

October 2026

The Identity Trust Gap: Improving Identity Verification in Banking

Jim Mortensen



Prepared for:  **veridocs**

The Identity Trust Gap: Improving Identity Verification in Banking

Jim Mortensen



Table of Contents

Executive Summary.....	3
Identity Verification: A Gap in the Front Line	4
Defining the Gap.....	4
Why it Matters	6
Identity Threats in the Era of AI.....	8
Third-Party Fraud	9
Synthetic-Identity Fraud	10
First-Party Fraud.....	10
The AI Accelerant	11
Closing the Identity Trust Gap	12
Building an Identity-Verification Framework.....	13
Partnering as a Strategy	14
Measuring Success	15
The Business Case for Change.....	17
Financial Impact	17
Balancing Fraud and Friction	18
Building Trust: The Path Forward	19
Methodology	20

List of Figures

Figure 1: New Account Application Channels	4
Figure 2: Identity-Based Fraud Typologies	8
Figure 3: Trends in Application Fraud Types.....	9
Figure 4: Layered Defense Model	12

List of Tables

Table A: Sample of Recent Regulatory Enforcement Actions Against Tier-2/3 Fls.....5

Table B: Identity Verification Best Practices.....13

Table C: Business Case Framework.....17

Executive Summary

The pressure on financial institutions (FIs) to move customers through account opening quickly has outpaced verification rigor because of an increase in digital onboarding. In *The Identity Trust Gap: Improving Identity Verification in Banking*, Datos Insights explores the widening identity trust gap that regulators are now enforcing against, and fraudsters are exploiting at scale and the imperative to act now:

- **Identity verification failures are systemic, not isolated.** Identity-related suspicious activity comprises 42% of Bank Secrecy Act (BSA) filings across the U.S. banking system, and enforcement actions show that regulators are holding banks accountable.
- **Threat sophistication has fractured into three distinct categories, each requiring different defenses.** Third-party fraud, synthetic-identity fraud, and first-party fraud operate through fundamentally different attack vectors.
- **Deepfakes and Artificial Intelligence (AI)-generated documents are redefining the threat landscape.** Fraudsters can now generate convincing synthetic-identity documents and deepfake facial images at industrial scale, outpacing traditional fraud-prevention responses.
- **Resource constraints are a structural vulnerability for smaller institutions.** Tier-2 and Tier-3 FIs face identical Know Your Customer (KYC) and Anti-Money Laundering (AML) standards as large banks but lack the technology budget and compliance resources.
- **Layered defense approaches are essential as no single control is sufficient.** Effective identity verification combines behavioral analytics, biometric verification, document validation, fraud scoring, consortium participation, continuous model retraining, and cross-channel monitoring, often delivered through strategic partnerships.
- **The business case extends far beyond compliance obligation.** The financial argument contains many dimensions including direct fraud loss reduction, operational efficiency gains, and revenue protection through lower false-positive rates.

The identity trust gap is the distance between the confidence an institution places in an identity and the assurance that identity has earned. It is both an acute regulatory liability and a genuine market opportunity for smaller institutions with branches that enable in-person verification.

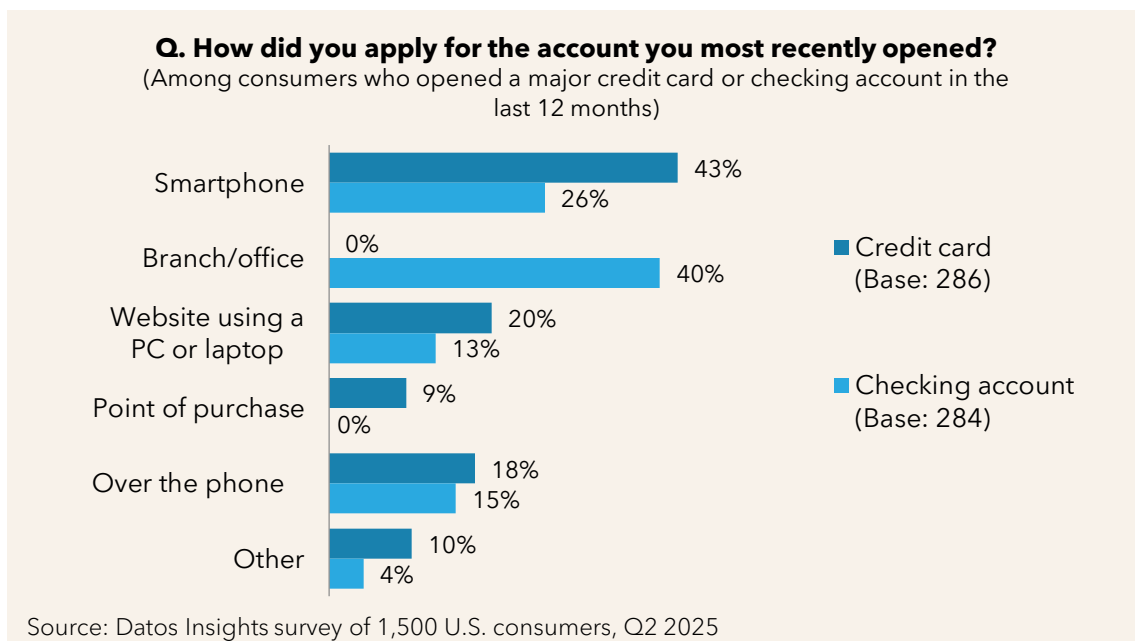
Identity Verification: A Gap in the Front Line

