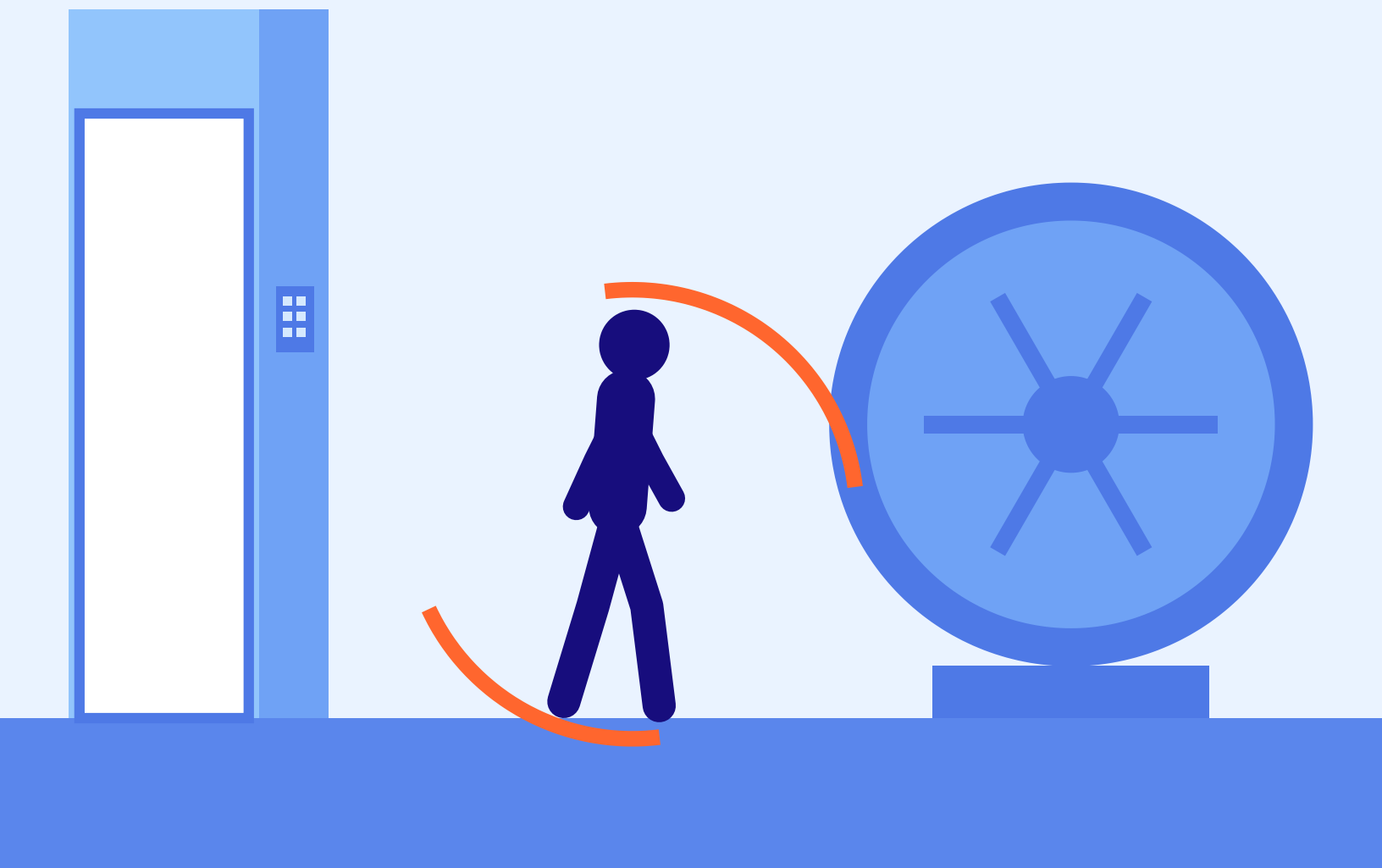




MIMOTO WHITE PAPER

# Beyond the Login: Mimoto for Financial Services

The Value of Mimoto Continuous Verification for Financial Services

# At a glance

- A credential is not a person.
- Unauthorized-party fraud, driven by compromised credentials and account takeover, is now roughly 71% of fraud incidents and losses at U.S. financial institutions (PYMNTS Intelligence / Block).
- Mimoto Continuous CAPTCHA and Mimoto Continuous Verification check, all session long, that a human is present and that it is the right human, with nothing added for customers.
- The same deployment covers retail, treasury, wealth, payments, and privileged internal systems.

