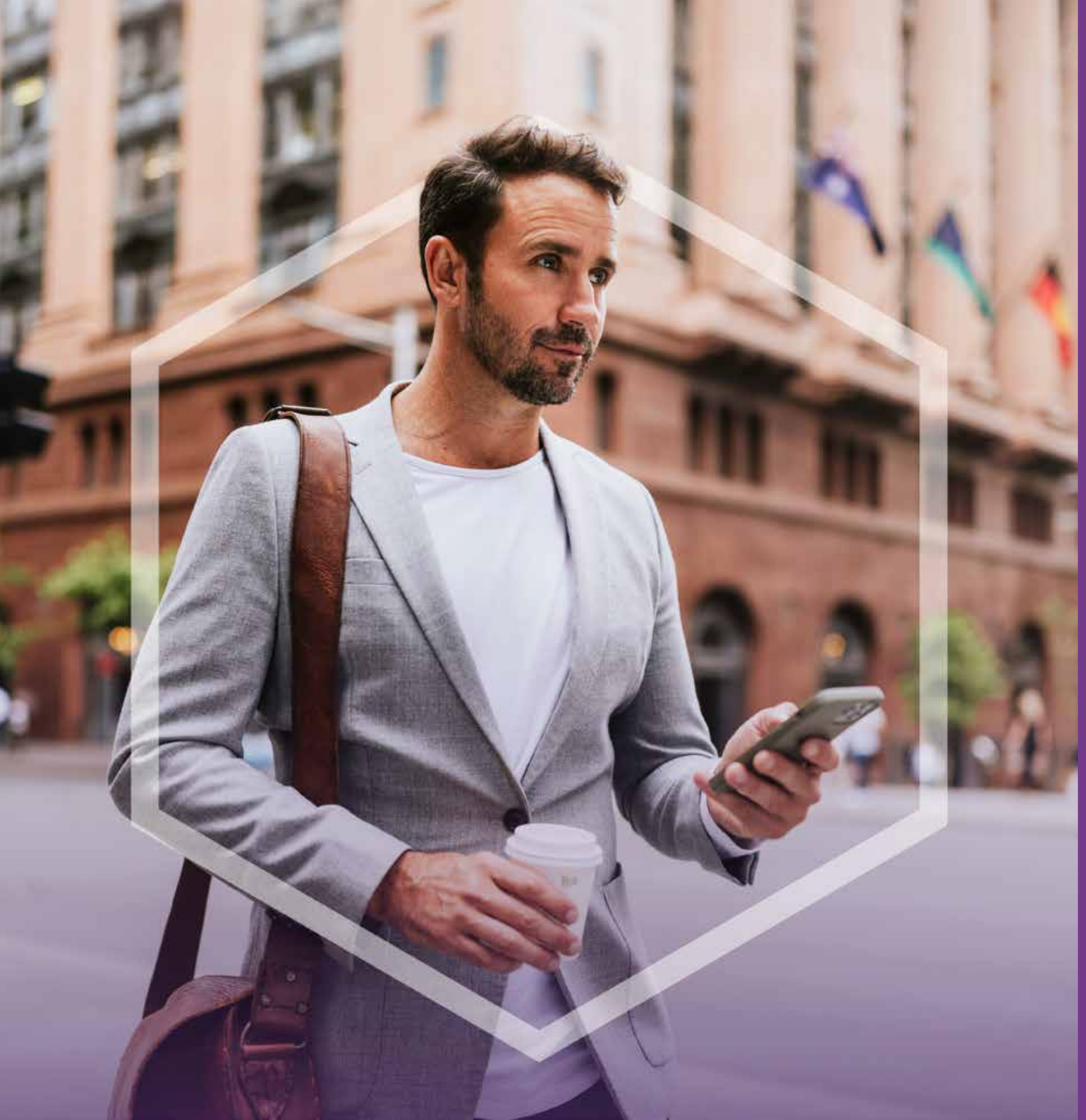


EBOOK

A Guide to Identity Verification for Financial Services

ENTRUST

SECURING A WORLD IN MOTION

INTRODUCTION

Identity: The Foundation of Trust

In financial services, trust is everything, and it begins with identity. Every account opened, transaction approved, and service delivered relies on the ability to verify who's on the other side.

