

APAC fraud in 2026

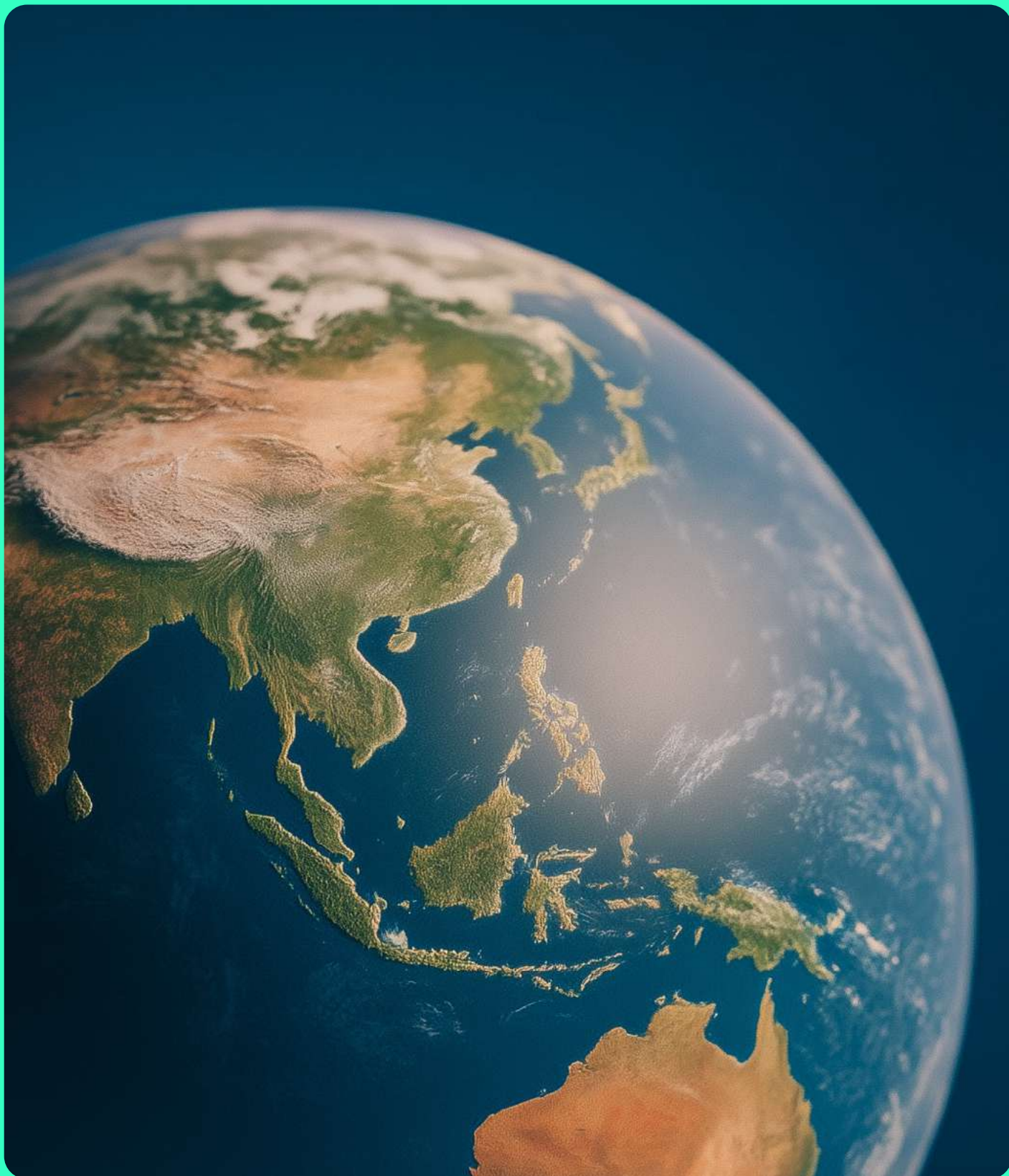


Table of contents

3	Introduction
4	Why APAC fraud is worth a deeper look at
7	From crude forgery to convincing fabrication
9	The connected attack system
10	APAC fraud typology
18	What this means by sector
21	Leadership priorities
22	The future of fraud in APAC is integrated
24	How Sumsub helps



Legal Disclaimer: The information provided in this material is for marketing purposes only and does not constitute legal, financial, or other professional advice.