Is the entity operating this account, right now, the human it belongs to?

## WHO SHOULD READ IT

CISOs, CIOs and CTOs, and risk leaders at financial institutions.

|           |          |
|-----------|----------|
| Published | 2026     |
| Length    | 13 pages |

## INSIDE

|    |                                                                          |    |
|----|--------------------------------------------------------------------------|----|
| 01 | Executive Summary                                                        | 3  |
| 02 | The Problem: Fraud Has Moved Inside the Session                          | 4  |
| 03 | The Solution: Mimoto Continuous CAPTCHA + Mimoto Continuous Verification | 5  |
| 04 | Where Mimoto Delivers Value Across Financial Services                    | 6  |
| 05 | The Value for Financial Institutions                                     | 8  |
| 06 | Why Continuous Verification Wins                                         | 10 |
| 07 | Deployment: Low-Friction Path to Continuous Verification                 | 11 |
| 08 | Conclusion                                                               | 11 |

## Executive Summary

Financial institutions have spent two decades hardening the front door. Strong login checks, device fingerprinting, and biometric onboarding have made the moment of login more secure than ever. Yet fraud losses keep climbing, because attackers no longer need to break the front door. They walk through it with stolen credentials, hijacked sessions, deepfaked identities, and increasingly, autonomous AI agents that behave convincingly like customers.

The problem is structural: **a credential is not a person**. Everything that happens between login and logout is, at most institutions, a trust vacuum, and that vacuum exists in every channel financial services runs on: retail digital banking, commercial treasury portals, brokerage platforms, payments infrastructure, and internal systems.

Mimoto closes this vacuum. Rather than challenging a user once and trusting the session thereafter, Mimoto continuously verifies that the entity behind every session is (1) human, not a bot or AI agent, and (2) the specific human the account belongs to: in real time, throughout the session, without adding friction for legitimate customers. Because verification is continuous and passive, the same architecture protects a retail customer moving \$500, a corporate treasurer releasing a \$5 million wire, a wealth client authorizing a portfolio change, and a bank employee inside a privileged system.

For financial institutions, the result is a measurable reduction in account takeover losses, lower fraud-operations burden, stronger regulatory posture, and a customer experience that gets better, not worse, as security improves.

## The Problem: Fraud Has Moved Inside the Session

### Account Takeover Is Now the Dominant Loss Driver

The economics of financial-services fraud have inverted. Unauthorized-party fraud, driven primarily by compromised credentials and account takeover (ATO), now represents roughly 71% of all fraud incidents and total dollar losses at U.S. financial institutions, up from less than half of all incidents a year earlier (PYMNTS Intelligence / Block, 2025 State of Fraud and Financial Crime in the United States). Global ATO losses were projected to reach \$17 billion in 2025, up from \$13 billion two years prior (SEON), and the FBI's IC3 logged more than 5,100 ATO complaints with over \$262 million in reported losses in 2025 alone, much of it from criminals impersonating bank support staff to harvest credentials, then draining accounts within minutes.

The critical point for risk leaders: in nearly all of these cases, **the attacker authenticated successfully**. The credentials were real, and every login check was passed, bypassed, or socially engineered. Every point-in-time control did its job, and the fraud happened anyway.

### AI Has Industrialized Impersonation

Generative AI has removed the last technical barriers to impersonation at scale. Fraud attempts involving deepfakes have grown over 2,000% at some financial institutions in three years, and industry analyses now attribute more than 40% of detected fraud attempts in the financial sector to AI-driven techniques (Signicat). Voice cloning requires seconds of audio. Deepfakes now defeat a meaningful share of motion-based liveness checks. Gartner predicted that by 2026, 30% of enterprises would no longer consider standalone identity verification and authentication reliable on their own.

The newest frontier is **agentic fraud**: autonomous AI systems that execute account takeover end-to-end: probing defenses, passing verification flows, adapting tactics in real time, and scaling successful methods across thousands of accounts simultaneously. These agents don't just steal a login; they inhabit a session, and they are engineered to look like a normal customer to every legacy control.

