



Face Verification for Banks: Securing Customer Identity Against Fraud and Financial Crime

Introduction

Today's fraud and financial crime controls were built for a world where real identities are compromised or stolen. They flag the misuse of credentials, unfamiliar devices, and unusual behavior. While these measures analyse information around an identity, they don't validate the identity itself.

Due to the proliferation of generative AI and hypercollaborative threat groups, the attack landscape has fundamentally changed, and banks are facing a burgeoning fraud problem. Gartner® notes that, "despite 53% of institutions increasing their fraud prevention budgets by 5% or more, 70% of banks continue to see rising fraud losses — with smaller and midsize banks most vulnerable. This continued rise in losses underscores an urgent need to reassess the effectiveness of current strategies."¹

Gartner also mentions, "over a third of banks detect less than 60% of fraud before losses occur, and only 31% achieve preemptive detection rates above 80%, exposing a big gap in capabilities."²

To solve this problem, banks need stronger identity verification at onboarding and continuous assurance throughout the customer identity lifecycle. This eBook explores how identity solutions with embedded face verification and proven, standards-aligned liveness detection can help banks combat modern threats and achieve these goals. Liveness detection is the technology integrated into biometrics that confirms that the user is real and not a spoof.

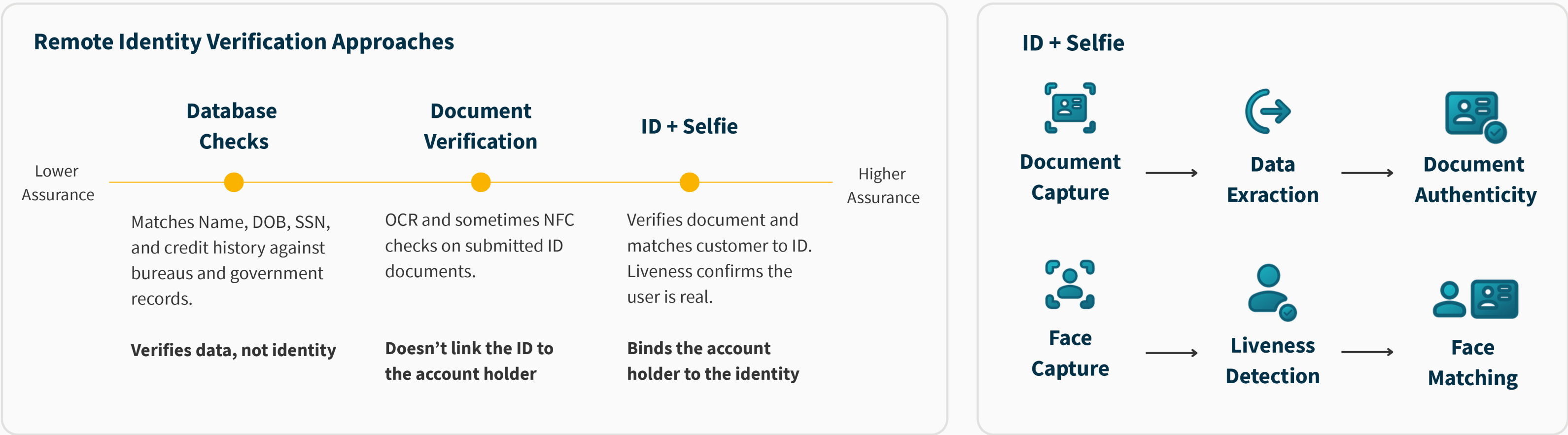
Face verification solutions do more than stem fraud losses and reduce financial crime exposure. They can also drive growth and cost efficiencies — reducing customer abandonment at onboarding and enabling automated, self-serve account recovery across the customer lifecycle.



Remote Onboarding

Onboarding is the most critical stage in the customer lifecycle. It's where credentials are issued, devices are registered, and the behavioural baseline is set. Every signal a bank later uses to detect anomalies (familiar device and location, typical transaction pattern) originates here. Allowing a synthetic or stolen identity through onboarding makes every one of those signals redundant.

Remote identity verification, sometimes called identity proofing, has evolved significantly over the past decade. Although all approaches remain in use today, they provide different levels of identity assurance. The sophistication of the identity check at onboarding determines the foundation on which every subsequent interaction is built. [See graphic.]



The Synthetic Identity Fraud Problem

Synthetic identity fraud underlines a fundamental flaw in relying on database checks to verify identities. Unlike identity theft, where a real person's credentials are stolen and misused, synthetic identities are manufactured. Bad actors combine stolen and invented identifiers — names, addresses, social security numbers — to create entirely new identities. They establish these over time, building credit histories and digital footprints until they appear consistent across every database check a bank runs. These checks ultimately validate an identity that doesn't exist.

Once inside, a synthetic identity doesn't trigger fraud alerts because it operates using the credentials and devices assigned at onboarding. The bank's signals — familiar device, expected behaviour, on-time payments — all read as normal. Then they bust out: default on loans, max out credit cards, and disappear. Because no real individual exists behind the identity, there is no one to pursue.

