Know your fraudster

How to identify evolving fraud threats, reduce risk and build trust across the customer journey.

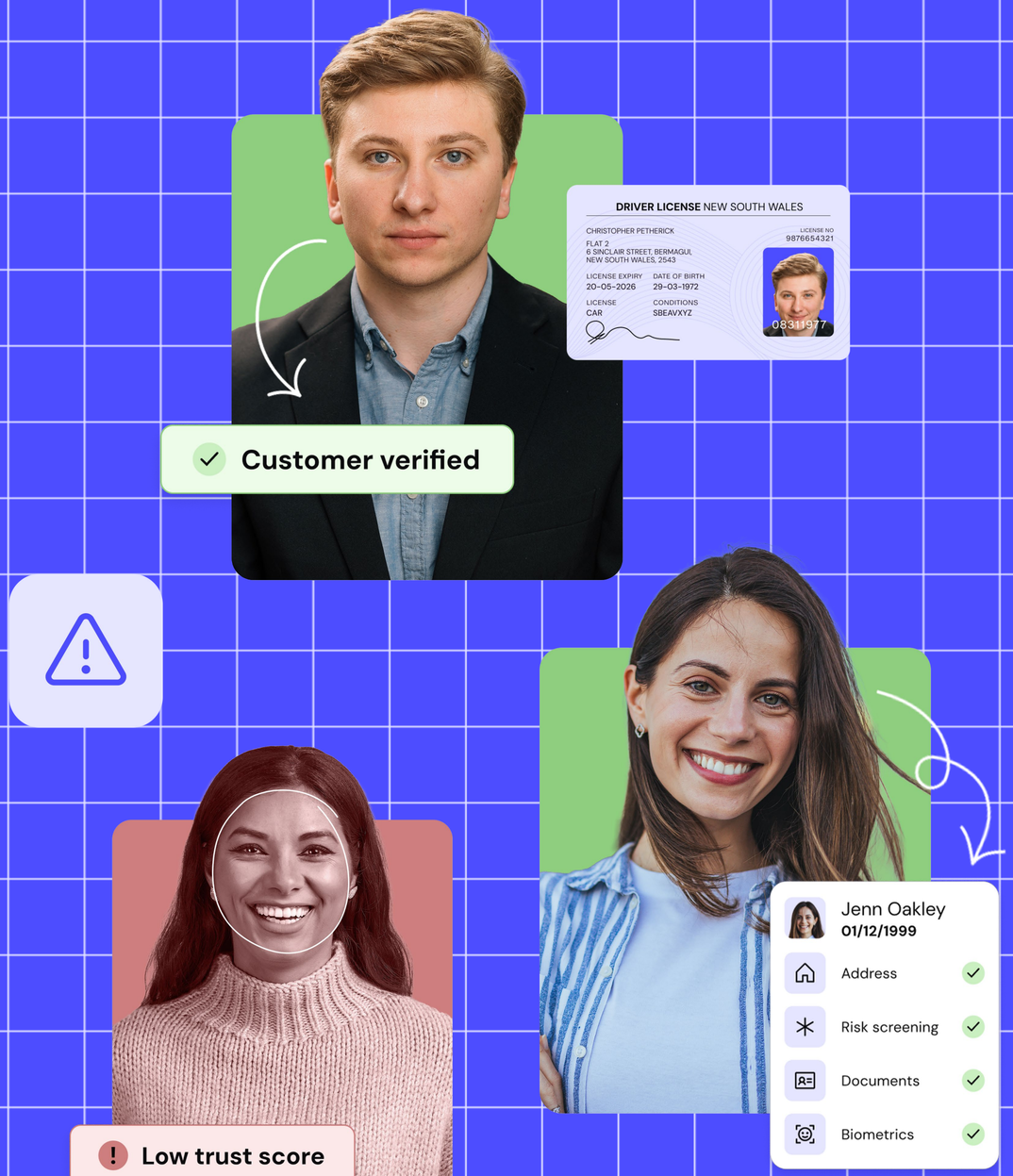
For Fraud Leaders, Identity Teams and Digital Trust Professionals.

