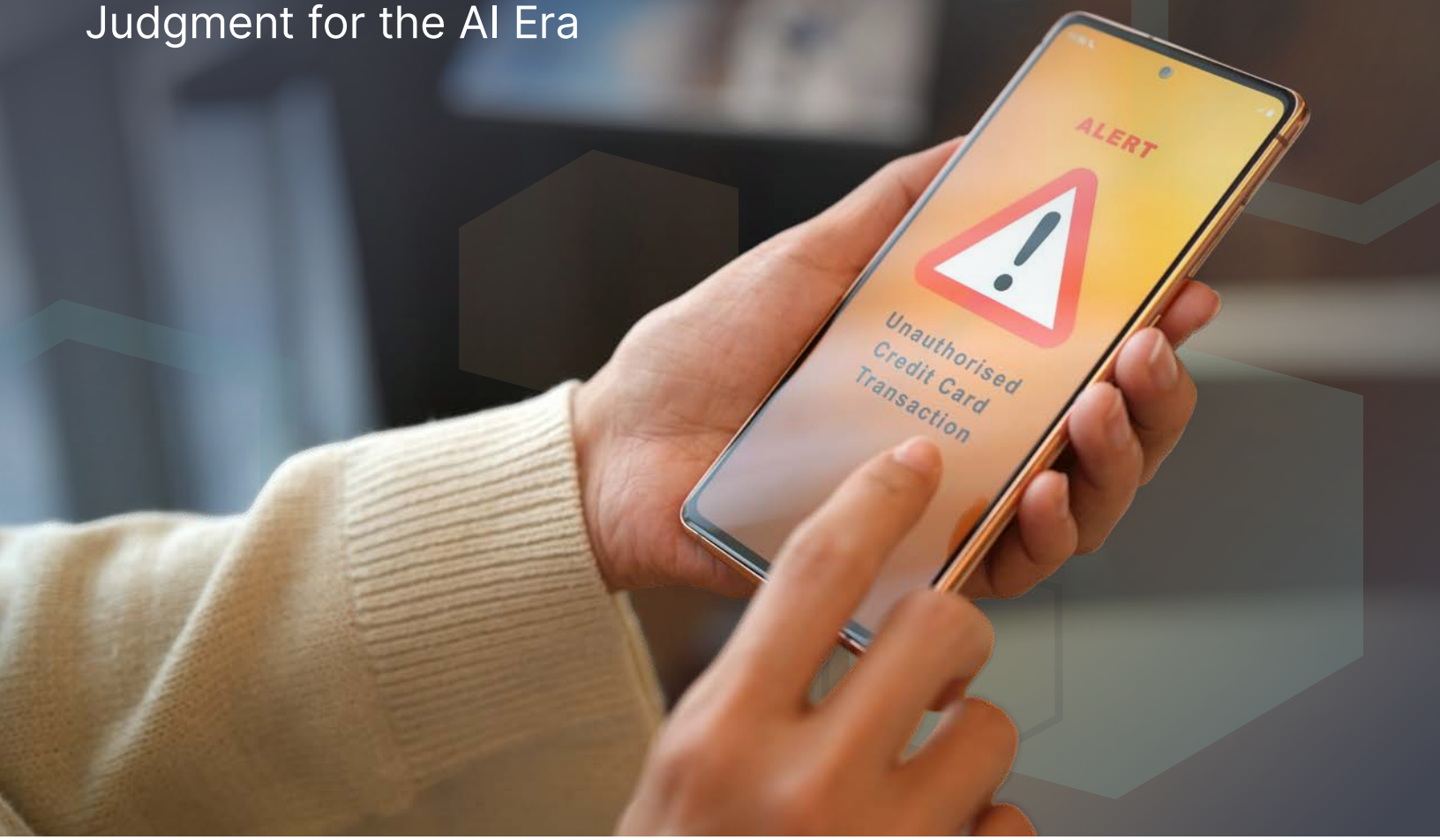
FUTURE BRANCHES
INSIGHTS

Fraud Protection at the Front Line of Banking

How Banks and Credit Unions Are Integrating Identity, Data, Technology, and Human Judgment for the AI Era