As digital-first banking and fintech adoption accelerate, identity verification (IDV) has evolved from a basic compliance checkpoint into a strategic imperative. Outdated or fragmented identity processes introduce risk at every turn: fraud, failed audits, customer drop-off, reputational damage – the list goes on.

Verifying identities quickly, securely, and in compliance with regulations is what protects customers and keeps operations resilient.

This guide explores how leading financial institutions are rethinking identity verification – not as a point-in-time task, but as a continuous capability that supports security, enhances customer experience, and drives sustainable growth.

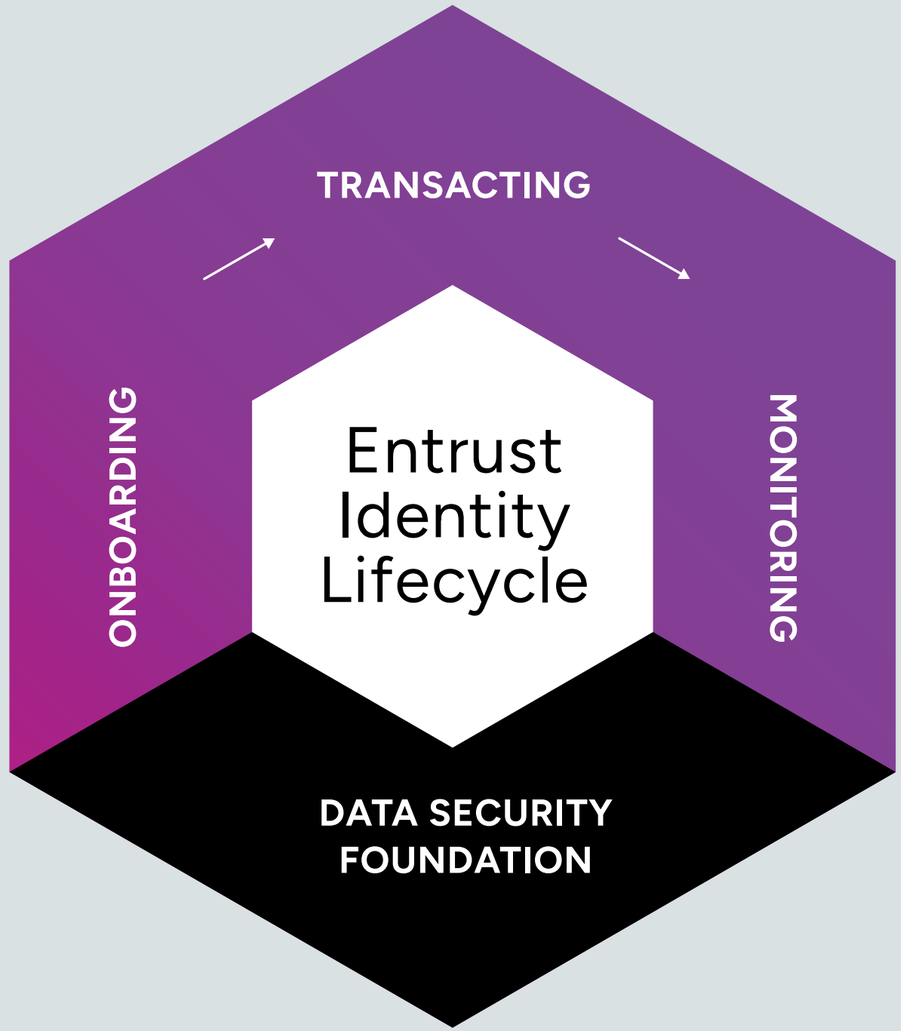
Understanding the Identity Lifecycle

Traditional identity verification often stops at account creation, but in today's threat environment identity must be confirmed and reconfirmed throughout the user journey. Rather than relying on a one-and-done approach, modern financial institutions are adopting a lifecycle-based model of identity:

- **Onboarding:** The initial entry point is one of the most common targets for fraud. Attackers exploit weak verification processes with stolen credentials, fake documents, or synthetic identities. If trust isn't firmly established here, every downstream interaction is at risk.
- **Transacting:** Once accounts are active, everyday activities – logins, payments, data changes – become potential attack vectors. High-value transactions are especially vulnerable to phishing, credential reuse, and session hijacking.
- **Upselling:** Moments of customer expansion, like applying for credit or accessing new services, can attract fraud attempts. Without reverification, institutions may unknowingly grant access or financial products to bad actors posing as legitimate users.
- **Monitoring:** Threats don't stop at login. Sophisticated fraudsters often operate over time, and policy violations or behavioral anomalies can surface days or even weeks after account creation. Ongoing monitoring and re-authentication are critical to catching these signals early.

This lifecycle approach isn't about mitigating risk; it also builds stronger customer trust and improves operational flexibility. When identity is treated as a dynamic, continuously validated credential – not static – institutions can better respond to threats, reduce fraud, and tailor seamless, secure user experiences.

In short, the most effective identity strategies don't end on day one. They build trust from the start and maintain it every day after.



The Fraud Landscape Has Changed

Today's attackers are advanced, coordinated, and faster than ever. Using tools like AI, they create hyper-realistic deepfakes, inject synthetic identities into onboarding flows, and exploit weaknesses through fraud-as-a-service platforms.

And the worst part? They're operating at unprecedented speed and scale. Consider the data:

In 2024, digital document forgery surged[1] 244%

40% of all biometric fraud attempts were deepfakes, occurring once every five minutes[1]

69% of organizations reported an increase in fraud attempts[2]

Identity fraud costs businesses an average of $7 million annually, rising to $13 million for companies with 5,000+ employees[2]

This level of sophistication has outpaced static or fragmented defenses. Financial institutions need intelligent identity systems that detect document tampering, analyze risk in real time, and evolve alongside new attack vectors.

There is reason for optimism: 74% of businesses plan to increase their investments in IDV to meet this challenge head-on.[2] And by 2026, 25% of digital onboarding processes in banking will rely on AI-driven systems – up from just 8% in 2022.[3]

1. https://www.entrust.com/resources/reports/identity-fraud-report
2. https://www.entrust.com/company/newsroom/identity-fraud-costs-organizations-an-average-of-7-million-annually-says-new-research-from-docusign-and-entrust
3. https://www.businesswire.com/news/home/20220418005042/en/Juniper-Research-Regtech-to-Account-for-Over-50-of-Regulatory-Compliance-Spend-Globally-by-2026-as-AI-Reshapes-Digital-Onboarding

The Complexity of Compliance

The global regulatory environment is more demanding than ever, and financial services organizations are feeling the pressure. From eIDAS 2.0 and DORA in Europe to evolving Know Your Customer (KYC) and Anti-Money Laundering (AML) mandates worldwide, institutions must navigate a patchwork of regulations that vary by region, product, and customer segment.

This complexity doesn't just raise the stakes – it introduces roadblocks to scale. Expanding into new markets often means duplicating internal processes or relying heavily on in-house experts to interpret local standards.

To move quickly and stay compliant, financial institutions need identity verification solutions that can adapt to global regulations and support localized workflows. This includes:

- Maintaining secure, auditable trails
- Enabling real-time policy updates
- Demonstrating adherence to data protection and anti-fraud mandates

Flexible compliance is no longer a backend task – it's a growth enabler. It's also a key reason why unifying and modernizing identity verification strategies are essential for forward-thinking institutions.

Customer Experience Is Your Competitive Advantage

Friction is the enemy of conversion, especially in digital finance. Today's users expect seamless account creation, effortless logins, and fast approvals. If identity verification adds unnecessary steps or lags behind expectations, customers won't stick around – they'll leave, often for a competitor.

The best identity systems strike a critical balance: invisible when they need to be, and robust when it counts. By tailoring verification flows to users' behavior and risk profile, financial institutions can deliver security without sacrificing experience.