Every downstream control an FI deploys, from fraud detection to account monitoring, rests on a single assumption: that the person applying for an account is who they claim to be. That assumption is weaker than most institutions realize. As digital onboarding has become the default channel for deposit accounts and credit products, the pressure to move customers through account opening quickly has often outpaced the rigor applied to verifying their identity on the front end. The result is a widening gap between how confident banks feel about customer identity and how well that identity has been authenticated, creating a vulnerability that fraudsters exploit at scale.

Defining the Gap

The identity trust gap is fundamentally a failure of first-line defense and represents the difference between the confidence an institution has in an identity and the veracity that the identity has demonstrated. FIs deploy multiple layers of fraud detection and transaction monitoring after an account opens, yet these controls operate with incomplete or unverified identity data. The gap widens because FIs have accepted a level of identity uncertainty at account opening due to digital channel volume (Figure 1).

Figure 1: New Account Application Channels



Digital onboarding may validate identity data without fully authenticating the credential from which that data originated. A counterfeit, altered, borrowed, or stolen credential can therefore introduce false trust at the beginning of the customer relationship, weakening every downstream KYC, AML, fraud, and servicing decision.

Notably, identity-related suspicious activity comprises 42% of BSA filings across the U.S. banking system indicating that identity validation failures are not isolated incidents but systemic vulnerabilities¹. As demonstrated in Table A, U.S. regulatory agencies are continuing to act against those institutions whose frameworks systemically miss obvious identity red flags or have controls that fail to stop identity-related fraud. Recent enforcement actions further underscore the consequences of systemic control failures: In October 2026, American Express National Bank received a US\$350 million penalty for deficiencies in its BSA/AML program, including weaknesses in customer identification and due diligence², while Bank of America faced more than US\$1.21 billion in penalties from the Office of the Comptroller of the Currency (OCC) and the Treasury Department for AML compliance failures, including inadequate customer due diligence and failures to identify and report suspicious transactions³.

Table A: Sample of Recent Regulatory Enforcement Actions Against Tier-2/3 FI

Bank	Description
Covington County Bank	BSA/AML and Customer Due Diligence (CDD) deficiencies, including weaknesses in customer risk profiles and integration of CDD with Customer Identification Programs (CIP) and suspicious-activity monitoring; Federal Deposit Insurance Corporation (FDIC) enforcement order
Police and Fire Federal Credit Union	Fictitious loans in members' names were originated by an employee who was convicted of bank fraud and aggravated identity theft; National Credit Union Association (NCUA) prohibited future participation in insured financial institutions
Quaint Oak Bank	BSA/AML deficiencies involving AML/Countering the Financing of Terrorism (CFT), CIP, and CDD procedures; Pennsylvania consent order

¹ "FinCEN Issues Analysis of Identity-Related Suspicious Activity," Financial Crimes Enforcement Network, January 9, 2024, accessed September 24, 2026, <https://www.fincen.gov/news/news-releases/fincen-issues-analysis-identity-related-suspicious-activity>.

² "OCC Assesses \$350 Million Civil Money Penalty Against American Express," Office of the Comptroller of the Currency, October 8, 2026, accessed October 14, 2026, <https://www.occ.gov/news-issuances/news-releases/2026/nr-occ-2026-87.html>.

³ "U.S. Treasury Announces Record Enforcement Actions Against Bank of America," U.S. Department of the Treasury, October 13, 2026, accessed October 14, 2026, <https://home.treasury.gov/news/press-releases/sb0657>.

Bank	Description
Navy Federal Credit Union	Bank fraud and aggravated identity theft connected to an employee at Navy Federal; NCUA issued a prohibition order
Hatch Bank	Deficiencies involving CIP, CDD, information sharing, and Suspicious Activity Reporting (SAR) controls; FDIC enforcement order
Southern Pine Credit Union	Employee was convicted of aggravated identity theft and bank fraud arising from misconduct at the credit union; NCUA issued a prohibition notice
CNB Bank & Trust, N.A.	Violations of the BSA/AML program, CDD, and CIP requirements, plus failure to correct previously reported BSA/AML problems; OCC enforcement action
Thread Bank	BSA/AML, CIP, and CDD deficiencies involving fintech firms/Banking-as-a-Service relationships, including customer information and beneficial-owner documentation; FDIC enforcement order
First Federal Savings and Loan Association of Lorain	BSA/AML deficiencies, including inadequate ongoing CDD; OCC enforcement action
Slovenian Saving and Loan of Franklin-Conemaugh	BSA/AML internal-control, audit, and training deficiencies, including CDD violations; OCC enforcement action

Sources: FDIC, OCC, Federal Reserve, NCUA, and State of Pennsylvania press releases

Since a substantial portion of applications originate digitally, the verification window is compressed further and creates time pressure that works in fraudsters' favor. This compression creates an issue as FIs measure their identity controls against what peers are doing. The gap has also grown due to deepfake-enabled attacks and synthetic-identity construction enabled by generative AI, which target digital channels.