## Point-in-Time Controls Can't Answer the Question That Matters

Traditional CAPTCHA asks "is this a human?" once, at a gate, and today's agentic AI passes it routinely. A login check asks "does this entity hold the right credential?" once, and SIM swaps, phishing, and social engineering routinely defeat it. Neither ever asks the question financial institutions actually need answered, continuously, for the life of the session:

---

## Is the entity operating this account, right now, the human it belongs to?

---

## The Liability Landscape Is Shifting Toward Institutions

Regulators and courts are raising the stakes. Recent litigation (including a 2025 ruling against Citibank) signals that institutions may increasingly bear liability for unauthorized transfers, and FFIEC guidance is explicit that single-factor authentication, even combined with layered security, is inadequate for high-risk transactions. Regulators are pushing institutions toward dynamic, layered "protect, detect, respond" architectures. Continuous, in-session verification is the natural end state of that guidance.

---

03

## The Solution: Mimoto Continuous CAPTCHA + Mimoto Continuous Verification

Mimoto's answer is two products built on one architecture. **Mimoto Continuous CAPTCHA (MCC)** answers "is this a human?" continuously, for the life of the session. **Mimoto Continuous Verification (MCV)** answers "is it the right human?": the specific, authorized owner of the account. Together, they close the trust vacuum between login and logout.

Mimoto reframes the CAPTCHA function from a one-time gate into a persistent, invisible property of the session. Delivered as a SaaS capability that integrates with an institution's digital channels and existing security stack, the combined offering provides:

**Continuous humanity verification.**

MCC continuously distinguishes genuine human interaction from bots, scripts, replay attacks, and autonomous AI agents, throughout the session, not just at login. Where a legacy CAPTCHA is a checkpoint an attacker passes once, Mimoto requires an attacker to prove who they are every moment of every session.

**Continuous person verification.**

Beyond "human vs. machine," MCV confirms that the human present is the specific, authorized human, detecting in real time when a session has been hijacked, handed off, coerced, or initiated by an impersonator, even one armed with valid credentials.

**Real-time impersonation detection.**

Because verification is continuous, the moment an account is operated by someone (or something) other than its owner, the anomaly is surfaced while the session is still live, when intervention can still prevent the money from moving, rather than after it's gone.

**Zero added customer friction.**

Mimoto's verification is passive. There are no puzzles, no image grids, no interruptions for legitimate customers. Security strengthens while the experience improves: a rare combination in financial services, where every added authentication step measurably increases abandonment and call-center volume.

**Integration with the existing stack.**

Institutions choose whether Mimoto enforces rules natively or signals existing fraud engines, SIEM, and case-management workflows, enriching rather than replacing existing investments. Risk signals and session-integrity events become another high-fidelity input to step-up, hold, or block decisions.

04

## Where Mimoto Delivers Value Across Financial Services

Continuous verification is not a single-channel control. Because it operates at the session layer, the same deployment protects every line of business where money, credentials, or sensitive data move.

## Retail and Digital Banking

The highest-volume battleground. Mimoto interdicts the canonical ATO pattern (valid credentials, a clean login, rapid transfer out) while the session is still live. It also detects **coerced and manipulated sessions**: when a customer is on the phone with a scammer who is walking them through a transfer, or when a remote-access tool has quietly handed control of a "legitimate" session to a third party, the behavioral signature of the session changes, and Mimoto surfaces the anomaly before the payment leaves. That matters most on instant-payment rails (Zelle, RTP, FedNow), where there is no settlement window in which to claw funds back.

## Commercial Banking and Treasury

A single hijacked treasury session can move more money than a thousand retail ATOs. Corporate portals are prime targets for business email compromise follow-through, credential theft from finance staff, and mid-session handoff. MCV continuously confirms that the individual releasing a wire, adding a payee, or changing ACH templates is the specific authorized user: not a colleague, an attacker with harvested credentials, or malware operating the session. Session-integrity signals can be wired directly into wire-release and dual-approval workflows as an additional, passive control on the highest-value transactions.

## Wealth Management and Brokerage

Wealth accounts combine high balances, infrequent logins, and older customer demographics: exactly the profile ATO attacks target and elder-exploitation schemes prey on. Continuous verification detects when an account is being operated by someone other than the client (a family member, caregiver, or fraudster), and recognizes sessions consistent with coercion or third-party direction before unauthorized trades, disbursements, or beneficiary changes complete. For firms, this is protection not only against loss but against the suitability and elder-abuse liability that follows it.

## Credit Unions and Community Institutions

Smaller institutions face the same attackers as money-center banks with a fraction of the fraud-operations staff. Because Mimoto is delivered as SaaS, requires no puzzle-based friction, and can enforce natively without a large downstream analytics investment, it gives lean teams a disproportionate capability lift: fewer false positives to triage, fewer post-incident investigations, and a member experience that stays simple, a core competitive promise for community institutions.

