → 42% expect stricter government regulations
- → Only 14% believe fraud will decrease due to improved technology and awareness

72%

expect more sophisticated attacks using AI

58%

expect increased use of deepfake technology for scams

53%

expect AI-generated fake documentation/ profiles

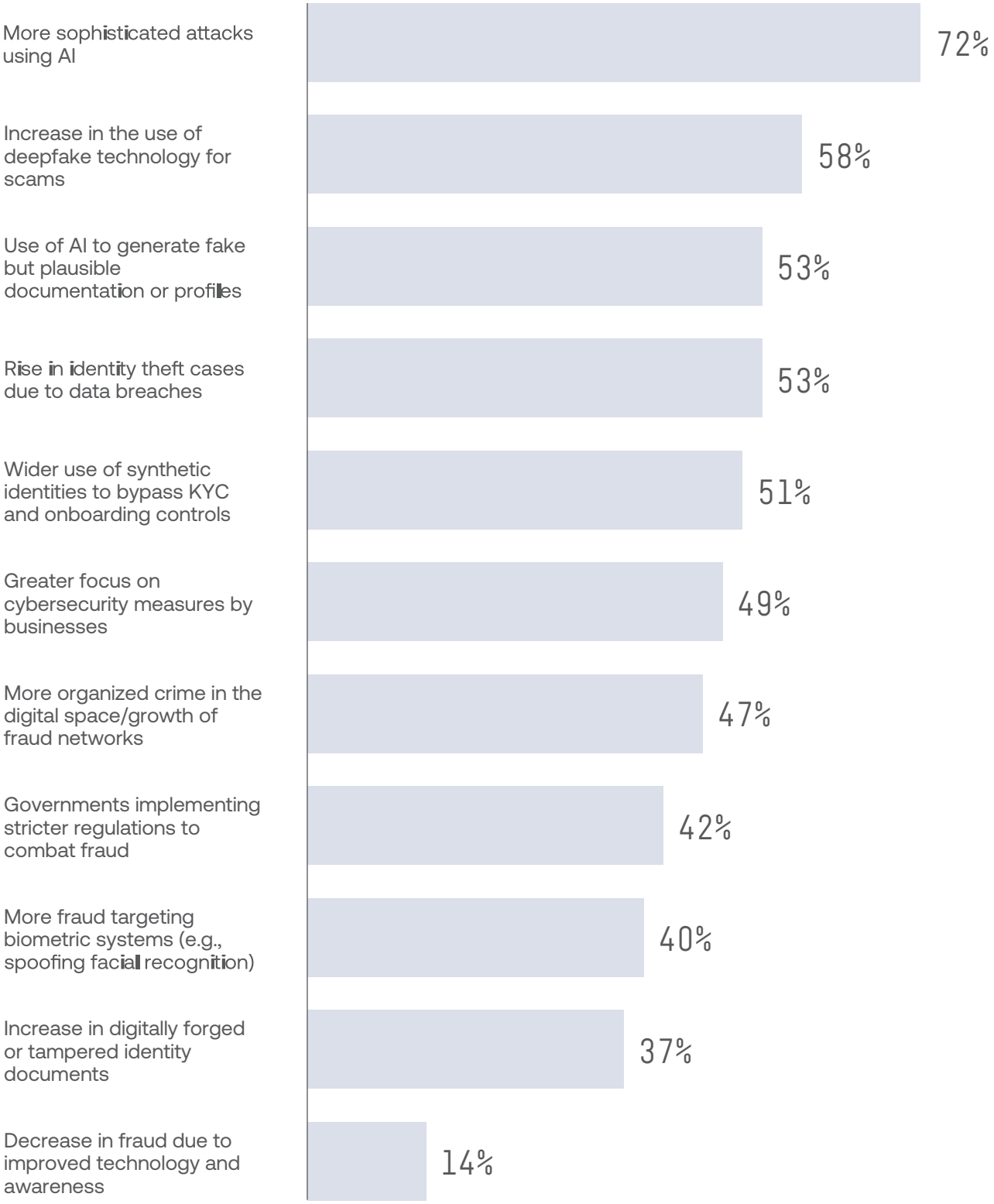


Chart 44.
Question:
What are your predictions for the future of the fraud landscape?

Sumsub's Fraud Exposure Survey 2025, Europe: Companies

Regulatory shifts redefining identity protection

As fraud becomes more complex, European authorities are reinforcing compliance through expanded AML and data protection mandates, alongside increased regulatory alignment across the EU. Here are some of the latest developments in Europe.

France

Velocity thresholds on non-3DS payments

On 18 April 2025, the Banque de France's Observatoire de la Sécurité des Moyens de Paiement (OSMP) issued new fraud-prevention recommendations on remote card payments outside 3-D Secure. Velocity thresholds for non-3DS transactions were progressively reduced—from €100 in October 2024 to €1.01 by May 2025, with a possible cut to €0.01 from January 2026. Once exceeded, issuers must either soft decline or require 3DS. Specific obligations also apply to "priority merchants" and to MOTO transactions. Though framed as recommendations, these thresholds operate as supervisory expectations enforced by the ACPR, directly targeting one of France's highest fraud vectors.

New payment and cyber-resilience rules

The EU Instant Payments Regulation (IPR), effective 9 October 2025, will require all Eurozone PSPs to perform Verification of Payee checks for instant and standard SEPA transfers, reducing misdirected and fraudulent payments. The Digital Operational Resilience Act (DORA), which enters into force on 17 January 2025, obliges financial entities to classify, detect, and report major ICT incidents, and to maintain robust continuity and cyber risk controls. Together, these measures significantly enhance fraud prevention by integrating identity checks into payment processes and improving incident response readiness.

Germany

BaFin AML guidance

On 29 November 2024, BaFin published updated Interpretation and Application Guidance (AuA), tightening AML and fraud prevention obligations. The guidance mandates shorter KYC review cycles, stronger ongoing due diligence, and explicitly brings agents and e-money agents into scope. While agents are exempt from appointing an AML officer unless required to do so, they must now enhance their risk assessments, documentation, and reporting of suspicious transactions. These measures close loopholes often exploited by intermediaries and harmonize fraud detection across the payments chain.

EU AML package implementation

From 2024 to 2025, Germany has been implementing the EU's new AML Package, comprising the 6th AML Directive (6AMLD), directly applicable AML Regulation (EU 2024/1624), and the creation of the Anti-Money Laundering Authority (AMLA), headquartered in Frankfurt. The reforms harmonize AML/CFT rules across the EU, expand beneficial ownership transparency, and mandate stricter customer due diligence and monitoring. AMLA will directly supervise high-risk cross-border institutions, closing gaps in enforcement and strengthening the detection of fraud across the EU.

Federal Office to Combat Financial Crime
Germany's Financial Crime Prevention Act (Finanzkriminalitätsbekämpfungsgesetz, or FKBG) established the Federal Office to Combat Financial Crime, which is set to become fully operational in 2025. The BBF combines investigation, analysis, supervision, and enforcement of sanctions within a single central body. Its Money Laundering Investigation Center will adopt a "follow-the-money" approach, allowing authorities to investigate suspicious financial flows proactively rather than waiting for predicate offenses to occur. The reform significantly strengthens Germany's capacity to pursue large-scale and cross-border fraud.

MiCA and crypto fraud enforcement
In mid-2024, Germany enacted the Finanzmarktdigitalisierungsgesetz (FinMADiG) to implement the EU's Markets in Crypto-Assets Regulation (MiCA). MiCA introduces strict governance, disclosure, reserve, and conduct requirements for crypto-asset service providers, embedding fraud prevention into the licensing process. Parallel BaFin enforcement highlights persistent fraud risks at the market's edges: in 2024–2025, authorities dismantled unlicensed crypto ATMs, issued alerts against unauthorized AI "trading bots," and warned about impersonation scams on WhatsApp and fake trading websites. This two-pronged strategy combines preventive regulation with aggressive enforcement against fraudulent crypto activity.

Netherlands

Instant payments regulation

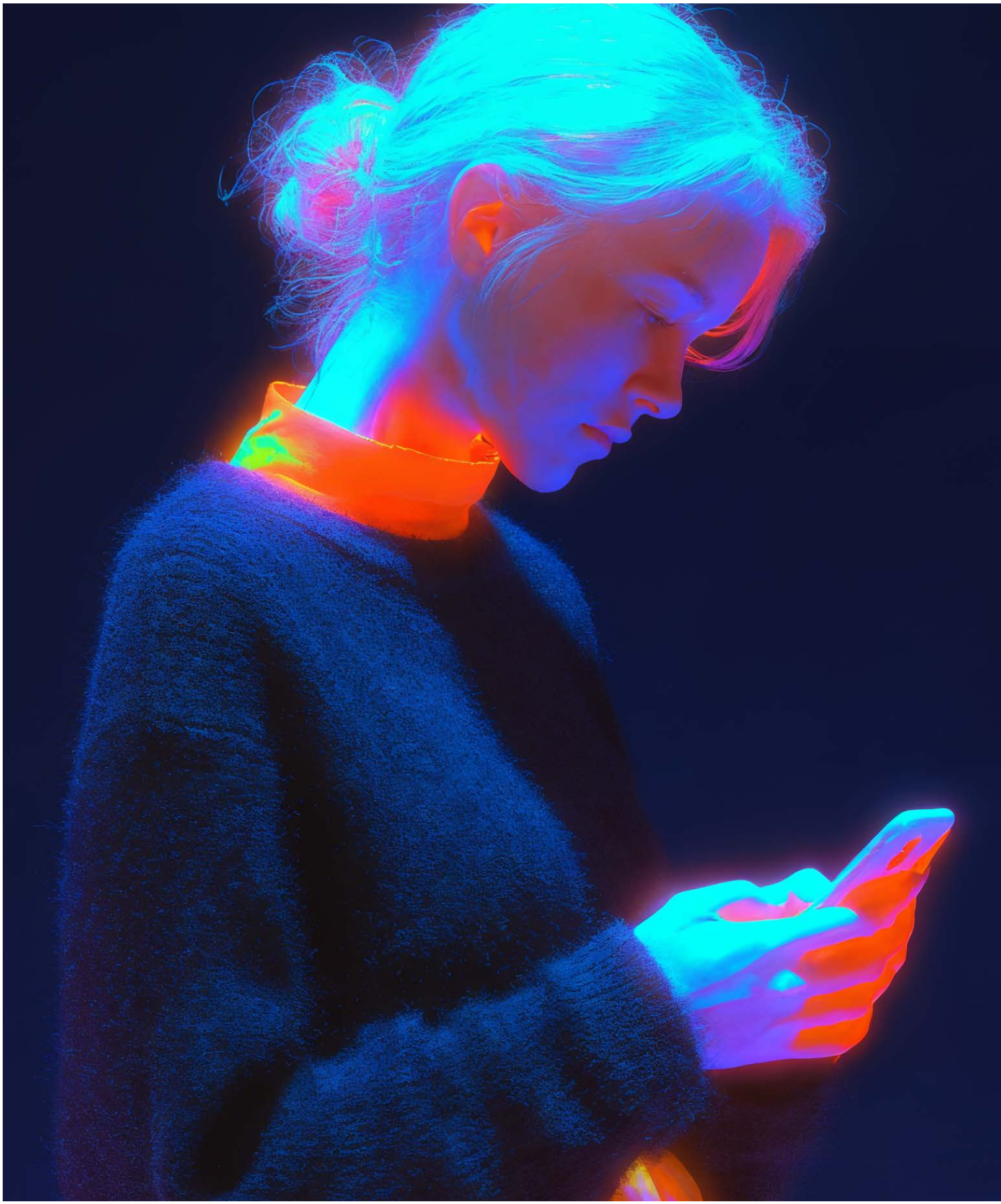
From January 2025, the Netherlands began implementing the EU Instant Payments Regulation, requiring all PSPs to introduce Verification of Payee services for SEPA transfers by October 2025. The service ensures that payer and payee names, as well as IBANs, match before execution, thereby reducing APP fraud and misdirected transfers. PSPs are also subject to daily sanctions screening and enhanced monitoring obligations.

Cash payment limit

On 18 June 2025, the Money Laundering Action Plan Act (Bill 36 228) amended the Wwft to prohibit cash payments of €3,000 or more for professional and commercial traders. The cap targets laundering and fraud in cash-heavy sectors, such as luxury goods and real estate, by limiting anonymous transactions and enhancing the detection of suspicious activity.

PSD3 and PSR proposals on fraud liability

The EU's proposed Payment Services Regulation (PSR) and PSD3, expected to reshape payment services law, will increase liability for PSPs in fraud cases, particularly where Strong Customer Authentication or payee verification is not properly implemented. The proposals also expand refund rights for impersonation and spoofing fraud, unless the PSP can demonstrate gross negligence or customer complicity. These reforms foreshadow greater emphasis on fraud analytics, transaction monitoring, and consumer protection obligations across the EU.



Spain

Anti-fraud law and e-invoicing reforms

Spain's Law 11/2021 (Anti-Fraud Law), reinforced by Royal Decree 1007/2023, mandates the use of certified invoicing software ("SIF/VeriFactu") with strict audit trails to prevent manipulation. Ministerial Order HAC/1177/2024, published in October 2024, set technical specifications for software vendors. Deadlines require corporate taxpayers to comply by January 1, 2026, and small businesses and self-employed individuals by July 1, 2026. These measures close off avenues for invoice fraud, shadow accounting, and dual bookkeeping.

Instant payments regulation

Under the EU Instant Payments Regulation, all Eurozone PSPs must provide free Verification of Payee services by 9 October 2025, ensuring recipient details are checked before payments are sent. The regulation also requires daily sanctions screening in instant payment flows, reducing risks of APP fraud and payments to sanctioned entities.

Telecom anti-fraud rules

On June 7, 2025, Spain enacted new telecom rules banning commercial calls from mobile numbers and requiring operators to block spoofed international calls and SMS messages. In the first months of enforcement, 14 million fraudulent calls were blocked. The measures directly target phishing, APP fraud, and identity theft linked to telecom impersonation, shutting down a major fraud vector.

UK

Failure to Prevent Fraud offense
From 1 September 2025, the new "Failure to Prevent Fraud" offense under the Economic Crime and Corporate Transparency Act 2023 will make large organizations criminally liable if an associated person (such as an employee, agent, or subsidiary) commits fraud for the organization's benefit and the company lacks "reasonable prevention procedures." To rely on the statutory defense, firms must evidence documented controls, fraud risk assessments, staff training, and ongoing monitoring. This reform significantly raises compliance expectations, placing fraud prevention on par with anti-bribery and tax evasion obligations.

HM Treasury Consultation on money laundering regulations
Between 2024 and July 2025, HM Treasury reviewed the UK's Money Laundering Regulations, publishing a response with targeted reforms. Key updates include narrowing enhanced due diligence to unusually complex or large transactions and to FATF "call for action" countries, removing pooled client accounts from simplified due diligence rules but creating a new framework with stronger recordkeeping, and clarifying obligations for non-financial firms such as estate agents, art market participants, and letting agents. The changes aim to make the AML regime more risk-based and proportionate.

FCA guidance on fraud and financial crime
In November 2024, the FCA updated its Financial Crime Guide (PS24/17), setting clearer expectations for sanctions screening and transaction monitoring. Firms must ensure monitoring systems are calibrated, tested, and auditable, with senior management directly accountable for escalation and oversight. The update signals tougher supervisory scrutiny of how quickly firms can identify and act on fraud indicators.

Draft FSMA (Cryptoassets) Order

The draft FSMA (Cryptoassets) Order 2025 will extend the FCA's regulatory perimeter to crypto trading platforms, custodians, dealers, stablecoin issuers, and staking providers. It deems activities involving UK retail consumers as being carried out "in the UK," even if they are operated overseas, bringing many offshore firms under UK oversight. Covered entities will need full FCA authorization and compliance with AML/KYC, financial promotions, and consumer protection rules. This marks a significant shift from the limited AML registration regime, closing loopholes that have been exploited by offshore and lightly regulated platforms.

Digital Identity and Attributes Trust Framework

In July 2025, the UK's Digital Identity and Attributes Trust Framework (gamma 0.4, July 2025) sets certification standards for digital ID providers. Fraud prevention is a core requirement: certified providers must conduct fraud audits, share fraud-related data, support victims of identity theft in restoring IDs, and enforce safeguards in digital wallets, including the revocation and re-verification of dormant accounts. Biometric services must also demonstrate resilience to fraud across demographics. This framework formalizes digital identity assurance as a regulated function for preventing fraud.

UK launches mandatory Digital ID to combat identity fraud and illegal working

In September 2025, the UK Government announced plans to roll out a nationwide digital ID system, which will become mandatory for Right-to-Work checks by the end of the current Parliament. The initiative aims to reduce forged document use and identity fraud while streamlining citizens' access to key government services. Designed with encryption and biometric verification, the system reflects a growing global shift toward trusted digital identities—mirroring similar frameworks in Estonia, Denmark, and India—and underscores how government-driven digital verification can strengthen fraud prevention across both public and private sectors.

Online Safety Act

The UK's Online Safety Act 2023, which received Royal Assent in October 2023, is being enforced in phases throughout 2025. From March 2025 onward, Ofcom began implementing key provisions, including duties for illegal content and risk-assessment requirements for regulated services. The Act represents one of the world's most comprehensive digital-protection frameworks, requiring online platforms, social networks, and search services to proactively assess and mitigate the risks of illegal or harmful content rather than simply react to them.

The OSA mandates robust age-assurance and identity-verification controls. By July 2025, adult-content platforms must deploy verified age-check mechanisms—such as government-ID matching, biometric facial estimation, or payment-card verification—to restrict access to minors. Ofcom's codes of practice emphasize that "highly effective" age-assurance must be embedded within user-to-user and content-sharing platforms likely to be accessed by children.

Service providers are directly liable if they fail to meet their statutory duties to prevent the dissemination of illegal or harmful material, which can include fraudulent or impersonation-based content. Ofcom, empowered as the designated regulator, may impose fines of up to £18 million or 10 percent of global turnover for non-compliance and, in cases of wilful failure to co-operate, pursue criminal liability against senior management.

For the fraud landscape, the OSA marks a pivotal evolution: age and identity checks are no longer peripheral compliance measures but core components of digital trust and user protection. As deepfakes, synthetic identities, and AI-generated content proliferate, these mechanisms now underpin platform accountability and consumer confidence.

Aligned with the UK's Digital Identity and Attributes Trust Framework, the OSA reinforces national efforts to combat impersonation, fraudulent content, and online financial scams by elevating verification standards and enhancing platform-level accountability.

Jacob Thompson,
VP of Business
Development EU&UK
at Sumsub

"Europe sits at the center of a paradox. We've tightened controls, harmonized standards, and invested in digital identity—yet fraud hasn't disappeared, it's evolved. Our 2025 data shows fraud involving inconsistencies between a user's selfie and their ID image now dominates the region, accounting for more than two in five cases and reflecting how deepfake-powered spoofing has gone mainstream. At the same time, synthetic identities have surged to around 15% of fraud, proving that attackers no longer just steal credentials—they manufacture convincing digital personas.

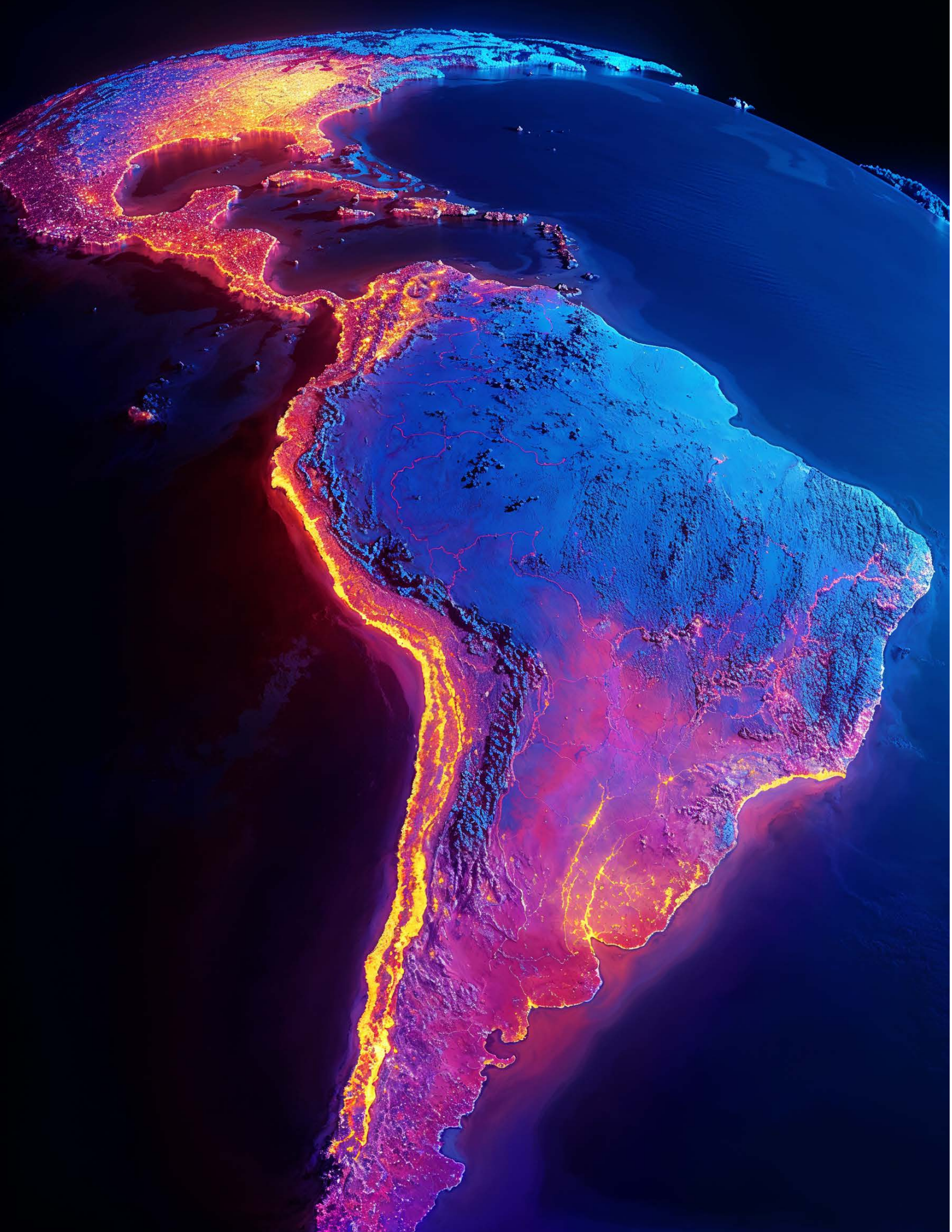
Country patterns tell the same story. The UK's overall rate is broadly flat, but deepfake attempts nearly doubled. Ukraine's headline fraud fell sharply, yet deepfakes still rose. Meanwhile, Central and Southeastern Europe—Poland, the Western Balkans—saw triple-digit deepfake growth, showing how cross-border rings shift to softer entry points as Western markets harden. This is the Sophistication Shift in action: lower volumes in some places, higher complexity almost everywhere.

The way forward is clear. Europe's regulatory backbone—AI Act, eIDAS 2.0, PSD reforms—must be matched by operational reality: multi-modal liveness, document-logic checks, behavioral analytics, and—crucially—shared intelligence that follows a synthetic identity across borders. If we connect these layers, we won't just keep pace with AI-enabled fraud—we'll raise the cost curve beyond what organized networks can sustain."

Latin America & the Caribbean

Latin America remains one of the fastest-evolving environments for fraud. Rapid expansion of digital payments, e-commerce, and remittance platforms has widened access to financial services, but it has also made the region highly attractive to fraudsters.

In 2025, LATAM showcases the Sophistication Shift clearly: crude attempts are shrinking, but AI-powered selfies, synthetics, and organized fraud rings are taking their place.



Fraud type evolution in LATAM

Fraud patterns in Latin America shifted significantly in 2025:

Selfie fraud dominates.
Fraud involving inconsistencies between a user's selfie and their ID image is the largest category, representing 42% of all fraud, although its share has declined compared to 2024. This reflects the explosive rise of deepfakes, many of which are flagged under these categories when they evade direct classification.

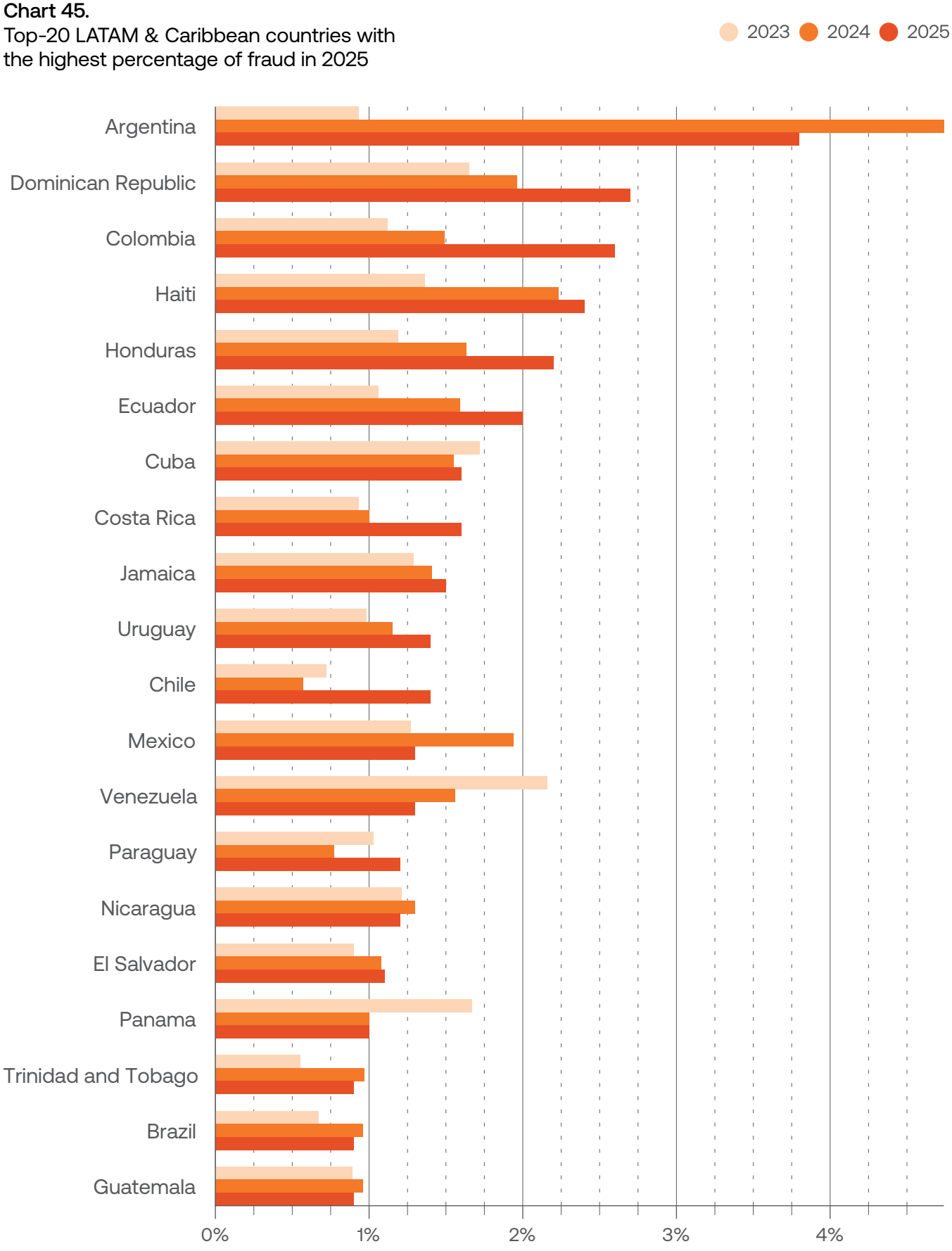
Synthetics expand rapidly.
Fake personal data increased nearly threefold year-over-year, accounting for 7.3% of all fraud. Fraudsters are creating fully fabricated digital personas (including names, addresses, and dates of birth) and combining them with fake selfies to pass onboarding checks.