Introduction

For a long time, you could look at fraud in the APAC region and sort it into buckets.

Document forgery over here, account takeover over there, some money laundering in between. The buckets made sense.

But now, they don't really make sense anymore, or at least they're less useful than they used to be. What's happening now is that these problems bleed into each other. A fake identity leads to a fraudulent account, which leads to money moving across borders, leading to something that looks a lot like organized laundering.

Criminals are moving away from easy, fake documents. Instead, they use AI-made deepfakes, synthetic identities, and constant attacks. According to the Identity Fraud Report 2025–2026, selfie-to-ID mistakes now make up 35.4% of all fraud. Synthetic identity fraud, where a person is “made up” from various data points, has grown by 142% in one year.

This guide walks through what's going on in APAC right now when it comes to fraud, which may result in more serious financial crime. We're looking at the main fraud types, how they've changed, how they connect to each other, and what fraud prevention leaders should be paying attention to.

Some of these new types of fraud are still emerging, and the picture is messier than any single report can capture. But if you're working in fraud, compliance, AML, payments, or risk in the region, the patterns are worth knowing about. Even the ones that feel uncomfortable or hard to pin down.

Why APAC fraud is worth a deeper look at

The APAC region is most interesting because we observe a whole variety of different fraud realities playing out at the same time.

You have countries like Singapore, Hong Kong, and Australia where the rules are tight and enforcement is quite strict. Fraud hasn't disappeared in those markets, but the easy problems have been squeezed out. What's left are the harder attack vectors: AI-generated selfies, synthetic identities that look coherent, automated systems that keep retrying your onboarding flow until something comes through. The numbers might look flat or even lower in some cases, but the cost per incident is going up, and detection is getting harder.

Then, you have markets where everything is digitizing really fast. Mobile wallets, lending apps, payment platforms, all growing faster than the regulatory frameworks around them. People are entering the financial system for the first time through products that were maybe not built with heavyweight fraud prevention in mind. That creates openings, and those openings get found by bad actors.

FATF put out a paper in February 2026 about the growing scale and complexity of cyber-enabled fraud and said the existing AML and counter terrorism financing frameworks need to be part of the response. AUSTRAC gave a speech in March 2026 that described APAC as a place where a highly integrated fraud system is taking shape. Key word: **system**. We're past isolated incidents at this stage.



The fraud team sees one part of the picture, the AML team sees another part, and nobody is necessarily stitching the whole thing together.

The practical consequence of all this is that the idea of checking someone once at the front door and then moving on probably doesn't work that well anymore.

When fraud was mostly about stolen documents and basic impersonation, a solid onboarding check could catch a lot of it. But when people are being fabricated from scratch, selfies are generated by AI, bots are learning from each failed attempt and coming back slightly different, the risk lives throughout the whole time a person is your customer.

There's also a problem with trying to apply one approach across the whole region.

40%

The fraud environment in Australia and the fraud environment in a market where digital wallets are growing at 40% a year with lighter regulation look very different [LINK](#)

The verification flows, the signals you watch for, the thresholds where you escalate, all of that needs to reflect where you are and who your users are.

Then there's the organizational part of the process, which might be the most stubborn problem. A lot of institutions still have fraud teams and AML teams working in different systems with different data.

That matters more now than it used to because the attacks themselves are more connected.

From crude forgery to convincing fabrication

Sumsu's Identity Fraud Report 2025 to 2026 says that cases where the selfie doesn't match the ID document now make up 35.4% of all fraud in the region. That grew 73% year over year.

A lot of these aren't obvious fakes, but AI-generated images that are designed to look close enough to a real person that they seem like ordinary mistakes or edge cases rather than deliberate attacks. They don't trigger the same alarms that a badly photoshopped document would.



142%

synthetic identity growth in
a year in the region

Synthetic identity fraud has grown 142% in a year and now sits at 15.7% of regional fraud. These are identities that are assembled from bits of real data mixed with fabricated information, creating a person who doesn't exist but who looks plausible enough to get through a check. They often look fine at onboarding, and become a problem only months later when the account starts moving money in patterns that don't match the profile.