The modern fraudster does not always look suspicious

They can arrive with convincing identity documents, realistic selfies and low-risk behavior designed to pass basic checks and blend into legitimate customer activity. With forged documents, synthetic media and manipulated selfies becoming harder to spot, human review alone is no longer enough to separate genuine customers from sophisticated fraud.

That is what makes today's identity fraud so difficult to stop. It is not only becoming more sophisticated. It is becoming harder to distinguish from legitimate customer activity and the costs of poor prevention are clear: revenue losses, added unnecessary operational costs, customer friction and dissatisfaction and new manual review burdens. As a result, connected identity intelligence with multi-signal fraud prevention is now a necessity for the modern industry leader.

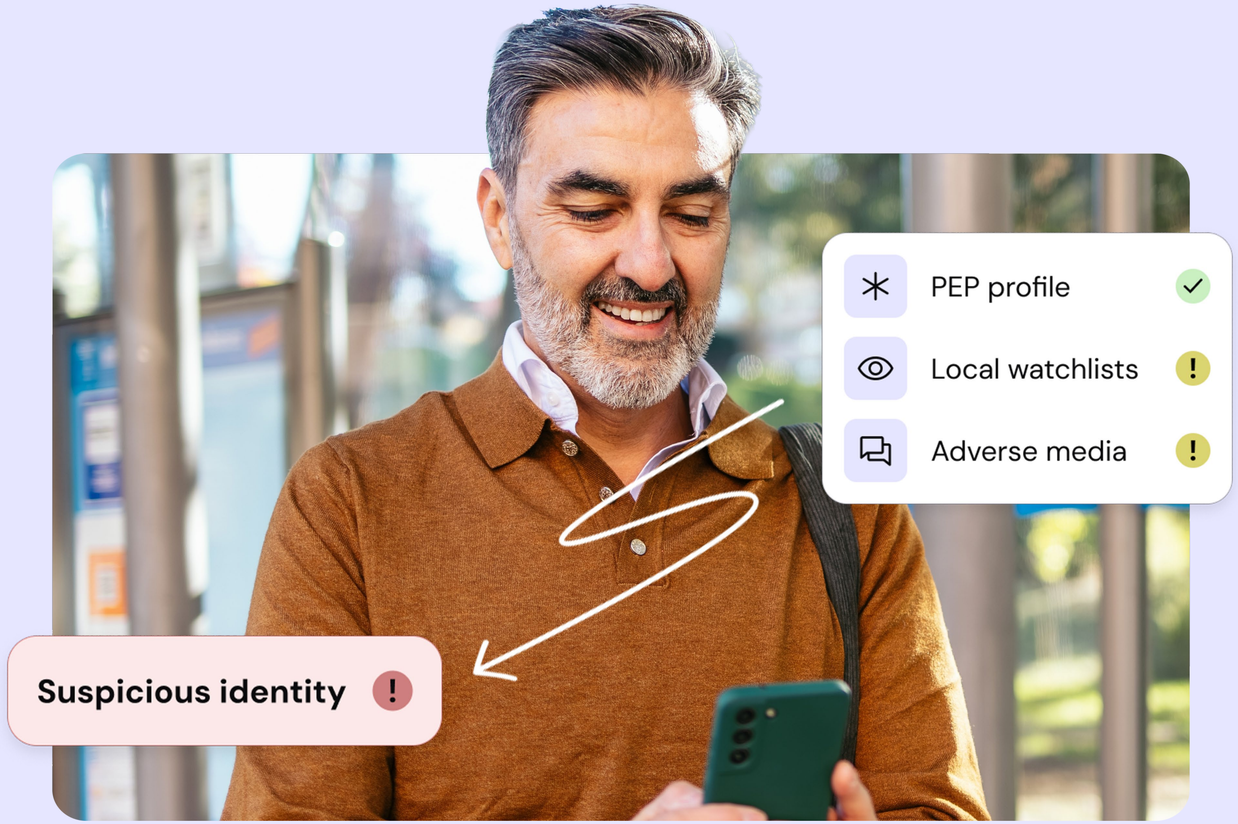
This guide shows how to recognize the modern fraudster and build the identity defenses needed to stop them.