The exposure doesn't stop at fraud losses. A synthetic identity inside the KYC perimeter can be used for money laundering, terrorist financing, or sanctions evasion. While fraud is financially painful, the regulatory consequences of financial crime are categorically different: AML violations, sanctions breaches, and KYC failures carry civil penalties, personal criminal liability, and in serious cases, restrictions on business activity.

In 2024, for example, TD Bank was fined \$3.09 billion and had its growth restricted after allowing \$670 million in illicit funds through its payment system.³ In the first half of 2025 alone, regulators levied 139 financial penalties totalling \$1.23 billion, a 417% increase on the same period in 2024.⁴

Stopping synthetic identity fraud requires verifying the human behind the identity, not the data attached to it. ID + Selfie verification was designed to do exactly that. But as attackers have shown, it is not immune to exploitation.



Injection Attacks: How Synthetic Identities Spoof ID + Selfie

To pass a bank's ID + Selfie system, an attacker must defeat two checks: document authenticity and liveness detection. There are two ways to do this:

- **Presentation attack:** The attacker buys, steals, or forges a physical identity document to fool the OCR check, then holds a printout, mask, or deepfake played on a screen in front of the camera.
- **Injection attack:** The attacker bypasses the camera entirely, injecting forged document imagery and a synthetic face directly into the data stream, typically using a virtual camera or virtualised environment.

While presentation attacks are abundant, injection attacks pose the greater threat to identity systems. Unlike presentation attacks, which are difficult to scale, injection attacks can be automated and run across multiple targets simultaneously.

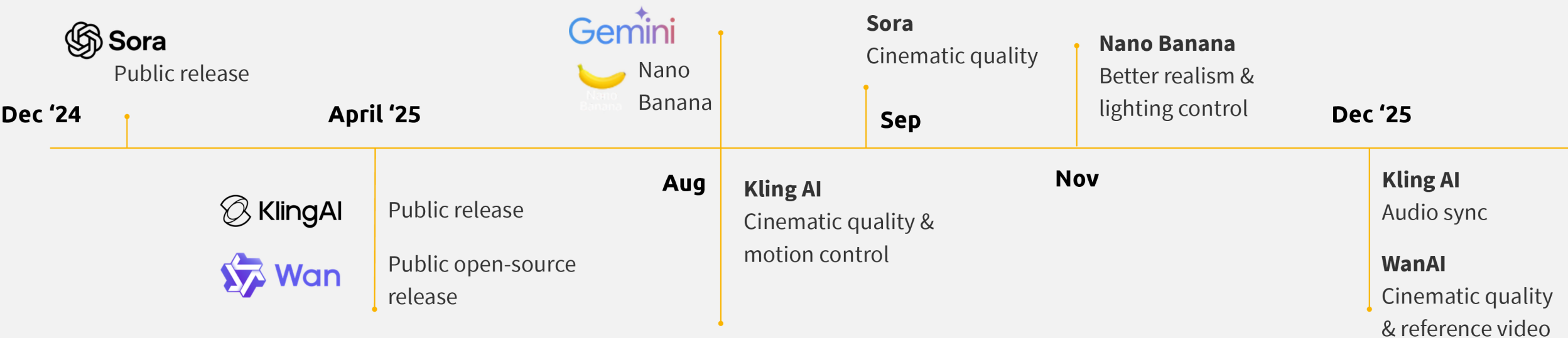
Generative AI has made the injected material significantly more sophisticated. Tools now exist to mass-produce fake identity documents at scale. For example, the operator of OnlyFake pleaded guilty to producing and selling more than 10,000 AI-generated fake identification documents, each designed to pass automated KYC checks.⁵

For the liveness element, image-to-video tools such as Kling AI and Nano Banana allow bad actors to map their own facial expressions and body movement onto a victim's static image in real time, producing high-fidelity deepfakes that simulate how real light and movement work in 3D.

Injection attacks continue to develop in ways that confound prior assumptions. iProov threat intelligence recorded a 1,151% increase in attacks against iOS systems in the second half of 2025 – a platform previously considered safer due to Apple's closed ecosystem.⁶ The recent development demonstrates that no environment or platform is permanently safe.

10 years of development in one year

2025 saw low-cost, easily accessible image-to-video tools flood the market. Attackers use these to create hyper-realistic deepfakes to spoof human agents and weak liveness systems.



Injection Attack Detection

To protect the integrity of ID + Selfie and prevent downstream fraud and financial crime, banks must detect injection attacks, and cannot rely on presentation attack detection systems alone. The need for defensive solutions is now reflected in regulatory standards. NIST SP 800-63-4, finalised in 2025, explicitly requires that remote identity proofing systems implement controls against AI-generated content and injection attacks.⁷

These controls come in different forms. Some liveness solutions analyse metadata. They look at the device, camera, geolocation, and behavioural elements like motion. The logic being that if imagery originates from a real camera on a clean device that’s moving normally, then the transaction should be legitimate.

While metadata is important, relying on these signals alone is not enough to stop the threat. Easy-access tools allow attackers to spoof every one of these signals. For example, cloud emulators (virtual phones) make the bad actor’s attack computer appear as a legitimate, high-end Android device. Behavioural signals, like motion and touch data, can be fabricated using AI.