Edited IDs persist, forged IDs decline.
Edited ID fraud rose slightly (+86% YoY), stabilizing at a 4.6% share, while forged IDs dropped in importance to a 2.6% share, indicating that fraudsters prefer digital manipulation over physical forgery.

Old tricks fall short.
Blocklist attempts have dropped by nearly half, confirming that basic errors can no longer evade anti-fraud filters.

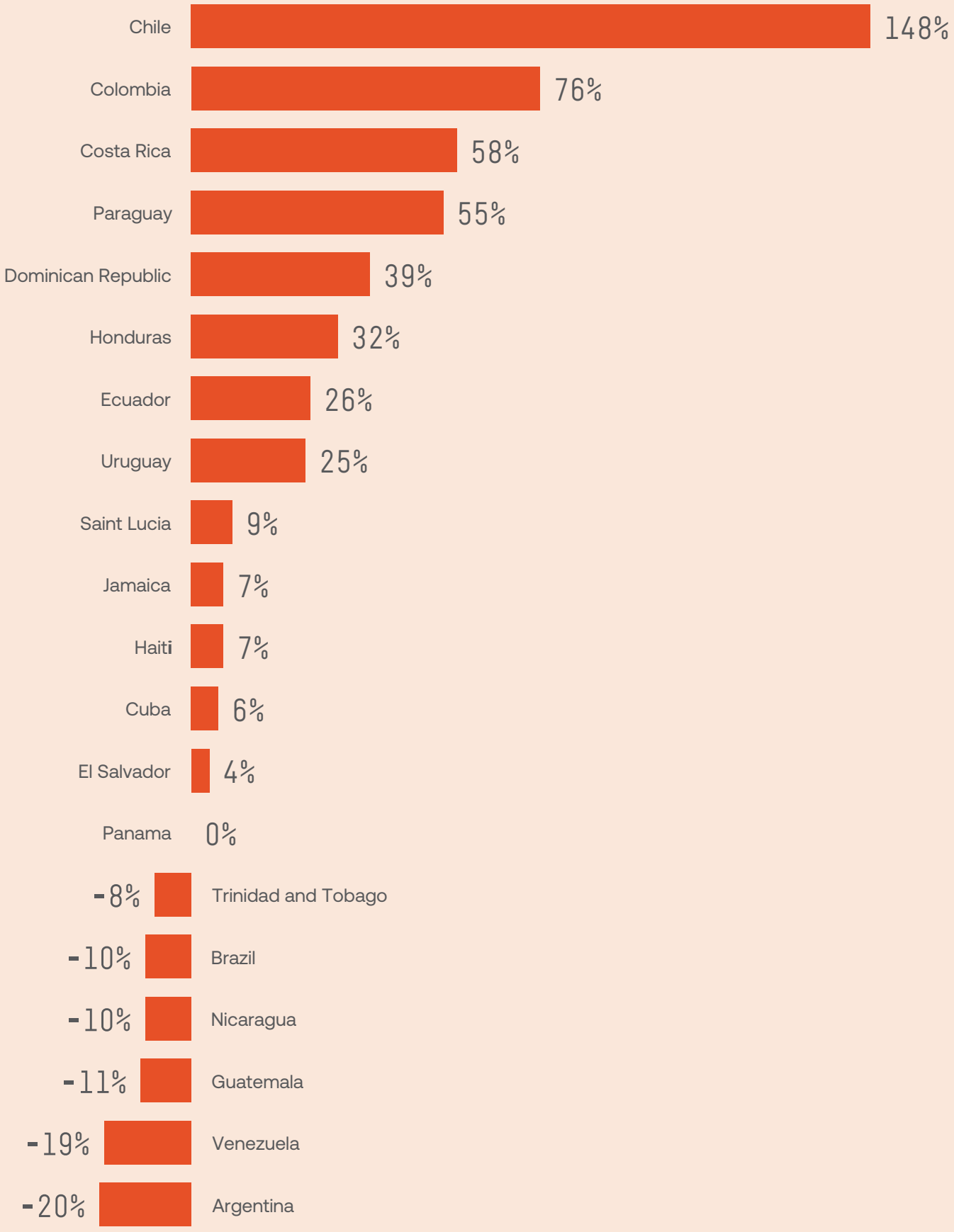
New signals of fraud rings.
Template-based fraud jumped (+56% YoY) and liveness bypass attempts surged (+60% YoY), indicating fraud networks systematically probing liveness checks and recycling document templates across multiple markets.

Chart 45.
Top-20 LATAM & Caribbean countries with the highest percentage of fraud in 2025



% of fraud in all analyzed verifications by country

Chart 46.
Top-20 LATAM & Caribbean countries
with the largest fraud growth YoY



Country-level dynamics

The regional averages hide striking national contrasts:

Rising hotspots

1. **Colombia** saw its fraud rate climb to 2.6% (+76% YoY), with deepfake activity rising +77% YoY. Fraudsters target its fast-growing digital banking and e-commerce sectors.
2. **Dominican Republic** reached 2.7% (+39%), supported by one of the highest deepfake participation rates in the region (6%).
3. **Honduras (2.2%, +32%) and Ecuador (2.0%, +26%)** both saw rapid increases, fueled by weaker KYC in mobile wallets.
4. **Chile** stood out, with fraud almost tripling to 1.4% (+148% YoY), showing how smaller markets are becoming testing grounds.

Stable but pressured

1. **Brazil (0.9%, –10% YoY)** continues to maintain one of the lowest fraud rates in the region, thanks to mature AML frameworks, the Central Bank's tighter KYC and Pix payment regulations, and a strong focus on real-time transaction monitoring. However, deepfake and synthetic identity activity is growing—particularly in digital banking and online betting—where attackers leverage AI-generated profiles to bypass onboarding checks. This shift shows that while Brazil has contained basic fraud, it is entering a new phase defined by AI-enabled impersonation and multi-account manipulation.

2 **Haiti (2.4%, +7%) and Jamaica (1.5%, +7%)** remain moderate but growing markets. Both are seeing deepfake adoption accelerating, with Haiti posting a +250% rise in deepfake attempts.

3 **Uruguay (1.4%, +25%)** remains relatively low, but saw 7% of applicants tied to fraud networks, one of the highest shares in Latin America.

Declining markets

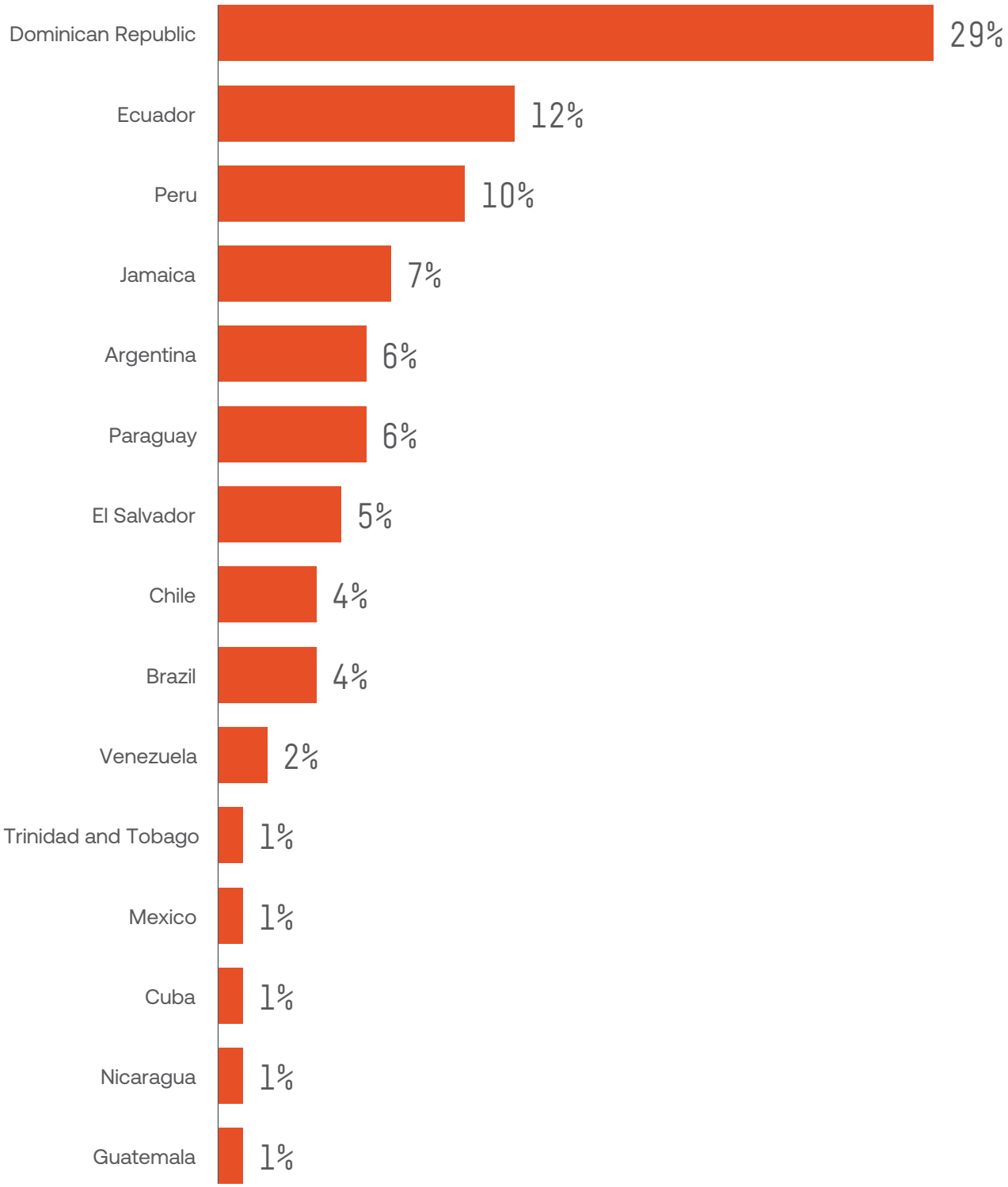
1 **Argentina fell to 3.8% (–20%)** after peaking in 2024, partly due to regulatory tightening around fintech onboarding. Yet deepfakes still rose +66% YoY, showing sophistication rising behind falling volume.

2 **Mexico dropped to 1.3% (–32%)**, but recorded one of the largest deepfake spikes globally (+484% YoY), signaling that attackers are shifting from volume to quality.

3 **Venezuela declined to 1.3% (–19%)**, while deepfakes nearly doubled (+99% YoY).

4 **Suriname** saw fraud collapse to 0.4% (–71%), yet deepfakes grew +400%, underlining the paradox: fewer cases, sharper attacks.

Chart 47.
Top-20 jurisdictions with the highest ratio of approved applicants involved in fraud networks



Deepfakes in LATAM: quality over quantity

Deepfakes are spreading across Latin America at an extraordinary speed:

Deepfake acceleration – where Brazil ranks mid-pack (126% YoY growth), while countries like Guatemala, Mexico, Panama, and Suriname are seeing exponential (+400–500%) growth.

Costa Rica and El Salvador both experienced a significant increase in deepfake activity, with rates tripling or more, despite relatively small overall fraud rates.

Suriname shows the paradox most clearly: overall fraud has shrunk dramatically, but deepfakes have increased fourfold, illustrating how sophistication rises even in declining markets.

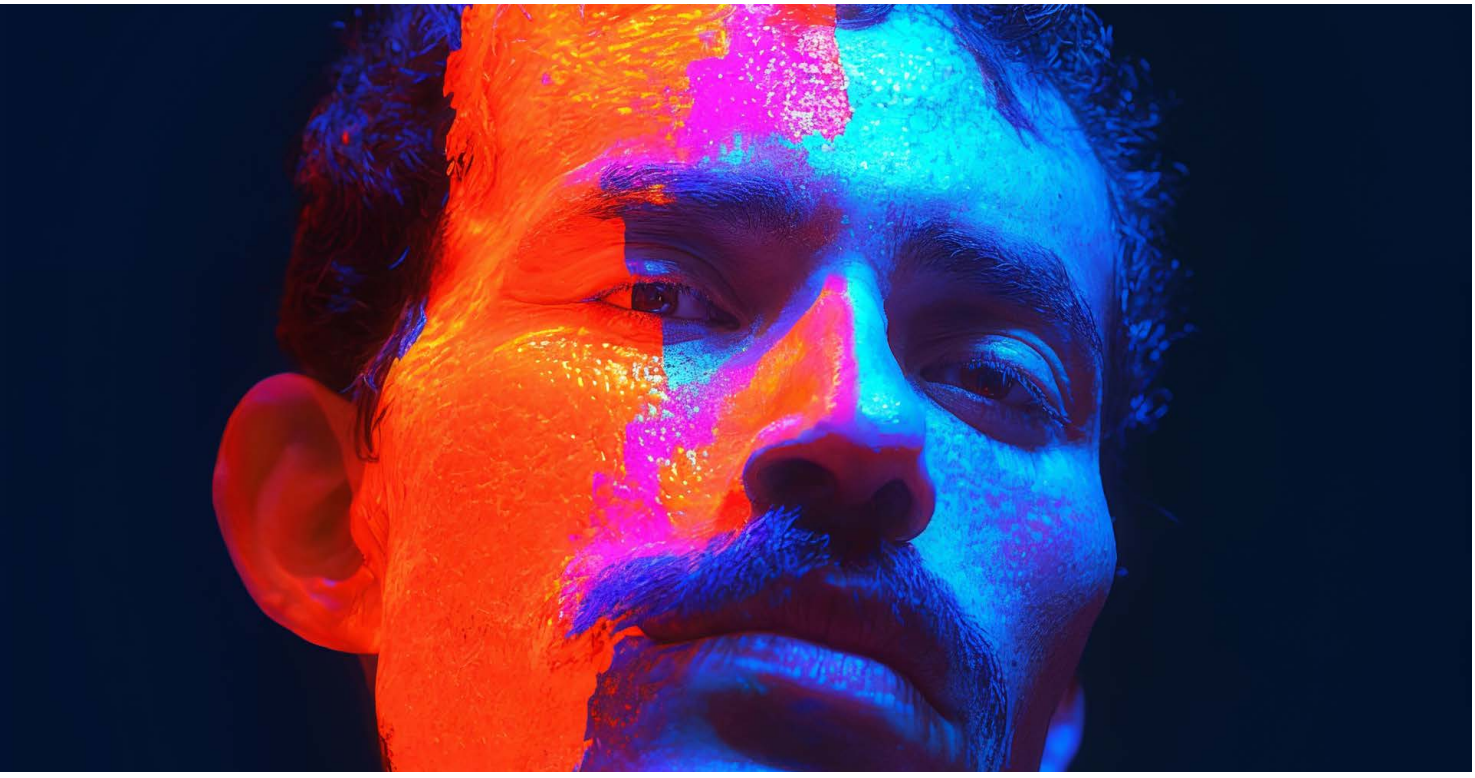
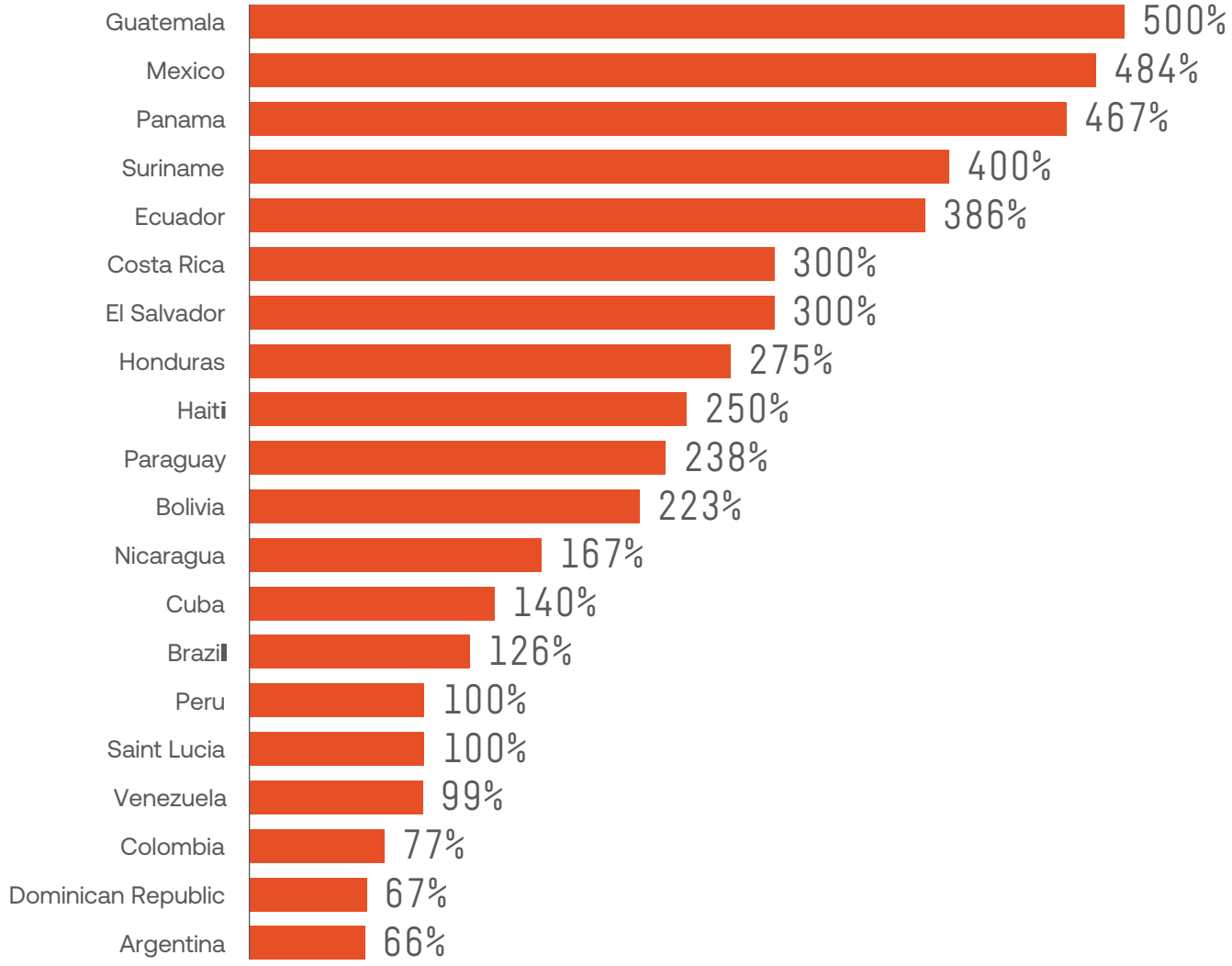


Chart 48.
Top-20 LATAM countries with the largest YoY deepfakes growth (2025 over 2024)



Across the region, deepfakes have evolved from novelty tools into precision-grade fraud instruments. Their role is shifting from simple video forgery to full ecosystem infiltration, combining voice, face, and behavioral imitation to bypass multi-factor verification. The data confirms that Latin America's battle against AI fraud is not about stopping its spread, but about staying ahead of its evolution.

Why some countries fell while others rose

Fraud rose fastest in countries with rapid fintech expansion, but weaker enforcement—such as Colombia, the Dominican Republic, and Chile. Fraudsters exploit high-growth ecosystems that lack consistent onboarding checks, often recycling synthetic identities across platforms.

By contrast, Argentina and Mexico pushed fraud rates down with stronger regulatory pressure, yet the share of deepfakes exploded. These cases highlight the core **Sophistication Shift**: crude fraud is being filtered out, but advanced fraud remains—and is more dangerous per case.

What to expect next

Latin America's outlook is defined by polarization:

Some markets will continue to suffer rising fraud rates as adoption outpaces defenses. Others will show falling percentages, but those wins will be undermined by deepfake-driven fraud that is harder to detect and costlier when missed.

Looking ahead to 2026, we can expect:

1 **Deepfakes moving mainstream**
Spreading beyond selfies into video liveness checks and even voice impersonation for call centers.

2 **Fraud rings are expanding**
With template-based fraud and liveness bypass attempts rising, it signals organized networks scaling across borders.

3 **Shift to synthetic ecosystems**
More fraud built on entirely AI-generated personas, not just stolen IDs.

4 **Greater regulatory fragmentation**
Some governments (Argentina, Mexico, Brazil) are tightening KYC rules, while smaller markets remain vulnerable due to fraud spillovers from neighbors.

Jovanny Huerta,
Safety Project Specialist
at inDrive (México)

"By 2026, fraud will be shaped most strongly by the rapid advancement of artificial intelligence. Fraudsters will industrialize deepfakes, voice cloning, and synthetic identities, making impersonation scams, social engineering, and account takeovers more convincing and difficult to detect. The accessibility of "Fraud-as-a-Service" will lower the entry barrier, allowing even less-skilled actors to launch sophisticated attacks at scale.

At the same time, the global expansion of real-time payment systems and digital assets will create fertile ground for high-speed, high-impact fraud. Instant, irreversible transactions will amplify risks of authorized push payment scams and account takeovers, while the continued rise of cryptocurrencies, NFTs, and DeFi platforms will invite increasingly complex schemes such as rug pulls, wallet draining, and fake protocols. Traditional detection methods will struggle to keep up with the speed and sophistication of these attacks.

Defenses will need to evolve just as quickly. AI-powered detection, behavioral biometrics, and multi-layered identity verification will become essential tools to counter AI-driven threats. Organizations must combine advanced technology with stronger human oversight, regulatory frameworks, and a zero-trust approach. In short, 2026 will mark a turning point: fraud will be faster, smarter, and more convincing than ever, and only those prepared to match AI with AI will be able to stay ahead."

Global challenge, local realities

Discover LATAM's performance in Sumsub's Fraud Exposure Survey 2025.

Companies

43%

Businesses in Latin America have fallen victim to fraud in 2025

Consumers

68%

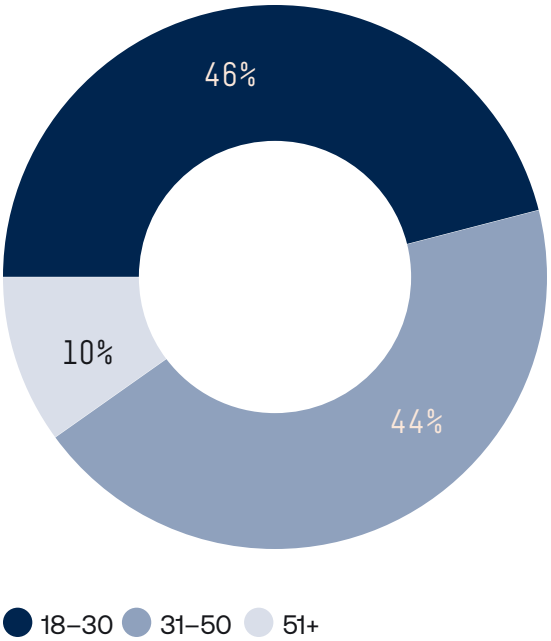
End users in Latin America have fallen victim to fraud at least once in 2025

Consumer fraud findings in Latin America

Take a closer look at who our LATAM-based consumers are, from their age to employment status.

Chart 49.