Why it Matters

The identity trust gap is an active liability that regulators are now enforcing against due to the increase in identity-related SAR filings. For Tier-2 and Tier-3 institutions, the stakes are particularly high because they face identical regulatory expectations to large banks while operating with significantly fewer resources to invest in advanced identity-verification tools. A regional bank with US\$2 billion in assets must meet the same KYC and AML standards as a US\$200 billion institution but lacks the technology budget and dedicated

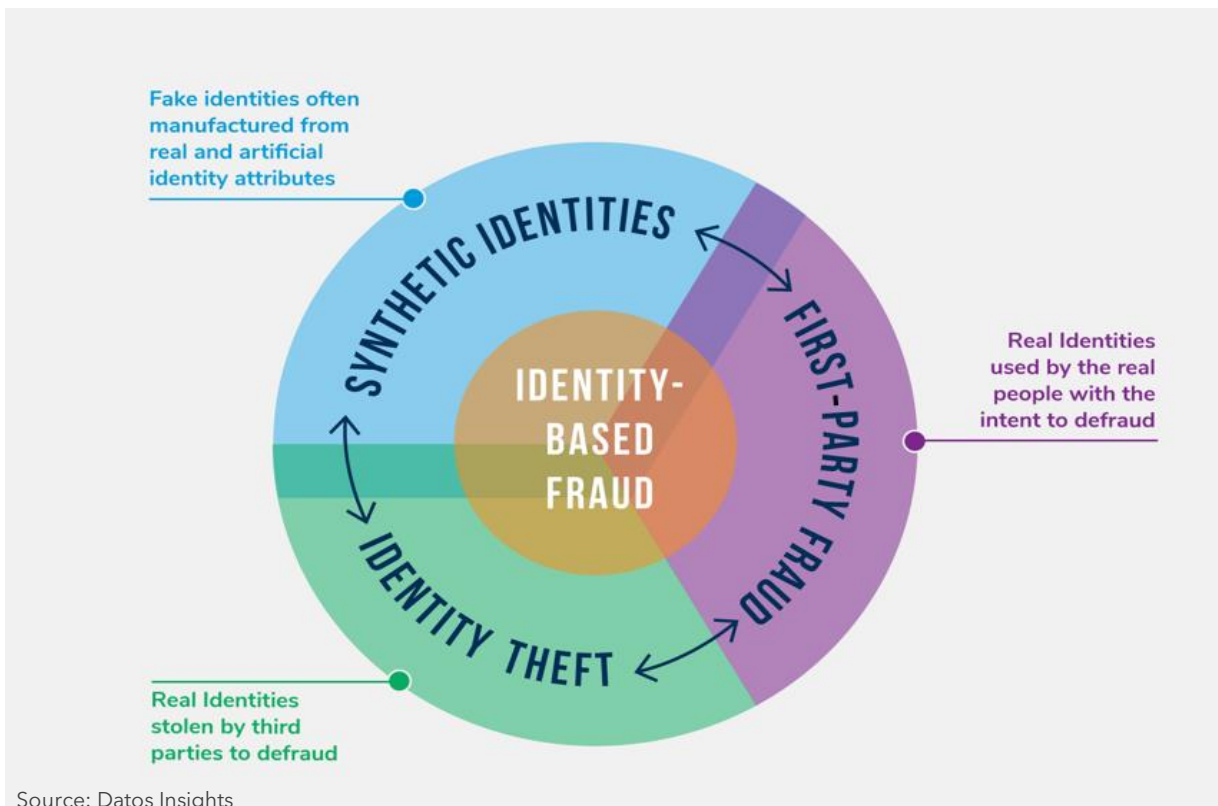
compliance teams to deploy equivalent defenses. This resource mismatch means that credit unions, community, and regional FIs are disproportionately exposed to identity-related fraud and regulatory risk.

Closing the identity trust gap creates tangible business value alongside compliance benefits. Strong front-end identity controls reduce the manual review burden downstream, lower false-positive rates that drive customer abandonment, and build faster case closure on fraud investigations. A competitive advantage accrues because better identity verification at the point of account opening, though it can introduce some initial friction, provides a natural fraud deterrent that is often missing in digital channels. Often, visual inspection and the increased scrutiny related to in-person interactions can result in more effective identity-related declines. Smaller FIs can act on this insight and use in-branch identity verification with the riskiest applicants to differentiate from fintech firms and digital-only competitors while simultaneously reducing fraud losses and regulatory exposure.

Identity Threats in the Era of AI

Fraud attack vectors have evolved and multiplied while fraudsters have increased their use of AI tools. What was once primarily identity theft, where fraudsters use stolen personal information to open accounts in someone else's name, has fractured into three distinct threat categories, each requiring different detection approaches and each accelerating at different rates (Figure 2).