Fraud has evolved. It’s now built to blend in.

Fraud has moved beyond isolated attacks. Today, it behaves more like a system: coordinated, adaptive, increasingly AI-enabled and designed to blend in.

It no longer shows up only as stolen credentials, fake accounts or suspicious transactions. Modern fraud is harder to spot because it is built to look legitimate and without connected defenses, hits your operational costs, customer attrition, compliance pressure and revenue harder than ever.



Where modern fraud shows up

Onboarding

Synthetic identities, fake or manipulated documents, incentive abuse

Account recovery

Impersonation, biometric spoofing, social engineering

Ongoing activity

Behavior designed to look legitimate, account misuse, low-and-slow fraud

Post-onboarding

Fraud that builds over time after trust has already been granted

Source: FBI IC3, 2025 Internet Crime Report

22,364

AI-related cybercrime complaints in 2025

Including fraud and scams enabled by generative AI.

$893M+

in reported losses

From AI-related cybercrime complaints in 2025.

AI has accelerated this shift. What once required specialist skills or manual effort can now be created, tested and repeated at speed and scale.

Fraudsters can generate more convincing documents, create synthetic media, mimic real users and refine attacks more efficiently than ever before.

Modern fraudsters are attacking the systems, processes and moments of human trust that businesses rely on to decide who gets in, not just identities.

They need to know what kind of fraudster is attacking them before they can effectively stop them.

Meet the modern fraudster

The term ‘fraudster’ is broader than you might initially expect

Identity builders, impersonators, account raiders and network operators use different methods and exploit different vulnerabilities to attack different areas of a business. As a result, your defenses have to cover every possible angle in the customer lifecycle with strategies that are both multi-layered and unilaterally connected.

In the same vein, for these strategies to be as effective as possible, you have to know how each type of fraudster behaves, and how they each try to affect your operations.

The Identity Architect

Synthetic identity fraud

How they operate

Identity Architects combine real and fabricated data, documents and digital signals to create a credible identity that will bypass unprepared or underutilized prevention systems.

Objective

Open accounts, exploit incentives, access services or build trust over time.

Exploit

Basic onboarding checks, disconnected data sources and systems that validate information in isolation.

Hard to spot because

Real data and convincing artifacts can make synthetic identities impossible to judge by sight alone.

The Impersonator

Deepfakes, biometric attacks and social engineering

How they operate

They mimic a legitimate person using AI-generated imagery, synthetic media, stolen data, fake selfies, spoofed biometric signals or synthetic voice to create fake ‘profiles’ that can fool basic fraud prevention solutions.

Objective

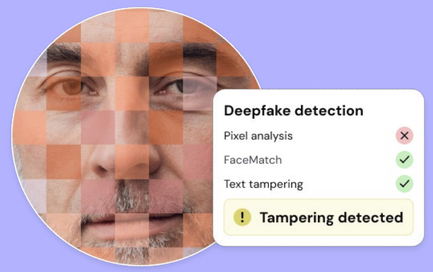
Pass as someone else during onboarding, authentication, account recovery, interviews or call center conversations.

Exploit

Weak liveness checks, remote verification journeys, recovery processes, interview workflows and moments where human trust overrides risk signals.

Hard to spot because

They mimic trusted signals and familiar behaviors well enough to appear legitimate.



The Account Raider

Account takeover and credential abuse

How they operate

They gain access through stolen credentials, compromised devices, weak authentication or vulnerable recovery flows to hijack the account of an existing member or create a new account using someone else’s details.

Objective

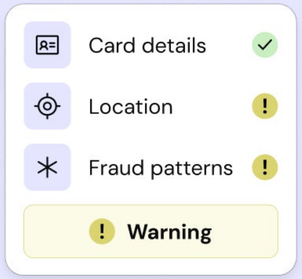
Use a trusted account to extract value, change details, make transactions or move deeper into the journey.

Exploit

Trusted accounts, weak recovery flows, support-team manipulation and limited post-login monitoring.