From onboarding to high-value transactions, a well-orchestrated identity journey builds confidence with every click – and makes your platform easier to trust, simpler to use, and harder to walk away from.

THE DATA BACKS THIS UP:

83% of people say the speed of account opening is important when choosing a financial institution.[4]

47% of consumers abandon banking applications that feel insecure or overly complex.[4]

44% of Gen Z 18- to 24-year-olds abandoned sign-ups simply because they take too long.[5]

4. https://www.entrust.com/cybersecurity-institute/reports/digital-first-banking
5. https://www.entrust.com/company/newsroom/8-out-of-10-consumers-prefer-full-digital-banking-experience-yet-some-are-left-short-changed

Onboarding:
The First Moment of Truth

Onboarding is where first impressions are made and where revenue is often won or lost. Slow, clunky verification processes frustrate potential customers and drive them away. Even worse, they can allow bad actors to slip through the cracks.

That's why leading financial institutions are reimagining onboarding as a strategic asset. With AI-powered verification, it's now possible to screen users in seconds – confirming legitimacy, detecting fraud, and meeting KYC and AML standards without adding manual review bottlenecks.

How? It's all made possible with three core capabilities:

- **Document Verification:** Scans and authenticates the visual, data, and metadata elements of a government-issued ID, checking for validity and signs of tampering.
- **Biometric Verification:** Compares a selfie or live video to the photo on the ID using AI-based facial recognition, flagging potential deepfakes, masks, or spoofing attempts.
- **Data Verification:** Cross-checks key identity attributes (e.g., name, address, date of birth) against trusted databases and watchlists to detect inconsistencies or fraud risk.

This first check doesn't just prevent risk; it also sets the stage for future access and trust. When organizations securely capture identity at onboarding, they can reuse it for reauthentication, transaction approvals, and continuous monitoring throughout the customer lifecycle.

In competitive financial markets, speed and security go hand in hand. A seamless onboarding experience helps win business. A secure one ensures you keep it.

Transacting: Protection at Every Access Point

Once an account is created, every login, transfer, or credential change becomes a potential attack vector. Fraudsters target these everyday moments because they mimic normal user behavior, making suspicious activity harder to spot and defenses easier to bypass. This is where adaptive authentication becomes critical.

Rather than applying the same level of verification to every transaction, risk-based systems dynamically adjust based on context – stepping up security when needed and staying invisible when it's not.

Entrust's AI-powered authentication tools analyze user behavior, device reputation, and contextual signals in real time. The result: fewer hurdles for legitimate users and stronger protection against threats like account takeovers, credential stuffing, and phishing-based attacks.

For example, a login from a user's trusted device and typical location may proceed uninterrupted, while the same attempt from a new device in a foreign country could trigger a biometric check or multi-factor authentication.

The outcome? A seamless experience for trusted users, and a security posture that builds confidence with every interaction.

Monitoring:
Trust That Doesn’t Expire

Fraud doesn’t end after onboarding, and identity verification shouldn’t either. Modern threats demand continuous monitoring, not just point-in-time checks.