There's also the retry problem. Duplicate submissions jumped 388% year over year, indicating systems that submit, fail, learn something from the failure, adjust, and try again. Each rejection gives fraudsters data about what your system is looking for.



**Selfie-vs-ID
fraud**

35.4%

of all APAC fraud (+73% YoY)



**Synthetic
identity fraud**

15.7%

of regional fraud (+142% YoY)



**Duplicate
submissions**

+388%

year-over-year globally

The connected attack system

One thing that keeps coming up when you look at fraud in APAC this year is that the lone fraudster idea feels pretty outdated.

What seems to be happening instead is something more like a business process. There are stages to it, and different people or groups handle different parts.

Someone finds victims through ads or messaging apps, social platforms or referrals, or by impersonating trusted institutions. Someone else builds up trust, sometimes using fake founders or fake experts or polished dashboards or deepfake video calls or testimonials that look real enough. Then there's the getting in part, which uses the synthetic identities, biometric deception, account takeovers, and persistence-based retries we talked about in the last section.

After that comes the money. It moves through payments, wallets, APP fraud, transfers, deposits, crypto rails, whatever path is available. Then the trail gets obscured by moving funds through lots of different accounts to hide where they came from. And eventually, the money gets washed into property or other assets or gets recycled to fund more operations.



APAC fraud typology

Romance scams show how much scam operations have changed. Dating is one of the most targeted industries according to Sumsb's Identity Fraud Report 2025 to 2026, with fraud accounting for 6.3% of activity in the sector.

Romance scams

Scammers spend weeks or months building a relationship before money ever comes up. They use AI-generated photos that can't be reverse-searched, write emotionally tailored messages at scale, and some now use deepfake video to simulate face-to-face calls.

TSB Bank reported that money sent to fraudsters posing as romantic partners increased 37% year on year, comparing 2024 to 2025, while case volumes rose 15%. UK Finance figures show that in the first half of 2025 alone, UK victims lost an estimated £20.5 million across nearly 3,000 cases.

37%

increase in funds lost to romance scammers was reported by TSB Bank (2024 vs. 2025), alongside a 15% increase in the number of cases. [LINK](#)



In Hong Kong, November 2025, police recorded more than 40 romance scams in two weeks, losses totalling HK\$17 million. Over 40% of victims were aged over 50. One woman lost HK\$2.6 million to someone posing as a Singaporean businessman on WhatsApp. Another, aged 81, lost over HK\$5 million to a fake PLA officer. [LINK](#)



By the time money comes up, the victim is emotionally invested in a way that makes clear thinking very hard. The damage goes beyond finances; there's psychological harm, reputational damage, and in some cases victims get pulled into money muling without realizing it.

Pig butchering

Romance scams increasingly overlap with what's called pig butchering, which is probably one of the most disturbing fraud typologies operating at scale right now.

The basic structure is that a scammer builds a relationship with a victim, often romantic but sometimes just friendly, and then gradually steers them toward investing in a fake cryptocurrency platform or other investment scheme. The victim is encouraged to put in more and more money. The platform shows fabricated gains. Sometimes, early withdrawals are allowed to build confidence. Then, at some point, the platform locks the victim out, or the scammer disappears.

The scale of this is **hard** to overstate.

Investigations by journalists and law enforcement have uncovered large scam compounds in Cambodia, Laos, and Myanmar, where trafficked workers were forced to run these schemes targeting victims across the US, Europe, and Asia. These operations use scripted messaging, translation tools, and AI-generated profile images. They've generated hundreds of millions and collectively billions of dollars in losses. INTERPOL reported warnings about the global spread of scam call centers run through human trafficking, with operations migrating from Southeast Asia to West Africa.

There's something uniquely awful about pig butchering because many of the scammers are victims too. People are recruited through fake job ads promising legitimate work, and when they arrive their passports are taken, and they're forced to work 16-hour days running scams under threat of violence.