## Payments and Fintech Platforms

Bot-driven abuse (credential stuffing, promo and bonus abuse, mule-account automation, synthetic-identity scripting) thrives wherever onboarding and money movement are digital-first. MCC's continuous humanity verification suppresses automation across the whole funnel, not just at signup, while MCV ties each session back to the specific verified owner. For platforms subject to sponsor-bank oversight, session-level verification is also increasingly a partnership requirement, not just a defense.

## Internal Systems and Privileged Access

The trust vacuum exists inside the institution, too. Employee credentials are phished; privileged sessions are hijacked; insiders hand off access. Applied to internal banking systems, admin consoles, and PAM-governed sessions, continuous verification confirms that the person operating a privileged session is the authorized employee for its entire duration: a direct, demonstrable control against insider threat and third-party compromise.

## 05

# The Value for Financial Institutions

## Direct Fraud-Loss Reduction

ATO is the fastest-growing fraud category, and its losses land disproportionately on large institutions, which report fraud losses nearly four times the industry average. Because Mimoto detects impersonation during the session, it interdicts the specific attack pattern behind the majority of today's losses: valid credentials, a clean login, rapid transfer out. Every session-level detection before funds move is a loss avoided, a reimbursement not paid, and a recovery effort not mounted.

## Lower Operational Cost per Fraud Event

Each ATO event triggers investigation, customer support, remediation, potential regulatory reporting, and account restoration: operational drag that scales with incident volume. By catching impersonation in-session, Mimoto shifts the cost curve from expensive post-incident cleanup to inexpensive real-time prevention, and its high-fidelity session signals reduce the false-positive noise that consumes fraud-analyst hours.

## Regulatory and Liability Posture

Mimoto gives institutions a concrete, demonstrable answer to supervisory expectations for layered, dynamic controls on high-risk activity:

**FFIEC authentication guidance.**

Examiners expect layered, risk-based controls that extend beyond login for high-risk transactions. Continuous in-session verification is direct, auditable evidence of a "protect, detect, respond" architecture in operation.

**Regulation E and unauthorized-transfer liability.**

As courts and regulators shift more responsibility for unauthorized transfers onto institutions, the ability to show continuous verification of the customer behind every session is both a defense against losses and evidence of commercially reasonable security.

**GLBA Safeguards and state cybersecurity rules (e.g., NYDFS Part 500).**

Continuous session verification for both customer and privileged internal access maps cleanly to requirements for access controls, monitoring, and risk-based authentication.

**Examiner-ready evidence.**

Session-integrity events, risk signals, and interdiction records flow into existing case-management and SIEM tooling, producing a documented control trail rather than a policy statement.

**Customer Trust and Retention**

The reputational math of ATO is unforgiving: roughly three-quarters of consumers say they would stop using a service after experiencing an account takeover, and nearly nine in ten would tell others. Deposits, assets under management, and payment volume all follow trust. Mimoto protects the relationship, not just the transaction, and does it without the friction that drives digital abandonment.

**Readiness for the Agentic Era**

Financial services is entering a period in which AI agents, both malicious and legitimate (customer-authorized assistants, aggregators, automation), will interact with digital channels at scale. Point-in-time controls cannot distinguish an authorized human, an authorized agent, and a hostile agent mid-session. Continuous verification can. Adopting Mimoto now positions an institution to govern agentic access deliberately, permitting sanctioned automation while challenging hostile agents, rather than reacting after losses mount.

# Why Continuous Verification Wins

| Dimension                               | Point-in-time controls (CAPTCHA, login checks, login biometrics) | Mimoto Continuous CAPTCHA + Mimoto Continuous Verification |
|-----------------------------------------|------------------------------------------------------------------|------------------------------------------------------------|
| When verification happens               | Once, at a gate                                                  | Persistently, for the life of the session                  |
| Question answered                       | "Did something pass the challenge?"                              | "Is the right human still here, right now?"                |
| Session hijacking / mid-session handoff | Invisible                                                        | Detected in real time                                      |
| Stolen credentials and a clean login    | Attack succeeds                                                  | Impersonation still detected                               |
| Bots and AI agents                      | Increasingly able to pass                                        | Continuously challenged                                    |
| Customer friction                       | Rises with every added control                                   | None added; passive verification                           |
| Loss timing                             | Detected after funds move                                        | Interdicted while the session is live                      |