Age



Employment status

73%
Employed full-time

11%
Self-employed full-/part time

9%
Employed part-time

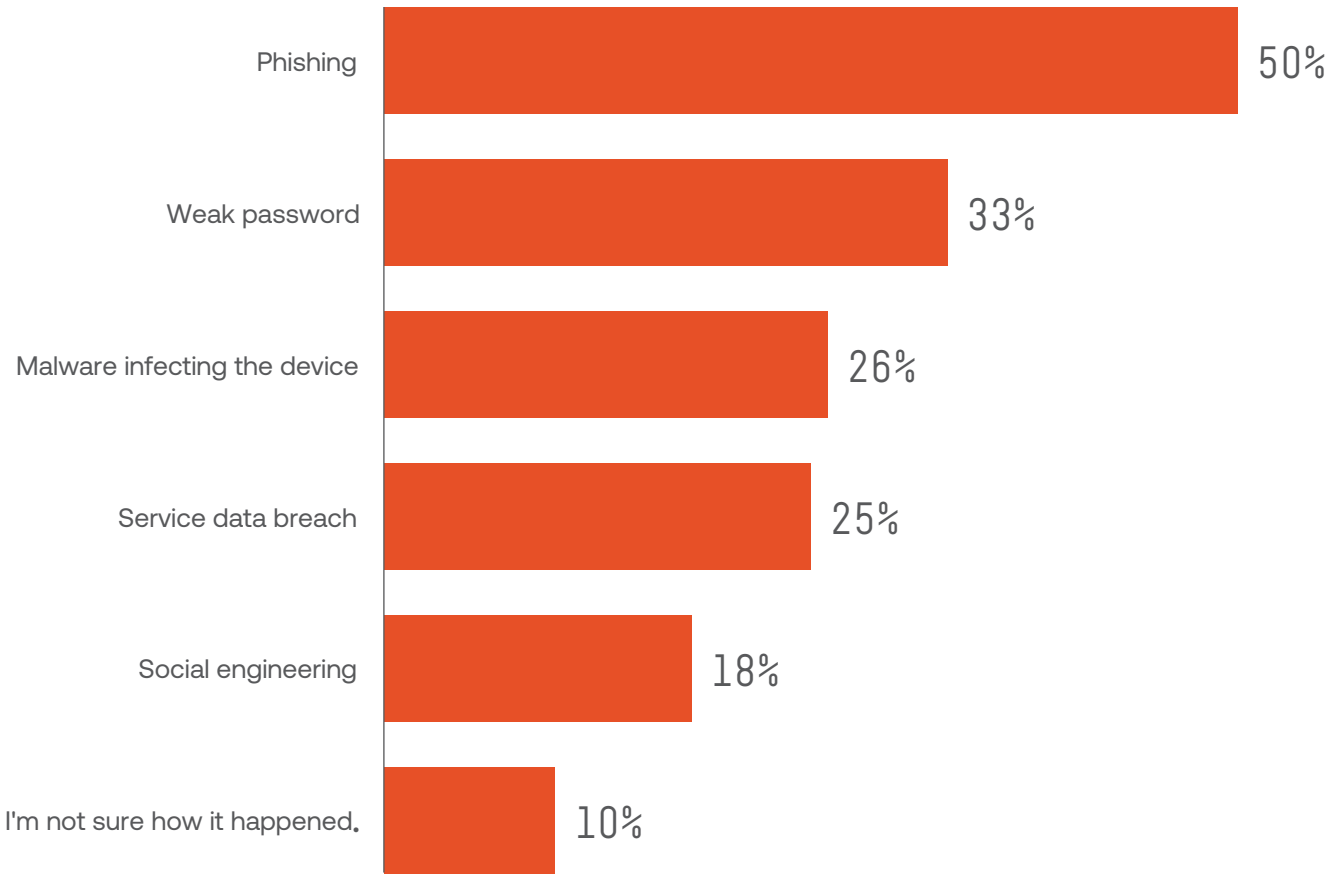
7%
Temporarily unemployed

Main attack vectors

Phishing remains the clear frontrunner — 50% of incidents begin with a deceptive message.

However, weak passwords (33%) and device-level malware (26%) remain major, user-controllable entry points, while service data breaches (25%) indicate that attackers are increasingly exploiting third-party exposures as much as individual mistakes. Fewer victims (10%) are unaware of the breach vector, indicating a growing trend of stealth and automation in attacks.

Chart 50.
Question:
What do you think was the cause of the fraud incident?



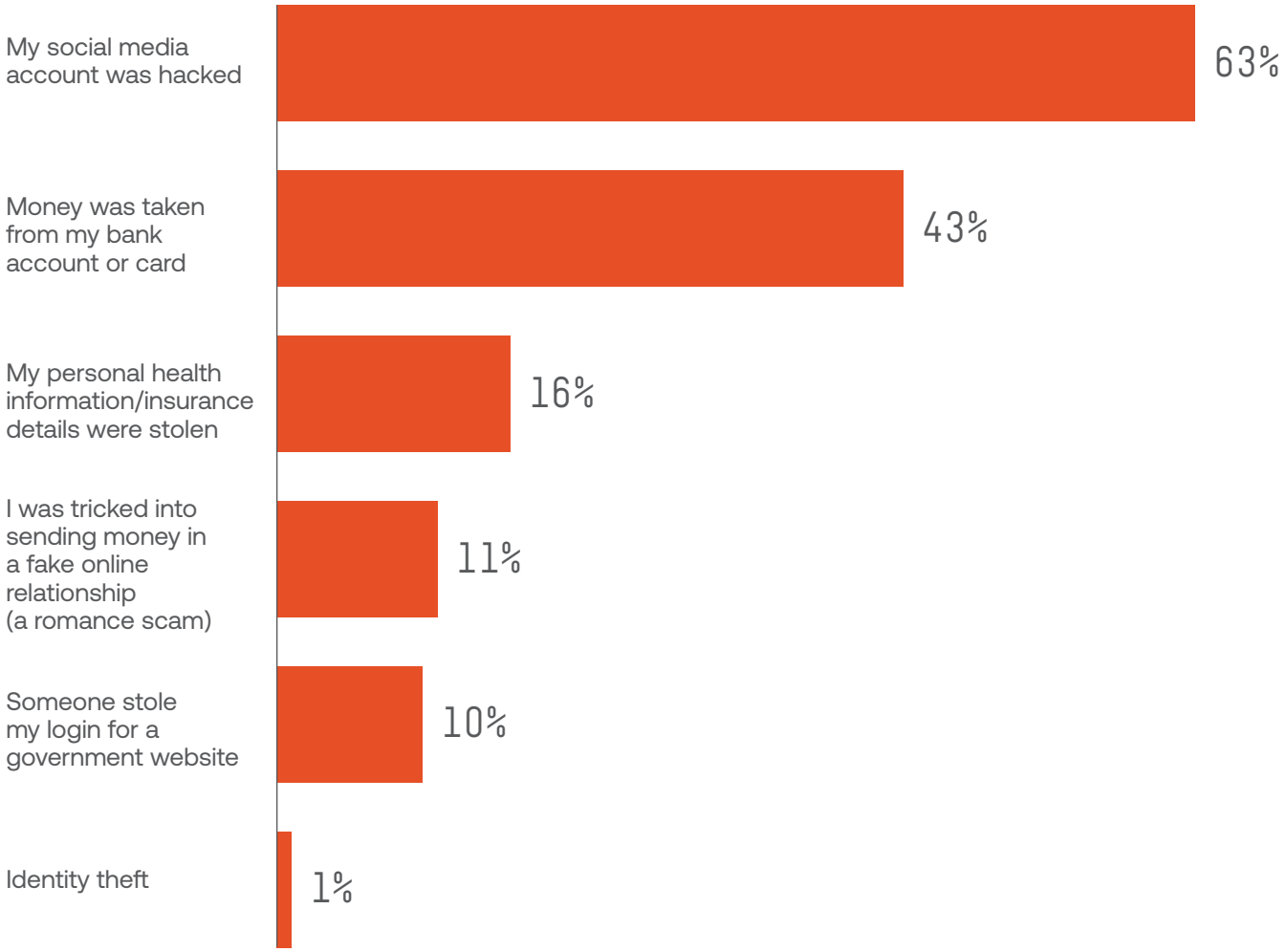
Sumsub's Fraud Exposure Survey 2025,
Latin America: Consumers

Main fraud outcome

A striking 63% of respondents had their social media accounts hacked, and another 10% lost access to government logins — both clear cases of account takeover (ATO).

Half of all respondents faced some form of identity hijacking. While 43% experienced direct financial theft, these attacks often begin with compromised credentials.

Chart 51.
Question:
What type of identity fraud did you experience?



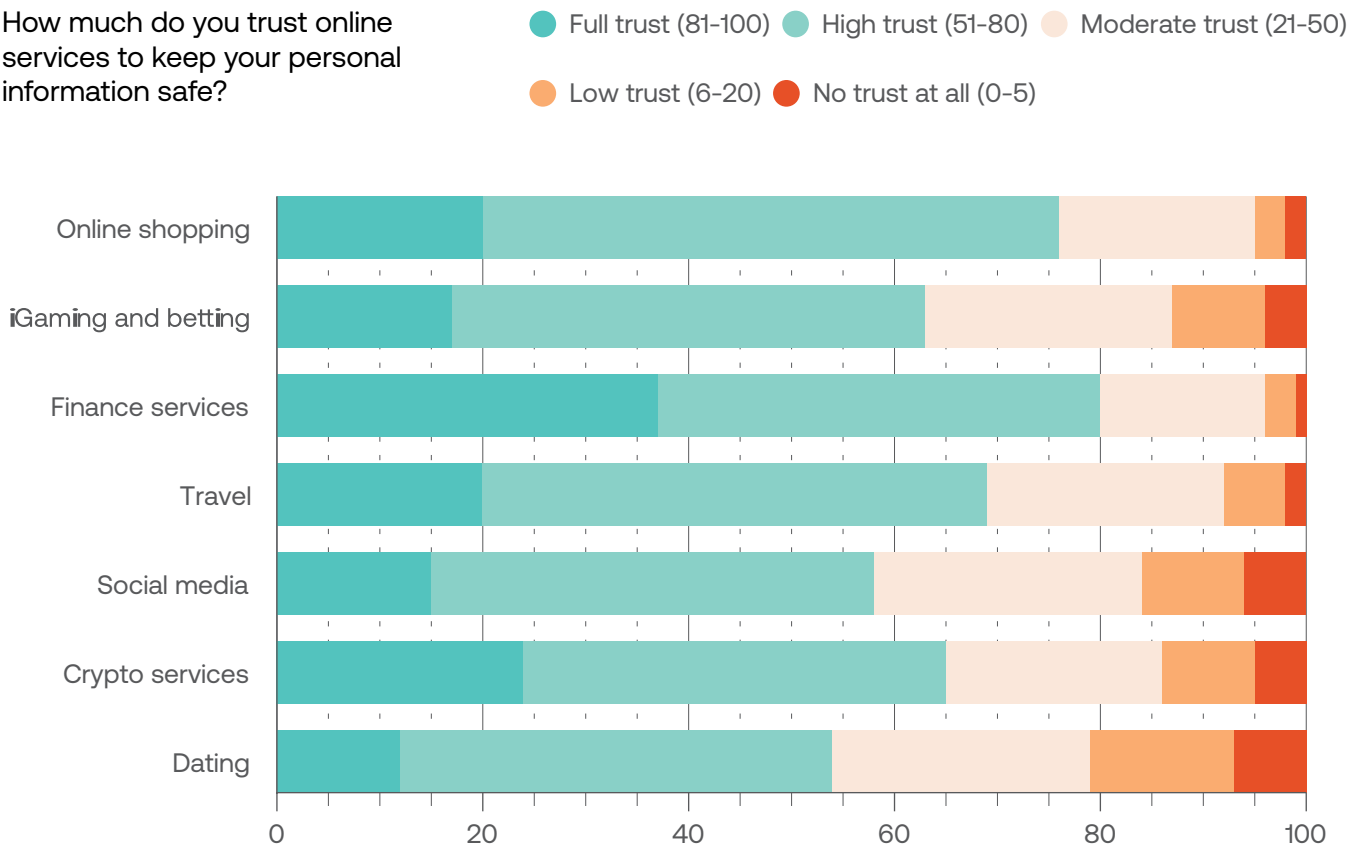
Sumsub's Fraud Exposure Survey 2025, Latin America: Consumers

Digital trust in Latin America

Respondents show the highest confidence in financial services, with 81% expressing high or full trust, confirming that banks remain the most trusted guardians of personal data.

Online shopping (77%) and **travel platforms (70%)** maintain relatively high trust levels, likely due to visible protections such as secure payment methods and clear refund policies. In contrast, **crypto (66%)**, **social media (59%)**, and **dating apps (57%)** reveal significant trust deficits, reflecting user concerns over data misuse, scams, and weak privacy safeguards.

Chart 52.
Question:
How much do you trust online services to keep your personal information safe?



Sumsub's Fraud Exposure Survey 2025,
Latin America: Consumers

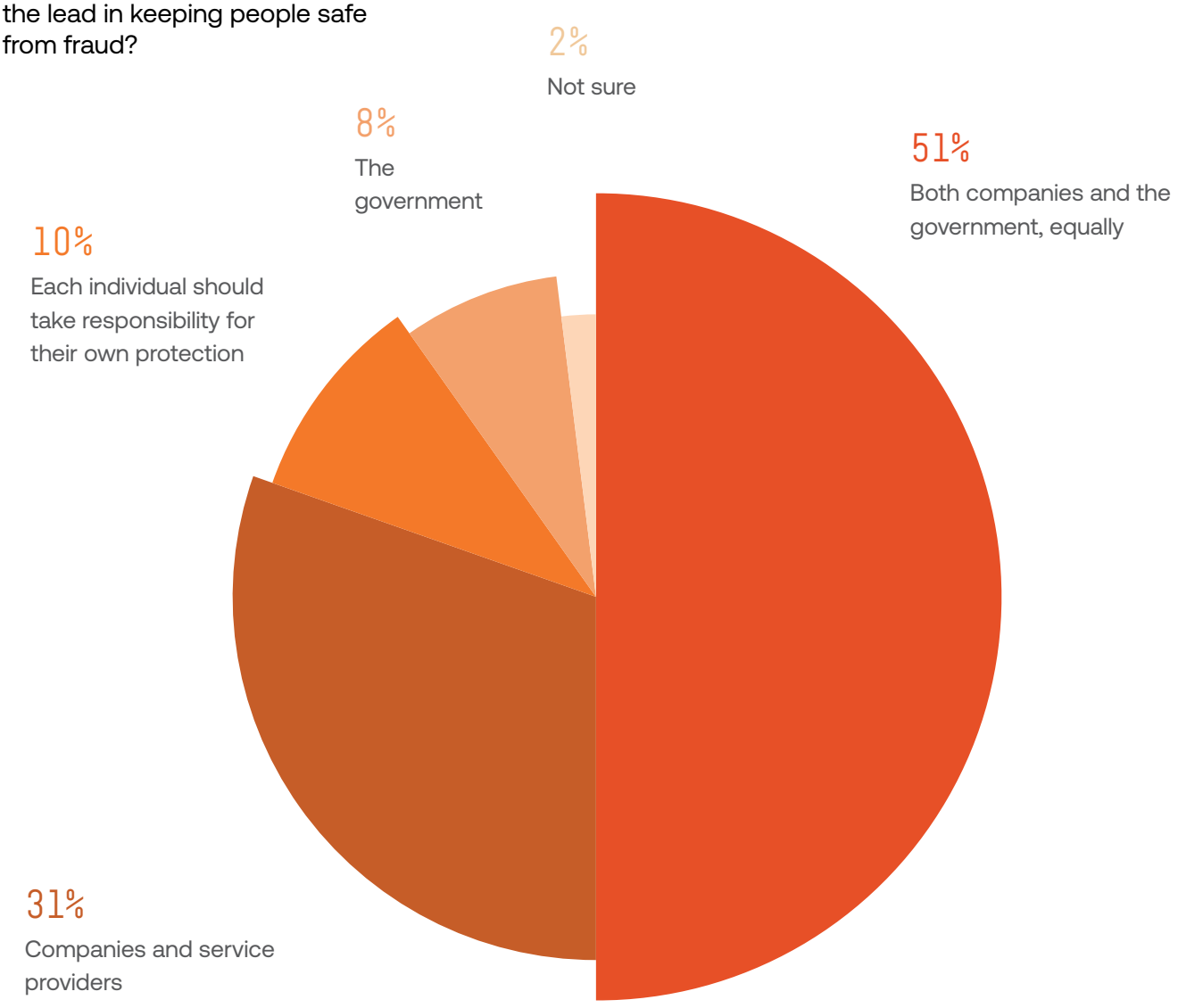
95% of respondents would choose a service provider only if they have strong anti-fraud measures in place.

95%

Responsibility for fraud prevention

More than half of respondents (51%) believe that fraud prevention should be a shared duty between companies and governments — reflecting growing expectations for systemic protection, rather than just personal vigilance. At the same time, 31% place primary responsibility on companies, signaling that users see platforms and service providers as the first line of defense — the ones who have the tools and data to detect threats early.

Chart 53.
Question:
Who do you think should take the lead in keeping people safe from fraud?



Sumsub's Fraud Exposure Survey 2025, Latin America: Consumers

Virtual cards as everyday tools

Virtual/disposable cards are widely adopted in Latin America, with **almost 9 in 10 using them and more than half relying on them regularly.**

87% of respondents use disposable/virtual cards at least sometimes, and 58% are heavy users.

Question:
Do you use disposable or virtual cards for online payments?

Sumsub's Fraud Exposure Survey 2025, Latin America: Consumers

Money mule recruitment goes mainstream

Awareness of money muling is relatively high, with nearly **70% of respondents** having at least heard of it. However, 40% admit they don't fully understand what it means, revealing a dangerous knowledge gap between recognition and comprehension.

Alarmingly, almost 1 in 3 respondents have been directly approached to move suspicious funds, confirming that mule recruitment remains an active and visible threat in the region.

Question:
Have you heard of "money muling" - letting someone move stolen money through your bank account?

Sumsub's Fraud Exposure Survey 2025, Latin America: Consumers

86% of respondents are highly convinced that fraud is becoming more sophisticated and AI-driven.

This confirms that companies are aware of deepfake risks, synthetic identities, and AI-driven forgeries, and are looking for next-generation fraud prevention solution.

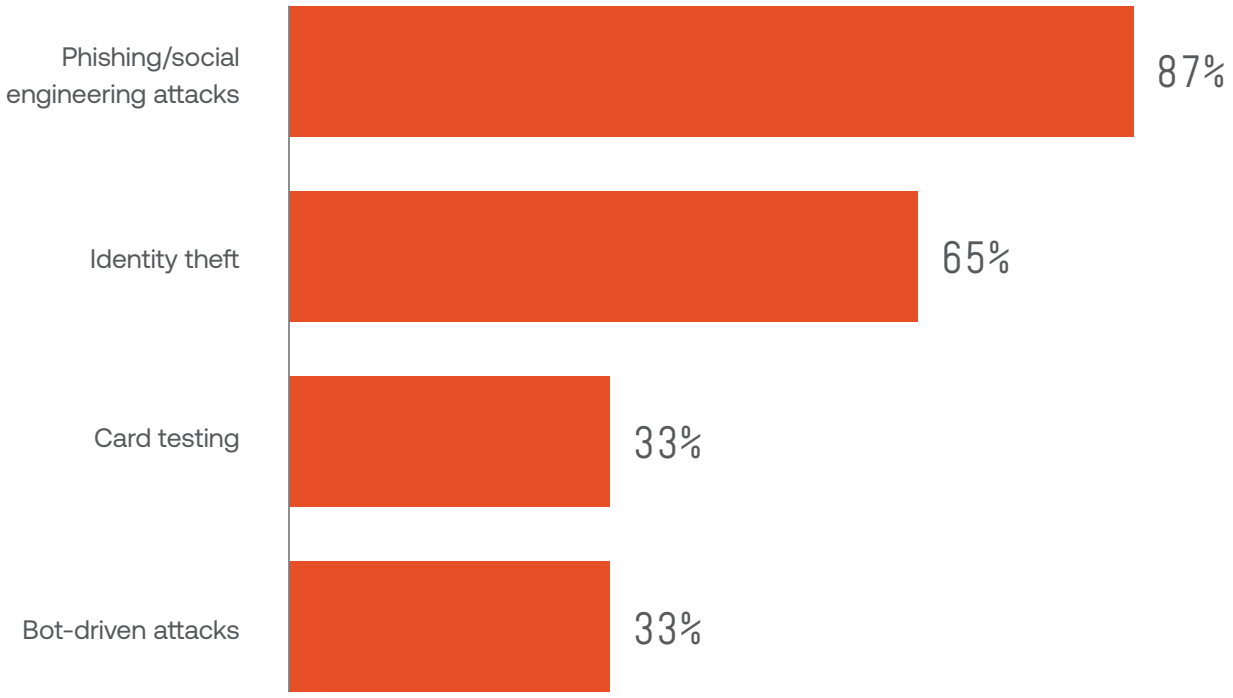
Company fraud findings in Latin America

Top 3 types of fraud faced by companies in Europe

1 Phishing/social engineering attacks (87%)
2 Identity theft (65%)
3 Card testing and bot attacks (33% each)

At the same time, they had to manage first-party fraud from their customers, who used synthetic identity and deepfakes (60% and 55% respectively) and conducted application (52%) and chargeback abuse (42%).

Chart 54.
Question:
What kind of third-party fraud has your business faced?



Sumsub's Fraud Exposure Survey 2025, Latin America: Companies

100% report that organized fraud attempts have become more frequent.

Major consequences companies have experienced as a result of fraud attacks:

1. Operational disruption
2. Financial losses
3. Reputational damage
4. Customer churn
5. Challenges with investors
6. Employee distrust/turnover
7. Challenges with partners
8. Fines/penalties
9. Licence cancellation

How companies manage fraud

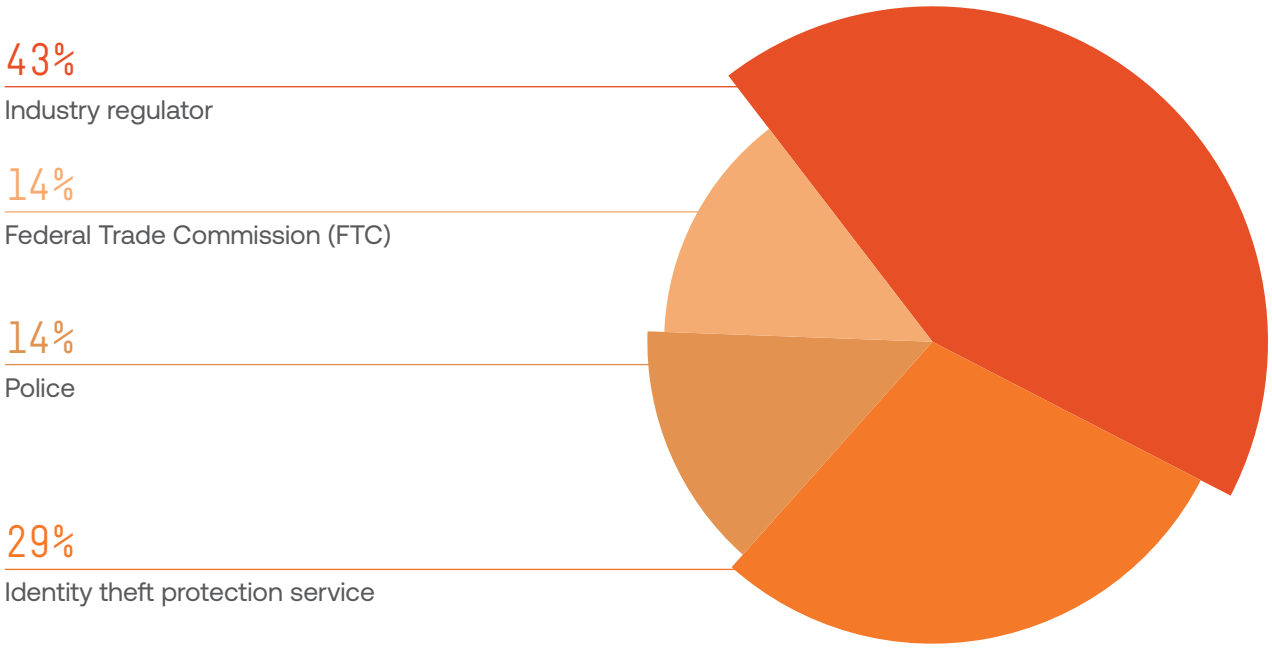
An **overwhelming 71% of businesses** rely on a hybrid fraud prevention model, which combines internal teams with external vendors to strike a balance between control, expertise, and scalability. However, an equally high 71% still depend on manual processes, revealing that automation and orchestration remain major gaps in fraud operations.

The data reveals a paradox — while companies acknowledge the need for collaboration and layered defense, manual workflows persist in slowing down detection and response.

When facing identity fraud, reporting remains fragmented. Less than half of businesses (43%) notify an industry regulator, while fewer engage with direct enforcement or financial partners.

Only 14% report incidents to the police or a bank/financial institution, and just 29% turn to identity theft protection services.

Chart 55.
Question:
Did your business report incidents of identity fraud to authorities or institutions



Sumsub's Fraud Exposure Survey
2025, Latin America: Companies

When asked about supporting stricter regulations against identity fraud, a majority — 57% of businesses — remain undecided, highlighting regulatory fatigue and uncertainty about how new compliance demands might impact daily operations.

Only 29% express clear support, while 14% oppose tighter rules altogether, suggesting that operational friction and compliance costs remain major barriers to broader alignment.

Alison Dorigão Palermo,
Compliance Expert

"In Brazil and LATAM, synthetic identity fraud combining real and fabricated data has surged, especially in digital lending and e-wallets. Social engineering attacks via WhatsApp and SMS are increasingly common, exploiting mobile-first behaviors. Fraudsters leverage fragmented ID systems—multiple IDs per person across states—making verification complex. Regulators such as Banco Central do Brasil is tightening KYC obligations, while AI-based anomaly detection and real-time risk scoring are proving effective at reducing fraud without degrading customer experience. Biometric spoofing and deepfakes are emerging concerns, requiring advanced, multi-layered verification systems.

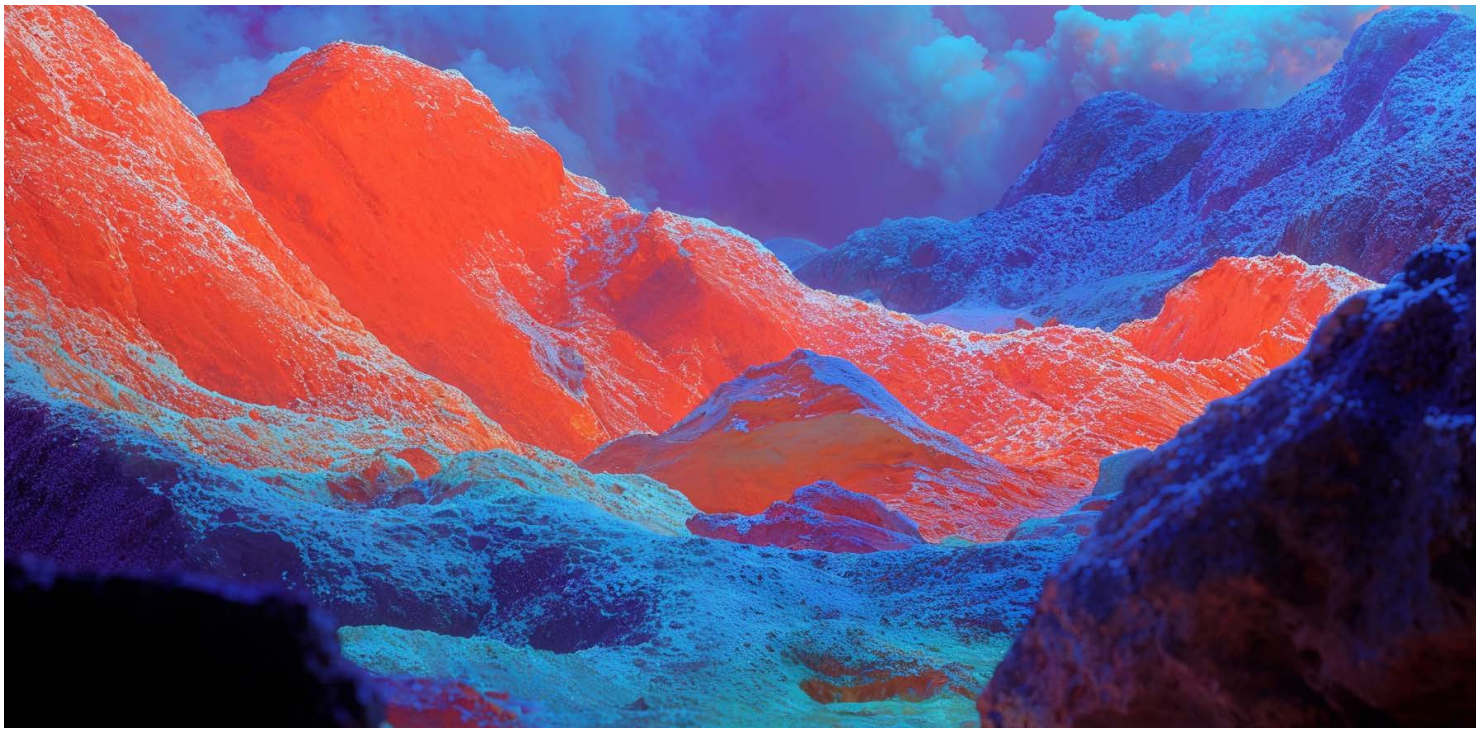
In 2026, the Brazilian and Latin American identity verification market will increasingly rely on AI-driven biometrics—facial recognition, liveness detection, and behavioral analysis—to reduce fraud and accelerate onboarding. A critical challenge in LATAM remains the absence of a unified ID system, unlike the EU where standardized documents simplify verification. In Brazil, citizens may hold up to five different ID documents (that is my case as an example), and if each state issued its own, this could rise to 30, complicating KYC and CDD processes. Open Banking and digital identity initiatives will help, but regional interoperability and secure, auditable verification remain essential. Blockchain-based decentralized IDs may gain traction for privacy-compliant, verifiable identity, particularly for underbanked populations, while regulators push for automated, continuously monitored FRAML compliance."