**Ponzi schemes,
fake investment
ecosystems, and
digital trust**

Ponzi schemes in APAC used to be more obviously what they were. Pyramid structures, informal investment clubs, things that had a certain recognizable shape to them. What's happening in 2026 is that they're being packaged in ways that look like legitimate fintech products. Crypto yield platforms, copy trading groups, exclusive trading communities, premium wealth apps, things that claim to use AI-powered investment strategies.

These scams get promoted through messaging channels, social platforms, influencers, and personal referrals.

First comes recruitment and trust building. Then, the victims fund through bank transfer, wallet, payment app, or crypto. Sometimes, early withdrawals are allowed, which reinforces confidence and gets people to put in more. Referral incentives encourage users to bring in others, which is part of what makes the growth feel organic.

Eventually, withdrawals get delayed or blocked or made conditional on paying extra fees or taxes or going through additional verification steps. By the time the scheme collapses, funds have usually been moved elsewhere. They overlap with cross-border laundering because the money often moves through several jurisdictions before settling.



**Mule networks,
cross-border
routing, and where
the money goes**

Fraud doesn't really end when someone gets deceived, but when the money gets somewhere it can't be recovered from.

Mule networks are one of the most important parts of that chain. They receive the proceeds of fraud, move them through multiple accounts or intermediaries, fragment the flows across institutions and jurisdictions, and create enough distance between the original fraud event and the final destination that recovery becomes extremely difficult. Some mule accounts are set up specifically for this purpose using synthetic or stolen identities. Some involve real people who have been recruited, sometimes knowingly and sometimes through deception, to move money on behalf of criminal networks.

High inbound flow followed by rapid outbound movement, minimal retained balance, repeated use of the same infrastructure across accounts that are supposed to be unrelated. Transfer corridors that don't match the customer profile or anything the person claimed during onboarding. These signals are known but spotting them requires connecting data across different systems and different time periods, which is harder than it sounds when your fraud monitoring, your transaction monitoring, and your customer data are sitting in separate places.

The wider laundering chain follows a similar logic. Once funds move past the initial fraud event, every step makes intervention harder. Cross-border transfers, digital payment rails, crypto conversion, integration into real estate or other stable assets, all of these reduce transparency and compress the time available for anyone to do something about it.

Other types of fraud on the rise

There are a few other scam typologies that seem to be getting worse in APAC and are worth flagging, even if we can't go as deep on each one.

Government official impersonation is one that keeps showing up. Someone calls or messages claiming to be from a tax authority or a police department or a regulatory body and tells the victim they're in some kind of trouble.

There's usually urgency built in, like you need to transfer money immediately or you'll be arrested, and the pressure combined with the authority of the supposed caller gets people to comply before they have time to think.

These scams work especially well in markets where there's a cultural tendency to defer to official authority and where people may not have easy ways to verify whether a call is legitimate. Government official impersonation is the second most common scam type in Singapore. In February 2026 alone, at least \$2.9 million was lost to fake MAS and Ministry of Law officers who convinced victims to hand over gold, jewellery, and watches for "investigation."

E-commerce and marketplace fraud is another area that's expanding. Fake storefronts, fake listings, triangulation fraud, where a criminal sits between a buyer and a legitimate platform and harvests payment details along the way. The growth of online shopping across APAC has created much bigger surface for this kind of thing, and a lot of platforms are still figuring out how to vet sellers and detect fraudulent activity at scale.



QR phishing (or “quishing”), is a newer type of fraud currently on a dramatic rise. Fraudsters place malicious QR codes in public spaces or send them digitally, and when someone scans one, they get directed to a fake website that harvests credentials or installs malware. It exploits the fact that most people have been trained to scan QR codes without thinking too hard about where they lead.

SIM swap fraud, where criminals convince a mobile carrier to transfer someone’s phone number to a new SIM card, which gives them access to SMS based authentication codes and lets them take over accounts, also remains a problem.

It’s been around for a while, but it still works often enough that it belongs on the list.

“



The common thread running through all of these is that they rely on social engineering and trust manipulation, as much as (or more than) technical exploitation.”

Artem Popov,
Technical Product Manager for
Fraud Prevention Solutions at Sumsb

The technology makes them more scalable and more convincing, but the core mechanism is usually about getting a human to do something they wouldn't do if they had more time or more information.