Figure 2: Identity-Based Fraud Typologies

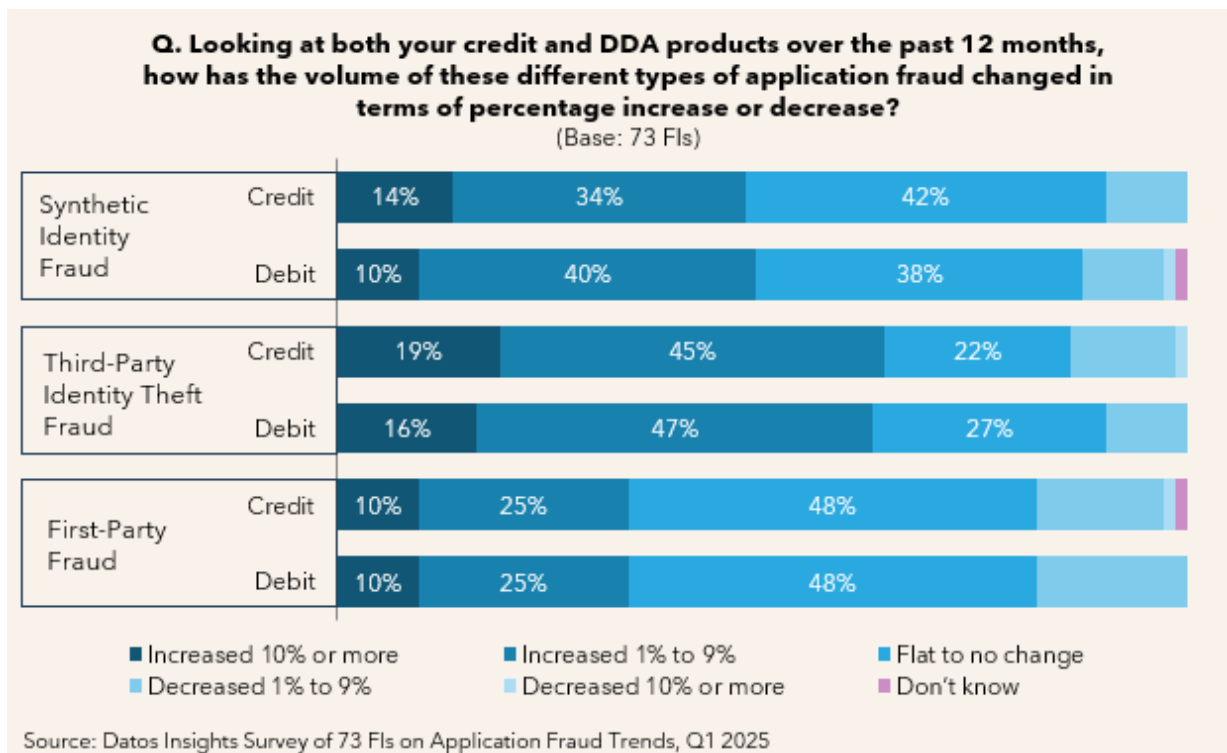


Third-party fraud remains the traditional identity theft vector. Synthetic-identity fraud, where fraudsters construct new identities by blending real and fabricated data, is now the fastest-growing category and the most structurally difficult to detect. First-party fraud involves legitimate customers misusing their own identities to defraud the FI. All of this while AI-enabled fraud, powered by generative AI and agentic tools, is redefining the threat landscape.

Third-Party Fraud

Third-party fraud, the use of a stolen identity to open accounts or obtain credit in someone else's name, experienced the largest percentage increase in both credit and debit card portfolios over a 12-month period in relation to the three main application fraud types (Figure 3). As the most recognizable form of application fraud, its primary mechanism is straightforward: Fraudsters acquire personally identifiable information (PII) through data breaches, the dark web, or social engineering, then use those credentials to apply for accounts at one or more FIs simultaneously. Because the identity is real and the PII is valid, many point controls—such as name-to-Social Security number (SSN) matching, address verification against credit bureau records, and basic KYC checks—will fail.

Figure 3: Trends in Application Fraud Types



The detection difficulty is compounded by the time lag inherent in how identity breach information moves through the financial system. Stolen PII may circulate on the dark web for weeks or months before it appears in consortium databases or triggers velocity alerts. By the time the original account holder reports the fraud to the bank and a SAR is filed, the organized ring has already moved to the next target. This temporal gap is a structural vulnerability in how fraud intelligence is shared across the industry, making third-party fraud particularly difficult to prevent through detection alone.

Synthetic-Identity Fraud

A fundamentally different threat from third-party identity theft is synthetic-identity fraud because it does not necessarily involve the theft of an existing person's identity; it fabricates an entirely new one. Fraudsters acquire real SSNs, often through data breaches, and pair them with made up or altered names, addresses, phone numbers, and email addresses to construct credentials that appear legitimate on the surface. A synthetic identity might pass individual point checks: The SSN verifies against Social Security Administration records, the address exists, and the phone number is active. Yet no real person corresponds to the combination, and crucially, the fraudster maintains control of all contact information.