Predictions for the future

1 Respondents foresee a dramatic escalation in identity-driven fraud, with **71% predicting a surge in identity theft** linked to ongoing data breaches.

2 Emerging technologies are a major concern: **57% expect deepfakes and AI-generated forgeries to become central tools for scammers,** while nearly half anticipate synthetic identities being used to evade KYC and onboarding controls.

3 At the same time, governments tightening regulations (57%) and businesses strengthening cybersecurity (43%) show that both sectors are bracing for this evolution — though only 29% believe AI-powered attacks or organized digital crime will dominate, suggesting some underestimation of how rapidly fraud innovation is advancing.



Regional case studies of fraud up close

The following case studies spotlight real-world fraud incidents that occurred in Latin America and the Caribbean in 2025.

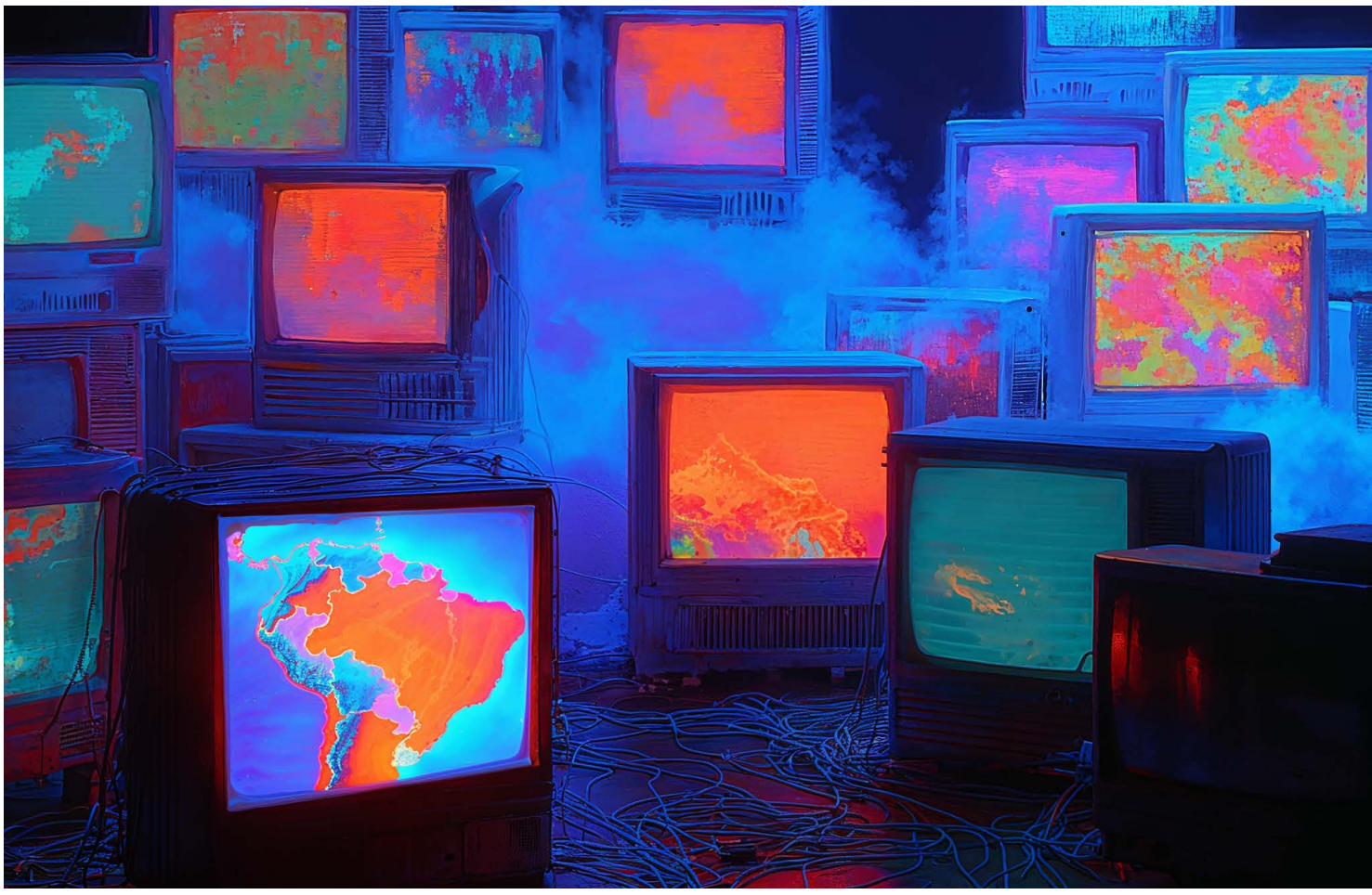
1 **Former Latin American Presidents convicted in major corruption cases**

In March 2025, Latin America saw landmark verdicts against former heads of state. In Colombia, former President Álvaro Uribe was convicted of bribery and procedural fraud, becoming the first Colombian former head of state to be found guilty at trial. In Peru, Ollanta Humala received 15 years in prison for laundering over US$3 million in Odebrecht bribe money. These rulings are part of a wider regional reckoning, with other former leaders in Brazil, Ecuador, El Salvador, Guatemala, and Panama also facing convictions or charges for large-scale corruption and fraud.

2 **OmegaPro founders charged in US$650 million global crypto ponzi scheme**

In July 2025, US prosecutors unsealed indictments against the operators of OmegaPro, a global crypto and forex investment scam that defrauded investors of more than US$650 million. Promising 300% returns in 16 months, the scheme paid early investors with new victims' funds while its founders lived lavishly and even projected their logo on Dubai's Burj Khalifa to appear legitimate. Described by officials as a "precision-engineered betrayal," the case highlights the international scale of investment fraud and the growing cross-border cooperation to prosecute its perpetrators.

3 **Public sector fraud scandals exposed across Latin America**
In May 2025, investigations revealed major corruption within Latin American public institutions. In Chile, investigations in the “Cabineros Fraud” case uncovered a long-running embezzlement scheme by senior police officials involving millions in diverted public funds (a scandal named “Verde Austral”). In Mexico, the Zaragoza case exposed money laundering networks using shell companies and crypto platforms to move illicit funds through banks and unregulated exchanges. Though some investigations began earlier, the prosecutions and new indictments in 2025 demonstrate continued efforts to tackle systemic corruption in the region.



Regulatory shifts redefining identity protection

As fraud operations become more sophisticated, Latin American nations are strengthening their AML, anti-corruption, and digital finance regulations to build greater regional resilience. Here are some of the latest developments across Latin America and the Caribbean.

Argentina

Law 27.739 reforms to the core AML statute.
In March 2024, Argentina reformed its primary AML framework (Law 25.246), enacting Law 27.739, raising the monetary threshold for prosecuting money-laundering offenses to 150 minimum wages (SMVM) to offset inflation. The law expanded the scope of obligated entities to include lawyers, accountants, notaries, VASPs, and custodians, while removing others, such as non-profits. It also created a Centralized Registry of Ultimate Beneficial Owners and introduced new definitions for “virtual assets,” “terrorist act,” “UBOs,” “risk-based approach,” and “unusual transactions.”

Presidential Decree 891/2024 – narrowing of obligated entities.
In October 2024, the decree further refined the scope of reporting obligations by excluding customs brokers and businesses involved in the purchase and sale of vehicles, agricultural machinery, vessels, yachts, and aircraft.

CNV Resolution 1058/2025 – dedicated VASP registry.
Authorized under Law 27.739, the Comisión Nacional de Valores (CNV) established a dedicated registry for VASPs through Resolution 1058/2025, bringing virtual asset service providers (VASPs) under formal regulatory oversight.

UIF Resolution 078/2025 – new reporting thresholds.
In 2025, the Financial Intelligence Unit raised reporting thresholds for real estate (750 SMVM) and vehicle transactions (50 million pesos, adjusted biannually). It also mandated client profiling for vehicle acquisitions exceeding 115 million pesos annually and required reporting of cash deposits or foreign exchange transactions equal to or above 40 SMVM.

Brazil

Online betting.
In addition to the earlier framework (Law No. 14,790/2023 and Ordinances 1,143/2024 & 722/2024), Brazil published Ordinance 817/2025, which outlines 13 priority projects for 2025-26 under SPA/MF, signaling a transition from licensing to ongoing supervision, anti-fraud integration, and AML strengthening. The regulated online betting market was launched on 1 January 2025, requiring operators to implement KYC procedures with facial recognition, as well as ongoing monitoring of the bettors' activity. In October 2025, the Ministry issued Ordinance No. 2,117/2025, launching the SIGPA system in partnership with SERPRO, aimed at verifying whether individuals are banned from betting due to their status as beneficiaries of social welfare programs.

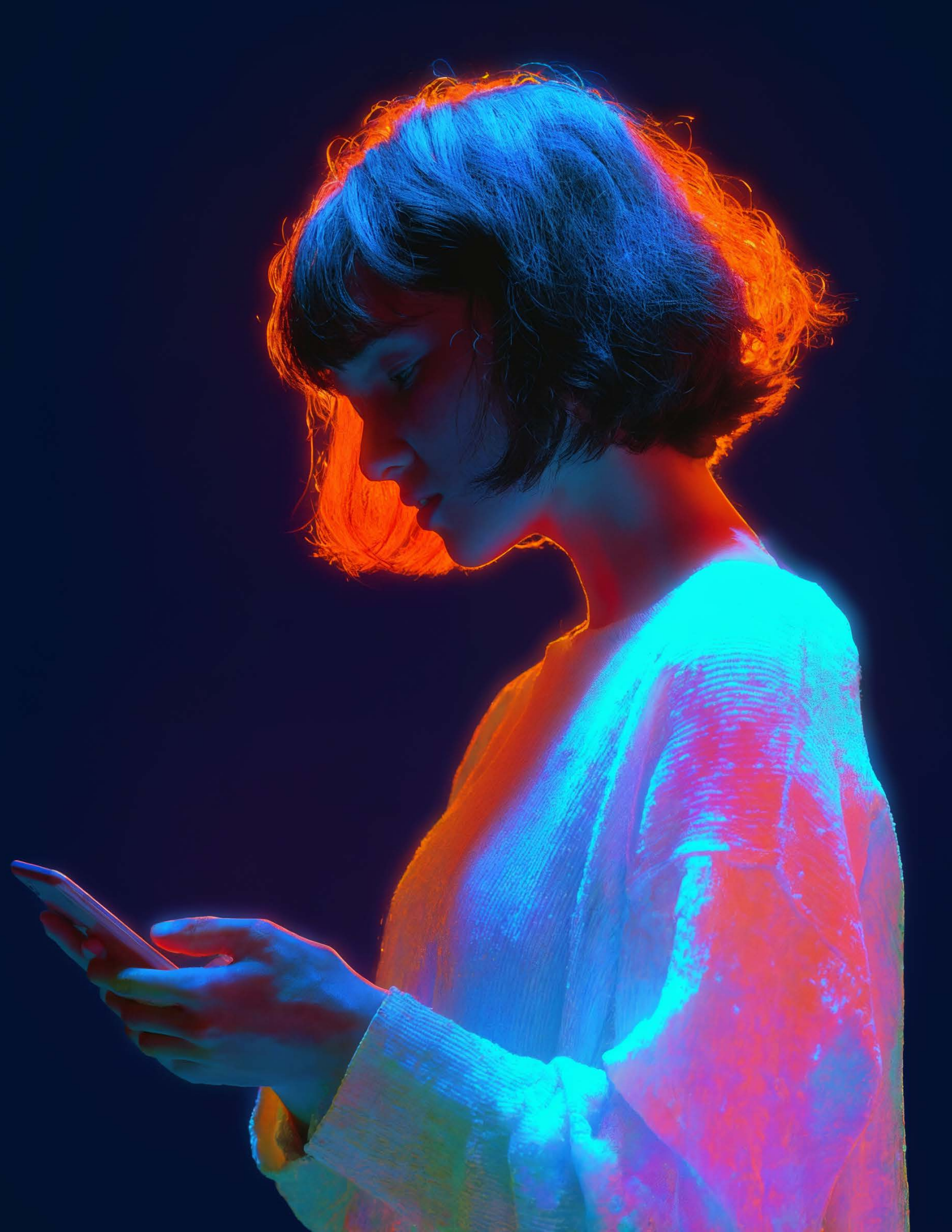
Central Bank Resolution No. 475/2025 – voluntary restriction registry.
Issued in May 2025 and effective from December 2025, this resolution created a registry where individuals can voluntarily request to be restricted from entering into new financial contracts. Financial institutions must check the registry before opening accounts or adding new account holders, reinforcing fraud prevention and KYC compliance.

Central Bank Resolution No. 498/2025 – Pix security measures.
Following a series of security breaches on the Pix platform, the Central Bank issued Resolution No. 498 in September 2025. The measure introduced transaction limits for Electronic Funds Transfers and Pix transactions by unauthorized payment institutions and those using IT service providers to connect to the financial system. IT providers must also hold a minimum capital of 15 million, implement internal controls, and comply with mandatory cybersecurity standards.

Mexico

CNBV amendments on fraud prevention.
In June 2024, the National Banking and Securities Commission (CNBV) introduced new obligations in the "General Provisions Applicable to Credit Institutions" to enhance fraud prevention and user security. A key measure was the creation of the "Fraud Prevention Management Plan," requiring institutions to address identity theft, data breaches, and electronic fraud. The reform also introduced the concept of a "User Transactional Amount," a threshold—set by users or estimated by institutions—for monitoring unusual or potentially fraudulent transactions across online and mobile banking channels.

AML/CFT reforms to LFPIORPI.
In July 2025, Mexico enacted a major reform to the Federal Law for the Prevention and Identification of Operations with Illicit Resources (LFPIORPI). Key updates include formal definitions for PEPs, controlling beneficiaries, and compliance representatives; classification of real estate developments as a vulnerable activity; mandatory automated monitoring, audits, and reviews for entities engaged in vulnerable activities; and revised reporting thresholds for prepaid cards, notaries, brokers, and virtual assets.



Anastasia Shvechkova,
Sales Director Americas
at Sumsub

"Latin America is moving faster than any other region from noisy, low-skill scams to engineered, AI-powered fraud. Our 2025 data shows it clearly: fraud involving inconsistencies between a user's selfie and their ID image dominates — that category nearly tripled — because deepfakes now slip into what used to be simple mismatch buckets. Synthetics are rising, too, with fake personal data growing sharply as criminals manufacture full digital personas instead of stealing them.

Country patterns tell the same story of polarization. Mexico cut overall fraud, yet deepfakes exploded—proof that volume can fall while sophistication spikes. Colombia, Dominican Republic, Honduras, Ecuador, and Chile saw rapid increases as mobile wallets and e-commerce outpaced consistent KYC, making them prime targets for cross-border rings. Meanwhile, even where fraud decreased—Argentina, Venezuela, Suriname—we still observed triple- and quadruple-digit deepfake growth. Brazil remains the region's largest and most influential market, accounting for nearly 39% of all deepfakes detected across Latin America. This is the Sophistication Shift in action across LATAM.

The operational signal is just as important: template-based and liveness-bypass attempts are up, and many businesses still lean on manual reviews even as they adopt hybrid models. The path forward is not more friction; it's smarter layering—document logic, multi-modal liveness, device telemetry, and behavioral analytics—plus regional intelligence-sharing so a synthetic burned in one market can't reappear in another. If we align those pieces, LATAM can turn industrialized fraud into industrialized defense."

Middle East

The Middle East sits at the crossroads of rapid digital adoption and increasing exposure to fraud. Many countries are investing heavily in e-government services, digital wallets, and online banking, yet uneven regulation and fragmented identity infrastructures leave openings for fraudsters.

In 2025, the region shows a clear Sophistication Shift: synthetics and deepfakes surge, while older tricks decline, and fraud rings exploit inconsistent defenses across borders.

Anton Golub,
Chief Business Officer,
Crypto Exchange at
Freedx

“Most surprising shift?
Compliance teams are now revenue-critical. In 2024–2025, we saw licensing decisions, banking partnerships, and even deals collapse, because a project couldn’t prove real-time KYC resilience. Fraud is no longer just a legal risk. It’s a strategic bottleneck.

The second big shift: middle-risk fraud is surging.
Not obvious scams.
Not elite attacks.
But deepfake-first attempts using synthetic identity blends - just sophisticated enough to bypass legacy controls. KYC vendors that fail to innovate here will be obsolete fast.

By 2026, KYC will be an adversarial AI problem. We’re entering a phase where attackers don’t just use deepfakes - they fine-tune models to break specific onboarding flows. Verification becomes less about document and face checks, and more about behavioral biometrics, graph intelligence, and triangulated metadata (e.g. device + wallet + exchange flow). Platforms will need to predict fraud attempts before the first frame hits the webcam.

The biggest winners will be firms that:
1 Use AI to detect AI
2 Treat KYC/AML as real-time fraud engines, not compliance afterthoughts
3 Collaborate across platforms (wallets, chains, exchanges) for shared defense infrastructure.”

Fraud type evolution in the Middle East

The fraud-type mix in 2025 illustrates how the region is being reshaped by AI and organized activity:

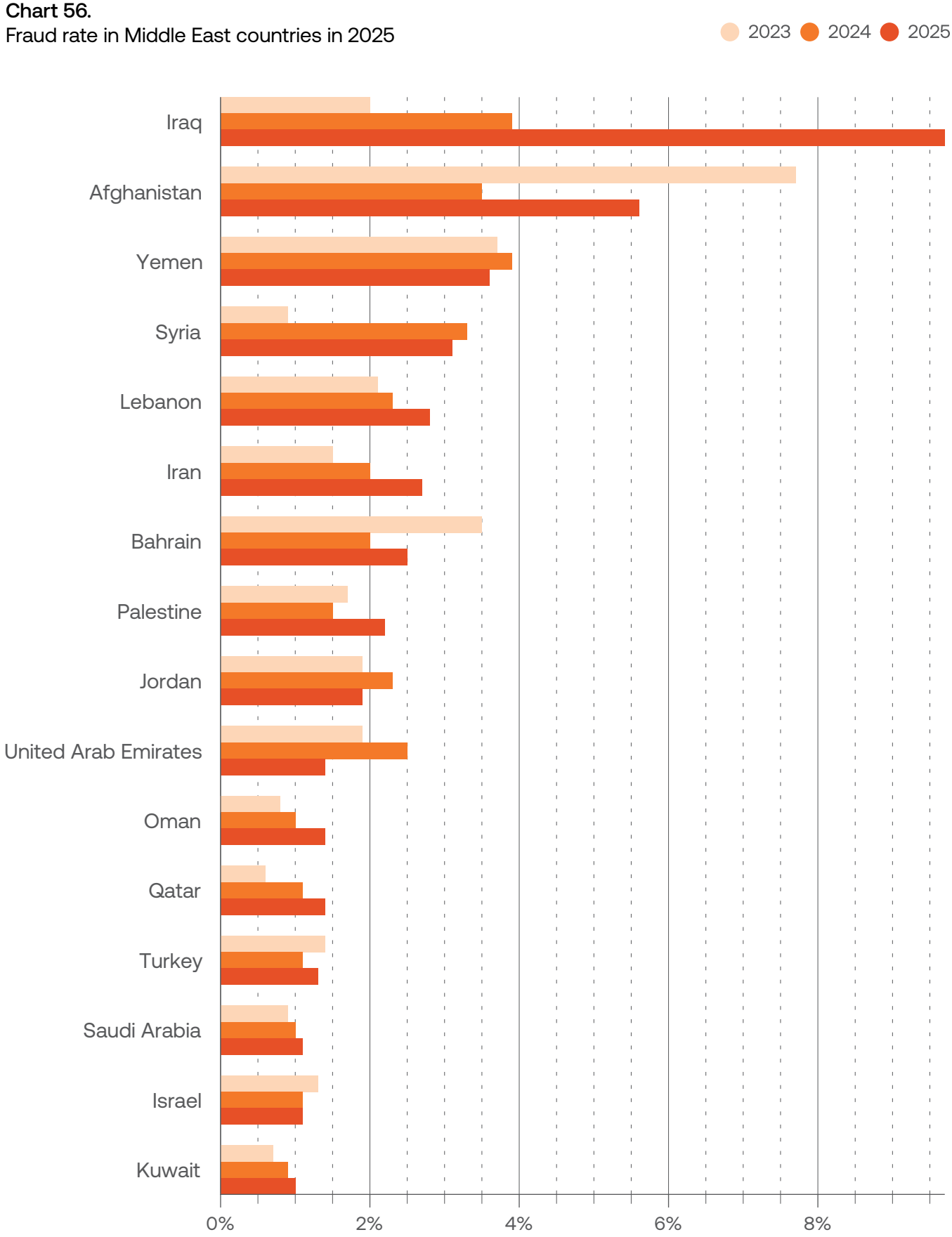
Synthetic data leads.
Fraud involving fully fabricated personal information soared by more than +540% YoY, now representing 22% of all fraud. This category covers fully fabricated personal data (including names, addresses, and dates of birth) generated at scale by fraudsters. It signals that the Middle East has become a breeding ground for the creation of synthetic identities.

Selfie fraud stays strong.
Fraud involving inconsistencies between a user's selfie and their ID image still accounts for 17% of fraud, despite a slower growth rate. This category captures both classic impersonation attempts and, increasingly, deepfake-driven liveness fraud.

Forged and edited IDs persist.
Forged ID fraud remains a significant issue, accounting for 11% of cases, and edited IDs are held at approximately 4%. Unlike other regions where physical forgery is waning, document tampering remains significant in the Middle East, reflecting a high reliance on ID cards and variable enforcement.

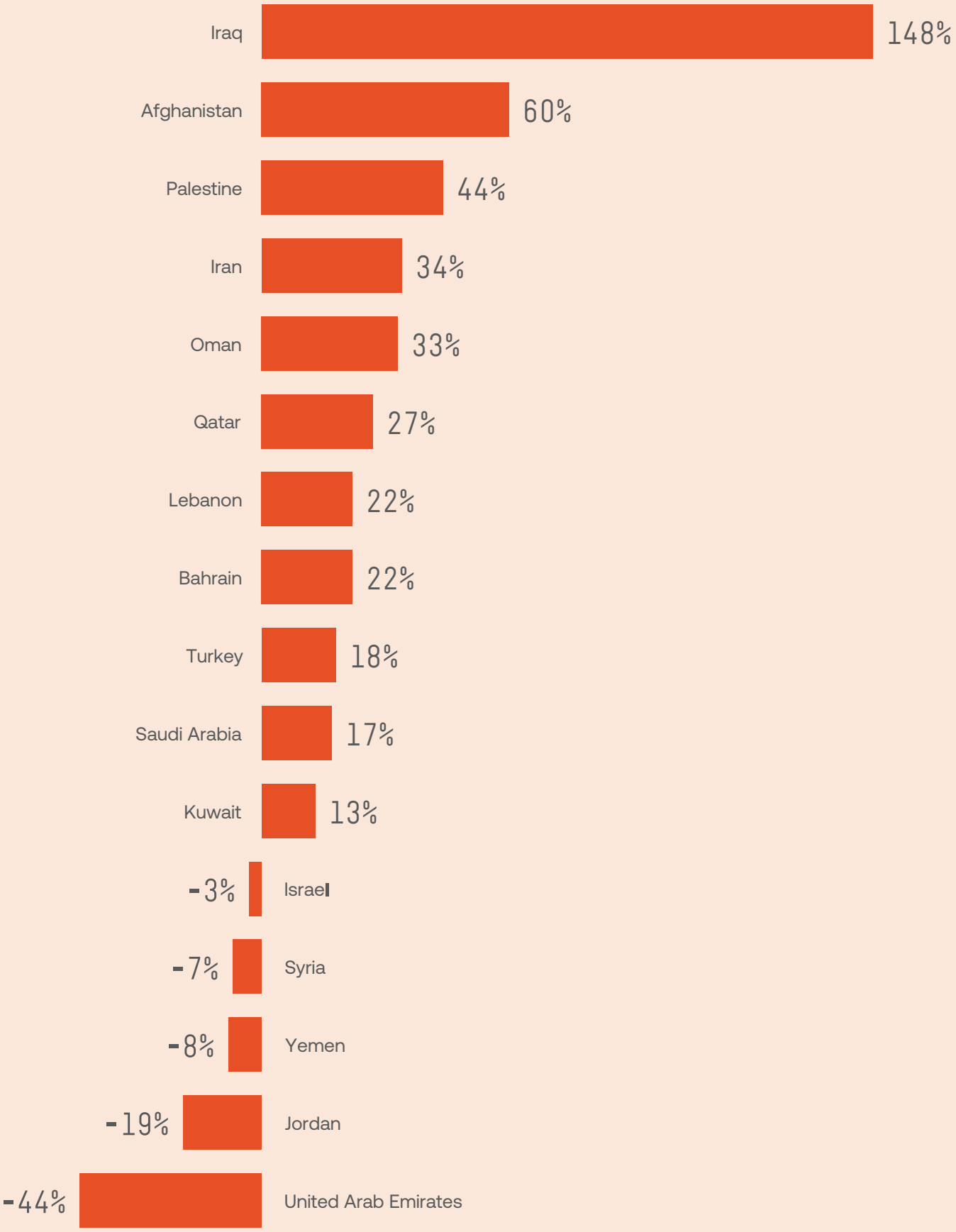
Blocklists and repeat actors.
Blocklist and blacklist fraud together account for almost 19% of the total, underscoring the persistence of fraud rings that recycle identities across borders.