What this means by sector

A single attack can start in one business model, move through another, and get cashed out in a third. Sector-specific controls still matter, but they need to be connected to a broader picture of how money, identity, and fraud flow between different types of institutions.

Banks and lenders are sitting at the center of most of this. They face onboarding abuse, account takeover, scam victim payments, synthetic identity exposure, mule routing, and downstream laundering risk. For lenders specifically, synthetic identities may be the nastiest problem because the losses often don't show up until well after credit has been extended.

Payment providers and wallets tend to be where fraud becomes visible in motion. APP scam flows, risky first-time beneficiaries, repeated funding of suspicious endpoints, deposit-heavy and withdrawal-light behavior, and mule routing patterns. All of these things show up in payment data. Where wallets function more like consumer finance products than simple payment instruments, which is increasingly the case in a lot of APAC markets, the attack surface gets wider.



Crypto platforms, brokerages, and trading apps face both direct and indirect risk.

Directly, they get targeted through synthetic identity onboarding, mule cashout, and fake investment ecosystems running on digital asset rails.

Indirectly, they sometimes get used as trust anchors in Ponzi promotion, meaning the scheme references the platform to seem legitimate even when the underlying fraud started somewhere else entirely.



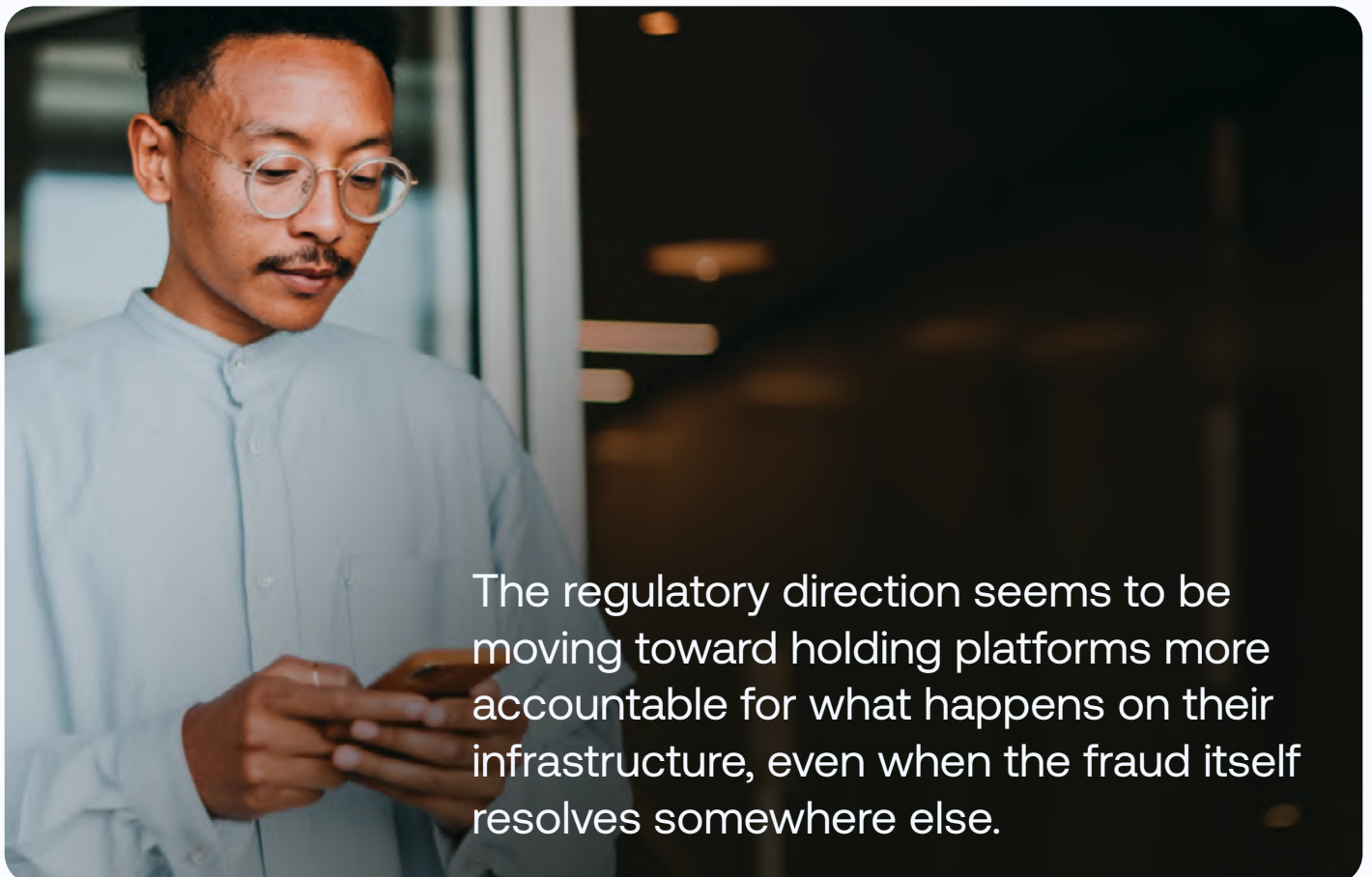
Marketplaces, platforms, and the changing perimeter