Sponsored by veridocs

Table of Contents

2 Executive Summary

3 About the Respondents

3 Key Insights

5 Fraud Defense Spans Multiple Systems

7 AI Threats Are Testing Confidence in Institutions' Fraud Protection

9 Legacy Systems and Data Silos May Limit New Fraud Investments

10 Identity Verification Creates Friction Across Channels

12 Leaders Say Frontline Teams Add Context to Fraud Decisions

14 Conclusion: Successful Fraud Defense Depends on Connected Decision-Making

14 Key Suggestions

15 About the Author

15 About Our Sponsor



Executive Summary

Fraud protection in retail banking now extends across branches, contact centers, digital channels, payment systems, and third-party platforms. Banks and credit unions must detect increasingly convincing identity and impersonation threats while giving legitimate customers and members timely service.

This study examines how 100 banking leaders build or buy fraud-prevention capabilities, prepare for AI-enabled attacks, set investment priorities, and verify identities during higher-risk branch interactions.

The findings show broad use of fraud technology, but limited confidence in detecting AI-generated fraud. They also point to persistent data and core-system barriers, along with customer friction during identity checks. This report examines which controls leaders consider effective, which threats concern them most, and where operational changes could improve fraud detection and response.

About the Respondents

Institution Type:

- **20%** Global Banks
- **18%** National Banks
- **21%** Regional Banks
- **21%** Community Banks
- **20%** Credit Unions

Seniority:

- **25%** C-Suite
- **25%** Vice President
- **24%** Department Head
- **26%** Director

All participating institutions have at least **$750 million** in assets

of those, 38% have **$10 billion** or more

Role:

Fraud | Security | Retail Operations | Compliance

Key Insights

43% primarily use a combination of in-house and third-party fraud capabilities, while 39% rely mainly on third-party vendors.

49% rate behavioral biometrics as very effective, the highest result among the technologies tested.

75% are only somewhat confident in detecting AI-generated fraud, while 18% have low or no confidence.

61% identify real-time payments fraud monitoring as a top investment priority.

56% cite data silos and 54% cite legacy-system limitations as internal barriers.

58% identify synthetic identity fraud as one of their most difficult or concerning external threats.

63% say identity verification creates significant friction during in-person branch interactions.

veridocs



This ID looks perfect.

To digital verification tools.

75% of institutions rely on them for higher-risk in-person transactions

40% lean on barcode scans. They read what's printed, not whether it's real.

> "Employee knowledge alone is no longer adequate
>
> A fraud leader in this report, on preparing frontline staff for AI-enabled fraud

Fake IDs are getting better. Most branch checks aren't.

How we close this gap

A trained eye can't see a forged security feature. Veridocs authenticates the ID itself, against counterfeits seized in live environments.

A clear pass or fail, in seconds. Right at the teller line, without adding wait time.

Verify once. One auditable record your branches, back office and fraud team all see, instead of checking again at every step.

- 20+ years authenticating IDs
- Proven in 450+ financial institutions and casinos
- Largest and fastest updating commercial document fraud library

INVESTAR BANK · switch · PENN ENTERTAINMENT · Resorts World · FRAUD FIGHTER · MGM GRAND · FONTAINEBLEAU

See it at Future Branches
Austin, Dec 1–3

Book a time with us:
https://www.veridocs.com/request-a-demo

Fraud Defense Spans Multiple Systems

Most institutions combine internal capabilities with outside technology, making system integration and cross-channel data access central to their fraud programs.

Forty-three percent primarily use a combination of in-house tools and third-party vendor solutions, while 39% rely mainly on outside providers. Only 11% build primarily in-house, and 7% are evaluating a change in strategy. Because 82% use either a hybrid or mainly vendor-led model, vendor integration and access to fraud data are central operating concerns.