84% of FIs identify synthetic identities as a moderate to high threat.

Datos Insights survey of 73 U.S. FIs on application fraud trends, Q1 2025

Organized fraud rings use synthetic identities to build credit history over weeks or months before activating them for large-value theft. They open deposit accounts, obtain secured credit cards, make regular deposits and payments, and establish transaction patterns that appear legitimate to automated fraud controls. By the time the account becomes active for fraud through bust-out attacks or high-value transfers, the synthetic identity has accumulated sufficient history to pass risk scoring models built on behavioral baselines. FIs approving a synthetic-identity application in isolation may see an acceptable risk profile, unaware that the same fraudster is opening accounts at a dozen other FIs using related credentials and coordinated device patterns.

First-Party Fraud

First-party fraud is fundamentally different from both third-party and synthetic-identity fraud because it involves real people using their own legitimate identities to defraud the FI. The fraudster applies for an account or credit product as themselves, providing accurate identity information that passes all standard verification checks. The deception lies in their intent and financial representations and not in who they claim to be. These misrepresentations occur at the application stage, where customers lie about income, employment status, or the intended use of credit to qualify for products they would not otherwise receive. Similarly, early payment defaults involve customers who had no intent to repay and default almost immediately after account opening.

The detection challenge is that traditional identity verification, document checks, and KYC controls cannot prevent first-party fraud because the identity is real and the documentation is genuine. An FI cannot reject an application because the applicant passes identity verification, even if that applicant plans to commit fraud. Detection requires behavioral analytics, income verification cross-checked against tax records or employment databases, and post-approval monitoring for velocity and pattern anomalies that suggest coordinated fraud. Many community banks and credit unions lack the data integrations and sophisticated behavioral models required to identify first-party fraud.

The AI Accelerant

AI operates as a force multiplier across all threat categories rather than as a discrete fraud type. Generative AI and agentic tools enable fraudsters to produce convincing synthetic-identity documents and deepfake facial images at industrial scale and at a pace that outstrips traditional fraud-prevention responses. A fraudster can now:

- **Generate a fabricated identity document**, such as a driver's license or passport, with sufficient visual fidelity to bypass most document verification controls
- **Create deepfake facial biometrics** that defeat liveness detection systems that were once considered highly secure
- **Execute social engineering attacks** and navigate FI application processes autonomously through agentic AI tools that adapt their behavior in real time

The structural asymmetry is what makes AI-enabled fraud particularly dangerous. Fraudsters can experiment with new attack vectors, deploy them rapidly across their target set, and modify tactics within hours of encountering a detection rule. FIs, by contrast, must validate and deploy countermeasures through compliance reviews and testing processes.

68% of FIs expect AI use by fraudsters to significantly increase in the next five years.

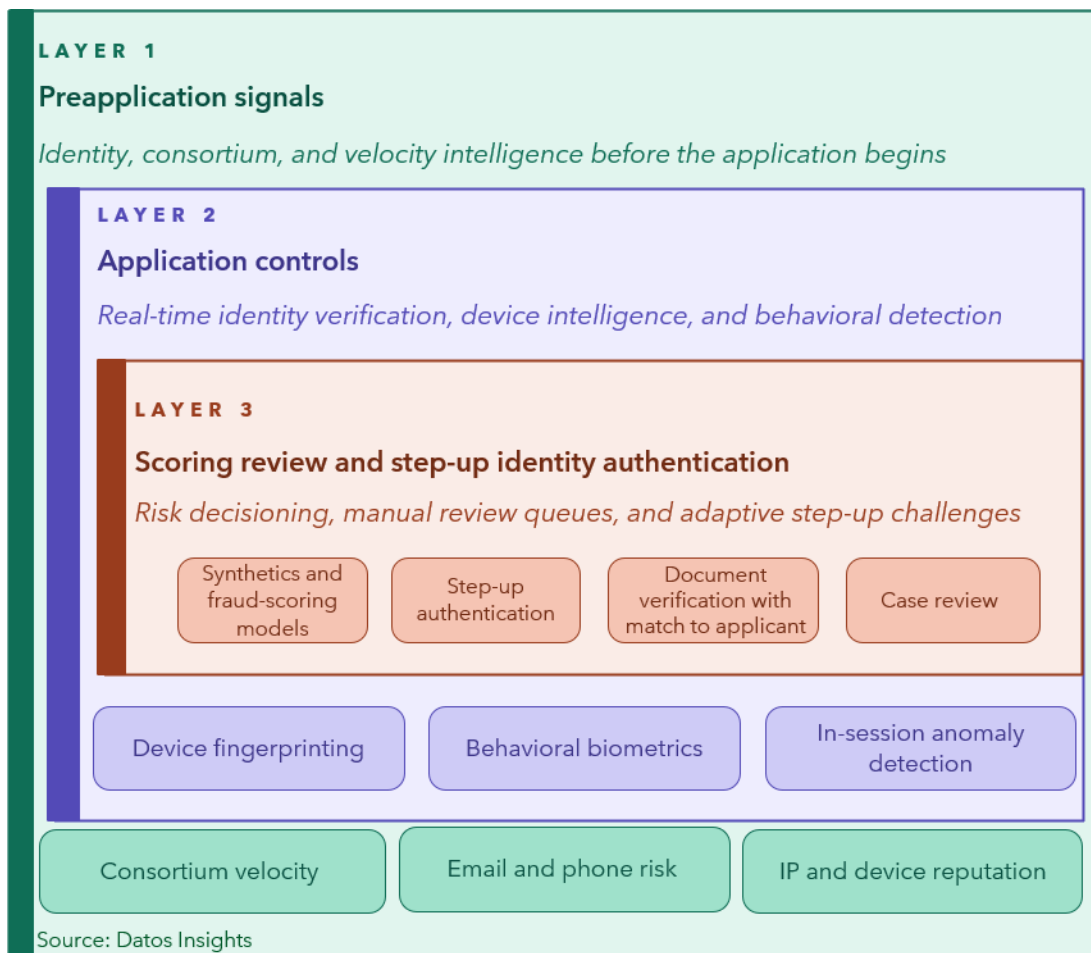
Datos Insights survey of 73 U.S. FIs on application fraud trends, Q1 2025