Hard to spot because

They operate inside an account the business already trusts.



The Network Operator

Coordinated fraud networks and scalable attack models

How they operate

They coordinate tools, data, automation and human actors to test defenses, share what works and scale successful tactics.

Objective

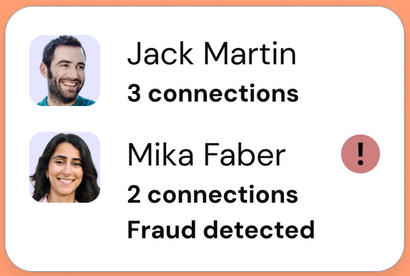
Attack at volume, adapt quickly and repeat successful methods across markets and journeys.

Exploit

Siloed systems, inconsistent controls and teams that only see fraud at account, document or transaction level.

Hard to spot because

The pattern is bigger than one interaction.



The commercial cost of modern fraud

Modern fraud rarely stays contained.
Once it gets through, the cost spreads.

Fraud leaders estimate fraud costs businesses

4-10%

of revenue

When fraud gets through, the impact spreads: higher direct financial losses, more manual reviews, support costs, weaker trust, higher customer churn and greater regulatory and compliance pressure.

Proactive fraud countermeasures increase the likelihood of stopping fraud attempts before they take root, yet many businesses still rely on reactive measures.

Source: TransUnion, Fraud and Identity Report 2025

How fraud spreads across the customer journey

Acquisition

The first trust decision. Fraudsters enter through onboarding
The first trust decision. Fraudsters enter through onboarding using synthetic identities, manipulated documents or convincing biometric interactions. The challenge is getting the balance right — too light and fraud gets through, too heavy and genuine customers abandon.

But a single check at the door can't tell you whether that identity holds true over time. Fraud doesn't stop at onboarding. Neither should identity intelligence.

The onboarding dilemma

Too light

Fraudsters pass through basic checks and enter the system.

Too heavy

Genuine customers face unnecessary friction and abandon the journey.

Engagement

Once fraud is inside the system, it becomes harder to distinguish from normal customer activity.

Retention and revenue

The cost compounds. Fraud drives losses, support demand, investigation time, churn risk and reputational damage.

38%

of new banking customers abandon onboarding if it takes too long

Source: Deloitte

4.3%

of US account logins suspected digital fraud

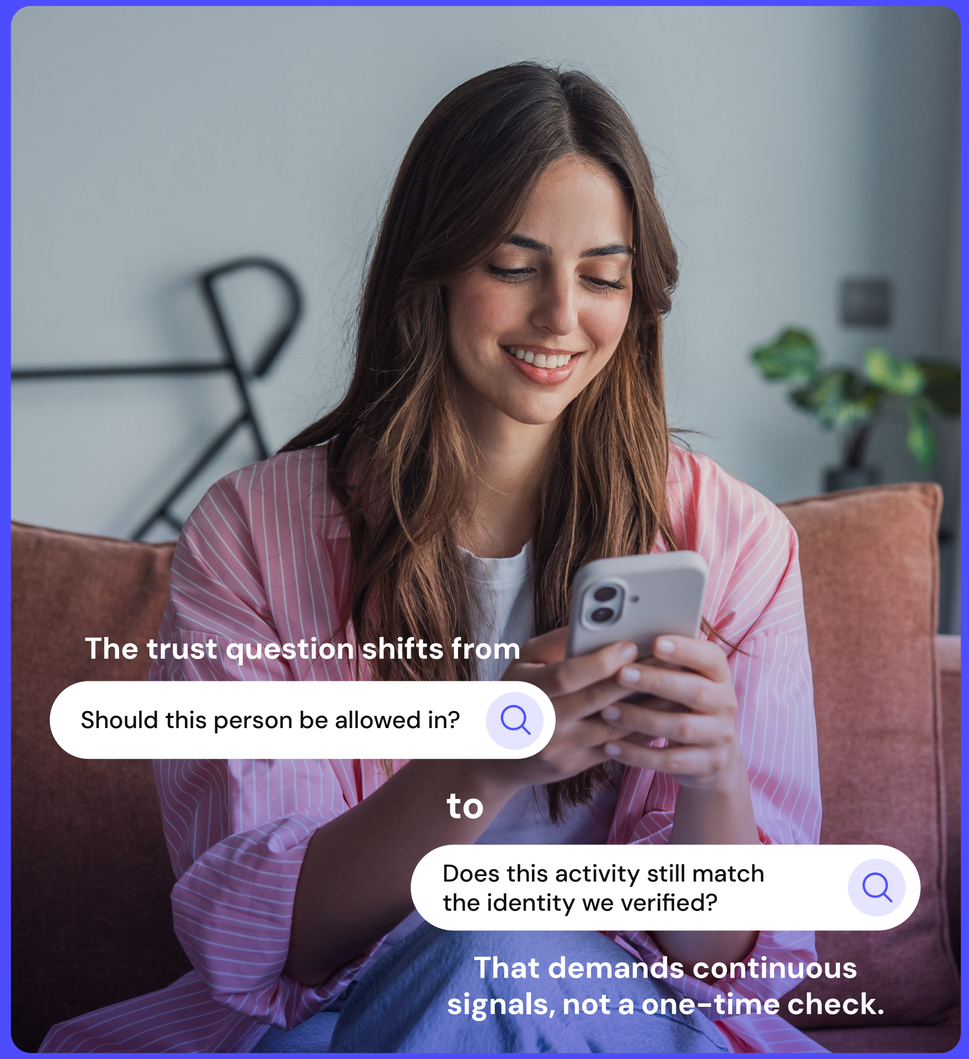
Account login was the second-riskiest consumer lifecycle stage in the US in H1 2025.