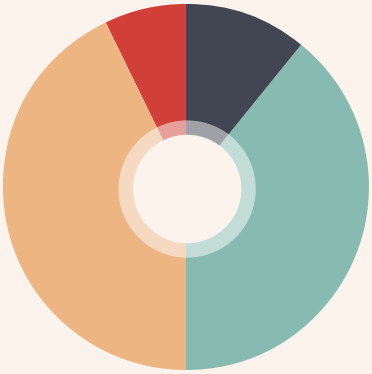
Respondents gave behavioral biometrics the highest "very effective" rating at 49%. Multi-factor and passwordless authentication followed at 42%. Views of digital identity verification and physical biometrics were more measured: 57% and 54%, respectively, called them somewhat effective, while 29% and 28% rated them very effective.

Multi-factor and passwordless authentication had the strongest combined effectiveness score at 89%. AI-driven real-time monitoring reached 85%, although only 20% rated it very effective.

The results show a distinction between technologies viewed as broadly effective and those that earn strong confidence. AI-driven monitoring illustrates that difference: 85% rate it at least somewhat effective, but only 20% call it very effective.



How does your institution primarily source its fraud detection and prevention capabilities?



- **11%** Built primarily in-house
- **39%** Primarily third-party vendor solutions
- **43%** A hybrid of in-house tools and third-party vendor solutions
- **7%** Currently evaluating a shift in strategy (build vs. buy)

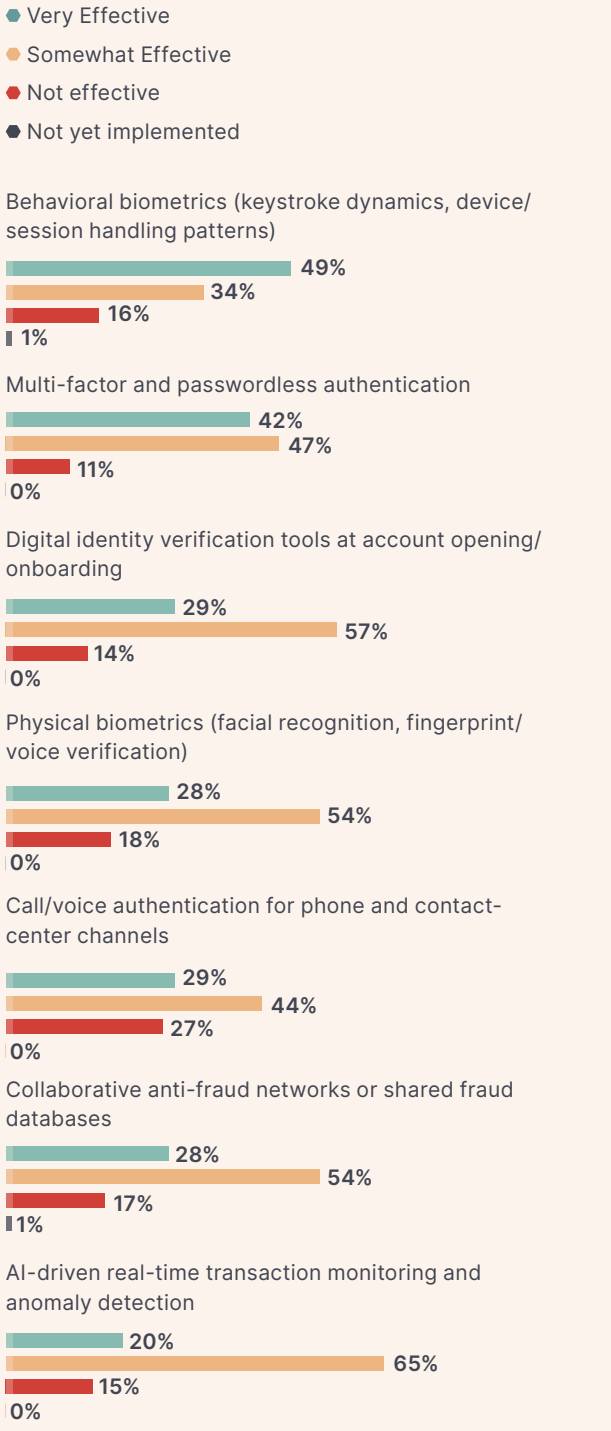
Practitioner Perspectives: **Coordinating Systems for Fraud Protection**

Practitioners at Future Branches Boston 2026 suggested that fraud protection efforts cannot remain divided among separate branches or departments. Prevention efforts should be coordinated across lending, deposit operations, card services, digital banking, and other departments.