Chart 56.
Fraud rate in Middle East countries in 2025



% of fraud in all analyzed verifications by country

Chart 57.
Top countries in the Middle East with the largest fraud growth YoY (2025 over 2024)



Country-level dynamics

Fraud rates in the Middle East are among the most volatile globally:

Explosive growth markets

1. **Iraq** recorded the highest regional fraud rate at 9.7% (+148% YoY), reflecting its status as a high-risk ecosystem with patchy identity enforcement.

2. **Afghanistan** remains extremely exposed at 5.6%, despite some decline from its 2023 peak.

3. **Iran's rate climbed to 2.7% (+34% YoY)**, and deepfake activity there surged by more than 250% YoY, indicating that attackers are testing AI-driven attacks in the financial services sector.

4. **Bahrain reported a 2.5%** increase in fraud (+22%), but its deepfakes grew by 760% YoY, the fastest growth in the region. In our Global Fraud Index 2025, Bahrain joined Lebanon in the top spots for Middle Eastern regions with high fraud activity.

5. **Turkey, at 1.3% (+18% YoY)**, also saw a return to growth after two years of relative stability. Rapid digitization in fintech, e-commerce, and government services has created both opportunity and exposure, with deepfake-enabled onboarding emerging as a key vector.

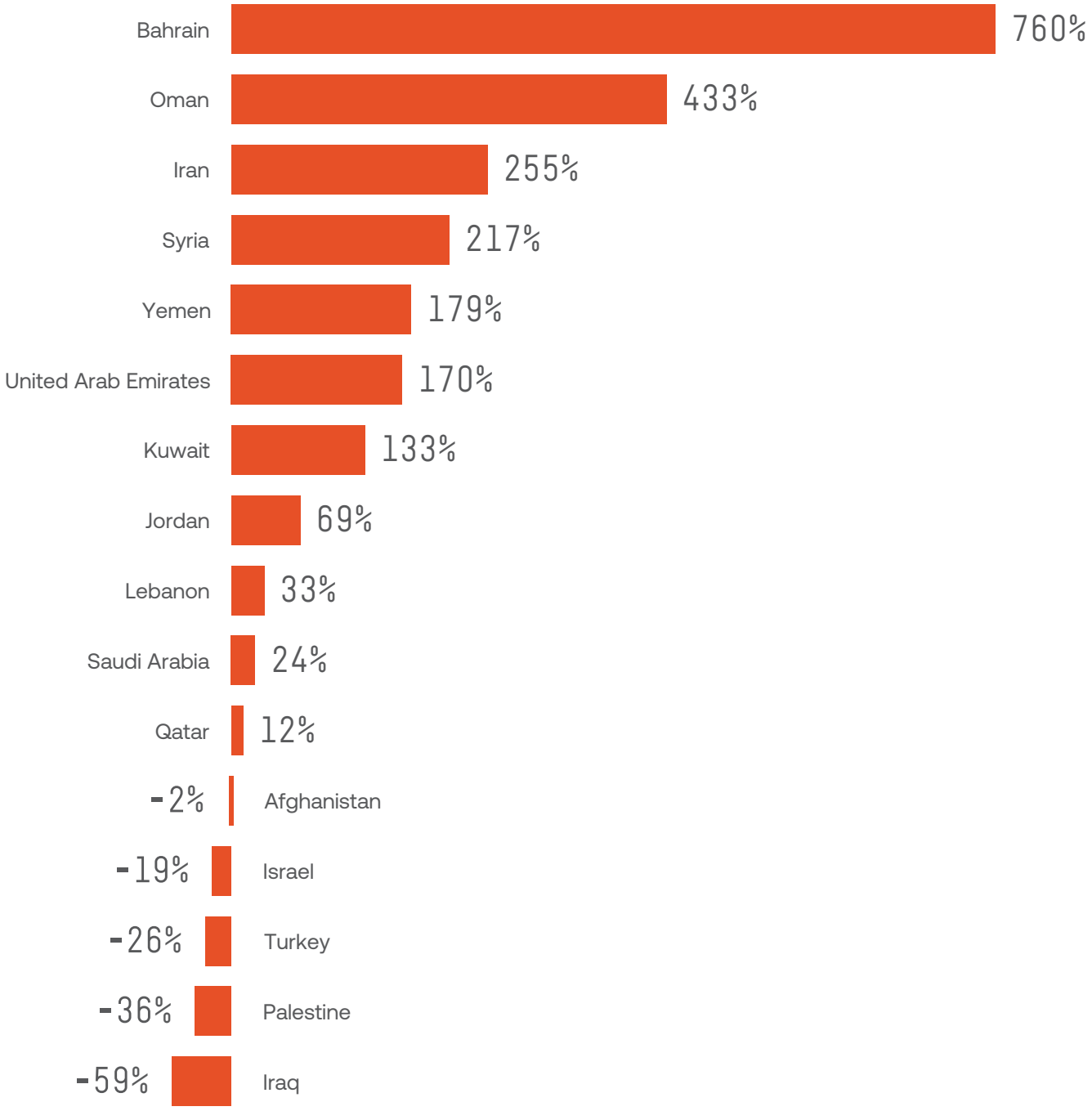
Moderate or declining markets

1. **Yemen and Syria** both experienced slight declines in fraud, but deepfake activity grew significantly (+179% and +217%, respectively), highlighting that sophistication is rising beneath the surface.
2. **Jordan decreased to 1.9% (–19% YoY)**, but deepfakes still rose nearly +70% YoY.
3. **The United Arab Emirates' rate halved to 1.4% (–44% YoY),** thanks to advanced digital ID systems; yet, fraud networks continue to exploit loopholes across borders.

Stable but increasingly sophisticated markets

1. **Qatar (1.4%), Oman (1.4%), and Kuwait (1.0%)** remain relatively low in absolute terms, but all reported triple-digit growth in deepfakes, indicating that attackers are advancing up the sophistication ladder.
2. **Saudi Arabia and Israel** stayed near 1.1%, flat overall, but both posted increases in deepfake attempts, marking another sign that volume stability masks growing complexity.

Chart 58.
Middle East countries with the largest YoY deepfakes growth (2025 over 2024)



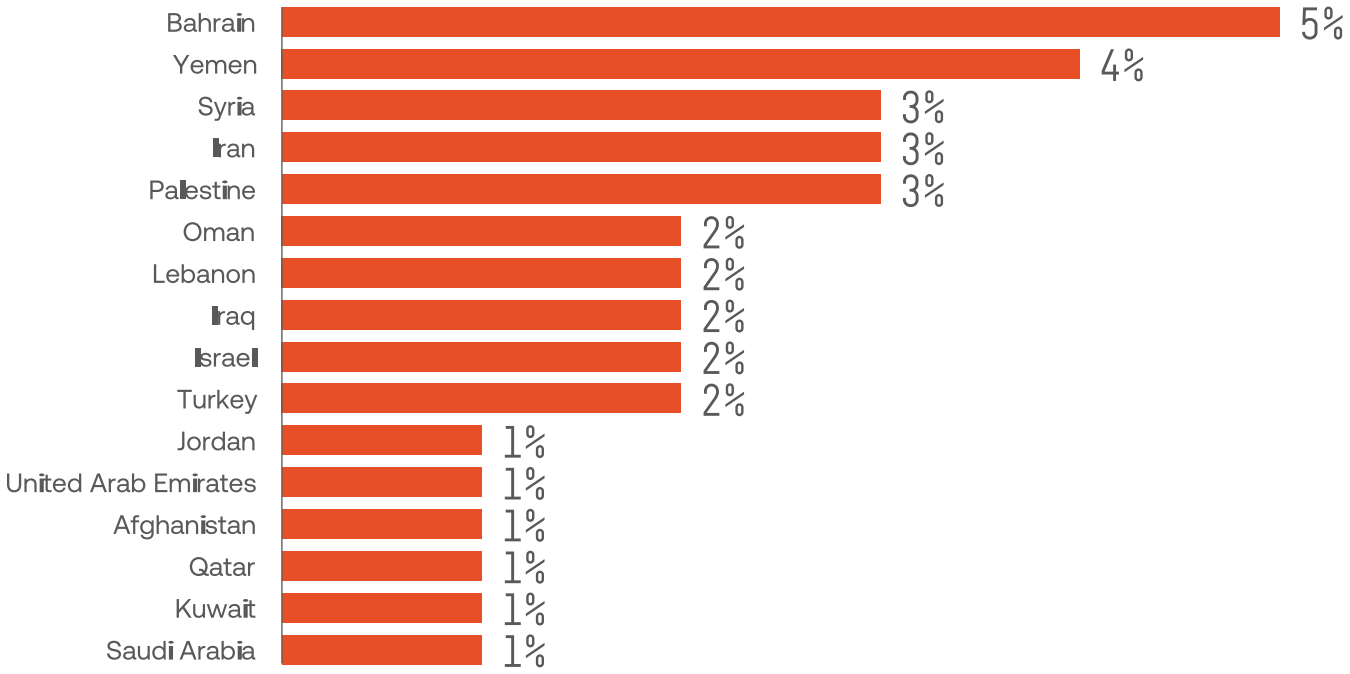
Sumsub's Fraud Exposure Survey
2025, Middle East: Consumers

Deepfakes in the Middle East: rising speed, uneven impact

Deepfakes are spreading rapidly across the Middle East, reshaping the fraud landscape from experimentation to mass use. In 2025, Bahrain recorded the region's sharpest increase, with deepfake-related fraud soaring by +760% YoY, followed by Oman (+433%) and Iran (+255%). While these countries lead in growth, the overall distribution tells a broader story: Turkey (22.9%), the UAE (18.2%), and Iran (9.5%) now account for more than half of all deepfake cases in the region.

At the same time, even traditionally lower-risk markets such as Saudi Arabia (9.4%) and Israel (5.8%) are experiencing noticeable increases — showing that AI-generated identity manipulation has moved from fringe to mainstream. The trend underscores a regional reality: high regulation may keep fraud volumes stable, but it no longer prevents the spread of sophisticated, AI-powered deception.

Chart 59.
Ratio of approved applicants involved in fraud networks



Why some countries fell while others rose

The contrasts reflect regulatory maturity and the focus of the attacker. Countries with strong investments in digital ID and biometric onboarding (like the UAE and Saudi Arabia) saw overall fraud drop, but now face a new wave of deepfake-enabled fraud. Meanwhile, countries with weaker regulatory capacity or ongoing instability (Iraq and Afghanistan) remain hotbeds for volume-driven fraud, where both crude and sophisticated attacks thrive.

Fraud rings are also highly mobile. As stronger markets close loopholes, attackers pivot quickly to softer jurisdictions, explaining why fraud is declining in the Gulf but soaring in Iraq.

What to expect next

Looking toward 2026, the Middle East will likely split along two paths:

1. **High-risk frontier markets** (Iraq, Afghanistan) will continue to face both high fraud rates and growing deepfake penetration, making them global hotspots for fraud testing.

2. **Digitally advanced economies** (UAE, Saudi Arabia, Israel, Qatar) will keep fraud volumes low but face the world's sharpest rise in AI-driven fraud, as attackers focus on deepfakes, synthetics, and multi-modal spoofing to bypass advanced checks.

Expect fraud rings to expand cross-border, recycling synthetic personas across multiple Gulf states, and deepfake fraud to move mainstream in financial services and telecom. Regulators are tightening frameworks, but uneven enforcement means the Middle East will likely remain one of the most volatile regions for fraud worldwide.

Global challenge, local realities

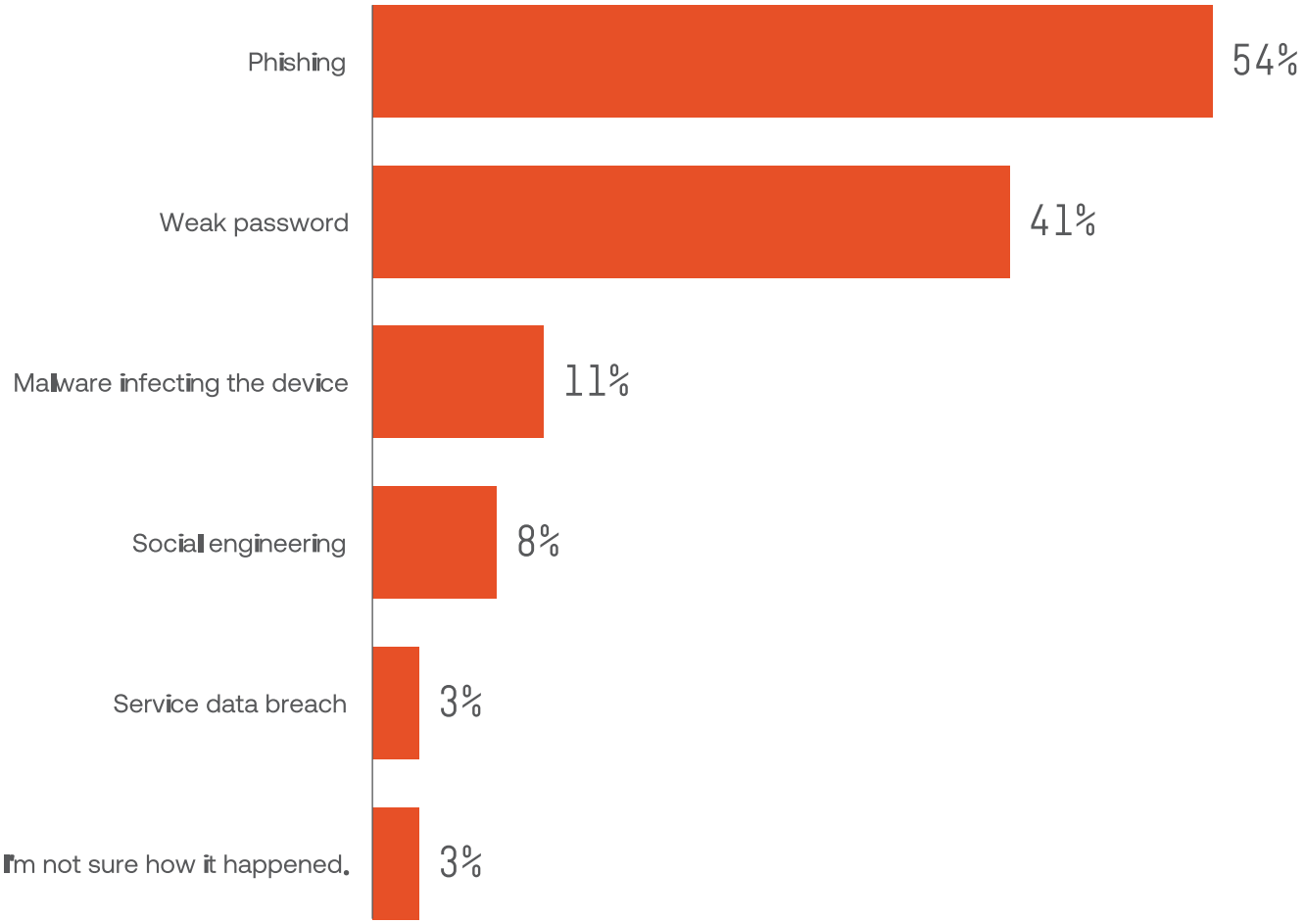
Discover the Middle East's performance in Sumsub's Fraud Exposure Survey 2025.

Consumer fraud findings in the Middle East

Main attack vectors

Phishing drives more than half of all fraud cases (54%), followed by weak passwords (41%) — both clear signs that user behavior remains the easiest way for attackers to gain access. With technical exploits like malware or social engineering playing a smaller role, the data indicate that simple hygiene — stronger passwords, better awareness, and smarter authentication — can prevent most attacks before they occur.

Chart 60.
Question:
What do you think was the cause of the fraud incident?



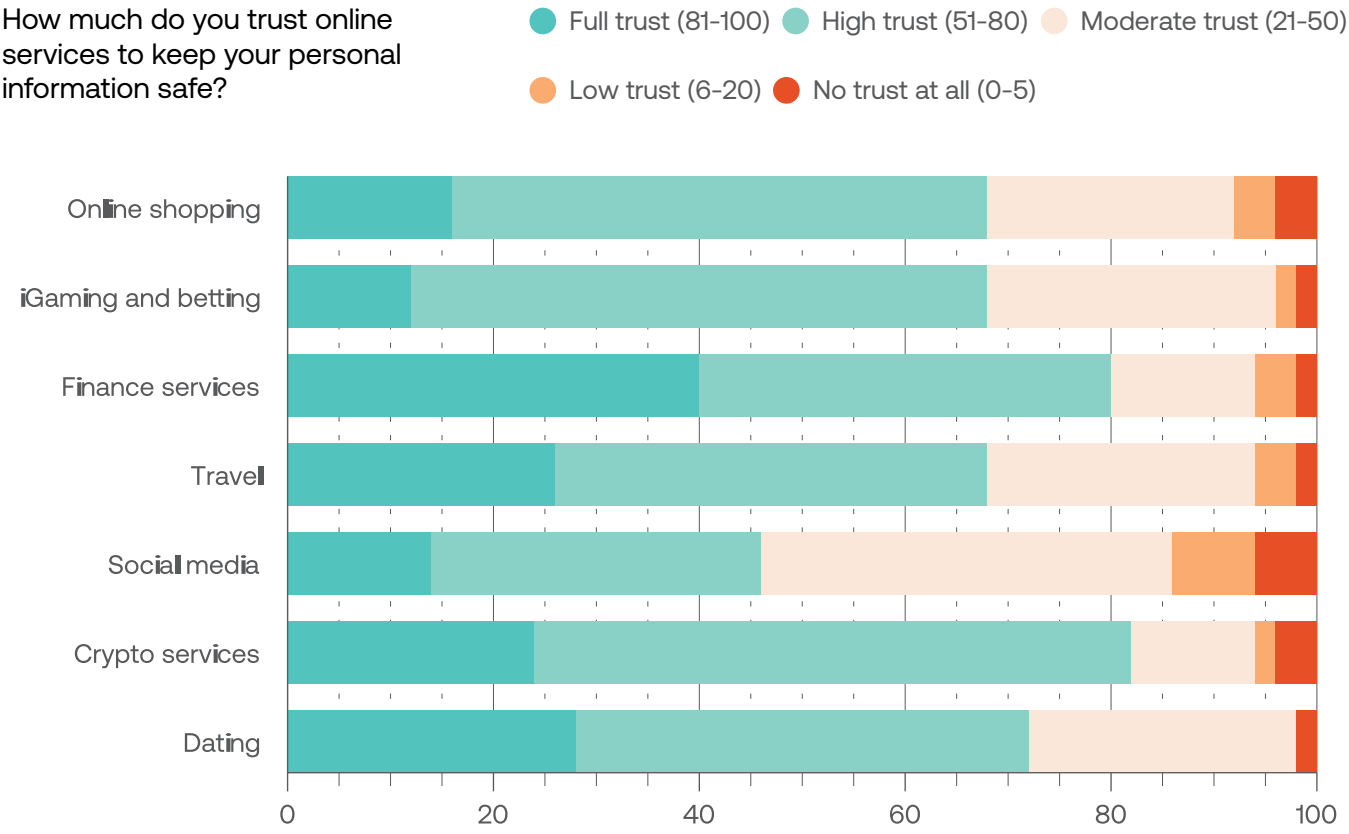
Sumsub's Fraud Exposure Survey 2025,
Middle East: Consumers

Digital trust in the Middle East

Finance and crypto platforms lead the way, with nearly all users expressing strong confidence in their data protection — a testament to tighter regulation and mature compliance frameworks. Travel and dating also show solid trust levels, with around two-thirds or more of respondents placing high or full trust in them — indicating users feel increasingly comfortable sharing data with lifestyle and entertainment platforms.

However, social media still lags behind, where only about 46% of users express trust. With repeated exposure to scams and data misuse, this sector faces the most challenging task of rebuilding user confidence.

Chart 61.
Question:
How much do you trust online services to keep your personal information safe?



Sumsub's Fraud Exposure Survey 2025, Middle East: Consumers

98% of respondents would choose a service provider only if they have strong anti-fraud measures in place.

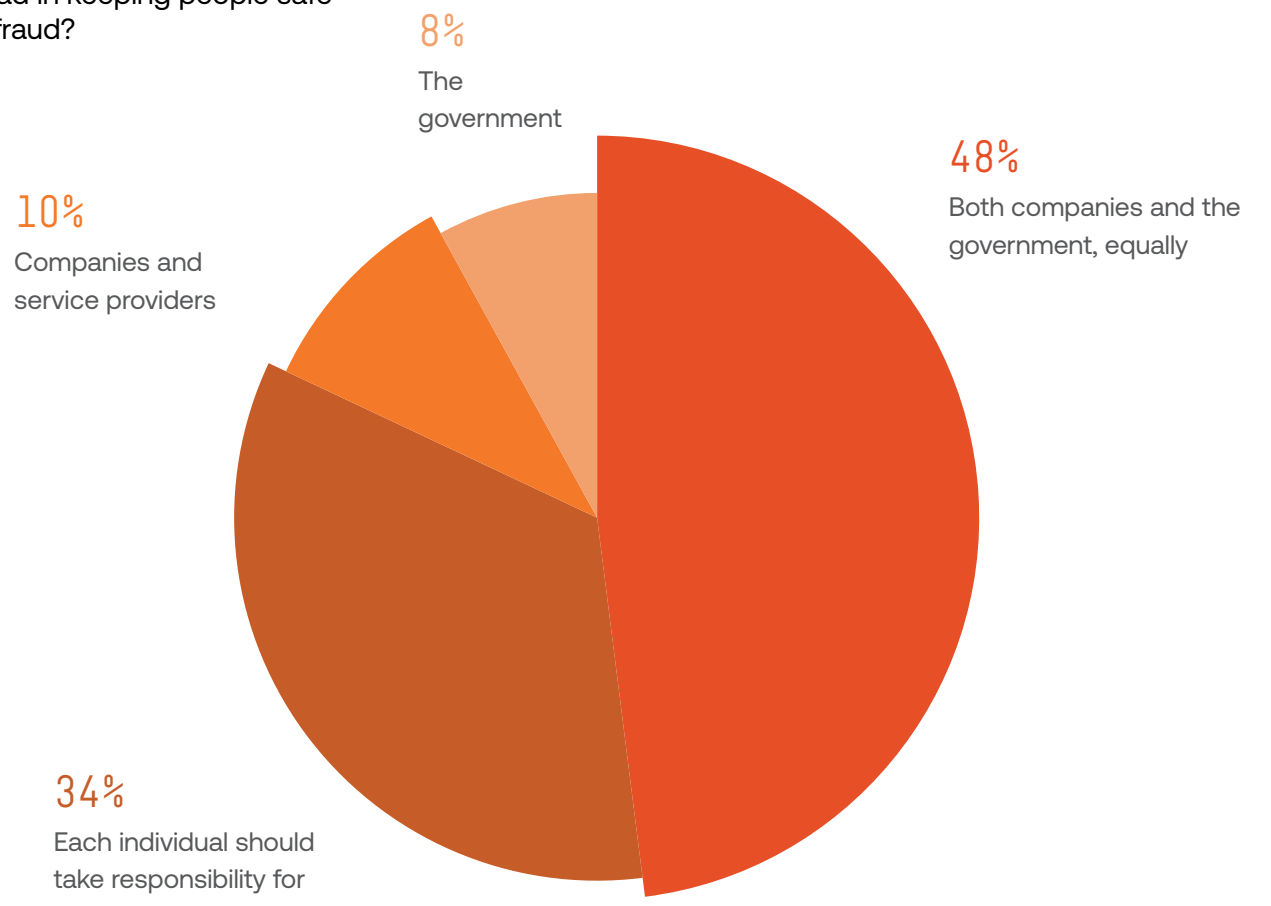
98%

Responsibility for fraud prevention

When it comes to fighting fraud, users see it as a shared responsibility — **nearly half (48%) believe companies and governments should work together** to keep people safe. At the same time, **one in three (34%)** think individuals themselves should take charge of their own protection, showing a growing awareness of personal accountability in digital security.

Only a small share expects companies (10%) or governments (8%) to act alone — reinforcing that trust in the fraud-fighting ecosystem depends on collaboration across all levels: public, private, and personal.

Chart 62.
Question:
Who do you think should take the lead in keeping people safe from fraud?



Sumsub's Fraud Exposure Survey 2025, Middle: Consumers

Virtual cards gain ground

Virtual and disposable cards are steadily becoming part of everyday payment habits. **Over 70% of respondents** use them at least occasionally — proof that consumers are actively embracing **safer, privacy-first payment methods.**

Still, **around 1 in 3** rarely or never use virtual cards, revealing an untapped opportunity for **greater education and accessibility** regarding digital payment protection tools.

Question:
Do you use disposable or virtual cards for online payments?