A community bank that discovers a new deepfake technique targeting its liveness detection cannot simply disable the control and revert to manual review overnight. Manual case review creates operational bottlenecks and poor customer experience. Instead, the FI must work with its vendor to develop, validate, and implement new countermeasures.

Closing the Identity Trust Gap

No single control is sufficient against the threat environment FIs face today. A layered defense approach is essential because sophisticated fraudsters deliberately develop techniques to defeat point solutions, and the threat categories themselves require different detection signals, levels of authentication, and intervention strategies (Figure 4).

Figure 4: Layered Defense Model



Third-party fraud detection relies on document verification, matching to physical biometric, and consortium velocity intelligence. Synthetic-identity fraud requires network analysis and cross-institutional coordination to surface inconsistencies that appear legitimate in isolation. First-party fraud demands behavioral analytics and income verification that extend beyond identity assurance. AI-enabled fraud requires continuous

model retraining and emerging detection methods like injection attack and deepfake artifact analysis.

Rather than searching for a single platform that covers all vectors equally well, Tier-2 and Tier-3 FIs must think strategically about which capabilities matter most to their specific risk profile, how those capabilities integrate with existing systems, and which partnerships enable them to participate in real-time fraud intelligence networks they could not build or maintain alone.

Building an Identity-Verification Framework

No single control can detect all three threat categories simultaneously, which is why Tier-2 and Tier-3 FIs must prioritize which capabilities align with their risk profile and which partnerships enable participation in real-time fraud intelligence networks. Table B provides eight best practices to address the identity trust gap and substantially improve the onboarding risk toolset.

Table B: Identity-Verification Best Practices

Best Practice	Description
Behavioral Analytics	Deploy systems that detect anomalies in how applicants interact with the application itself, including keystroke dynamics, mouse movements, navigation patterns, and cognitive indicators of data familiarity that reveal copy-paste behavior or external data sources.
Biometric and Liveness Verification	Implement facial biometrics with passive or active liveness detection to verify that the person presenting credentials matches their identity document, while anti-spoofing controls detect presentation attacks using photos, videos, masks, or deepfakes.
Document Verification	Authenticate identity documents across thousands of document types globally through optical character recognition and security feature analysis, detecting fraudulent or manipulated credentials with high accuracy.
Fraud Scoring and Decisioning	Use fraud-scoring models as synthesizers of upstream signals rather than stand-alone decision makers, combining identity data, behavioral indicators, device signals, and consortium intelligence into risk scores that drive final disposition.
Consortium Participation and	Participate in real-time fraud intelligence networks to flag coordinated activity across institutions through velocity checks on SSN, device

Best Practice	Description
Velocity Intelligence	identifiers, and internet protocol (IP) addresses, catching synthetic and third-party fraud attempts within minutes of detection.
Continuous Model Retraining	Deploy vendors that update fraud-detection models on a weekly or monthly cadence based on tagged fraud data across their entire client network, ensuring that novel attack patterns enabled by AI are captured and blocked before they become widespread.
Progressive Authentication	Identity verification and authentication should continue beyond account opening. Institutions can use lower-friction verification when risk is low, then step up assurance when a customer enters a branch, requests a higher-risk service, or reaches another consequential moment of trust.
Cross-Channel Fraud Intelligence	Link digital onboarding signals to post-approval transaction monitoring and account behavior, identifying accounts that passed initial screening but exhibit suspicious patterns after funding, catching first-party fraud and account-takeover attempts.

Source: Datos Insights

For community banks and credit unions, implementing all eight practices simultaneously may exceed budget and resource constraints, but prioritizing the capabilities most relevant to institutional risk profile, deposit product mix, and existing technology infrastructure remains essential. A community bank with significant branch presence can lean into biometric and document verification, using in-person identity assurance as a competitive differentiator. A fintech firm or digital lender must prioritize behavioral analytics and consortium participation to compensate for the absence of face-to-face verification.