A vice president overseeing BSA and fraud at a credit union described replacing long email chains with centralized CRM workflows. Once a fraud alert is opened, the CRM would assign tasks across the institution. The same institution uses separate tactical and strategic working groups to address active cases, process improvements, and longer-term priorities.

A director of fraud analytics at a different credit union discussed the importance of combining identity signals like device data, identity markers, behavioral analysis, and transaction records rather than assessing them separately. Fraud teams should also participate when institutions introduce or change products and services.

How effective are the following fraud prevention technologies at your institution today?

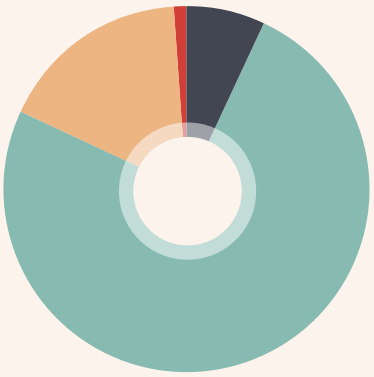


AI Threats Are Testing Confidence in Institutions' Fraud Protection

AI-generated media and synthetic identities have made familiar identity credentials less conclusive. Most respondents reported some readiness, but few expressed strong confidence in their institutions' ability to identify newer forms of impersonation.

Only 7% are very confident that their institution can detect deepfake video or audio, voice cloning, synthetic identities, and related tactics. Seventy-five percent are somewhat confident, while 18% are not very confident or not confident at all. Those clustered in the latter two categories remain uncertain about how well their institutions would detect more advanced attacks.

How confident is your institution in its ability to detect AI-generated fraud tactics, such as deep-fake video/audio, voice cloning, and synthetic identities?



- 7% Very confident
- 75% Somewhat confident
- 17% Not very confident
- 1% Not confident at all

Since you indicated your institution is not very confident or not confident at all in detecting AI-generated fraud, which one of the following is the most significant problem affecting your AI security capabilities?

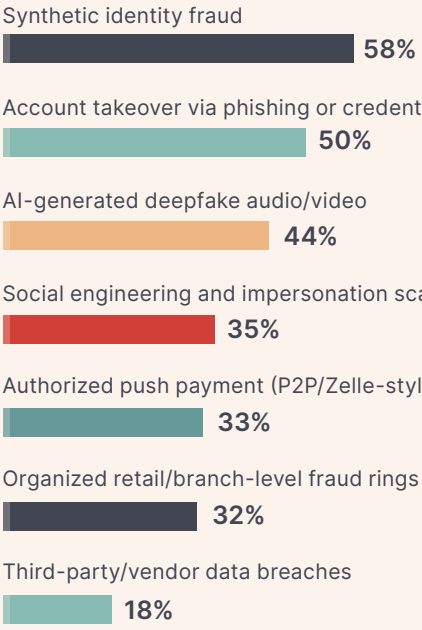


Among the 18 respondents with low or no confidence, 39% identified insufficient internal expertise as the main problem. Another 22% said fraud tactics are evolving faster than their defenses, and 22% cited a lack of leadership prioritization. The response base is limited to 18 leaders, but their answers identify internal expertise and leadership priorities as prominent sources of low confidence.

Synthetic identity fraud led the list of difficult or concerning external threats at 58%. Account takeover through phishing or credential theft followed at 50%, while 44% selected AI-generated deepfake audio or video. Social engineering and impersonation scams reached 35%, authorized push payment fraud reached 33%, and organized branch-level fraud rings reached 32%.

Each of the three leading threats can exploit apparently credible identity information or familiar customer behavior. Institutions will need to assess behavior, device data, documentation, and transaction history together when determining whether an interaction is legitimate.

Which 1–3 of the following external fraud tactics are creating the most difficulty for your institution right now (or, which are you most concerned about)?



