IDENTITY VERIFICATION AND AUTHENTICATION

Prevent Account Takeover at the Source

Verify the Person, Not Just the Login, With Biometric Authentication

If There's a Gap, Fraudsters Will Find It

Account takeover (ATO) losses are increasing, even among the most prepared organizations. Even with prevention measures such as multi-factor authentication (MFA), adaptive risk engines, and passwordless accounts with passkeys, account takeovers shouldn't be happening, but they still are.

Identity verification at onboarding has come a long way, with most institutions confirming a customer's identity through document checks, selfie matching, and liveness detection. This initial identity verification process has added security measures to the beginning of the identity lifecycle.

But what happens after onboarding? Once complete, that verified identity is rarely seen again. Authentication falls back to credentials that can be stolen, one-time passwords (OTPs) that can be intercepted, and security questions answered from a simple Google search. The majority of financial institutions still depend on SMS, OPTs, and push notifications at their highest-risk moments. These methods authenticate information, not people.

Attackers know exactly how to exploit that. They don't always strike immediately, they blend in. They perform the same actions your real customers do, build trust with your systems over time, and wait for the moment permissions allow them to act. By the time risk signals fire, it's often too late. And when step-up authentication kicks in, it asks for the same information an attacker already has. **Risk signals alone can't tell a fraudster from a genuine customer. That's not a detection problem. That's an identity problem.**

Often, the goal of a fraudster is to target the highest strategic value at its weakest point. ATO losses in the US now exceed $17B annually and account for 31% of all fraud-driven revenue loss. The attack surface isn't your perimeter. It's the moments of truth after initial onboarding that is of particular interest to fraudsters.

KEY BENEFITS

Stop fraud at the source

- ATO blocked at enrollment and recovery
- AI-generated deepfakes defeated at highest-risk moments
- Auditable proof of identity in every transaction
- Closes gaps OTPs and knowledge-based authentication (KBA) leave open

Protect customer relationships

- Recover accounts without interrupting the customer experience
- High-risk moments feel safe and trusted
- Reduced risk of negative reputation and customer turnover rates

No new infrastructure

- Works with your existing identity and access management (IAM) solution, no rip and replace
- Customers verified through Entrust carry that identity forward, no repeat verification
- Replaces fragmented point solutions with one portfolio

ENTRUST
SECURING A WORLD IN MOTION

Friction That Works for Customers, Not Fraudsters

Every institution already has a response to high-risk moments. When fraud rises, the instinct is to add friction. More OTP prompts. Stricter lockouts. Longer recovery flows. It feels like the right response. But your customers don't see it that way.

The customer locked out of their own account doesn't experience security control. They experience a 20-minute hold, a script-reading agent, and a series of questions that feel designed to prove they're a criminal. And still their security is at risk, because each question asked is one a bad actor can already answer. With AI, attackers can also build custom profiles in seconds, call your help desk, and sound exactly like the person they're impersonating.

Friction isn't just painful. It's a liability. In fact, 56% of customers stated that they would switch banks after a fraud incident. Organizations, particularly financial institutions, are paying for it in churn, fraud losses, and in the operational cost of help-desk communications.

Entrust's biometric authentication portfolio replaces that liability with something faster, harder to fake, and tied back to the initial, verified identity your customer established at onboarding. This ensures the right person gets through, and the wrong one doesn't.

The Right Protection at Every Moment

Deliver the right level of assurance at every moment of risk, with continuous connection to the verified identity established at onboarding, powered by Entrust's biometric authentication solution that extends what your existing controls leave off.

Motion Authentication is for the moments where you can't afford to be wrong, such as a high-value financial transfer, or a suspicious account recovery. These actions cannot be undone. An active liveness challenge confirms a real, live human is present, not a photo, not a deepfake, not an AI-generated impersonation. These high-risk moments need the strongest protection, with motion.

Face Authentication handles the moments in between. A quick selfie replaces the OTP that never arrived or the security question any attacker can answer. Fast enough for customers, secure enough to prevent fraudsters. In fact, in a recent study of U.S. customers, two-thirds said that they would choose biometrics for stronger protection.

Biometric Passkey covers both everyday login and high-risk step-up authentication in a single credential. It works exactly like a passkey – phising-resistant, native to the device – while being fast and familiar to your customer. Everyday access stays completely seamless. When risk is detected, that same credential quietly triggers a biometric check tied back to the verified identity from enrollment, confirming it's not just the right device, it's also the right person. This feature fits into your existing tech stack, limiting disruptions for your customer and eliminating another app to download and manage.

Prevent ATO by Creating a New Barrier

Account takeover isn't a one-size-fits-all problem. Your authentication stack, customer journeys, and moments of risk are unique, and closing the gaps between them requires a tailored approach.

Start with a conversation to identify where your current controls leave off and what stronger, continuous identity assurance looks like in practice.

Connect with an Entrust specialist or visit entrust.com to request a demo.

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

ENTRUST
SECURING A WORLD IN MOTION