Sumsub's Fraud Exposure Survey 2025, Middle East: Consumers

Money mulling awareness grows, but understanding still lags

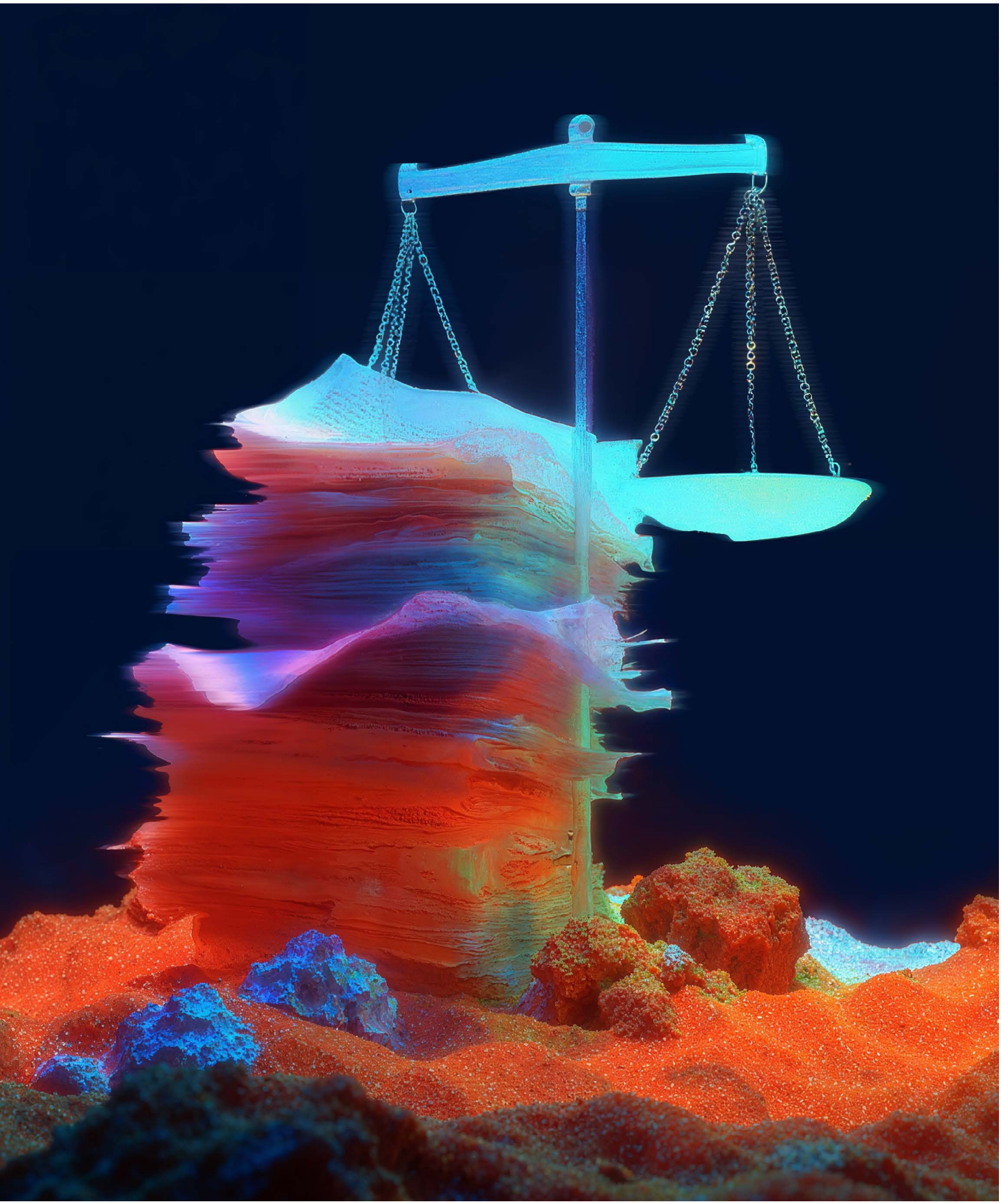
Awareness of money muling is growing — **nearly half of respondents (46%)** have heard the term, yet most still don't grasp its seriousness or legal risks.

Alarmingly, almost **1 in 5** have been personally targeted to move stolen money, showing that mule recruitment remains an active and evolving threat.

With **over a third** still unaware of the concept, there's a clear need for stronger public education and preventive communication to stop people from becoming unwitting participants in financial crime.

Question:
Have you heard of "money muling" - letting someone move stolen money through your bank account?

Sumsub's Fraud Exposure Survey 2025, Middle East: Consumers



Regulatory shifts redefining identity protection

As fraud tactics evolve, Middle Eastern governments are accelerating their adoption of robust financial compliance laws, digital identity frameworks, and enhanced supervisory powers. Here are some of the latest developments in the Middle East.

Bahrain

Payments and cybersecurity reforms
In July 2025, the Central Bank of Bahrain reinforced fraud prevention and cybersecurity obligations under Rulebook Volume 5 for licensees, including payment service providers, e-wallets, and financing companies. The reforms introduced stricter requirements for cyber risk management, incident detection and reporting, and oversight of outsourcing arrangements, supported by a “Cyber Security Requirements” communication that emphasizes continuous monitoring and stronger controls.

Saudi Arabia

Counter-fraud fundamental requirements framework
In April 2025, the Saudi Central Bank introduced the Counter-Fraud Fundamental Requirements Framework, replacing earlier anti-fraud rules. Finance companies and payment service providers must adopt risk-based controls across governance, prevention, detection, and technology, with full compliance required by 13 April 2026. Obligations include board-approved compliance roadmaps, reporting to SAMA, and oversight of internal audits.

The new Nazaha Law

On 7 November 2024, the revised Nazaha Law expanded the Oversight and Anti-Corruption Authority's powers to investigate and prosecute corruption and financial crime. Key changes include stronger investigative authority over financial fraud, enhanced cooperation with international bodies, expanded whistleblower protections, and greater penalties, including asset forfeiture.

UAE

Stronger authentication and fraud prevention policy

In 2025, the Central Bank of the UAE issued a directive requiring banks to phase out SMS and email OTPs and static passwords for consumer transactions by March 2026. Institutions must adopt more secure methods, such as biometric verification, app-based approvals, passkeys, and device-bound authentication, to mitigate the risks of phishing, SIM swapping, and account takeover fraud.

Telemarketing and scam call regulations

In July 2024, the UAE tightened its Telemarketing Regulations, restricting call hours, limiting unsolicited outreach, and requiring licensed telemarketers to keep records. The measures are supported by ongoing warnings from regulators about fraudulent trading platforms, loan scams, and shell companies, as well as public awareness campaigns in 2025 focused on phishing, phone/SMS fraud, and high-return investment schemes.

Alexey Podoynitsyn,
Sales Director,
Middle East at Sumsub

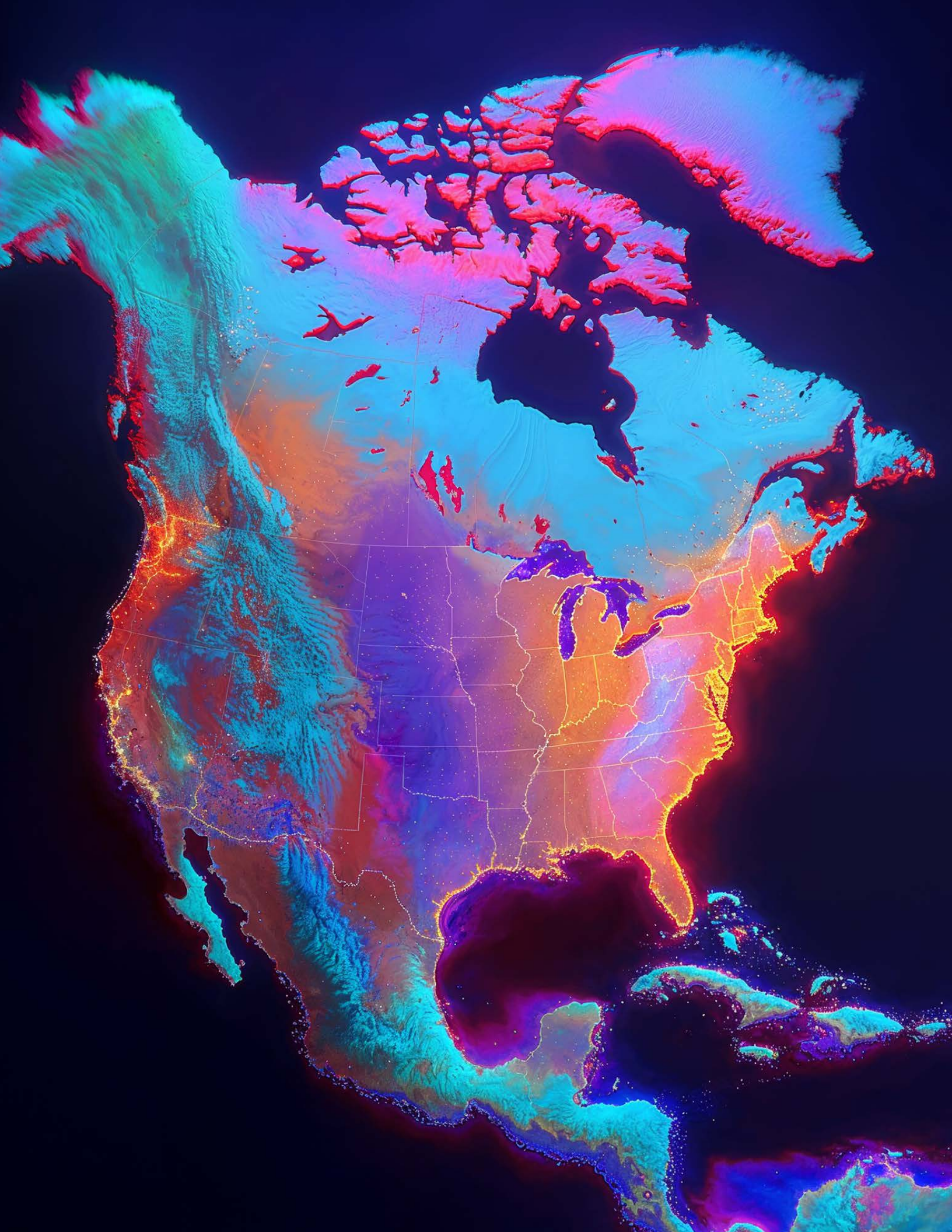
"The Middle East is at a defining moment in its digital journey. Across the Gulf, governments are investing heavily in eKYC, biometric systems, and national digital identity frameworks — setting a global benchmark for secure onboarding. At the same time, we're witnessing the rapid emergence of new threats that exploit this digital acceleration. In 2025, AI-generated deepfakes and synthetic identities have moved from isolated incidents to systemic risks, targeting financial services, telecom, and e-government channels alike.

What's striking is how uneven the landscape has become. Markets like the UAE, Saudi Arabia, and Bahrain have built sophisticated compliance ecosystems that are pushing fraud rates down. Yet, at the same time, frontier markets across the Levant and North Africa are facing an explosion in advanced fraud, driven by organized networks that operate across borders and exploit weak verification controls.

The next frontier of protection in the Middle East won't be about adding more checkpoints — it will be about intelligence and collaboration. AI-driven behavioral analytics, federated data-sharing, and real-time fraud intelligence between regulators and the private sector will be essential to outpace this new wave of fraud. The region has both the ambition and the technological capability to lead this global shift — transforming the Middle East from a high-risk target into a global model for digital trust and resilience."

U.S. & Canada

North America remains one of the most mature regions globally in terms of fraud-fighting, with robust KYC frameworks, widespread biometric adoption, and industry-standard fraud analytics. Yet 2025 reveals a quieter evolution: while headline fraud rates fell, the quality of attacks improved dramatically. The region exemplifies the late stage of the Sophistication Shift—volume down, sophistication up.



Fraud type evolution

The North American data shows that attackers are moving away from brute-force abuse toward AI-assisted precision.

Deepfake and synthetic identity fraud dominate any new attempts.
Traditional document forgery is nearly obsolete; instead, fraudsters combine AI-generated selfies and fabricated personal data to bypass liveness checks. Synthetic identity attempts grew steadily throughout 2025, and deepfake incidents surged—rising +237% in the U.S. and +124% in Canada year over year.

Nearly a third of respondents (31%) have already encountered deepfakes online, while another 26% aren't sure — highlighting how convincingly real synthetic media has become. Although only 11% admit to being personally targeted or deceived, this still marks a worrying sign of how AI-generated manipulation is shifting from novelty to an everyday risk.

Question:
Which of these best describes your experience with deepfake videos or audio?

Sumsub's Fraud Exposure Survey 2025, U.S. & Canada: Consumers
All responses represent the personal experiences of all survey participants.

Fraud involving inconsistencies between a user's selfie and their ID image remains the leading category.
These categories account for nearly half of all flagged cases, and many are now driven by AI-manipulated video streams rather than basic impersonation.

Behavioral tampering on the rise.
Investigators reported growing evidence of telemetry manipulation, where attackers attempt to spoof device and environmental data during verification sessions. This aligns with the global shift toward behavioral evasion, where instead of falsifying identity, fraudsters fake the context.

Chart 63.
Fraud rates in the U.S. and Canada (2023-2025)

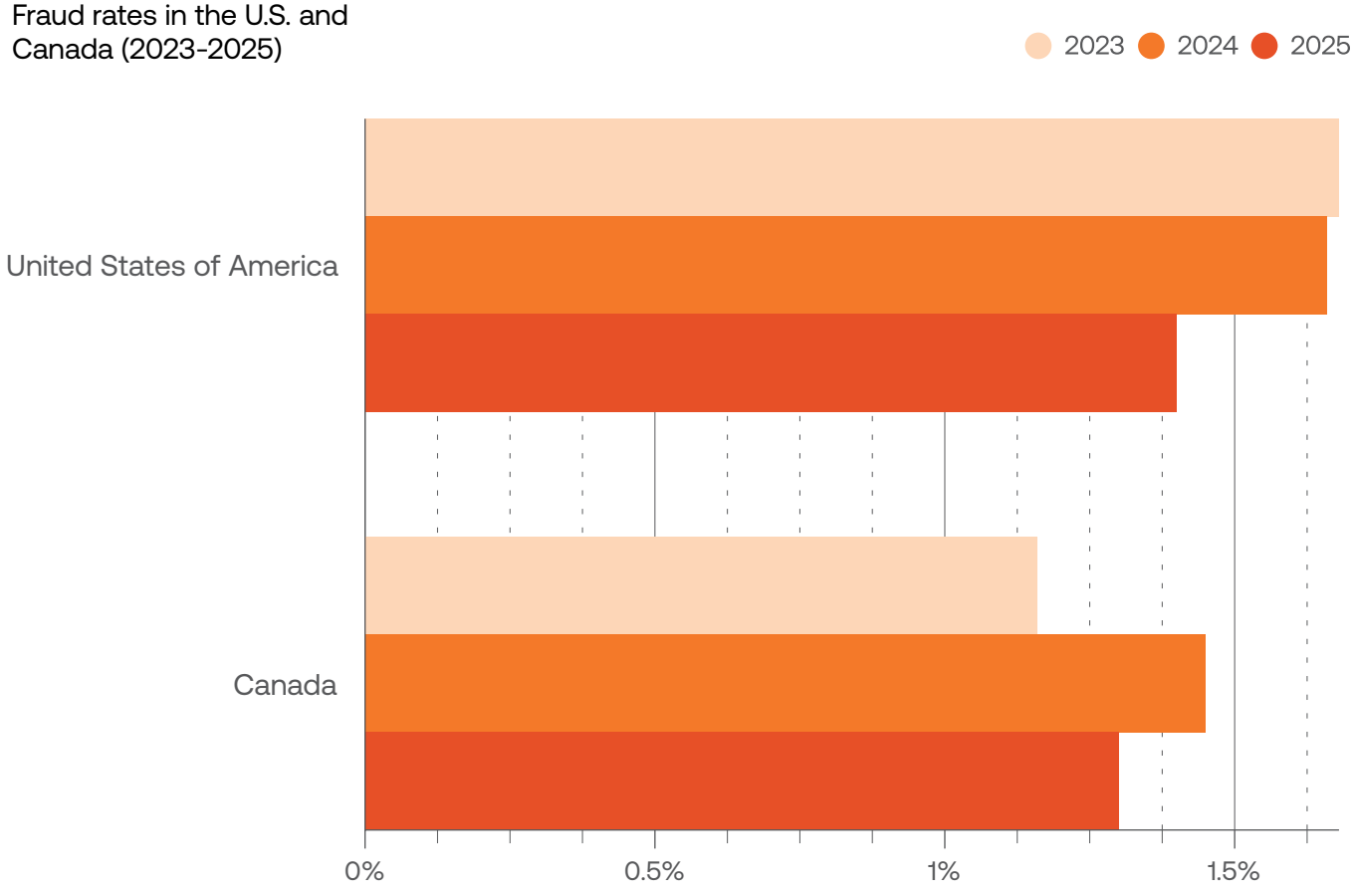
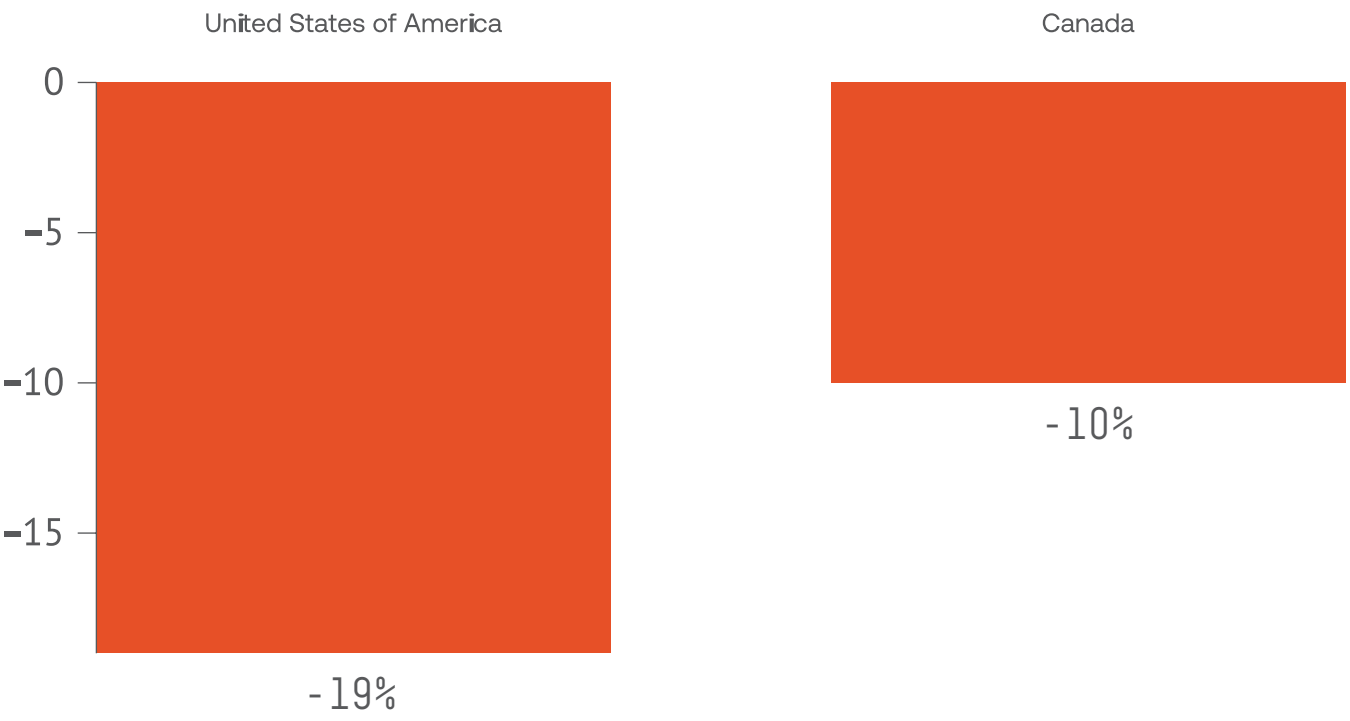


Chart 64.
Fraud dynamic in the U.S and Canada (2025 over 2024)



Country-level dynamics

United States

Fraud fell to 1.4% in 2025 (–19% YoY), marking one of the lowest rates globally. The drop follows widespread adoption of real-time ID checks and liveness-driven verification in fintech and banking. However, deepfakes increased more than twofold (+237%), particularly in lending, gig-economy onboarding, and account recovery scenarios. Fraud is now less about scale and more about quality—a few, high-impact synthetic identities that slip through sophisticated systems.

Canada

Canada's overall fraud rate also declined to 1.3% (–10% YoY), supported by stronger onboarding verification requirements from regulators and expanded digital ID initiatives at the provincial level. Still, deepfakes surged by +124%, and synthetic-data attacks rose as fraudsters exploited differences between provincial and national data-sharing frameworks. Canada's challenge mirrors that of the U.S.: fewer attempts at fraud, but more subtle and coordinated ones.

Chart 65.
YoY deepfakes growth
(2025 vs 2024)

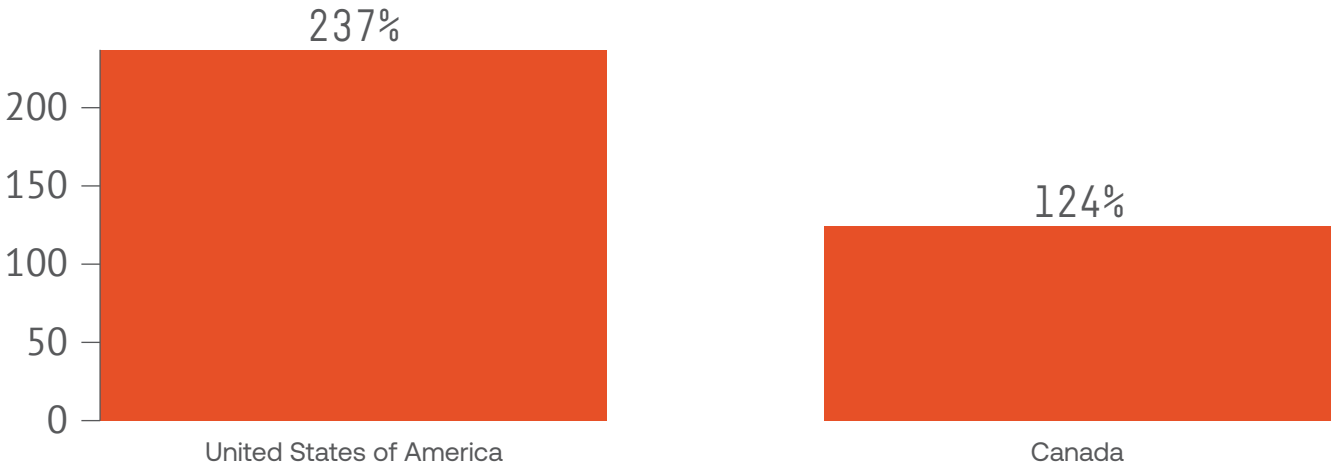


Chart 66.
Ratio of approved applicants involved
in fraud networks in 2025

Matthew Rosenquist,
CISO and Cybersecurity Strategist
at Mercury Risk and Compliance,
Inc.; Founder & CISO Advisor at
Cybersecurity Insights.

"Cybercriminals will successfully leverage Artificial Intelligence tools to greatly increase both the quantity of social engineering attacks as well as the effectiveness of the victimization. AI will automate the distribution of more compelling fraudulent communications. We will witness more interactive engagements, customized for specific individuals, that take advantage of cognitive vulnerabilities in support of the attackers objectives. Bottom Line: AI powered social engineering attacks will be much more difficult to detect and avoid, creating a global spike in data loss, fraud, and the harvesting of credentials.

The rise of technical vulnerability exploitation has surprisingly increased while the longtime favorite of credential abuse has seen a decline. This is likely due to the widespread implementation of Multi-Factor Authentication and tighter controls associated with Zero Trust architectures."

What to expect next

Through 2026, North America is expected to continue experiencing low-volume but high-impact fraud. Key trends include:

1. **Deepfake normalization.**
   AI video and voice tools will be used not only in onboarding, but also in the customer service sector and insider impersonation.

2. **Cross-platform synthetic identities.**
   Fraudsters will deploy single synthetic personas across banking, gig work, and digital lending—making detection a multi-sector challenge.

3. **Rise of behavioral forensics.**
   Companies are investing in behavioral and telemetry-based analysis, not just document verification, to detect fraud attempts that “feel” legitimate but act abnormally.

4. **Regulatory evolution.**
   Expect updated federal guidelines in both countries requiring transparent AI governance for identity verification providers.

The paradox remains: North America’s fraud rate may be falling, but the real risk is rising. Fewer attacks reach the system, yet each one that does is engineered with AI precision, harder to detect, and far more costly when successful.

Global challenge, local realities

Discover North America's performance in Sumsub's Fraud Exposure Survey 2025.

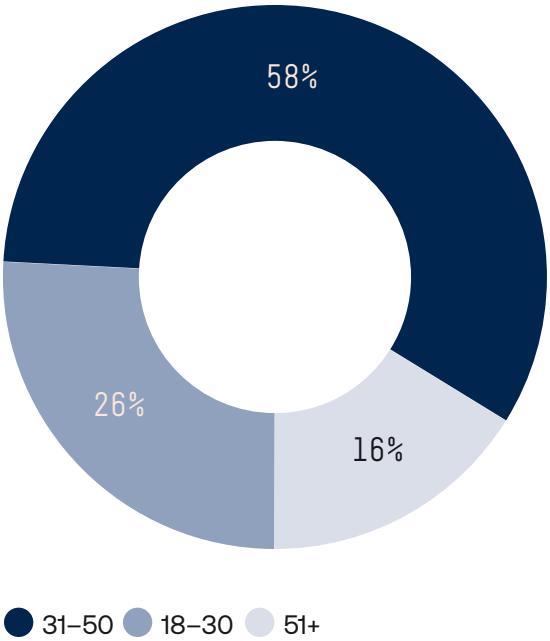
Both the enterprise and consumer sectors in the U.S. & Canada exhibit high exposure, with 78% of businesses and over 62% of users facing fraudulent activity this year.

Consumer fraud findings in the U.S. & Canada

Take a closer look at who our consumers in the U.S. & Canada are, from their age to employment status.

Chart 67.