Practitioner Perspectives: **Types of AI-Enhanced Threats**

With AI, criminals have more opportunities to fabricate identities based on real information. An assistant vice president of fraud prevention at a community bank explained at Future Branches Boston 2026 that fraudsters can use legitimate Social Security numbers and birth dates alongside false documents, such as:

- Bank statements
- Utility bills
- Driver's licenses and ID cards
- Lease and rental agreements
- Pay stubs and W-2 forms
- Business-formation and ownership documents

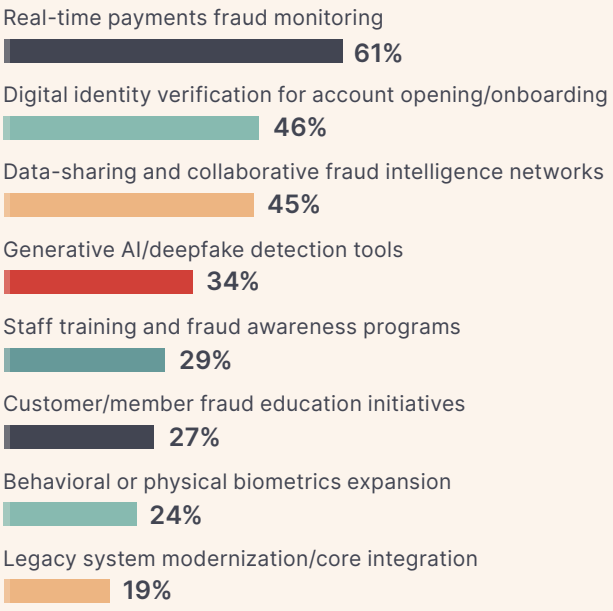
With multiple documents, bad actors can create credible synthetic profiles. Static personal information is therefore becoming less reliable as proof of identity.

A director of fraud analytics at a credit union added that criminals are using many of the same AI tools that financial institutions are deploying. Banks and credit unions can't rely solely on submitted credentials to verify identity. They must examine IP addresses, devices, locations, behavior, and ongoing transaction activity for signs that a seemingly legitimate identity has been manufactured or compromised.

Legacy Systems and Data Silos May Limit New Fraud Investments

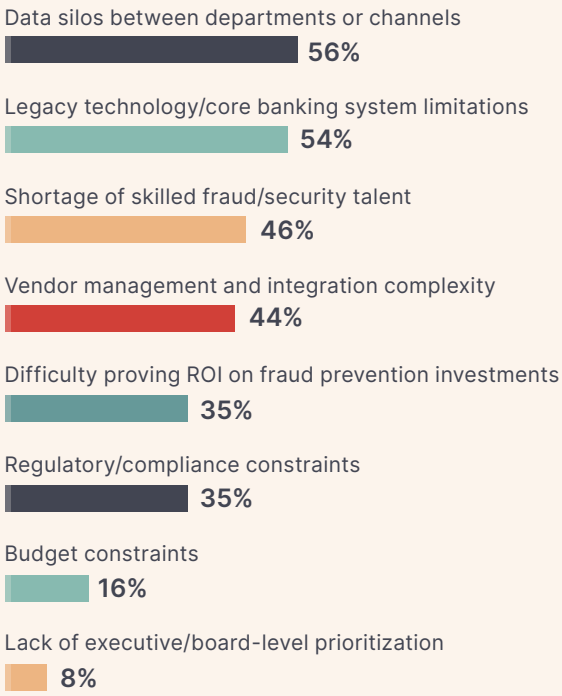
Banks and credit unions are directing their fraud investments toward earlier detection and stronger identity decisions. The value of those investments will depend partly on whether institutions can address the data and system problems that restrict their current fraud programs.

Which 1–3 of the following fraud prevention investments are the top priorities for your institution over the next 12 months?



Real-time payments fraud monitoring is a top priority for 61% of respondents. Digital identity verification for account opening follows at 46%, while 45% prioritize data-sharing and collaborative fraud intelligence networks. Generative AI and deepfake detection tools rank fourth at 34%, followed by staff training at 29%, customer or member education at 27%, biometrics expansion at 24%, and legacy modernization at 19%.