Marketplaces and digital platforms deserve their own mention because their role in financial crime has changed in a way that a lot of platform operators perhaps haven't fully reckoned with yet.

Platforms used to worry mostly about things like fake reviews, merchant abuse, counterfeit goods (which still matters, of course). But increasingly, platforms are part of the acquisition layer for fraud. Scam operations use ads, communities, messaging features, and social proof on platforms to find and recruit victims.

Romance scams start on dating apps and social media, pig butchering operations use messaging platforms to build relationships, fake investment schemes get promoted through influencer content and community groups. The platform itself may not be where the financial crime happens, but it's where the funnel begins.

That means fraud exposure for platforms is no longer limited to what happens inside the marketplace transaction. Platform governance, advertiser vetting, content moderation, and cross-functional coordination between trust and safety teams and financial crime teams all play a bigger role than most businesses assume.



The regulatory direction seems to be moving toward holding platforms more accountable for what happens on their infrastructure, even when the fraud itself resolves somewhere else.

Leadership priorities

So given everything we've covered, what should people in leadership positions be thinking about doing differently? We're not going to pretend there's a neat checklist that solves all of this, but there are a few things any business can do:



Controls for deepfakes, synthetic identities, and persistence attacks

This sounds obvious, but a surprising number of institutions are still running verification flows that were designed for a world where the main threat was a stolen document or a photoshopped ID. That means things like liveness detection that can catch AI-generated faces, linkage analysis that connects retry attempts to each other rather than treating each one as an isolated event, and ongoing monitoring that can flag synthetic identities after they've passed onboarding and started behaving strangely.



Fraud and AML detection, connected

Fraud teams see the deception, AML teams see the money movement. When those two views don't talk to each other, you get a situation where nobody has the full picture, and fraud makes it through.



Detection and escalation logic for fake investment and Ponzi-style activity

When these schemes are using your platform's payment rails or your customers' accounts, it becomes your problem whether or not it fits into your existing risk taxonomy.



Speed

Reducing decision and escalation latency to match the real speed of fund movement. When money can move across borders in minutes, a review process that takes days or weeks is going to miss most of what matters.

The future of fraud in APAC is integrated

APAC region seems to be showing how financial crime reorganizes itself when digital infrastructure and regulatory environments are both changing fast.

The model that's emerging has a few characteristics:

- More coherent fabricated identities
- More persuasive digital trust, meaning better fake platforms and more convincing fake people
- More persistent attack logic that learns and adapts
- Faster fund movement across more rails and more jurisdictions
- Tighter links between the fraud event itself and the laundering that happens afterward

Deepfakes, synthetic identities, fake investment ecosystems, romance scams, pig butchering operations, mule routing, cross-border money movement: these are increasingly parts of the same system rather than separate issues that happen to coexist in the same region. The people running these operations seem to understand that and build their workflows across the full chain from victim acquisition to cash integration.



For institutions, the question is whether their defenses reflect that same level of integration. The gap between how attackers operate and how defenders are organized seems like one of the bigger risks heading into the second half of 2026.

The regulatory environment is tightening, which should help. Technology for detection is improving, which should also help. But the other side is improving too, and they tend to move faster because they don't have compliance committees and procurement cycles.