## Key Statistics Underscoring the Need

71%

of fraud incidents and dollar losses at U.S. financial institutions now stem from unauthorized-party fraud, driven by compromised credentials and ATO

PYMNTS INTELLIGENCE / BLOCK

\$17B

projected global account takeover losses in 2025, up from \$13B two years prior

SEON

5,100+

ATO complaints and \$262M+ in reported losses logged by the FBI's IC3 in 2025 alone

4x

large banks report fraud losses nearly four times the industry average

PYMNTS INTELLIGENCE / BLOCK

42.5%

of detected fraud attempts in the financial sector are now AI-driven

SIGNICAT

30%

of enterprises will no longer consider standalone identity verification and authentication reliable by 2026

GARTNER

~75%

of consumers say they would stop using a service after experiencing an account takeover

SIFT

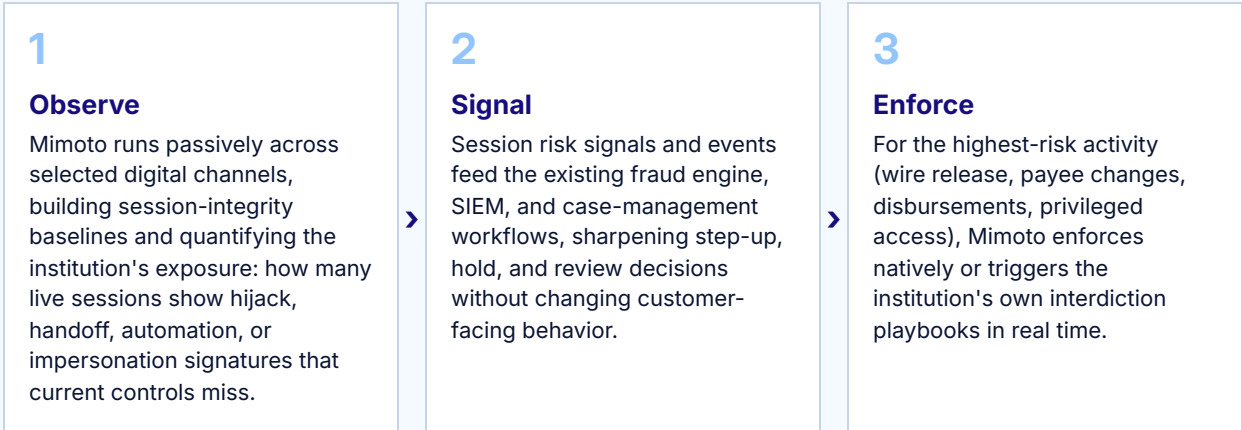
07

# Deployment: Low-Friction Path to Continuous Verification

Mimoto is designed to add a control layer, not a migration project. A typical financial-services rollout proceeds in three phases:

DEPLOYMENT

## Three phases, one control layer



Institutions typically measure impact against a familiar KPI set: ATO loss dollars interdicted pre-settlement, fraud-alert false-positive rate, average investigation cost per incident, authentication-driven abandonment, and call-center volume tied to account-security events. Because Mimoto adds no customer-facing friction, security KPIs improve without degrading experience KPIs, the combination that has historically been out of reach.

08

# Conclusion

The fraud problem financial institutions face in 2026 is no longer a credential problem. It is an identity-continuity problem. Attackers, increasingly powered by AI, have learned to pass every gate an institution puts in front of them. The only durable answer is to stop treating identity as something proven once and start treating it as something verified always.

The combination of Mimoto Continuous CAPTCHA and Mimoto Continuous Verification delivers that shift: continuous, passive, real-time verification that every session (retail, commercial, wealth, payments, or internal) is being conducted by a human, and the right human. The value compounds across every dimension that

## CONCLUSION

matters: lower fraud losses, leaner fraud operations, stronger regulatory standing, protected customer relationships, and a security architecture built for the agentic era rather than the password era.

**The front door is secure. It's time to secure everything behind it.**

To learn more about how Mimoto can protect your institution beyond the login, visit [mimoto.ai](https://mimoto.ai).

ABOUT MIMOTO

# Is this a real human? Is it the right human?

Mimoto provides person-based continuous verification for the AI agentic era. It checks, all session long, that the person in a session is real and is the right person, and catches stolen credentials, hijacked sessions, and impersonation by people or AI agents while they are happening.

---

**See where the gap sits in your environment.**

Schedule a Conversation with the Mimoto team at [mimoto.ai/contact](https://mimoto.ai/contact).