Effective injection attack detection requires multiple layers of defence, but these layers must be conceptually independent. Banks require biometrics vendors that combine metadata analysis with advanced imagery analysis, which examines the biometric content itself for signs of synthetic generation or manipulation. If each layer analyses the same signals in similar ways, a sophisticated attacker can develop a single method that defeats all of them. The layers must be built on different datasets and different detection logic, so that breaking one provides no advantage against the next.

Legitimate ID + Selfie Transaction	Injection Attack
Document Real passport or driver’s license	Forged Document Altered, injected file
Biometric Real face	Spoofed Imagery Face swap, motion reenactment
Camera Physical hardware	Virtual Camera Fake video feed
Device Authentic OS & hardware	Emulated Device Virtual environment
Time & GPS Real timestamp and genuine GPS	Spoofed Time & GPS Fabricated GPS, replay timestamp
Device Signals Normal motion & touch data	Fabricated Signals AI-generated motion, touch data

Beyond Defensive Measures: Face Verification Solutions as a Business Driver

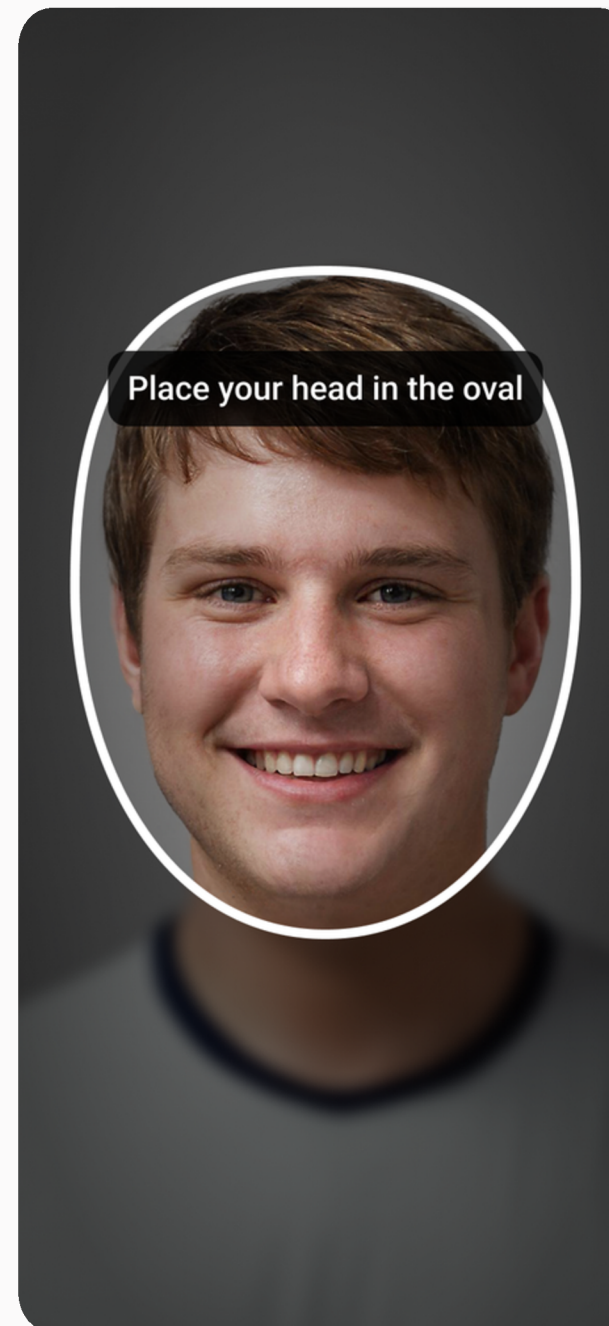
Onboarding isn't only the highest-risk stage of the customer lifecycle, but also the moment where users either become revenue-generating customers or walk away to the competition. Banks not only need to prevent attacks, but also provide a fast, effortless experience for genuine users.

69% of organizations cite balancing security with user experience as their top identity challenge.⁸ At the same time, CIO interactions related to customer experience increased approximately 174% between 2024 and 2025, reflecting that identity friction is a wider business problem, not just a UX one.⁹

Customer Acquisition Costs in financial services run as high as \$784 per customer. With Customer Lifetime Value ranging from \$2,000 to \$4,000, a one per cent change in onboarding pass rate translates to million-dollar differences at any meaningful scale.¹⁰

Face verification offers a completely self-serve and quick way for users to open accounts, but not every solution delivers the same positive customer experience.

There are several design principles and product features to look for in a face verification solution that can drive high pass rates and improve onboarding conversion rates.



Move beyond single-frame liveness

Multiple frames captured quickly reduce error probability without sacrificing speed.

Mitigate cognitive load

User challenges (smile, turn head) add cognitive load, frustrate users, and drive drop-off. Reduce cognitive load with passive user experiences and live user feedback.

Use richer signals, not more steps

Analyzing signals from the user, imagery, and device increases accuracy and improves pass rates.

Omit manual liveness reviews

Humans can no longer spot deepfakes and elongate time-to-onboard. Opt for a fully automated solutions that return results in the session.

Design for inclusivity

Bias testing and accessibility conformance are essential to ensure high pass rates for everyone.