This is going to stay difficult for a while, and **the time to adapt is now.**

How Sumsub helps

We would like to say something about what we do, since you're reading a guide we wrote. A technological solution to a bad actor problem.

We've built the platform around the idea that verification can't just be an onboarding event. It needs to cover the whole user lifecycle, from the first time someone shows up to every transaction and interaction after that. Identity verification, liveness and deepfake detection, AML screening, transaction monitoring, fraud prevention, business verification, travel rule compliance, case management, all of it runs on one platform with one integration and one dashboard.

99.98%

of deepfake attempts are detected by
our system in a single scan





Your profile has
been verified!

Average verification time is about **20 seconds** for an ID check with liveness. We support documents from over 220 countries and territories. We've been named a Leader in the Forrester Wave for Identity Verification Solutions and in Gartner's Magic Quadrant for Identity Verification two years running.

We also have an AI copilot called Summy that helps compliance officers, fraud analysts, developers, and support teams work faster by surfacing relevant information, generating reports, and providing regulatory guidance in real time, making the investigation and reporting part so much easier.

None of that replaces the hard organizational work of connecting your fraud and AML functions and building the right culture around financial crime prevention. But the tooling matters, and we've tried to build something that matches the way these threats are evolving rather than the way they used to work.

Keep your business safe from advanced fraud with Sumsub



User Verification



Business Verification



Transaction Monitoring



Fraud Prevention

1.5 billion

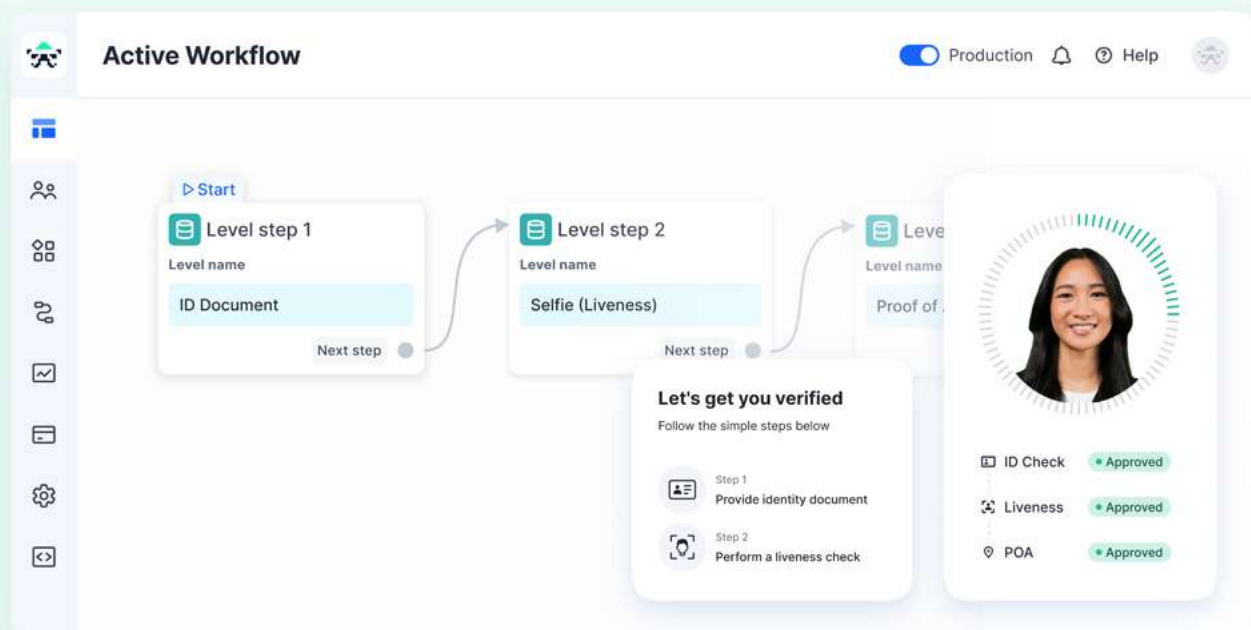
identities enriched via our fraud prevention system

2.3+ million

fraudster identities in the database

690,000+

fraud attempts prevented monthly



Try Sumsub

[Book a demo →](#)