Age



31–50 18–30 51+

Employment status

68%
Employed full-time

12%
Employed part-time

10%
Self-employed full-/part time

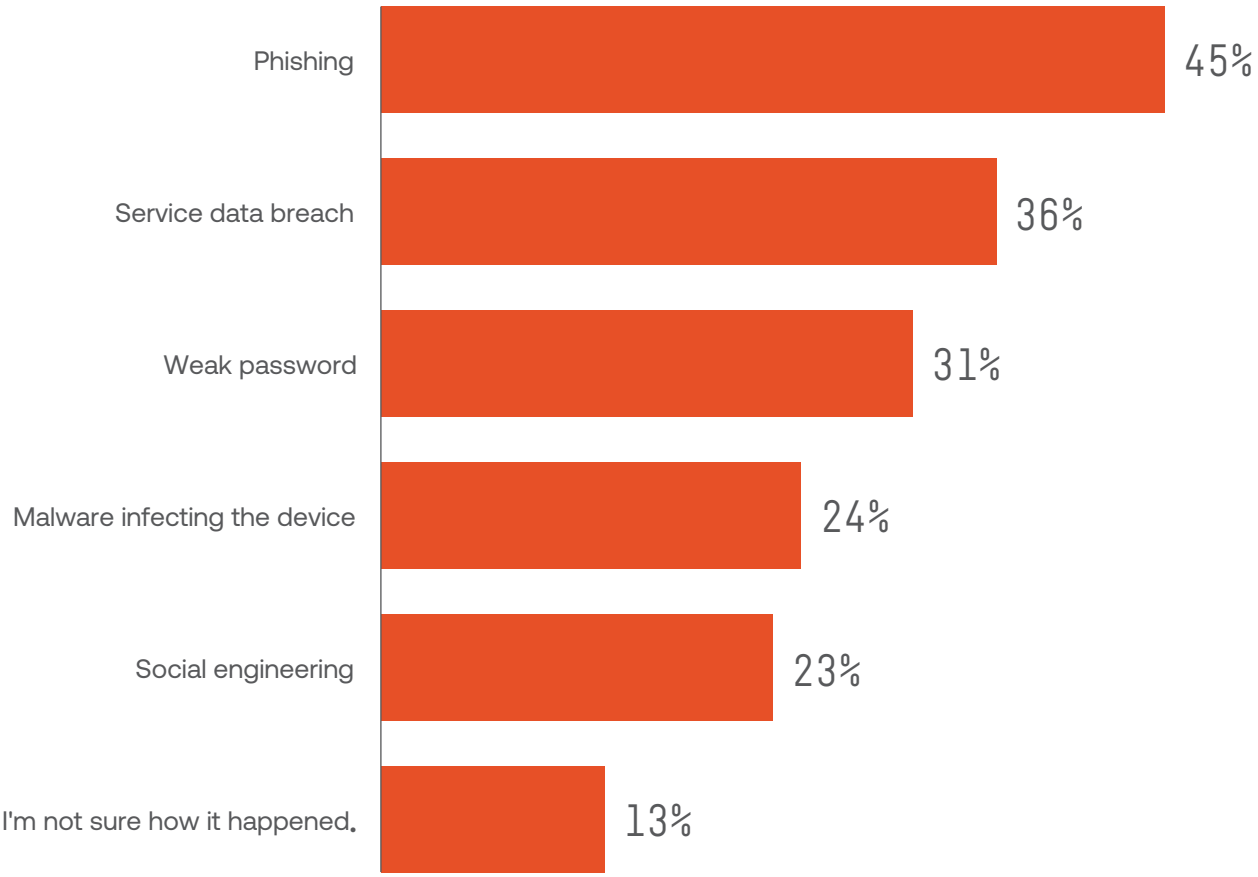
10%
Temporarily unemployed

Main attack vectors

Phishing remains the single largest entry point (45%), but the picture is clearly multi-vector: **service data breaches (36%)** and **weak passwords (31%)** together account for a large share of compromises — meaning attackers exploit both platform failures and user habits.

Device malware (24%) and social engineering (23%) indicate that attackers are combining technical and psychological techniques, while 13% of cases with unknown vectors suggest a growing trend towards stealth and automation.

Chart 68.
Question:
What do you think was the cause of the fraud incident?



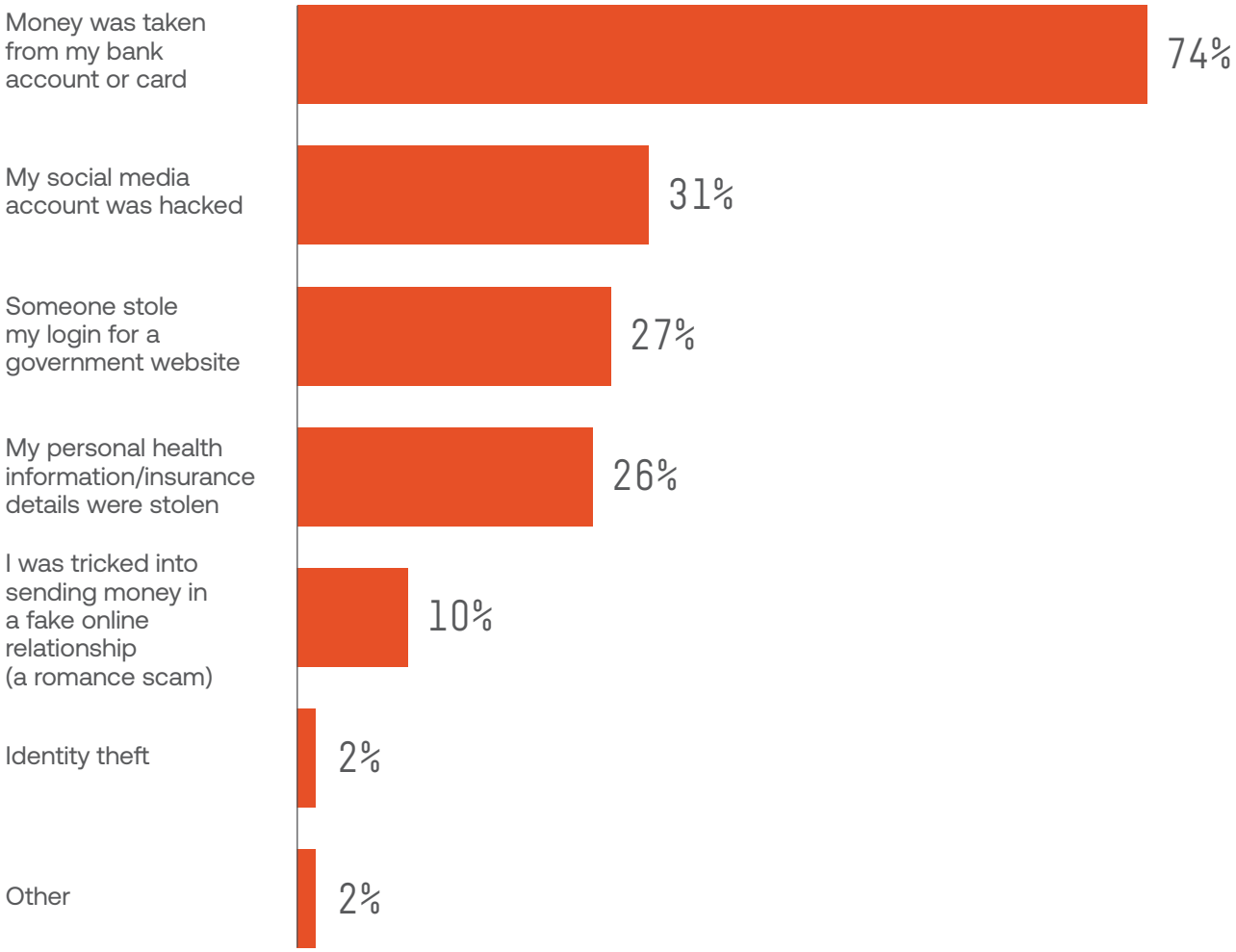
Sumsub's Fraud Exposure Survey 2025, the U.S. & Canada: Consumers

Main fraud outcome

Financial theft dominates the fraud landscape — nearly three-quarters (74%) of victims had money stolen directly from their bank accounts or cards.

At the same time, account takeovers remain rampant, with 31% of respondents losing access to social media and 27% having government logins compromised — both gateways to identity misuse and further fraud chains.

Chart 69.
Question:
What type of identity fraud did you experience?



Sumsub's Fraud Exposure Survey 2025, the U.S. & Canada: Consumers

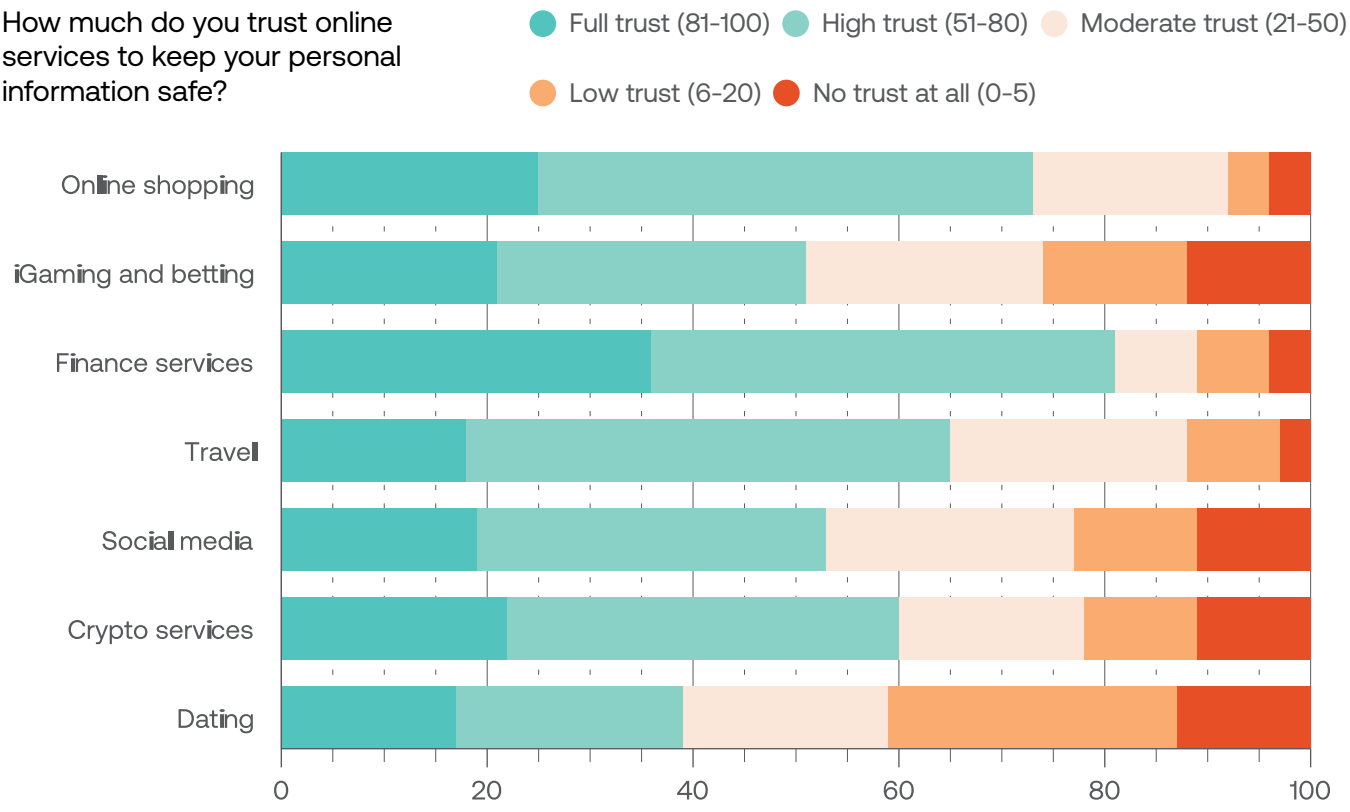
84% of respondents would choose a service provider only if they have strong anti-fraud measures in place.

Digital trust in the U.S. & Canada

Finance leads with 81% trust—the strongest and most stable confidence profile. Online shopping (73%) and travel (64%) also score well, likely benefiting from clear protections (refunds, dispute rights, strong checkout security).

Crypto is polarized, with 60% of respondents having high trust versus 22% having low or no trust. Social media shows a similar split (53% vs. 23%), consistent with scams, ATO, and privacy concerns. iGaming (51% vs. 26%) carries the same uneven trust tied to licensing variance and bonus abuse risks. Dating is the outlier, with only 41% of users trusting it, and the highest level of distrust (37%)—users remain wary of catfishing, data misuse, and impersonation.

Chart 70.
Question:
How much do you trust online services to keep your personal information safe?

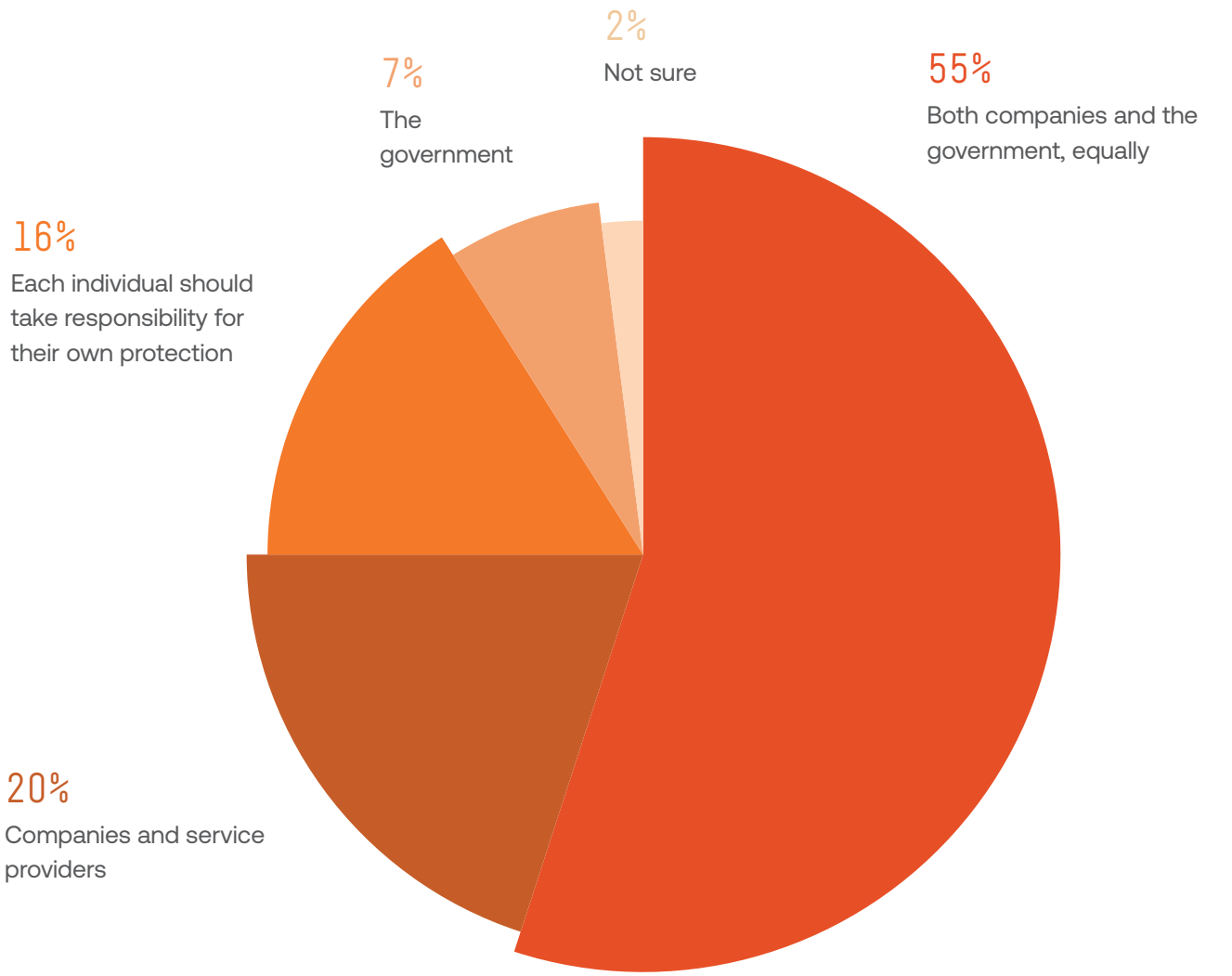


Sumsub's Fraud Exposure Survey 2025, the U.S. & Canada: Consumers

Responsibility for fraud prevention

More than **half of respondents (55%)** believe that **companies and governments must work together** to keep people safe, indicating a strong appetite for **collaborative, system-level protection** rather than user-only vigilance.

Chart 71.
Question:
Who do you think should take the lead in keeping people safe from fraud?



Sumsub's Fraud Exposure Survey 2025, the U.S. & Canada: Consumers

Virtual cards still have room to grow

When it comes to online payments, virtual and disposable cards are gaining steady traction — but not yet universal. Roughly **one in four users (28%) report using them frequently**, while **another 26% do so occasionally**, showing that digital payment hygiene is improving but remains uneven.

Still, **nearly half (46%) of respondents rarely or never use** virtual cards, suggesting that awareness and accessibility gaps persist — especially outside tech-savvy or finance-driven segments.

Question:
Do you use disposable or virtual cards for online payments?

Sumsub's Fraud Exposure Survey 2025, the U.S. & Canada: Consumers

High awareness, high exposure: money mule scams remain active

While 56% of respondents have at least heard of money muling, most don't fully grasp what it means or how serious it is. 20% of respondents report being asked to transfer money to unknown accounts.

This suggests that money mule recruitment attempts are widespread, and a substantial portion of individuals have already been directly targeted.

Question:
Have you heard of "money muling" - letting someone move stolen money through your bank account?

Sumsub's Fraud Exposure Survey 2025, the U.S. & Canada: Consumers

67% of respondents are highly convinced that fraud is becoming more sophisticated and AI-driven

This confirms that companies are aware of deepfake risks, synthetic identities, and AI-driven forgeries, and are looking for next-generation fraud prevention solutions.

67%

Company fraud findings in the U.S. & Canada

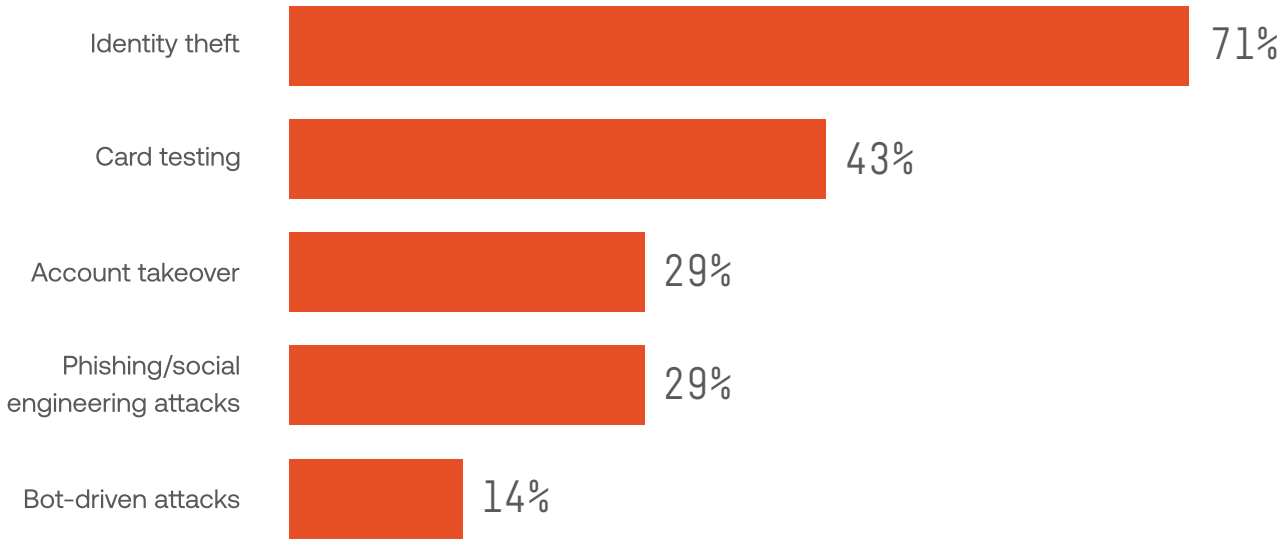
Top 3 types of fraud faced by companies in Europe

1. Identity theft (71%)
2. Card testing (43%)
3. Account takeover and phishing/social engineering attacks (29% each)

At the same time, they had to manage first-party fraud from their customers, who used synthetic identity (86%) and deepfakes (57%) and conducted application and money muling (29% of cases, respectively).

57% report that organized fraud attempts have become more frequent.

Chart 72.
Question:
What kind of third-party fraud has your business faced?



Sumsub's Fraud Exposure Survey 2025, the U.S. & Canada: Companies

Major consequences companies have experienced as a result of fraud attacks:

1. Financial losses: 57%
2. Reputational damage: 43%
3. Employee distrust/turnover: 29%

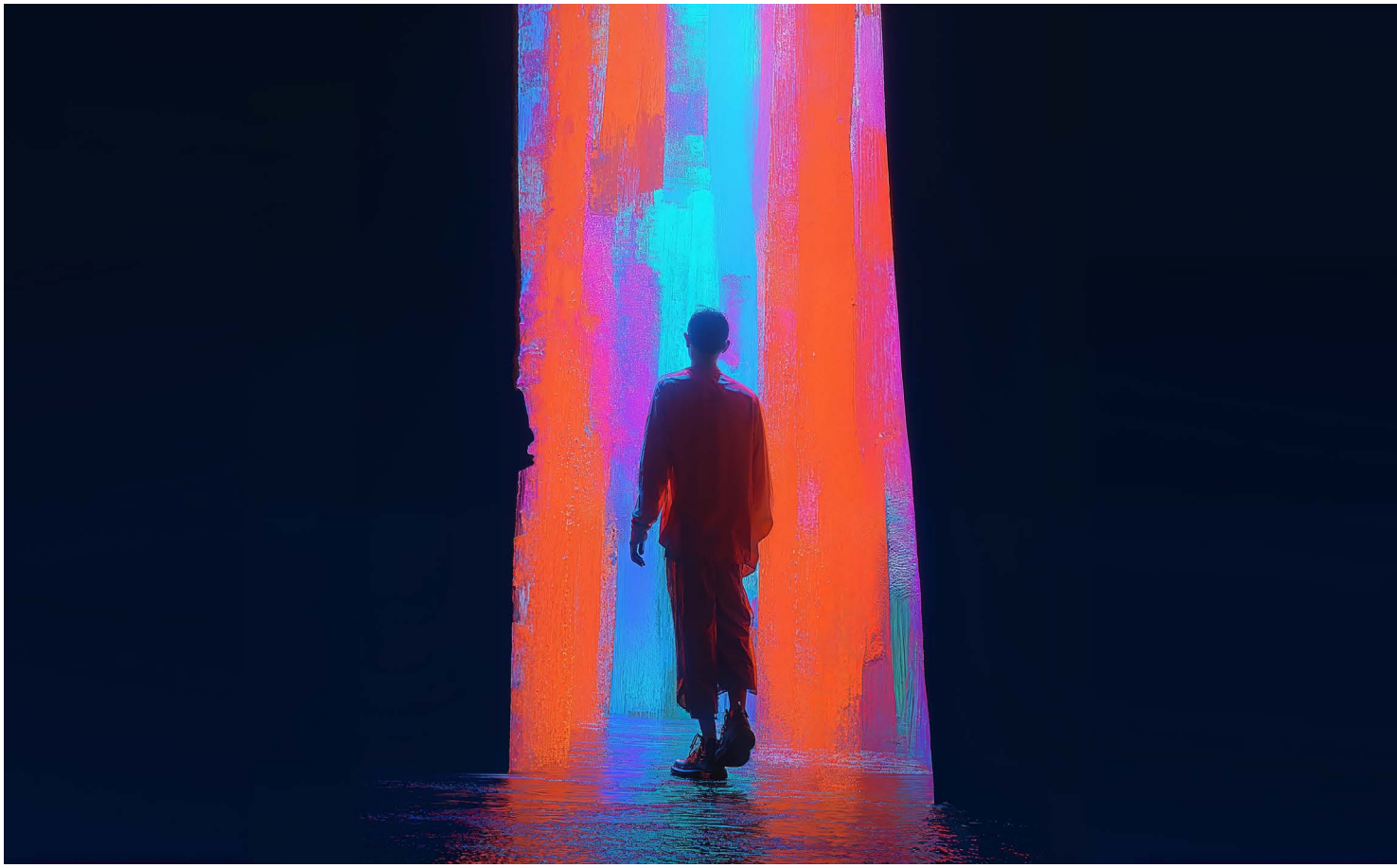
How companies in North America manage fraud

Businesses in this region demonstrate a strong internal grasp of fraud prevention, with **over half (56%) relying primarily on in-house technology.** At the same time, one in three companies (33%) combine in-house tools with external solutions or manual processes, showing that hybrid models remain essential for balancing automation with human expertise.

When identity fraud strikes, **two-thirds of businesses (67%)** report incidents to both industry regulators and law enforcement, signaling a high level of procedural maturity and commitment to accountability.

More than half of respondents (56%) say they'd welcome stricter regulations to fight identity fraud — even if compliance becomes more demanding. The remaining 44% remain cautious, likely weighing the cost of operational friction against potential security gains.

Employment fraud has become a serious problem in the U.S. as scammers harvest personal data and drain bank accounts by posing as potential employers. The Federal Trade Commission (FTC) reported job scams being one of the fastest-growing types of fraud, with losses rising from $90 million in 2020 to $501 million in 2024.



Predictions for the future

1 Two-thirds of respondents (67%) expect a surge in attacks targeting biometric systems, while over half foresee synthetic identities and cybersecurity pressure as defining challenges of the next wave.

2 With AI-powered deception — from deepfakes to forged documents — cited by nearly half of participants, the industry anticipates a shift from isolated fraud incidents to automated, scalable, and hyper-realistic threats.