Partnering as a Strategy

Generally, Tier-2 and Tier-3 FIs cannot build comprehensive identity-verification and fraud-detection capabilities independently. The infrastructure required, the ongoing model retraining on fraud patterns, the consortium participation, and the continuous adaptation to emerging threats all demand scale and specialization that community banks and credit unions often don't have. Strategic partnerships solve this resource constraint by embedding advanced fraud-detection capabilities into existing FI workflows without requiring large internal technology investments.

The most effective partnerships operate at the infrastructure layer, not as a point-solution integration. A partnership with a core processor or orchestration platform provider enables

identity verification, full authentication, and fraud detection to integrate seamlessly with deposit account opening, loan origination, and AML monitoring workflows that FIs already rely on daily. This approach reduces implementation complexity to accelerate time to value and ensure that fraud detection remains current as vendors update their models and tactics.

The partner landscape for smaller FIs differs significantly from larger banks. Tier-1 FIs embed multiple specialized vendors across identity verification, behavioral biometrics, and consortium intelligence, then orchestrate those signals internally. Community banks and credit unions benefit more from partners who curate and integrate multiple fraud-prevention capabilities into a single-entry point, minimizing the number of vendor relationships and integration projects.

Core processors, payment networks, and orchestration platforms that already connect to FI systems are natural starting points for embedding identity verification and fraud detection. Companies that operate through a partner ecosystem that includes core providers, like Fiserv, and technology partners, like Alloy, enable community banks and credit unions to access advanced identity assurance without building custom integrations or managing separate vendor contracts.

Measuring Success

Establishing performance baselines before deploying any identity-verification or fraud-detection solution is as important as solution selection itself. Without documented baselines, it is impossible to isolate the effect of a new capability from underlying fraud trend changes. Before implementation, FIs should measure and record their current fraud-catch rate, false-positive rate, and application-abandonment rate at each step of the onboarding process, along with the fraud analyst queue volume. These baselines reveal the starting point and enable meaningful post-implementation comparisons. FIs should also document approval rates, decline rates, and step-up frequencies, because a solution that reduces fraud losses while increasing customer friction can damage overall profitability.

Post-implementation measurements should track four distinct dimensions simultaneously: detection performance, financial impact, operational efficiency, and customer experience. Quarterly reviews should compare current performance against baseline across all four dimensions, identifying which metrics are moving positively and where tradeoffs are emerging. If fraud-catch rates improve but abandonment rates increase significantly, the

solution may be over-aggressive. If operational efficiency improves but fraud losses remain excessive, you may need to review and adjust the risk level of applications going to review.

The Business Case for Change

The case for strengthening identity verification extends beyond compliance obligation and fraud loss mitigation. A regulatory enforcement action for identity-related failures can easily exceed the multiyear cost of implementing robust identity-verification controls, making the business case particularly acute for smaller FIs that cannot absorb large fines the way enterprise banks can.

The financial argument runs deeper than avoiding enforcement risk. Fraud prevention, when measured correctly, generates return on investment through multiple channels: direct fraud loss reduction, significant operational efficiency gains from reduced manual review and faster case closure, and revenue protection through lower false-positive rates and customer abandonment. FIs that close the identity trust gap gain both compliance advantages and competitive differentiation, because physical and forensic identity verification creates a defensible market position against digital-only competitors and builds customer trust.

Financial Impact

The scale of identity-related fraud and the regulatory response create an urgent financial case for Tier-2 and Tier-3 FIs to strengthen identity-verification controls. The business case for change operates across multiple dimensions, each with measurable financial impact as demonstrated in Table C.

Table C: Business Case Framework

Component	Financial Impact
Regulatory Enforcement Avoidance	Single identity-related enforcement actions can cost several million dollars for midsize FIs; multiyear cost of robust identity-verification systems can range from US\$500K to US\$2M annually for smaller FIs.
Direct Fraud Loss Reduction	FIs implementing advanced identity verification report a reduction in application-stage fraud losses.
Operational Efficiency (Analyst Resources)	Reduced false positives can lower the manual review queue by 20% to 40%, which eliminates the need for additional analyst headcount and frees existing staff for higher-value investigations.

Component	Financial Impact
Customer Experience and Revenue Protection	False-positive rates carry hidden revenue cost through application abandonment; reducing false positives through better identity verification recovers lost approvals.
Post-Approval Monitoring Integration	Early detection of account-takeover and first-party fraud through linked onboarding and transaction signals reduces downstream losses and accelerates case closure.
Competitive Differentiation	Tier-2 and Tier-3 FIs leveraging in-branch identity assurance as a market differentiator can attract compliance-conscious customers and enjoy measurable brand value in high-fraud geographies.

Source: Datos Insights

The business case is not just a choice between fraud prevention, customer experience, and cost control. It is an imperative driven by three converging forces: the cost and reputation damage of enforcement actions, the measurable operational efficiency gains from reduced false positives and faster case closure, and the competitive advantage that comes from offering customers a more trustworthy account opening experience.