Source: TransUnion, H2 2025 Fraud Trends Update

2.5%

account takeover attack rate in 2025, up 4% YoY

Source: Sift, Q3 2025 Digital Trust Index



The gaps modern fraud exploits

Today's fraud is highly coordinated, adaptive and AI-enabled. Yet many identity systems still rely on fragmented point-in-time checks that verify once, apply fixed rules and assess risk in isolation. Without a connected view of identity signals across the customer lifecycle, the gaps are inevitable.

Every gap has a cost: fraud losses, operational drag and eroded customer trust.

The solution isn't more checks; it's closing the gaps between them. That means connected identity intelligence working continuously across the full customer lifecycle, not just at the point of entry.

Where traditional systems fail

One-time verification vs. continuous attack

Traditional systems often treat onboarding as the main moment of truth. Once a customer passes the initial check, trust often carries forward. But fraud does not stop at onboarding: synthetic identities mature, accounts are taken over and low-risk journeys can change as behavior, device or context changes. The weakness is the assumption that trust remains fixed.

Point solutions vs. connected intelligence

Many businesses still assess identity checks in isolation. A document may look valid. A biometric check may suggest a match. A device signal may look acceptable. A database result may return no concern. Individually, each signal can look low risk. Together, they may tell a different story.

Connected intelligence closes that gap. We link document authenticity, biometric consistency, behavioral patterns and device context into a single, continuously updated picture. Document verification confirms the identity is genuine; biometrics confirm the person matches it; and behavioral intelligence tracks whether activity remains consistent with that identity over time. Connected signals flag coordinated fraud even when no single check raises an alert.

Static rules vs. adaptive fraud

Fraudsters test, learn and adjust. If a rule blocks one route, they look for another. Static rules still have a role, but modern fraud protection needs to adapt as patterns change by connecting documents, people, devices, behaviors and contexts.

The answer is not more checks. It is smarter identity decisions built on connected signals. Isolated checks create point-in-time assessments. Contextual signals create more resilient defenses.

How to stop them

Documents and biometrics are critical identity signals, but they are strongest when they work together.

A document can help confirm an identity appears valid. A biometric check can help confirm the person presenting it is present and matches. Modern fraud demands both in one connected view of risk.

What modern identity defense looks like

1. Identity evidence that is easy to capture and strong enough to trust

The challenge

Poor-quality document images slow journeys and hurt decision-making. Blurred scans, glare or bad framing force customers to repeat steps and give fraudsters room to exploit the gaps.