Which of the following are internal barriers your institution has faced in its efforts to improve fraud prevention?



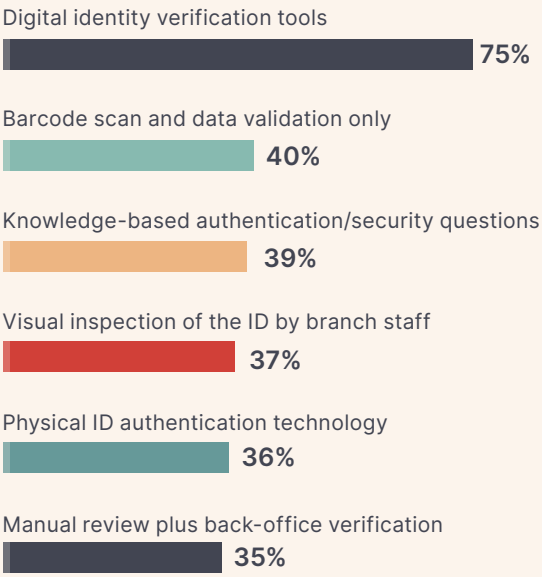
Data silos between departments or channels are an internal barrier for 56% of respondents, and 54% cite limitations in legacy technology or core banking systems. Talent shortages affect 46%, while 44% report vendor-management and integration complexity. Regulatory constraints and difficulty proving ROI each reach 35%.

Only 19% rank legacy modernization among their top investments, even though 54% identify legacy limitations as a barrier. This difference suggests that many institutions are favoring targeted fraud tools that can produce nearer-term results. Without broader data access and core integration, institutions may struggle to apply those tools consistently across channels.

Identity Verification Creates Friction Across Channels

Higher-risk branch transactions often require employees to use several verification methods. The survey shows strong use of digital identity tools, along with repeated checks and reviews that can slow legitimate interactions.

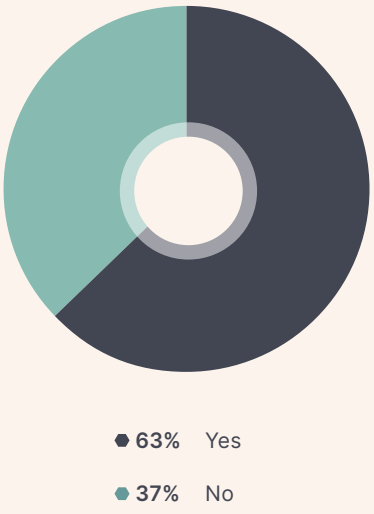
How are branch employees primarily verifying a customer's identity during higher-risk in-person transactions today?



Digital identity verification tools are used by 75% of institutions during higher-risk in-person transactions. Forty percent selected "barcode scan and data validation only." Knowledge-based authentication follows at 39%, while 37% use visual ID inspection, 36% use physical ID authentication technology, and 35% use manual review plus back-office verification.

Multiple verification methods can strengthen protection, but disconnected tools may require employees to repeat work or reconcile conflicting results.

Is identity verification a significant source of friction during in-person branch interactions?



Sixty-three percent identify identity verification as a significant source of friction during in-person branch interactions.

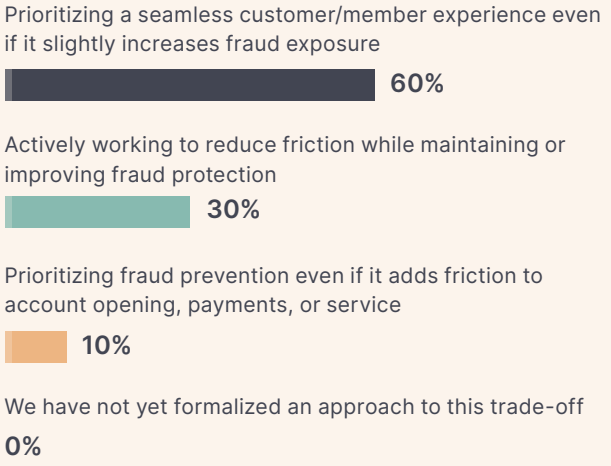
Among those 63 respondents, 67% cite repeated verification across channels as a source of friction. Transaction holds and secondary reviews affect 49%, while 46% point to multi-factor authentication requirements. Repeated verification also reflects the cross-channel data silos identified elsewhere in the study.