Authentication

Strong face verification at onboarding establishes identity and mitigates many downstream risks. But it doesn't stop threats entirely. Once a customer is onboarded, the risk shifts to account takeover – bad actors infiltrating genuine users' accounts via phishing or social engineering to divert funds, max out credit, or move illicit funds. Account takeover fraud resulted in more than \$15.6 billion in reported losses in the U.S. in 2024, up from \$12.7 billion in 2023.¹¹

At the same time, Gartner notes that "step-up authentication and transaction authorization add friction to customer journeys. Account takeover (ATO) prevention tools show benefits as a way of providing continuous passive authentication, minimizing the need for those actions."¹²

Deployed at the right moments throughout the user lifecycle, face authentication can not only deliver continuous identity assurance and resilience against account takeover, but also enables fully self-serve interactions that improve user experience and reduce customer support costs.



The Move to Passwordless Authentication

The weaknesses of passwords are now well established. The approach doesn't confirm a user is who they claim to be, only that they know a secret. That secret can be stolen, bought, or guessed. A common attack method is credential stuffing, systematically testing passwords until the correct combination is found.

One-time passcodes (OTPs) are an improvement on passwords, as they introduce a degree of randomness. But they are not without major flaws. OTPs are transmitted over non-secure channels (SMS, email) that can be intercepted, redirected, or socially engineered. 83% of organisations are concerned about OTP security, and regulators globally are phasing them out.¹³

Due to the clear vulnerabilities of legacy authentication methods, banks are shifting towards a future that's more secure with an improved customer experience. Gartner predicts that over 40% of customer authentication transactions will be passwordless by 2027.¹⁴

Passkeys are one of the leading alternatives and a genuine improvement. They replace passwords with a cryptographic key pair stored on the user's device, are resistant to phishing, and deliver a significantly better user experience – there's no password to remember or passcode to retrieve.

However, most passkey implementations link to device-native biometrics, like Apple's Face ID or Android fingerprint recognition, to unlock the key. This approach delivers trust in the device, not the person holding it. On many devices, these biometrics can be bypassed if an attacker knows the PIN. This trade-off is acceptable for the majority of transactions, but for higher-risk, higher-consequence use cases, banks require stronger identity assurance.

Regulators are driving the move away from OTPs globally, especially in Asia



EU / UK

PSD3 tightening Strong Customer Authentication requirements, pushing toward phishing-resistant methods; OTPs increasingly restricted as a standalone factor



UAE

CBUAE Notice 2025/3057, full OTP phase-out mandated by March 2026, already in transition



Vietnam

State Bank Circulars 17 and 18/2024, biometric authentication is mandatory for payments over VND 10 million (\$400) from January 2025. 50% reduction in fraud reported after implementation



Philippines

Circular 1213, June 2025. Banks are required to move away from interceptable authentication methods, like OTPs.

The Case For Face Authentication

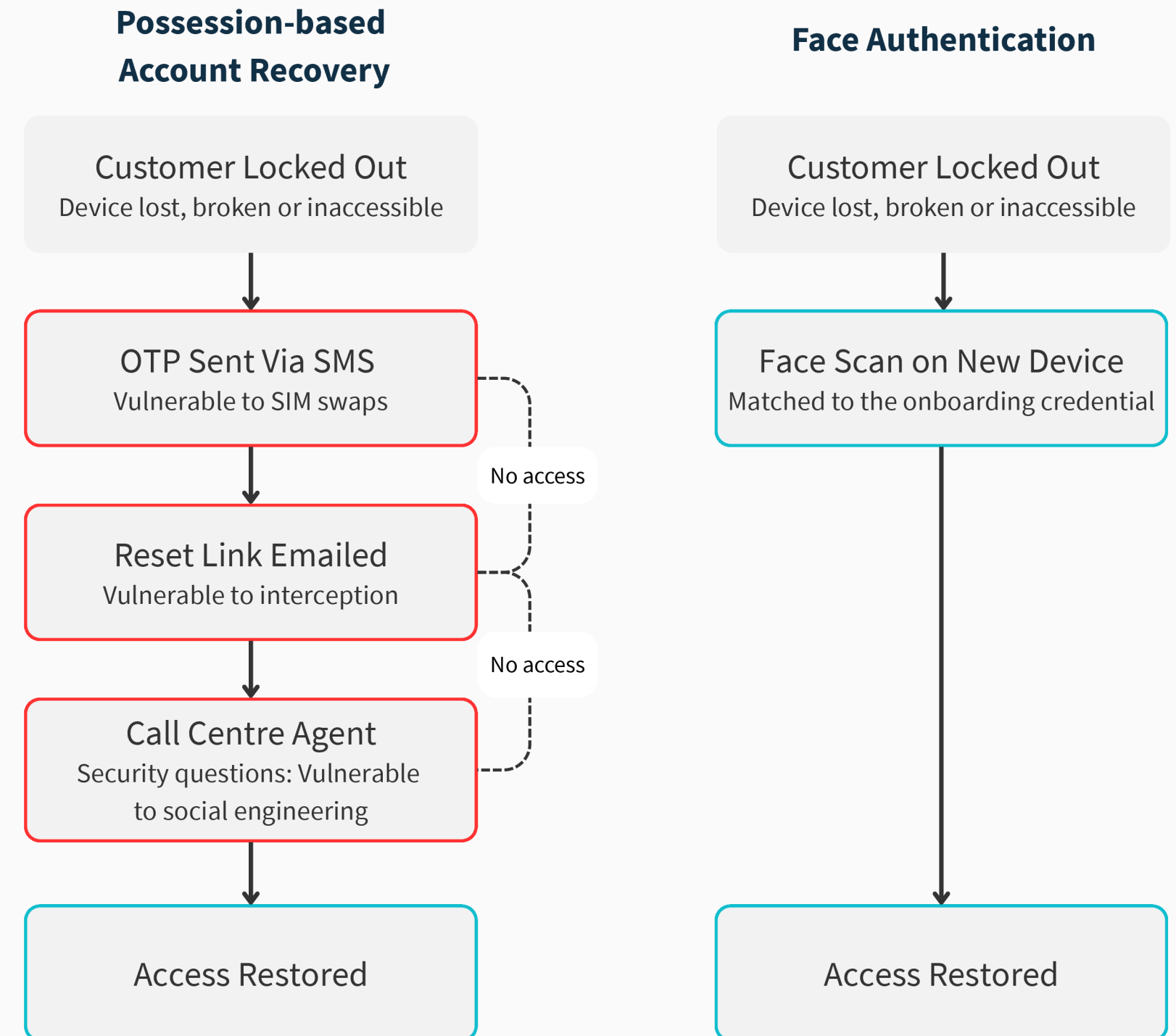
Cloud-based face authentication with liveness detection delivers trust in the user, not their device, a secret they know, or a token they hold. Unlike device-native biometrics, the credential is established at onboarding and bound to the user's identity document. Every subsequent authentication reuses that same credential. This makes the technology uniquely suited to high-risk use cases where strong identity assurance is vital.

