TransUnion

The Authentication Gap: Why Fraud Is Penetrating Your Call Center

A practical guide to risk-based decisioning for fraud, interactive voice response and call center strategists.

Contents

TransUnion

Rising call center fraud demands a new approach to authentication

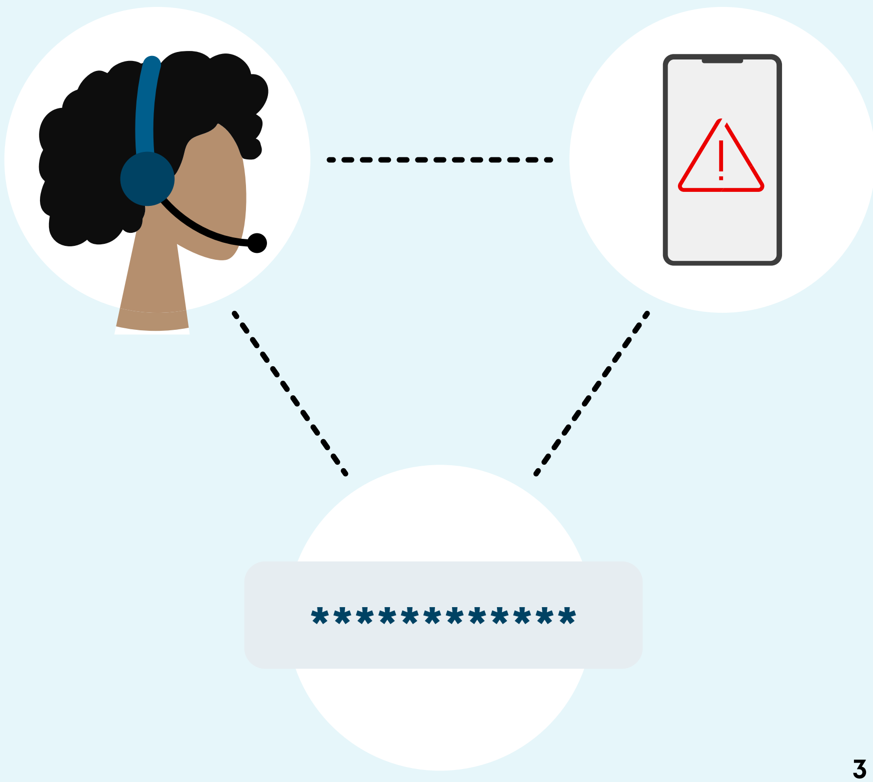
Fraud managers see rising losses. Call center managers see average handle times increasing. What both teams are discovering is they're looking at the same problem from different angles: There's a gap in caller authentication that fails to stop fraud and drives up costs.

Something has to change. According to TransUnion's 2025 research, 64% of US business leaders said fraudsters increased their call center attacks year over year — a 50% jump from the previous year.[1] Account takeovers were the leading cause of fraud loss cited by companies.[2] It's the fraud type most enabled through the call center and it's only getting worse. Javelin Research reports cybercriminals engaging in account takeover fraud schemes caused over $15 billion in consumer losses in 2025.[3]

This guide is designed to help fraud, interactive voice response (IVR) and call center strategists collaborate to combat fraud attacks and reduce call handling time by making the shift from knowledge-based authentication to a risk-based call authentication model. The benefits of switching are significant: Organizations could realize 181% in potential return on investment, according to a Forrester Total Economic Impact™ study, commissioned by TransUnion® in January 2025.

64% Increase in reported call center attacks, 2024–2025

Source: TransUnion, H2 2025 Update: Top Fraud Trends



Fraudsters are passing your call center verification

Fraudsters can make any call appear to come from a legitimate customer, giving them instant credibility before anyone picks up. In 2025, 83% of US business leaders reported more spoofing activity to impersonate consumers than the year before.[4] Increasingly, fraudsters are using compromised identity and learned knowledge of your systems to pass authentication — opening the door to ATO without you recognizing it.