How GBG responds

GBG SmartCapture SDK guides customers to capture clear, usable identity evidence the first time. Better capture means fewer repeat steps, less manual review and stronger evidence to base the identity decision on.

2. Secure ID authentication that can detect fake or manipulated documents

Why it matters

A convincing document isn't necessarily a genuine one. Fraudsters use altered, fabricated or stolen IDs to pass onboarding checks that rely on appearance alone.

How GBG helps

We authenticate documents against a library **of 8,500+ government-issued IDs across 195 countries, running 50+ forensic checks in seconds** to detect fakes, tampering, photo substitution and text manipulation before a fraudulent identity can take hold.

3. Biometric verification that proves ownership and presence

Why it matters

Verifying a document isn't enough. Businesses also need confidence that the person presenting it is the genuine owner and is actually there.

How GBG verifies

Our secure biometric verification helps confirm that the person presenting an identity document is the rightful owner and genuinely present in the journey.

Its face-match capability compares the ID photo with the customer-captured selfie, using 68 biometric facial landmarks to help confirm that the document holder is the same person as the document owner.

When customers use Smart Capture in onboarding and reverification workflows, deepfakes can be detected at the point of capture, helping make the journey a harder target for fraudsters.

4. Protection across the identity proofing process

The challenge

As AI, deepfakes, screen replays and injection attacks become more accessible, fraudsters can fake presence, manipulate documents or bypass remote verification journeys.

How GBG protects

We help protect document and biometric verification from forgeries and deepfakes at each stage of the identity proofing process.

Enhanced tamper detection flags physical document forgeries, including photo and text substitution. Liveness testing protects against screen replays and deepfake video injection attacks, securing **up to 100% protection against the increased threat of generative AI.**

5. A connected identity decision, not separate checks

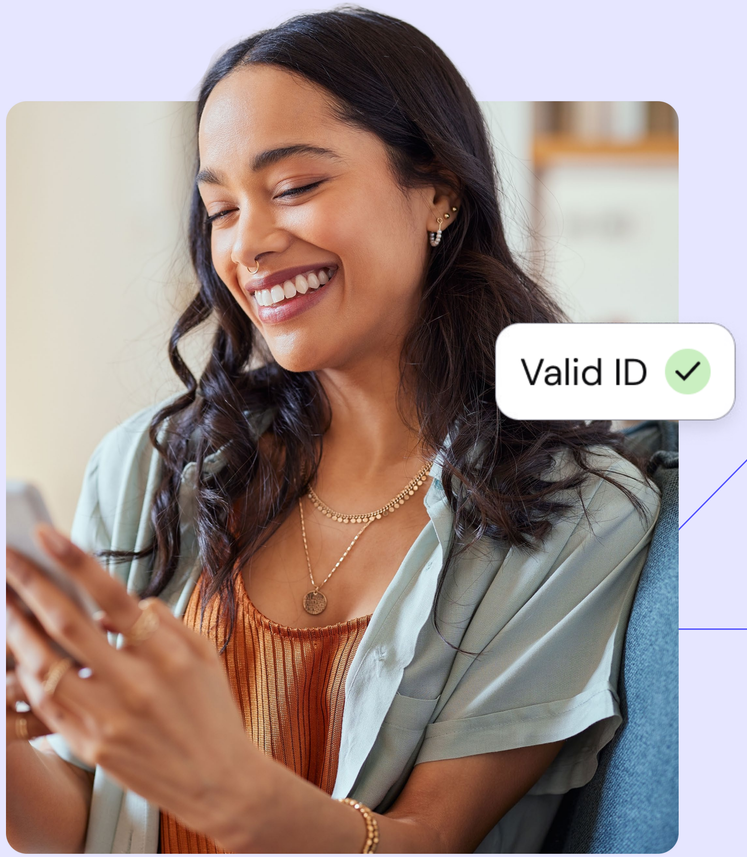
Why it matters

Modern fraud exploits the gaps between checks. A document may look valid. A selfie may appear convincing. A journey may seem low risk. But the stronger decision comes from connecting those signals.