Account Recovery

Multi-factor authentication is only as strong as its weakest recovery path. When a customer loses access to their primary authenticators, banks are forced to fall back on a single, often the weakest, factor. The strength of the MFA that preceded it becomes irrelevant.

Possession factors — authenticator apps, OTPs, email links — exacerbate this problem, creating opportunities for attackers to socially engineer a customer service agent or intercept passcodes. They also depend on the customer having access to devices that, by definition, they may not have.

Face authentication is not bound to a device, phone number, or credential, meaning a customer who has lost their phone can unlock their account on a separate device immediately. There is nobody to deceive and no credential to intercept. Completely self-serve, it requires no agent intervention — reducing support costs while closing one of the most persistently exploited entry points for account takeover.



The Case For Face Authentication

Step-up and Risk-based Authentication

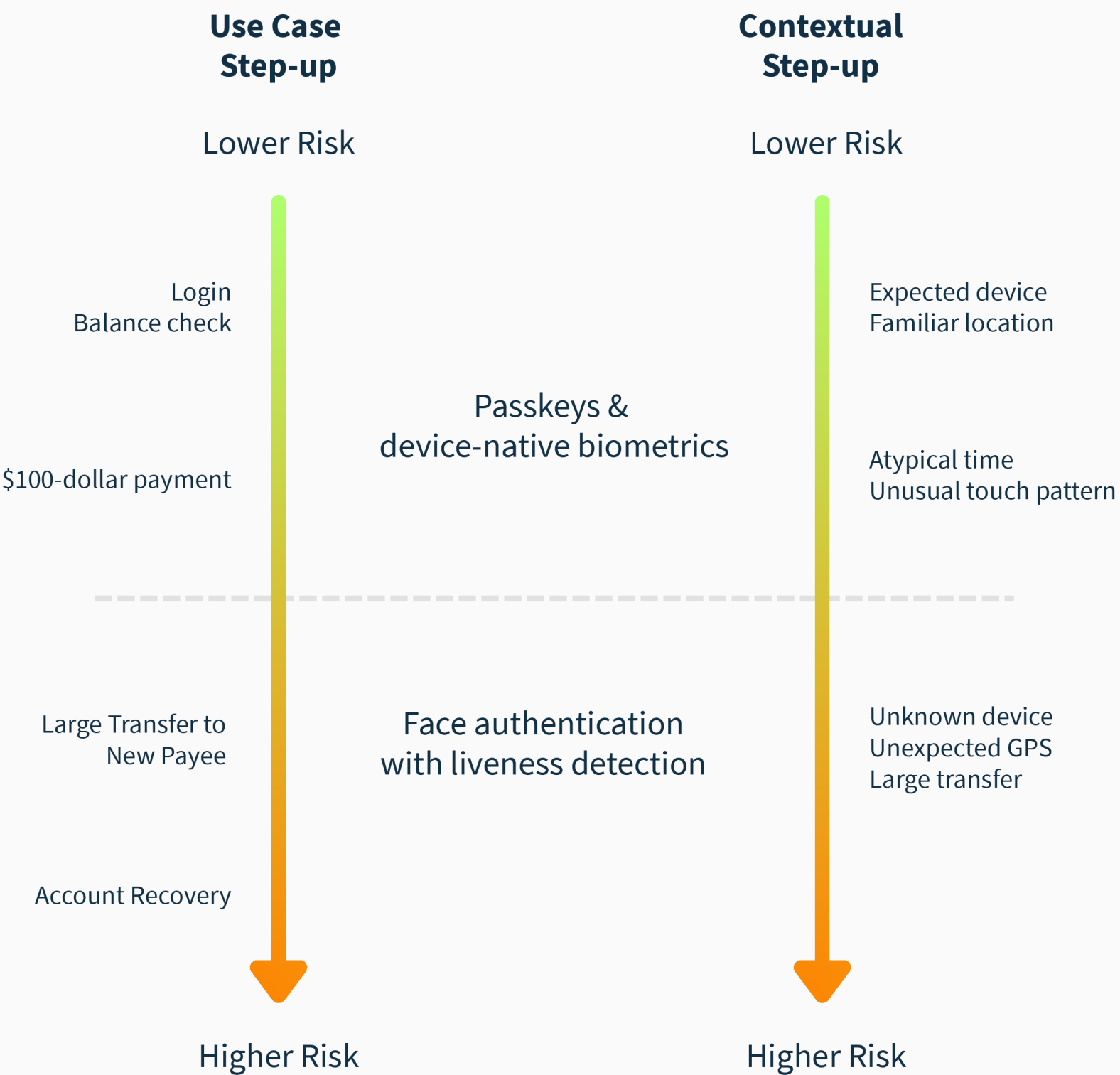
Not every interaction warrants the same level of identity assurance. Risk-based authentication, also known as adaptive authentication, addresses this by triggering stronger authentication only when the risk of account takeover is elevated.