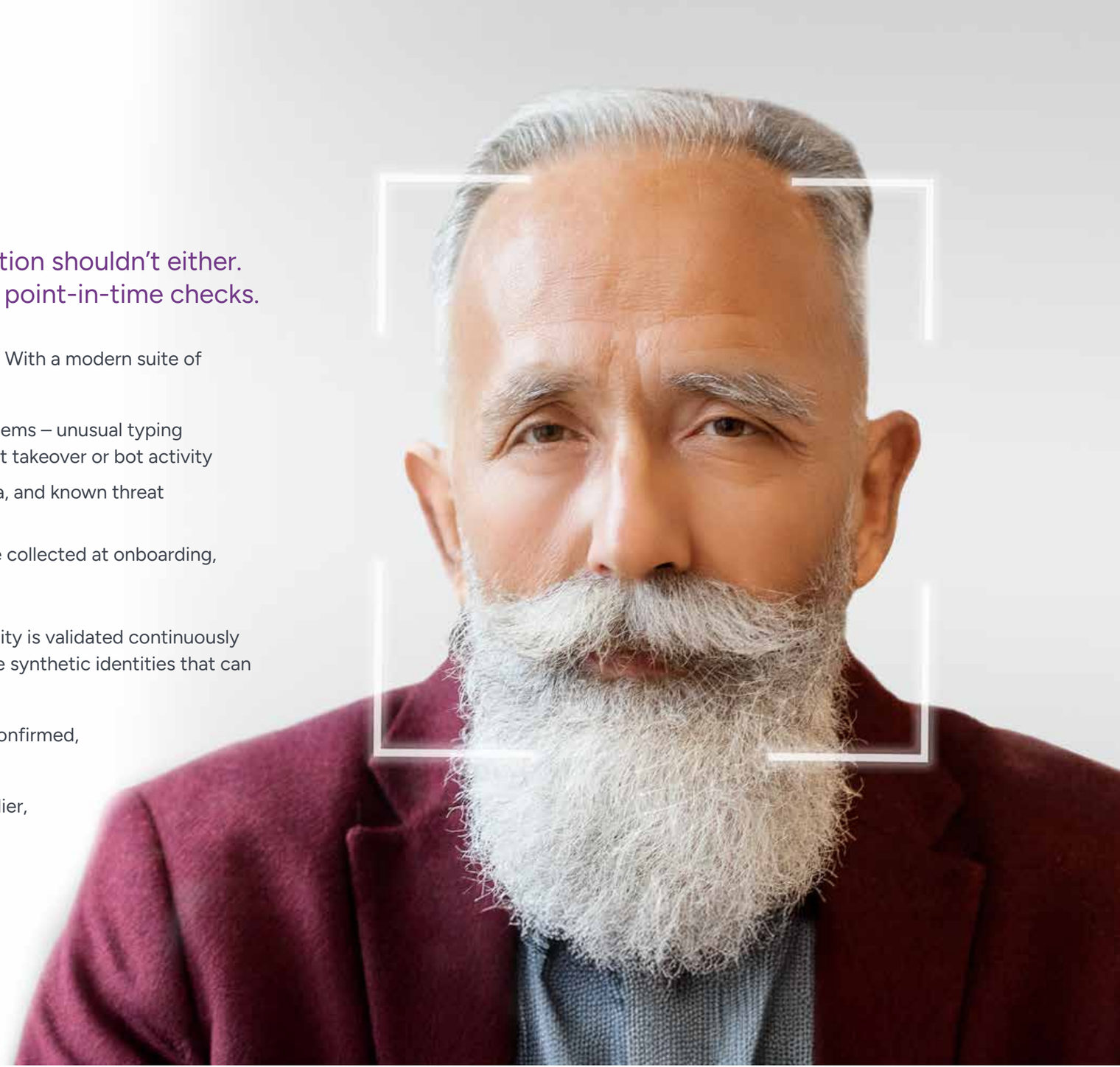
Fortunately, there are tangible solutions you can implement to answer the call. With a modern suite of identity-centric security tools, financial institutions can leverage:

- **Behavioral biometrics** to detect anomalies in how users interact with systems – unusual typing speed, mouse movement, or navigation patterns – that may signal account takeover or bot activity
- **Fraud signal analysis** that combines device intelligence, geo-location data, and known threat markers that continuously assess risk behind the scenes
- **Bio-to-bio reauthentication** that compares new biometric inputs to those collected at onboarding, silently confirming that a returning user is still who they claim to be

These capabilities are essential for supporting a Zero Trust model, where identity is validated continuously and dynamically based on risk. They also help uncover slow-moving threats like synthetic identities that can linger for months before exploitation.

Why does this matter? Because trust is not a static asset. It must be earned, confirmed, and reconfirmed across the customer lifecycle.

With continuous verification in place, financial institutions can catch fraud earlier, respond faster, and build a stronger foundation for enduring digital trust.