How GBG connects

We bring together our GBG SmartCapture SDK, secure ID authentication and secure biometric verification to help businesses verify identity ownership in seconds, wherever customers are.

That gives businesses a more connected way to answer the questions that matter: is the document genuine, is the person real and present, do they match and should this journey continue?



Know fraud well enough to stop it

Modern fraud is harder to detect because it is designed to look legitimate.

It can arrive through onboarding, resurface during recovery, hide inside trusted accounts and scale through coordinated networks. Businesses can only stop that movement when they understand how it works.

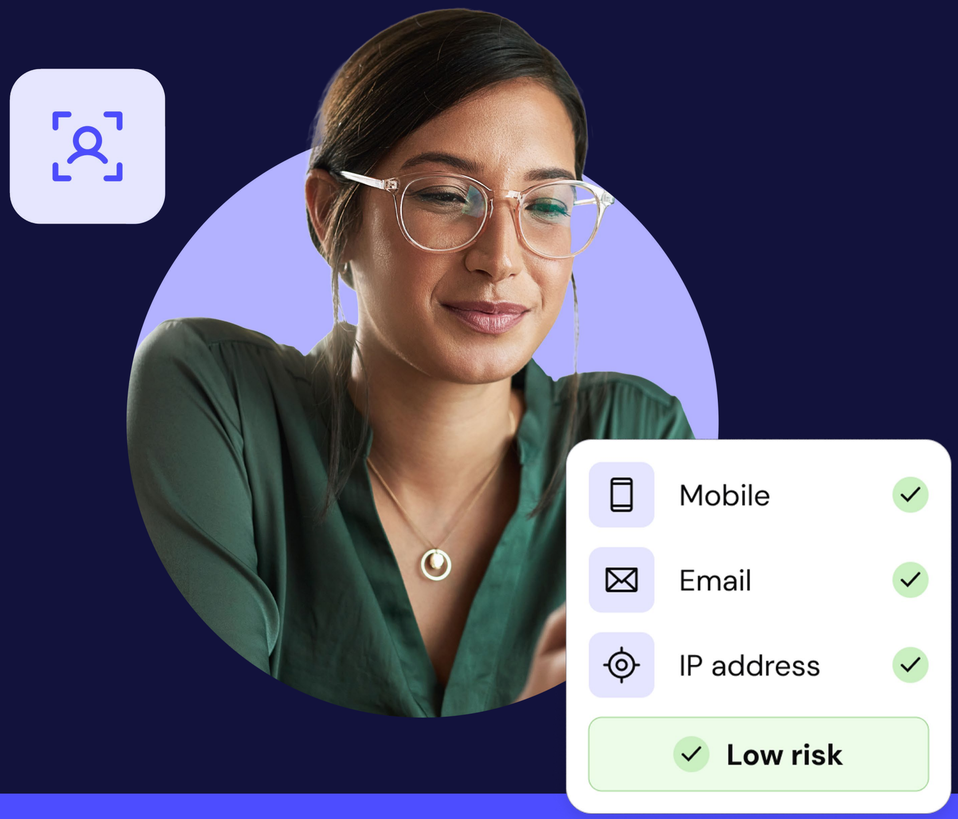
When documents, biometrics, data and customer behavior are treated as separate checks, fraud can find the gaps between them. When they're connected across the full customer journey, you gain a clearer, continuous view of identity risk.

The goal is not simply to catch more fraud. It is to make fraud harder to enter, harder to scale and easier to stop before it damages revenue, operations and customer trust.

To know your fraudster is to understand how they think, where they move and what they exploit. Only then can you build the identity defenses needed to stop them.

GBG

Modern fraud is built to blend in.
Stop it before it becomes trusted.



We connect document authentication, biometric verification and fraud protection into a single, continuous view of identity, helping businesses detect synthetic identities, account takeover and coordinated fraud that point-in-time checks often miss.

Ready to close the gaps fraudsters can exploit?

Book a demo with a fraud specialist