Balancing Fraud and Friction

Every additional identity-verification step increases the abandonment risk, particularly in mobile environments where customer patience is thinner. Banks that implement aggressive fraud detection may successfully reduce fraud losses while inadvertently routing legitimate applicants to competitors offering faster, simpler account opening. The hidden cost lies in false positives, the incorrect flagging of legitimate applicants for review.

The solution is risk-based step-up authentication, which applies additional verification scrutiny only to applications where fraud signals warrant increased inspection or where there are increased consequences. Rather than subjecting all applicants to facial biometrics and full document authentication, a risk-based approach uses initial signals to segment applicants into risk tiers. Low-risk applicants with strong identity matching, established credit history, and minimal behavioral anomalies move through account opening with minimal friction. High-risk applicants with synthetic-identity indicators, device spoofing signals, or velocity red flags receive additional verification steps and manual review. This tiered approach preserves customer experience for the majority while focusing analyst resources and advanced verification controls on applications where fraud risk and potential consequences justify the friction.

Building Trust: The Path Forward

The identity trust gap is an active regulatory liability enforced through consent orders and intensifying compliance scrutiny. For Tier-2/3 FIs, closing this gap has become an imperative driven by regulatory tension, fraud loss pressures, and competitive opportunity.

Institutions should act now and consider the following key recommendations:

- **Establish a current-state baseline before deploying any new capability.** Document fraud-catch rates, false-positive rates, application-abandonment rates, analyst queue volume, approval rates, and decline rates to create a reference point.
- **Prioritize identity-verification and full-authentication capabilities aligned with your specific risk profile and product mix.** You do not need to implement all best practices simultaneously; instead, assess which capabilities address your highest-risk fraud vectors and which partnerships enable you to access advanced detection.
- **Embed identity verification and full authentication into your core processing or orchestration layer, not as a stand-alone point solution.** Partnerships with core processors, payment networks, and orchestration platforms that already connect to your systems reduce complexity and accelerate time to value.
- **Use your physical presence and in-branch capability as a competitive differentiator.** Use facial biometrics and document authentication in-branch for high-risk applicants and new account openings to create a defensible market position.
- **Combine identity data verification with credential authentication, person-to-document matching, and relevant fraud signals.** Orchestrate those components across onboarding and subsequent higher-risk moments throughout the customer life cycle.
- **Develop a vendor evaluation framework that prioritizes continuous model retraining and emerging threat adaptation.** Require vendors to document their cadence for updating fraud-detection models and their approach to detecting AI-enabled threats.

The regulatory environment will continue to tighten, and the threat landscape will continue to evolve, making identity verification and full authentication an ongoing strategic priority rather than a one-time implementation project. Taking proactive action will not only reduce regulatory exposure and fraud losses but will also establish persistent competitive advantages.

Methodology

This report synthesizes existing Datos Insights proprietary research, secondary source materials, and publicly available regulatory information to examine identity-verification practices and fraud trends across U.S. FIs with a particular focus on Tier-2 and Tier-3 banks and credit unions. The analysis draws on:

- Datos survey research conducted in Q1 2025 measuring identity confidence practices and fraud threat perception among 73 U.S. financial institutions
- Regulatory enforcement actions published by the FDIC, OCC, and Federal Reserve, as well as publicly reported fraud trends and identity-related suspicious-activity filings
- Best practices and recommendations are derived from industry standards, established fraud-prevention frameworks, and Datos Insights' advisory work with financial services organizations across multiple segments

The report applies existing research findings and regulatory trends to the Tier-2/3 specific market segment and contextualizes them against the resource constraints and competitive dynamics unique to community banks and credit unions.

About Datos Insights

Datos Insights is the leading research and advisory partner to the banking, insurance, securities, and payments industries—both the financial services firms and the technology providers that serve them.

In an era of rapid change, we empower firms across the financial services ecosystem to make high-stakes decisions with confidence and speed. Our distinctive combination of proprietary data, analytics, and deep practitioner expertise provides actionable insights that enable clients to accelerate critical initiatives, inspire decisive action, and de-risk strategic investments to achieve faster, bolder transformation.

Contact

Research, consulting, and events:

sales@datos-insights.com

Press inquiries:

pr@datos-insights.com

All other inquiries:

info@datos-insights.com

Global headquarters:

6 Liberty Square #2779

Boston, MA 02109

www.datos-insights.com

Author information

Jim Mortensen

jmortensen@datos-insights.com

© 2026 Datos Insights or its affiliates. All rights reserved. This publication may not be reproduced or distributed in any form without Datos Insights' prior written permission. It consists of information collected by and the opinions of Datos Insights' research organization, which should not be construed as statements of fact. While we endeavor to provide the most accurate information, Datos Insights' recommendations are advisory only, and we disclaim all warranties as to the accuracy, completeness, adequacy, or fitness of such information. Datos Insights does not provide legal or investment advice, and its research should not be construed or used as such. Your access and use of this publication are further governed by Datos Insights' Terms of Use.

AI Usage Restrictions: This publication may not be uploaded or otherwise provided to publicly accessible AI systems (including LLMs) such as ChatGPT, Claude, Gemini, or similar where such content may be used for model training or may become accessible to other users.