Hiding behind legitimate mobile numbers

No longer relying solely on non-fixed VoIP masking, fraudsters are shifting tactics to exploit trusted mobile phones on your customer file — through port-outs, reassignment, SIM swapping or spoofing. While VoIP calls accounted for just 3.7% of US call center volume in 2025, 69% were flagged as high risk — a slight 1% increase over 2024.[5] However, the bigger shift was toward mobile: 87% of call center volume came from mobile phones in 2025, with high-risk mobile calls jumping 41% year over year.[6]

Using compromised identity data to social engineer agents

By the time a fraudster reaches an agent, they know account details, answers to challenge questions and how to apply social engineering pressure to get what they need. And with more fraudsters using AI to coach them in real time, that pressure is getting harder to detect.

Mapping your IVR to automate attacks

Bad actors use bots to silently map your IVR's decision tree, testing account numbers, checking balance ranges and identifying information needed to pass a live authentication challenge.

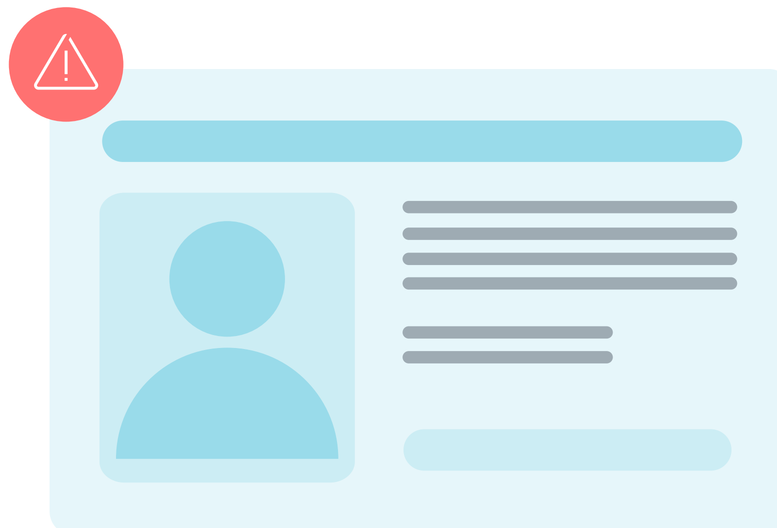
Knowledge-based authentication is no longer secure

Knowledge-based authentication (KBA) assumes the person who knows the answers to specific challenge questions is the legitimate customer. That assumption is no longer valid.

In 2025, full Social Security numbers were exposed in 78% of US data breaches, while checking and savings account numbers appeared in 38%.[7] More than half (59%) of US business leaders cited an increase in the use of stolen personal information to pass KBA challenges in 2025.[8]

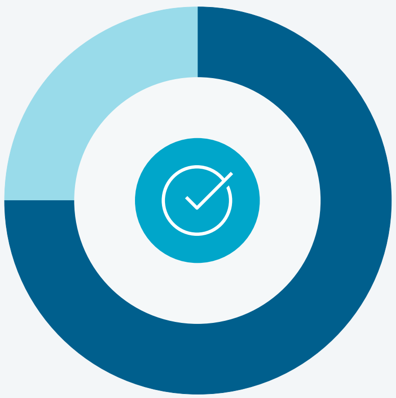
47% increase of US data breach volume 2025 compared to 2024

Source: TransUnion, H1 2026 Update: Top Fraud Trends



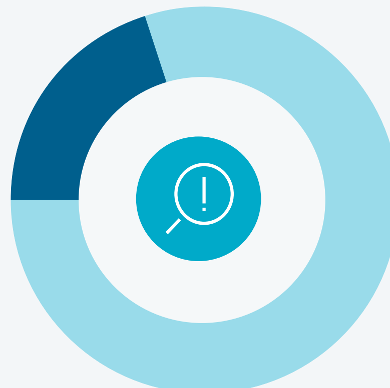
Reduce fraud with risk-based call authentication

Overall, 47% of US businesses say they'd prefer to authenticate callers before calls are even answered.[9] Applied to inbound volume, a pre-answer risk-based authentication — one that assesses the validity of the device, phone number, network and individual from which a call originates — creates three risk populations to help you reduce friction for legitimate callers while applying maximum effort to stop fraud attacks.