The Benefits of a Unified Identity Strategy

Identity shouldn't be siloed. Managing onboarding, authentication, and monitoring separately creates gaps that fraudsters can quickly exploit.

A unified identity strategy streamlines protection across the entire customer journey – delivering consistent UX, centralized fraud detection, and cohesive policy control in one system.

The result? Fewer weak links. Better performance. Stronger security.

With the right solution in place, you can:

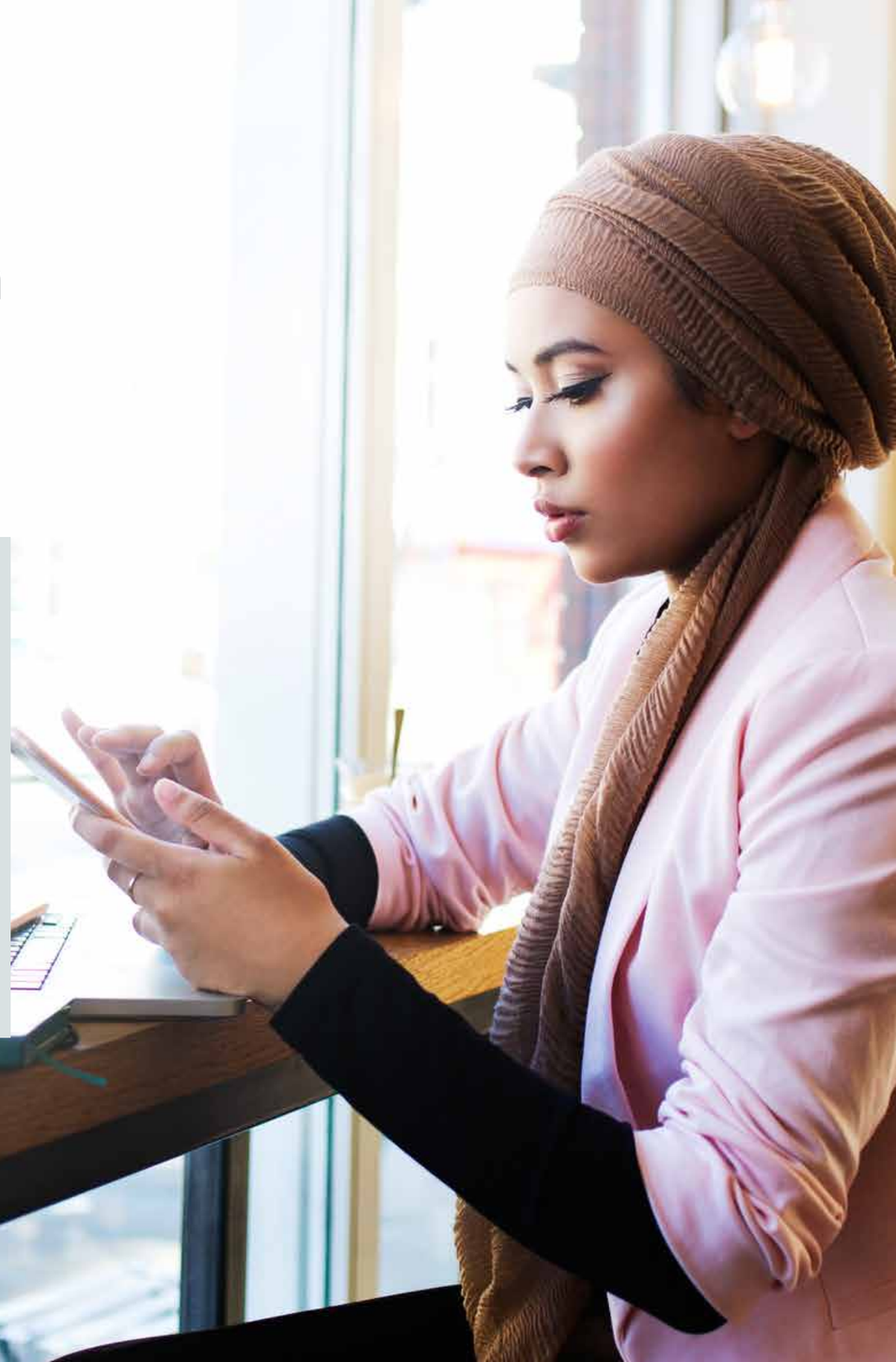
- **Strengthen fraud defenses** with layered, AI-powered identity checks that work together across every stage of the user journey
- **Simplify compliance** with centralized policies, audit trails, and adaptable workflows that align with global standards
- **Enhance user experience** with consistent, low-friction verification flows across all channels and touchpoints – no matter where or when customers engage
- **Reduce vendor sprawl** by consolidating identity verification, authentication, and orchestration into one platform, minimizing resource demands and lowering total cost of ownership
- **Improve visibility and control** with real-time analytics, fraud signals, and dynamic risk-based decisioning to make smarter, faster identity calls
- **Scale globally** using a single system that supports localized compliance, multilingual UX, and flexible orchestration logic