Since you said Yes, which aspects of identity verification create the most customer friction during in-person branch interactions?



Sixty percent prioritize a smooth customer or member experience even when doing so slightly increases fraud exposure. Another 30% are working to reduce friction while maintaining or improving protection, and 10% prioritize prevention even when it adds friction. Sharing completed identity checks and risk signals across channels could reduce repetition while preserving added review for higher-risk activity.

How is your institution balancing stronger fraud controls with customer/member experience?



Practitioner Perspectives: **Security's Impact on Customer and Member Experiences**

At Future Branches Boston 2026, practitioners cautioned against subjecting every applicant or account holder to the same verification process.

A senior vice president of member experience at a credit union described using risk signals to vary onboarding requirements. Branches could allow lower-risk applications to proceed with fewer manual steps while reserving added scrutiny for cases with warning signs. A director of fraud analytics at another credit union framed the challenge in terms of context and personalization:

"You want the experience to be easier and more seamless for legitimate applicants and members, but more difficult for the fraudsters. We must continue to evolve with the AI-driven tools and supports available, including systems like biometrics."

Leaders Say Frontline Teams Add Context to Fraud Decisions

Respondents described how their institutions are preparing branch and contact-center employees for AI-enabled fraud. Four themes appeared throughout their answers.

Realistic Exercises Reinforce Fraud Awareness

Many institutions are using realistic exercises in addition to standard awareness training. Scenarios now cover voice cloning, deepfakes, synthetic identities, and social engineering so employees can practice responding under pressure. Role-playing also prepares staff to handle customers who resist added verification.

Recognition is only part of the employee's job. Staff must also decide when to ask another question, pause an activity, or seek help while the interaction is underway.

"By employing realistic deepfake, voice cloning, and social engineering scenarios in frontline exercises, we are going beyond conventional awareness training."

Department Head, Fraud Protection, Regional Bank

"In order to practice spotting questionable client interactions, frontline personnel are given real-world scenarios."

Vice President, Fraud Prevention, Community Bank

"Deepfakes, voice cloning, and more recent impersonation techniques are being covered in regular fraud training."

Vice President, BSA/AML Compliance, Community Bank

"Use realistic fraud examples and role-playing exercises to give employees hands-on practice in spotting suspicious situations and deciding how they should respond."

Director, Fraud Analyst, National Bank

Customer Behavior Adds Context to Identity Verification

Frontline teams are being taught to consider more than credentials and security questions. Changes in communication style, account activity, transaction purpose, or customer behavior may reveal risk when documents and personal details appear credible. Several respondents also emphasized patterns that extend across more than one channel or interaction.

This expands the frontline employee's role in fraud detection. Staff need enough customer and transaction context to judge whether the interaction is consistent with prior behavior, especially when a fraudster possesses genuine personal information.

"Teams from branches and contact centers are being trained to treat unusual behavior as an additional risk signal instead of depending only on passwords or static identity checks."

Vice President, Fraud Analyst, Community Bank

"Training also highlights the importance of noticing changes in a customer's usual communication style, particularly when those changes occur alongside unusual requests."

C-Suite Executive, Fraud Operations, Regional Bank

"We encourage colleagues to consider the complete customer journey rather than evaluating an individual transaction or conversation in isolation."

Director, Fraud Protection, National Bank

"More attention is being placed on whether documents, explanations, and transaction purposes are consistent with one another."

Director, Fraud Protection, National Bank

Employees Need More Authority to Pause and Verify Activity

Respondents repeatedly mentioned pausing, verifying, and escalating suspicious activity. This sequence gives staff a practical response when the available evidence is unclear. It can also help them resist urgency, pressure, or requests to bypass normal procedures.