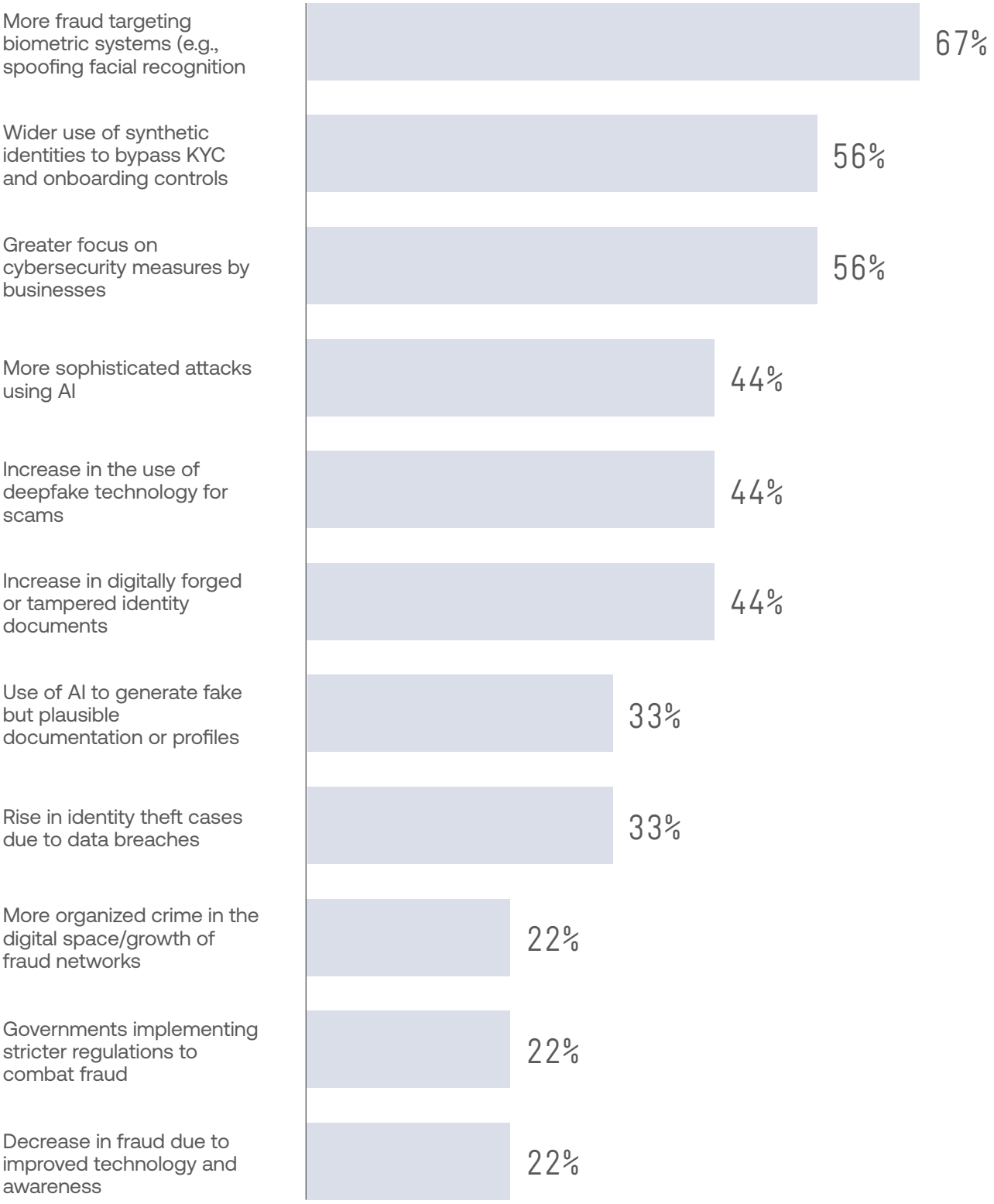


Chart 73.
Question:
What are your predictions for the future of the fraud landscape?

Sumsub's Fraud Exposure Survey 2025, the U.S. & Canada: Companies

Regional case studies of fraud up close

The following case studies spotlight real-world fraud incidents that occurred in North America in 2025.

1 **Singer Sean Kingston and his mother were convicted of wire fraud**

In March 2025, rapper Sean Kingston and his mother, Janice Turner, were found guilty in a Fort Lauderdale court of defrauding luxury retailers. Kingston used his fame and social media presence to obtain high-value goods—such as jewelry, cars, and electronics—before sending fraudulent wire transfers instead of payment. Turner managed logistics and communications to secure deliveries before sellers realized the deception. After just three and a half hours of deliberation, both were convicted: Kingston was placed under house arrest, and Turner was taken into custody for possible obstruction of justice.

2 **Over 300 charged in $14.6 billion US health care fraud crackdown**

In June 2025, the U.S. Justice Department announced the largest coordinated healthcare fraud takedown in its history, charging over 300 individuals in schemes that totaled $14.6 billion in false claims. Authorities seized $245 million in cash, cryptocurrency, and luxury assets. The biggest case involved a $10 billion fake catheter billing scheme. Among those charged were around 100 medical professionals, including 25 doctors, with the government citing $2.9 billion in confirmed losses. Officials described the operation as a major step in recovering taxpayer funds stolen through systemic billing fraud.

3 **Credit Suisse admits to US tax fraud, fined $510 million**
In May 2025, Credit Suisse pleaded guilty to helping American clients conceal more than $4 billion in assets from the IRS through offshore accounts. The Swiss bank agreed to pay $510 million in penalties as part of the settlement. Employees assisted clients in falsifying documentation to appear compliant while evading taxes, with at least 475 undeclared accounts involved. Following its 2023 acquisition by UBS, additional hidden accounts were discovered and reported to US authorities, expanding the scope of the investigation into long-running cross-border tax evasion.

4 **FBI's Operation Level Up prevents $400 million in scam losses**
In July 2025, the FBI's Operation Level Up identified and warned 6,475 potential victims of online investment and romance scams, preventing an estimated $400 million in further losses. Many targets were unaware they were being defrauded until contacted by investigators. Authorities noted the severe psychological toll, with 64 victims requiring suicide intervention, underscoring the deep emotional and financial impact of large-scale digital fraud.

5 **"Gold courier" scams targeting seniors exposed in the U.S.**
In April 2025, U.S. authorities disrupted a wave of so-called "gold courier" scams targeting elderly victims. Fraudsters posed as couriers or officials to collect cash and gold under false pretenses. Arrests in Maryland uncovered a network that stole over $700,000 in valuables, while parallel investigations in California dismantled similar operations. The cases highlight the growing sophistication of scams exploiting trust and vulnerability among older populations.

6 **North Korean hackers target crypto with job-offer scams**
In September 2025, new research exposed a widespread campaign where North Korean hackers were posing as recruiters on LinkedIn and Telegram, funelling candidates to complete ‘skills tests’ requiring downloads of video tools or spoofed sites, compromising their devices and draining crypto wallets. This North Korean operation, previously dubbed “Contagious Interview”, contained more than 230 targets and netted an estimated $1.34 billion worth of cryptocurrency in 2024 alone. The U.S. and United Nations monitors alleged that the thefts were being used to support its sanctioned weapons program.

Regulatory shifts redefining identity protection

As fraud grows increasingly advanced, North American regulators are focusing on transparency, cross-agency collaboration, and the responsible use of AI in compliance. Here are some of the latest developments in the U.S. and Canada.

Canada

New regulation amending Canada's PCMLTFA
In March, Canada amended its main AML/CFT law (PCMLTFA) by broadening the scope of regulated entities, bringing in factoring companies, cheque-cashing businesses, and financing or leasing companies under their AML/CFT obligations. Another amendment requires reporting entities to verify and report discrepancies between beneficial ownership information and Corporations Canada's registry, thereby improving transparency and preventing the misuse of corporate structures for illicit financial activities.

Canada's Border Services Agency granted enhanced powers
Also in March, to combat trade-based financial crimes, the CBSA was given the authority to require traders to declare whether goods are linked to money laundering, terrorist financing, or sanctions evasion.

U.S.

Exemption from beneficial ownership information

In March 2025, the FinCEN announced that all entities created in the United States and their beneficial owners are now exempt from the requirement to report beneficial ownership information under the Corporate Transparency Act. However, existing foreign companies that qualify as “reporting companies” must still report their beneficial ownership information to FinCEN.

Big Tech’s efforts to implement parental controls on AI chatbots

AI chatbots have become not only more human, but have been blamed for self-harm in both teenagers and adults. However, Big Tech is demonstrating adaptive efforts to manage these bots. In October, Meta announced new safety features for AI chatbots, including parental controls and chat limits, designed to safeguard teenagers’ mental health. These new guardrails will limit to age-appropriate topics and send summaries of conversations to their parents. Similarly, in September, OpenAI announced plans to introduce new parental controls, including improved responses to distress signals and assistance in reaching emergency services.

Anastasia Shvechkova,
Sales Director Americas
at Sumsub

"In North America, fraud has entered its most sophisticated phase yet. The numbers look encouraging—fraud rates fell to 1.4% in the U.S. and 1.3% in Canada, among the lowest globally—but beneath that stability lies a sharp evolution. Deepfake activity grew by +237% in the U.S. and +124% in Canada, while synthetic identities continue to climb. This tells us that the story isn't about more fraud; it's about smarter, stealthier fraud that hides inside the gaps of even the strongest systems. The defining change in 2025 is precision. We're seeing fraudsters move away from broad, low-effort scams and toward AI-orchestrated attacks—a handful of high-impact, cross-platform personas engineered to slip through advanced verification. Many exploit behavioral or telemetry manipulation rather than just forged IDs. In other words, fraud in North America is now less visible but far more dangerous when it succeeds.

The U.S., in particular, has become a testing ground for international fraudsters, who roll out and refine new schemes before exporting them worldwide. Emerging trends, like "employee fraud"—where fake workers or payroll identities are generated to exploit benefits, internal systems, or compliance blind spots—often debut here, targeting the region's mature digital and employment infrastructure. The region remains at the forefront of defense: real-time ID checks, biometric onboarding, and behavioral analytics are becoming standard. But staying ahead will mean matching AI with AI—deploying adaptive models that learn as fast as the threats do, and sharing intelligence across sectors to connect the dots between financial, social, and digital identities. North America's challenge is no longer scale—it's complexity. And solving that will define the next stage of global fraud prevention."

Fraud forecast for 2026

1 **AI remains a double-edged sword**
AI technology will continue to be exploited by fraudsters, enabling them to launch more sophisticated attacks with automation that can detect vulnerabilities at scale with less effort. The rise of synthetic identities, social engineering schemes, and autonomous AI Agents posing as real users will be a turning point for 2026. Fraud prevention will extend beyond the detection of deepfakes or tampered identity documents, but will increasingly depend on behavioral and contextual signals to verify identity based on an individual's actions.

2 **AI agents mark a new wave of identification**
Marked as one of our key trends for 2025, biometrics will be integrated with AI Agents in 2026, enabling the delegation of transactional tasks such as buying airline tickets or grocery shopping — all done securely and in your name. AI Agents may blur the lines between legitimate users and synthetic identities by providing real-time responses, complete verification flows, and imitating behavioral patterns to pose as genuine users.

3 **The multiplication of money mules**
Money mules are no new threat, but their numbers are expected to balloon in 2026. High-volume user base industries, such as financial services, iGaming, or e-commerce, may be exploited by fraudsters to blend in, as operating thousands of money mules moving illicit funds proves harder to detect in a user base of hundreds of millions. What continues to evolve is the sophistication of these money mule networks. Mules are part of coordinated, AI-enabled operations that mimic legitimate behavior. Combating this trend requires

tighter transaction monitoring, holistic user profiling, and cross-platform intelligence sharing to uncover hidden mule rings before they cause systemic damage.

4 **Social engineering targets the vulnerable**
Social engineering will continue to be an effective tool for fraudsters, who will leverage their AI-powered toolkit to automate phishing, voice spoofing, and impersonation using deepfakes. In markets where consumers are less digitally literate, there may be waves of Authorized Push Payment (APP) and account takeover fraud. With the ease of moving money globally, fraud has become an attractive, low-risk side hustle, particularly for vulnerable individuals in low-income areas or regions where documents are easier to forge and government databases are less comprehensive.

5 **Document-free verification steps in to prevent AI fraud**
Document-free verification, also known as Non-Doc Verification, is now the fastest-growing identity verification method, with a year-over-year adoption rate of more than 338%. As deepfakes and document forgery using AI were made more accessible, Non-Doc Verification provides a safe and compliant alternative. By directly connecting to government databases and trusted registries, Non-Doc eliminates the need for traditional identity document uploads, overall reducing friction, improving accuracy, and closing loopholes exploited by fraudsters. Non-Doc Verification has already garnered popularity in markets like Canada, Singapore, and France. In 2026, credibility will increasingly hinge on access to verified state data, moving from physical document reviews to database-backed confirmation, setting a new benchmark for compliance and user experience. Traditionally forged documents have continued to drop across most markets, so will likely fall even further as the adoption of document-free solutions continues

to rise. Learn more about this rapidly adopted method in our 2025 Non-Doc Verification guide.

6 **From scattered tools to unified compliance and fraud prevention ecosystems**

Fragmented compliance stacks are a liability businesses can no longer afford. The future lies in unified compliance workbenches that blend compliance, fraud, reporting, and case management, with AI providing the backbone for efficiency, integration, and transparency. This shift goes beyond a technology upgrade and will become an operational necessity. By consolidating verification, fraud detection, and reporting within a single environment, companies gain greater transparency, agility, and real-time visibility, thereby reducing risk and resource drain.

7 **Fraud prevention and compliance converge**

2026 may be the year when the traditional divide between compliance and fraud prevention teams begins to disappear. Businesses may choose to merge these functions into unified risk intelligence units, responsible for the entire user verification and assessment lifecycle.

As fraud becomes increasingly sophisticated, the success of fraud prevention tactics will depend on both behavioral defenses and technical verification methods.

Vyacheslav Zholudev,
CTO at Sumsub

"Identity verification is entering a new phase — one where automation, AI, and data fusion converge. In 2026, the biggest breakthroughs won't come from better document scanning, but from AI agents verifying other AI agents.

As digital assistants begin transacting and representing users, we'll need systems that can confirm not just who someone is, but which entity is acting on their behalf — securely and traceably.

At the same time, verification will move beyond single checks into continuous assessment — blending device telemetry, behavioral analytics, and contextual intelligence into one adaptive layer. It's no longer just about stopping fraud at the door, but about building trust that evolves with every interaction. That's where the next generation of AI-driven verification will truly redefine digital identity."

Preventing

How we must respond

Fraud

How to create a winning fraud prevention strategy

Fraud in 2026 has entered the era of the Sophistication Shift. While the overall percentage of fraud attempts may be declining, each successful attack is more calculated, more damaging, and harder to detect. Deepfakes, synthetic identities, and carefully orchestrated post-KYC abuse are replacing crude document forgeries and copy-paste scams.

The vast majority of end-users (approximately 89%) prefer online services that implement strict verification and anti-fraud measures.

Sumsub's Fraud Exposure Survey 2025: Consumers

For businesses, this means the stakes are higher: every missed case can result in larger financial losses, reputational damage, and increased regulatory scrutiny.

To thrive in this environment, fraud prevention strategies must evolve. A "winning" strategy is not built on a single control or quick fix. It's built on layered, intelligence-driven defenses that adapt as quickly as fraudsters innovate.

What makes an effective fraud prevention strategy?

Layered verification

No single check is enough anymore. Combine document verification, biometrics, device fingerprinting, and behavioral signals at different touchpoints. Genuine users flow through seamlessly, while fraudsters encounter multiple, adaptive barriers.

AI-driven fraud detection

Machine learning cuts through the noise of high-volume data. Utilize AI to minimize false positives, identify suspicious patterns, and analyze anomalies across regions and industries in real-time. The goal: faster, sharper decisions that scale.

Behavioral analytics

Static identity checks stop at onboarding, but fraud doesn't. Monitor behavioral signals, such as typing cadence, navigation flow, or unusual transaction patterns, to identify fraud that slips past traditional defenses.

Global intelligence sharing

Fraud is borderless. Protect your ecosystem by leveraging consortium data, shared watchlists, and intelligence networks to enhance your security. The ability to learn from fraud attacks happening elsewhere means spotting threats before they hit your platform.

Andrew Novoselsky,
CPO at Sumsub

"We're seeing the rise of what we call the 'Unified Compliance Workbench' — a single environment where case management, risk assessment, and fraud detection converge. This is not just a technical shift but an operational one. Regulators are demanding transparency, and customers are demanding trust. Compliance and fraud prevention can no longer operate as separate silos. In 2026, compliance leaders will need AI-native toolkits to achieve both."

Are you prepared for 2026?

Fraud-defense readiness checklist

For companies

Evaluate your organization across these six critical domains. Be honest in your scoring to identify blind spots before fraudsters do.

Governance and strategy

- [ ] Fraud prevention policy reviewed and updated within the last 12 months
- [ ] Fraud risk appetite is defined, documented, and approved by leadership
- [ ] Clear roles and responsibilities assigned for fraud prevention across teams
- [ ] Annual fraud risk assessment conducted and actioned
- [ ] Independent fraud resilience review performed in the past 12–18 months

Layered verification & KYC

- Multi-layer checks (ID, biometric, device, behavioral) integrated into onboarding
- Beneficial ownership and identity authenticity verified for all accounts
- Ongoing monitoring and reverification schedules are in place
- Enhanced checks are applied for high-risk users or regions
- PEP, sanctions, and adverse media screening are automated and continuous

Transaction & behavioral monitoring

- A Transaction Monitoring system is live and regularly scrutinized
- AI models deployed to detect anomalies in real time
- Behavioral analytics (e.g., keystrokes, session flow) implemented for high-risk flows
- Alerts triaged, investigated, and documented with clear outcomes
- Escalation and reporting procedures are clearly defined

Incident response & investigations

- [ ] Documented fraud incident playbook with clear escalation paths
- [ ] All investigations are tracked in a central case management system
- [ ] Average investigation time benchmarked and reviewed
- [ ] Lessons learned from past incidents are documented and shared across teams
- [ ] FIU and regulator reporting processes tested and validated

Training and awareness

- [ ] Staff across roles (frontline, fraud, compliance, product) are trained annually
- [ ] Training includes evolving threats such as deepfakes and AI scams
- [ ] New hires complete fraud awareness onboarding within 30 days
- [ ] Refresher updates are issued when new fraud vectors emerge
- [ ] Simulated fraud drills are conducted to test readiness

Vendor and technology oversight	☐ Third-party fraud tools are regularly tested for performance and adaptability ☐ Vendor responsibilities for fraud prevention are clearly defined in contracts ☐ Outsourced services (e.g., verification, monitoring) are independently audited ☐ Data integration between fraud, compliance, and product systems verified ☐ Technology roadmap aligned with fraud prevention goals (AI, biometrics, blockchain)

Scoring your readiness

Score 1 point for every question you answer "Yes". Calculate your total to understand your current exposure and maturity level.

28–32	Strong resilience. Maintain, test regularly, and continue optimizing.
23–27	Solid base. Address identified gaps before they become vulnerabilities.
18–22	At risk. Fraudsters could exploit weaknesses, so prioritize immediate fixes.
<18	High exposure. Take urgent action to upgrade tools, governance, and processes.

Fraud-defense readiness checklist

For consumers

Complete this self-check to know whether you're ready to withstand the new wave of sophisticated AI-driven fraud, or if you're leaving your data, identity, and finances vulnerable.

Awareness and mindset

- [ ] You stay alert to new scam types (e.g., deepfakes, investment or delivery scams).
- [ ] You regularly read updates from trusted sources, such as your bank, telecom provider, or national fraud authority.
- [ ] You think twice before sharing personal details online or clicking unexpected links.
- [ ] You treat "too good to be true" offers as red flags, not opportunities.

Identity and account protection

- [ ] You use unique, strong passwords for every major account.
- [ ] Two-factor authentication (2FA) or passkeys are enabled wherever possible.
- [ ] You review your privacy settings on social media and limit what you share publicly.
- [ ] You know how to freeze or lock your account if your ID or phone is stolen.
- [ ] You don’t share personal data or passwords with anyone.

Device and network security

- [ ] Your phone, laptop, and apps are set to update automatically.
- [ ] You only download apps from official stores.
- [ ] You use antivirus or built-in protection tools and regularly scan for threats.
- [ ] You avoid public Wi-Fi for sensitive transactions (or use a VPN if necessary).
- [ ] You back up important data securely in case of loss or ransomware.

Payment and transaction safety

- [ ] You double-check payment requests—even if they appear to come from someone you know and trust.
- [ ] You verify websites and sellers before entering card details (look for HTTPS and reputable reviews).
- [ ] You use secure payment methods such as credit cards or digital wallets that offer buyer protection.
- [ ] You monitor your bank and card statements weekly for unusual charges.
- [ ] You know how to report a suspicious transaction quickly to your bank.

Responding to scams

- [ ] You are aware of the official reporting channels (e.g., Action Fraud in the UK, FTC in the U.S., etc.).
- [ ] You don’t respond to or forward suspicious emails, calls, or texts—you report and delete them.
- [ ] If you’ve been scammed, act quickly: contact your bank, change your passwords, and alert the relevant platforms.
- [ ] You discuss scams openly with family and friends to help them stay alert as well.

Digital literacy and AI awareness	☐ You understand that AI can create convincing fakes—voices, images, and identities. ☐ You question unexpected video calls, voice notes, or messages that pressure you to act quickly. ☐ You verify identities through secondary channels (call the person back, or confirm directly). ☐ You stay informed about new AI-driven fraud tactics from trusted security sources.

Scoring your readiness

Score 1 point for every question you answer "Yes". Calculate your total to understand your current exposure and maturity level.

26-30	Strong resilience. You're digitally savvy and proactive. Keep up with new scam trends.
20-25	Solid base. You're doing well, but could strengthen habits, especially around AI-based scams and data privacy.
14-19	At risk. You have good intentions, but key gaps leave you exposed. Review the checklist and take action now.
<14	High exposure. Your defenses are low. Learn the basics, update your devices, and seek advice from trusted organizations.

How Sumsub can help

The first genuine fraud prevention solution, fortified by our leading KYC engine

Fraud prevention is no longer just about catching bad actors—it's about building systems that adapt faster than fraudsters can innovate. That's where Sumsub comes in.

1.5B+
identities enriched our fraud prevention system

As pioneers in the identity verification market, we've verified over 1.5 billion identities worldwide, providing us with unparalleled visibility into fraud trends across various industries and regions. Every interaction enriches our system with unique data on fraud patterns, sharpening our ability to distinguish genuine users from sophisticated threats.

23K+
fraud samples analyzed daily

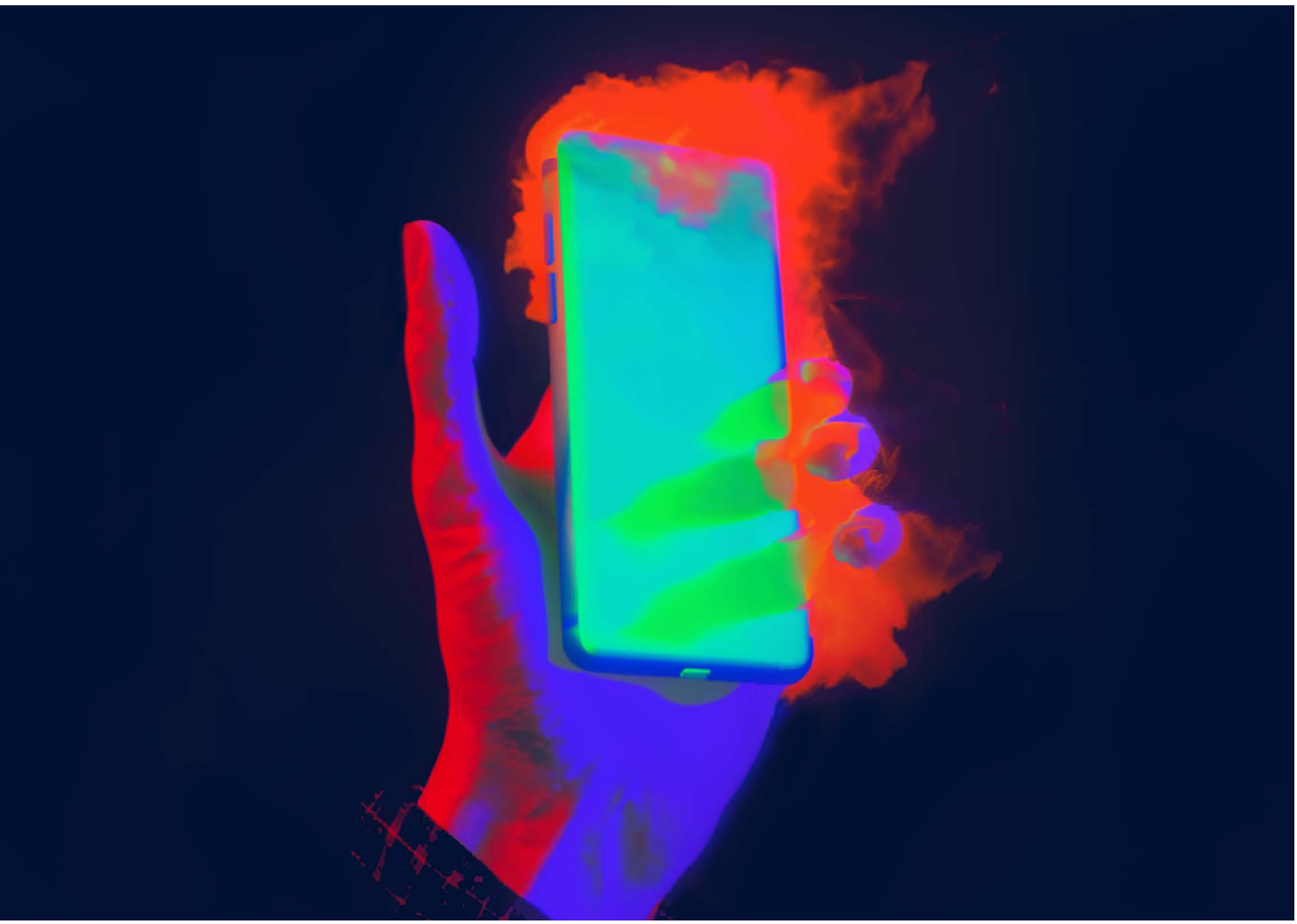
Our platform analyzes more than 23,000 fraud samples daily and leverages a global database of over 2.3 million known fraudsters, ensuring that our detection technologies evolve in real-time. The result? Near-total prevention of fraudulent attempts, with far fewer false positives that slow down business.

2.3M+
known fraudsters in our unique database

By combining our KYC engine with AI-powered monitoring, behavioral analytics, and fraud network detection, Sumsub offers a unified defense against account takeovers, multi-accounting, payment fraud, and emerging deepfake-enabled attacks—all through a single, seamless integration.

With Sumsub, businesses can:

1. Block fraud before it damages revenue or reputation
2. Automate manual reviews to cut operational costs
3. Gain a 360° view of user risk with centralized case management
4. Stay audit-ready and compliant with global regulations



INTERPOL

"In the past year, INTERPOL has observed a rise in the use of AI across a variety of fraud types. In particular, criminals are increasingly using AI-generated video and audio to impersonate trusted individuals in order to deceive victims. The rise in availability of deepfake tools has democratised and industrialised AI-driven fraud, which has led to their use not just in sophisticated fraud, but in phishing, vishing, and voice cloning. As such, the attack surface of organisations and individuals has expanded to include previously trusted voice-based, video-based, and identity-based channels.

Looking ahead, AI-enabled fraud will become both increasingly sophisticated and accessible. Detection tools for synthetic media are improving, but the public and private sectors must collaborate to create effective solutions. Such solutions will also require a comprehensive and holistic approach, such as AI detection combined with strong identity checks, the use of secondary authentication channels, and increased legal and regulatory adaptation.

INTERPOL is dedicated to assisting member countries to combat AI-driven fraud through collaboration with law enforcement and the private sector in developing innovative approaches."

Want to keep the whole user lifecycle fraud-free?

Book a demo →