Risk-based authentication relies on signals: device familiarity, geolocation, transaction size and frequency, and behavioural biometrics such as touchscreen pressure patterns. When anomalies are detected — an unfamiliar device, an unusual location — the risk engine escalates the authentication requirement accordingly.

For everyday interactions, like log-in, where the user is behaving normally, passkeys with device-native biometrics are a suitable, user-friendly option. For high-risk transactions, like a large payment to a recipient, or when behavior deviates from usual patterns, liveness detection is far more suited to the risk level. The technology links back to the identity document verified at onboarding – the highest-assurance signal available – applied at the moment it's needed.



Risk-based authentication signals originate at onboarding. They function as anomaly detectors only if the baseline was set against a real, verified identity. Having cleared onboarding, a synthetic identity would not trigger any of these signals, which highlights why strong identity assurance at onboarding is the prerequisite for everything that follows.



Evaluating a Face Verification Vendor

The right face verification with liveness detection solution can deliver strong identity verification, mitigating downstream fraud and financial crime, while defending against account takeover for ongoing high-risk interactions. All while delivering a highly convenient customer experience and mitigating abandonment.

Given the threat landscape outlined in this report, demonstrable injection attack and deepfake detection is the paramount capability to validate in any face verification solution. Banks must look beyond vendor claims to third-party, standards-aligned testing and validation.



iBeta Level 1, 2, and 3:

iBeta tests Presentation Attack Detection (PAD) against ISO/IEC 30107-3, evaluating a liveness solution's ability to stop masks and printed spoofs. Most reputable liveness vendors hold iBeta Level 1 and Level 2 accreditation. Gartner considers this baseline – necessary, but not a differentiator.¹⁶



FIDO Alliance Face Verification Certification

FIDO Alliance certification covers a broader range of presentation attack types than iBeta, including on-screen deepfakes, and tests over a longer period. Critically, FIDO retests solutions continuously as the threat landscape evolves. FIDO accreditation is vital for demonstrating the ability to defend against modern presentation attacks.



CEN TS 18099

CEN/TS 18099 is the technical specification designed to assess a biometric system's resistance to injection attacks. Ingenium, a testing laboratory, conducts evaluations against CEN/TS 18099 and beyond, providing the highest level of standards-aligned assurance currently available. [Find out more here.](#)

ISO 25456:

An international global standard for injection attack detection. Expected 2027

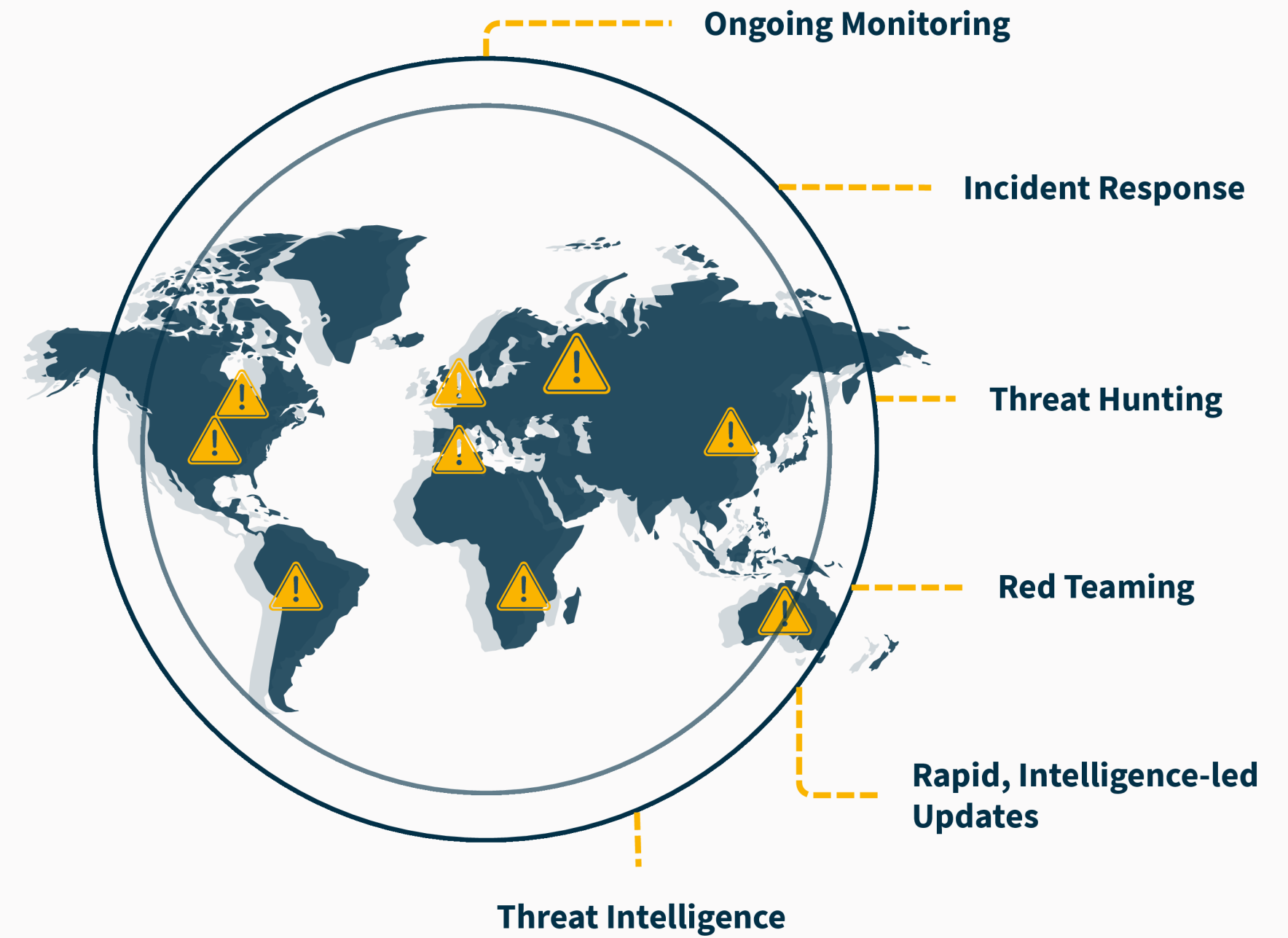
Continued Resilience is Critical

While independent, standards-aligned testing is a strong indicator of a solution's attack-detection capabilities, it's unrealistic to lab-test every attack variation. The threat landscape moves faster than any certification cycle, and a solution that passed testing twelve months ago may face attack techniques it was never evaluated against.

Alongside independent injection attack testing, banks must consider how face verification vendors remain resilient as the attack landscape evolves. Gartner recommends organizations "invest in a threat intelligence team focused on tracking emerging deepfake-related threats and collecting intelligence on various techniques being used by attackers."¹⁵

Banks should ask vendors how they monitor for new threats, how quickly they respond when new attack methods emerge, and what evidence they can provide of ongoing adaptation.

The capabilities to look for include active threat intelligence programmes, regular red team testing against live attack tooling, threat hunting, and rapid speed of response when a new attack is identified. A vendor that can demonstrate this operational posture can assure that their defences remain resilient as attacks emerge.



iProov

iProov powers resilient face verification and liveness detection solutions for tier one banks and governments globally. Our award-winning solution promotes security and inclusivity by design, ensuring market-beating pass rates and advanced AI fraud mitigation.

- Protects against the full range of presentation, injection, and deepfake attacks.
- Independently validated against iBeta Level 1 & 2, FIDO Alliance Face Verification Certification, and CEN TS 18099
- The first vendor to meet NIST SP 800-63-4 guidelines for identity proofing
- Continuously hardened against AI attacks with ongoing threat management
- Passive user experience, free from instructions or cognitive challenges
- Real-time feedback helps users capture optimal images and correct issues
- No material bias across age, gender, and skin tone
- Conformant to WCAG 2.2 Level AA for 'Accessible Authentication'