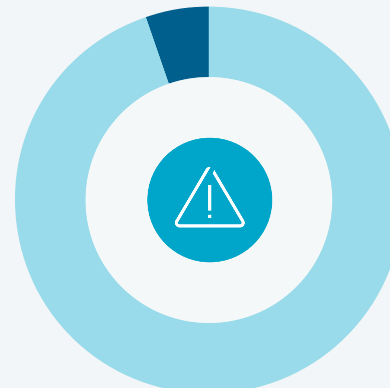
High-trust (75% of calls)

Device, number and call signals are consistent with legitimate customers. These callers move through with minimal friction, more self-service options and agents who already know the call has been screened.



Mid-risk (20% of calls)

Signals are ambiguous and require a targeted step-up challenge — one question, not five.



High-risk (5% of calls)

Meaningful fraud signals route these callers to fraud specialists before any account action is permitted.

This approach reduces unnecessary authentication while concentrating effort where it matters most. And because risk is assessed before the call is answered, trusted callers can connect to the IVR or an agent within milliseconds, leaving friction to high-risk interactions.

Risk-based inbound call authentication delivers benefits across the organization

How do you convince your organization to secure investment approval for changes you know will work? This often requires demonstrating benefits accrue across the organization. Inbound call authentication delivers for fraud and call center teams — while also benefitting marketing and overall brand.

Reduces fraud and operational costs.
Deflecting high-risk calls reduces fraud, as well as the time and resources spent by fraud teams to manage those calls. Upwards of 30% of fraudulent calls could be avoided by authenticating inbound calls.[10]

Improves agent effectiveness.
Customer service agents spend less time verifying customers' identities and more time helping them and resolving inquiries.

Lowers call center operating costs.
Eliminating unnecessary KBA can save about 45 seconds per call, while richer IVR self-service authentication options can increase IVR containment by 1.1% — avoiding the $1.00 cost per call to have an agent authenticate the caller.[11]

Improves customer experiences.
Customers expect near-frictionless interactions in the call center, and repetitive authentication questions create frustration. Forrester estimated organizations could see a two-percentage-point increase in NPS with inbound call authentication.[12]

Supports customer retention.
Customers want great experiences but are unwilling to sacrifice security to get them. Brands must demonstrate trust to retain customers; 76% of consumers said confidence in the protection of their personal data is their top priority when deciding where to do business.[13]

Deliver for your business and customers with smarter call authentication

Call center managers and fraud professionals often unintentionally work against each other. Fraud teams introduce friction, call center teams absorb the operational costs. And yet, the fraud the friction was supposed to prevent still slips through.

The solution lies in risk-based call authentication, which evaluates signals like whether a number is tied to a physical device, how long it's been with its current carrier and recent SIM changes. That intelligence categorizes callers into trust tiers, focusing scrutiny on high-risk calls while providing legitimate callers with the fast, seamless experiences they expect.

And when the right calls get through faster and the wrong ones get stopped sooner, your customers are happier — and both teams win.

End notes

[1, 2, 4, 8] TransUnion, H2 2025 Update: Top Fraud Trends, 2025

[3] Javelin, 2026 Identity Fraud Study: The Illusion of Progress

[5, 6, 7, 9] TransUnion, H1 2026 Update: Top Fraud Trends, 2026

[10, 11, 12] Forrester, The Total Economic Impact™ of TruValidate Inbound Authentication

[13] TransUnion, Consumer Pulse Study, US Q4 2025

Protect the phone channel with TransUnion

Streamline call authentication, mitigate phone fraud, reduce call center costs and improve customer satisfaction.

Learn More

transunion.com/inbound-authentication