Employees in branches and contact centers need clear authority to pause an interaction, even when doing so may delay a legitimate customer. Defined escalation channels can move difficult cases to fraud specialists before an employee approves a high-risk request.

"The main message provided is simple. Pause if something seems wrong, verify before acting, and escalate if the risk is unclear."

Director, Fraud Protection, National Bank

"We let our employees pause transactions when further verification is needed."

C-Suite Executive, IT Security, Community Bank

"Managers emphasize the importance of taking a pause, particularly when someone is pushing for an exception to normal procedures."

Vice President, Retail Operations, Community Bank

"We are bolstering our escalation protocols so that staff members are aware of when to send a questionable conversation to fraud experts."

Vice President, BSA/AML Compliance, Regional Bank

Technology Supports Frontline Judgment

Respondents described technology as a source of decision support for frontline staff. Real-time alerts, behavioral analytics, identity assurance, device intelligence, and transaction risk assessments can give employees more evidence during an interaction. Staff can act on these signals faster when they appear within existing workflows.

Employees still need to interpret warnings when signals conflict or a legitimate customer behaves unexpectedly. Institutions are pairing stronger monitoring with staff education so employees can evaluate alerts and choose the appropriate response.

"We are combining frontline procedures with real-time fraud intelligence so staff may receive risk warnings while the client engagement is still taking place."

C-Suite Executive, Fraud Operations, National Bank

"Technology supports employees through alerts and monitoring, while human judgment remains important."

C-Suite Executive, IT Security, Credit Union

"The emphasis is moving toward layered controls, where automated detection, device intelligence, and transaction-level risk assessment assist frontline judgment."

Vice President, Fraud Analyst, Regional Bank

"Because employee knowledge alone is no longer adequate, our strategy incorporates behavioral analytics, enhanced identity assurance, and staff training."

Department Head, Fraud Protection, Global Bank

Conclusion: Successful Fraud Defense Depends on Connected Decision-Making

Most institutions rely on several internal and external fraud capabilities. Respondents see value in biometrics, authentication, identity verification, shared intelligence, and transaction monitoring. Even so, few are highly confident in their ability to detect AI-generated fraud, and synthetic identities, account takeover, and deepfakes rank among their most difficult threats.

Banks and credit unions will need to connect identity, transaction, behavioral, and cross-channel data so staff and systems can make consistent decisions during an interaction. Realistic training and clear escalation procedures will also help frontline teams act on that information without forcing every legitimate customer through the same level of scrutiny.

Key Suggestions

1. **Connect fraud data across departments and channels before adding isolated controls.** Shared customer, identity, device, and transaction signals can reduce blind spots and repeated verification.

2. **Require vendors to demonstrate integration, data access, and performance against AI-enabled threats.** Institutions need access to fraud data throughout the detection, investigation, and response process.

3. **Redesign higher-risk branch verification around reusable, risk-based decisions.** Start by reducing repeated cross-channel checks, avoidable transaction holds, and unnecessary authentication steps.

4. **Train frontline teams with realistic fraud scenarios, and give them greater authority and clear escalation paths.** Training should cover deepfakes, synthetic identities, social engineering, and coercion.

About the Author

FUTURE BRANCHES INSIGHTS

Generating Demand with Visibility, Engagement & Trust

Future Branches Insights is the 365-day demand-generation partner for solution providers in the retail banking and branch transformation market. Powered by WBR's banking event portfolio and a proprietary database of 25,000 verified decision-makers, Future Branches Insights connects solution providers with senior financial services leaders responsible for branch banking and customer experience.

Our data-driven research reports, webinars, and targeted campaigns are based on verified buyer intelligence. They help brands remain visible and relevant to decision-makers throughout the buying process.

For more information, please visit **futurebranches.wbresearch.com**

About Our Sponsor

veridocs

Veridocs is an identity verification platform built for high-consequence, in-person decisions. It combines physical ID authentication, person verification, and screening within a single workflow, helping organizations confirm a person's identity before granting access or approving a transaction.

For more information, please visit **www.veridocs.com.**