Drive high performance across global demographics

1.08

attempts to pass

98.5%

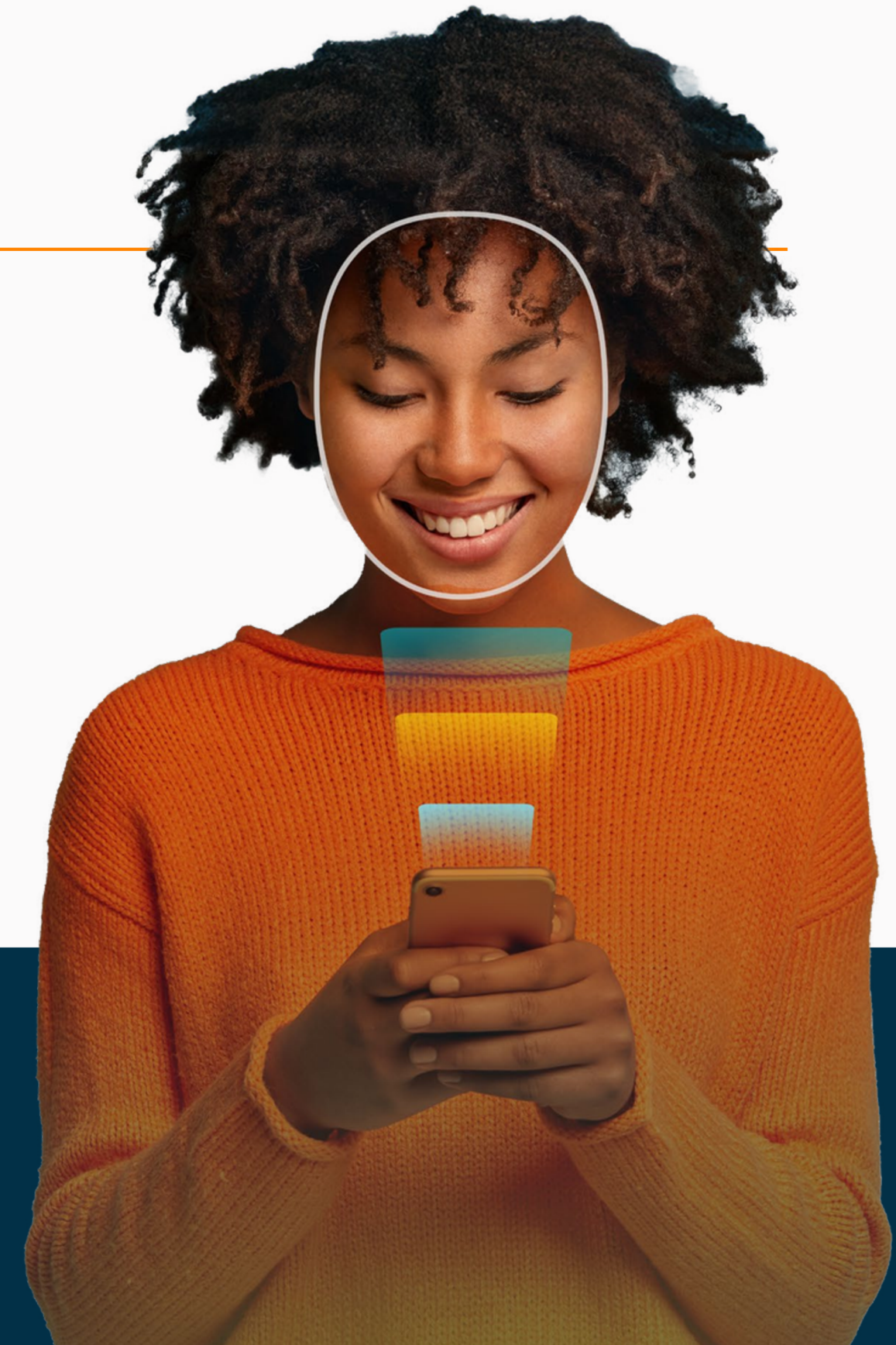
completion rates

21,000+

devices globally

99.99%

uptime



Ready to Protect Customer Accounts?

Reduce fraud losses, mitigate financial crime exposure, and improve conversion rates across the customer identity lifecycle.

[Find Out More](#)

References

1. Gartner, *Major Fraud Trends That Banking CIOs Must Counteract*, Sharma, V, March 2026,
2. Ibid
3. American Banker, *'Profits over compliance': TD takes record \$3 billion guilty plea*, October 2024
4. Fenargo, *Regulatory penalties for global financial institutions skyrocket 417% in H1 2025*, August 2025
5. United States Attorney's Office, *Creator Of "OnlyFake" Charged And Pleads Guilty To Selling More Than 10,000 Digital Fake Identification Documents*, February 2026
6. iProov, *Threat Intelligence Report*, April 2026
7. iProov, *NIST 800-63-4 Guidelines: An Identity Call To Action*, December 2025
8. Gartner, *A Journey Guide to Delivering Human-Centric User Authentication*, Allan, A, April 2025
9. Gartner, *Top Digital Customer Experience Trends for Bank CIOs in 2026*, Jackson, J, January 2026
10. Vena Solutions, *Average Customer Acquisition Cost by Industry*, September 2024
11. The Federal Reserve, *Account takeover fraud: A persistent threat*, February 2026
12. Gartner, *Make Customer Authentication Simple and Smooth to Optimize UX*, Allen, A, July 2025
13. Liminal, *Market and Buyer's Guide for Customer Authentication*, January 2024
14. Gartner, *Quick Answer: How to Secure User Credential Management and Account Recovery*, Hoover, J, June 2024
15. Gartner, *Emerging Tech: The Impact of AI and Deepfakes on Identity Verification*, Khan, A, February 2024
16. Ibid

GARTNER is a trademark of Gartner, Inc. and/or its affiliates.

iProov.com

©iProov Limited 2026. All rights reserved. "iProov" and the "i" symbol are registered trademarks of iProov Limited (registered in England & Wales under number 07866563). Other names, logos and trademarks featured or referred to within this document are the property of their respective proprietors. Errors and omissions excepted. Content herein shall not form part of any contract.