Identity doesn't have to be complicated. **When it's unified, it just works.**

How Entrust Protects Your Financial Institution

Entrust delivers identity-centric security through an integrated portfolio designed to help financial institutions fight fraud, streamline operations, and stay ahead of evolving regulations. Key components include:

- **Identity Verification:** Quickly and securely verify users at onboarding using AI-powered document, biometric, and data checks – each optimized to detect today's most advanced threat vectors.
- **Workflow Studio:** Design and deploy no-code verification workflows tailored to specific risk levels, regions, and customer types – helping to ensure agility, compliance, and a seamless user experience across the entire identity lifecycle.
- **Identity & Access Management (IAM):** Protect sensitive accounts and transactions with strong, adaptive authentication features that include passwordless login, risk-based access controls, and biometric step-up verification.
- **Fraud Detection:** Detect and respond to evolving fraud patterns in real time using advanced risk signals – including device intelligence, geolocation, behavioral analysis, and known fraud markers.
- **Compliance Suite:** Navigate complex regulatory requirements such as DORA, NIS2, eIDAS 2.0, and GDPR with tools built for localized compliance, audit-ready reporting, and quick adaptation to emerging mandates.



Together, these solutions help financial institutions secure the entire identity journey – from day one to every day after.

Identity in Action

Entrust technologies are already helping financial institutions around the world accelerate growth, reduce fraud, and improve consumer journeys.

According to a joint study by Entrust and Docusign, organizations that invest in IDV solutions save an average of $8 million.[6] Compared to their peers, institutions with strong IDV programs are:

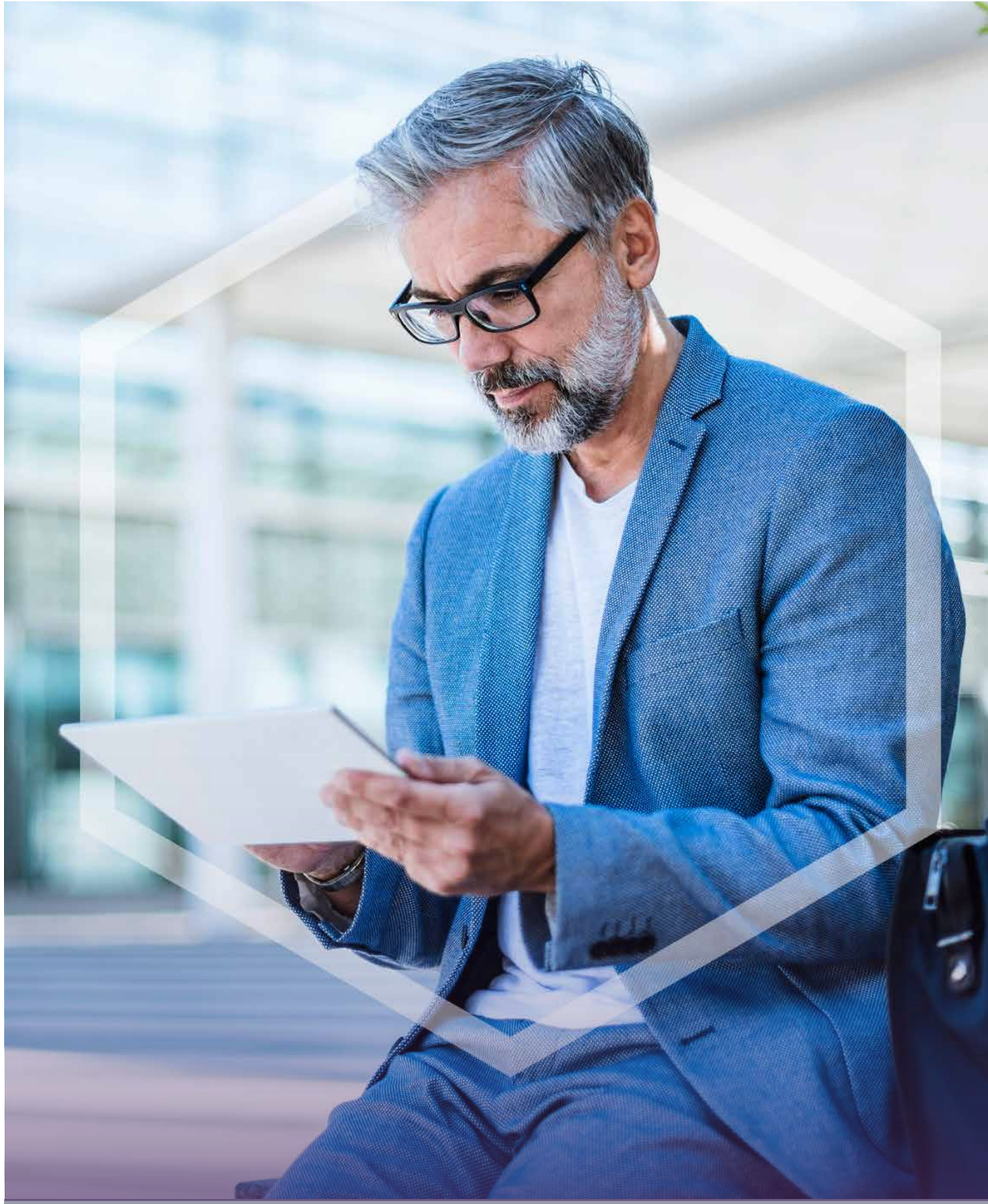
2.7x **more likely** to report a competitive advantage

2.2x **more likely** to see cost savings

1.7x **more likely** to significantly reduce identity fraud

1.6x **more likely** to report a positive brand impact

6. https://go.entrust.com/docusign-future-global-identity-verification



Identity Is Your Growth Strategy

Identity verification isn't just a security checkpoint or a compliance requirement. Today, it's a strategic driver of business performance.

It influences how quickly you can onboard a customer, how effectively you detect fraud, and how confidently you grow your business. With the right approach, IDV reduces friction, unlocks efficiencies, and builds long-term trust.

A strong identity strategy empowers financial institutions to:

- Scale securely
- Adapt faster
- Serve customers with confidence

Entrust helps unify the identity experience.

Whether you're modernizing onboarding, securing daily transactions, or navigating new compliance regulations, we deliver the tools, insights, and reliability to help you succeed.

Ready to build the future of identity security?

Learn how Entrust can help your financial institution protect data, devices, and people – today and tomorrow.

ABOUT ENTRUST

Entrust fights fraud and cyber threats with comprehensive identity-centric security that protects people, devices, and data. Our solutions help enterprises and governments safeguard critical systems from every angle, enabling secure onboarding and issuance, providing everyday identity protection, and empowering them with 360-degree visibility and orchestration across keys, secrets, and certificates so they can transact and grow with confidence. Building on our decades as a pioneer and innovator in establishing trust, Entrust has a global partner network and supports customers in over 150 countries.

For more information, visit entrust.com.

IV26Q2-identity-verification-services-for-financial-institutions-eb

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

ENTRUST
SECURING A WORLD IN MOTION