TransUnion

EBOOK

When ‘Verified’ Isn’t Safe: The New Reality of Phone Channel Fraud

The Hidden Cost of Trust in a High Risk Channel

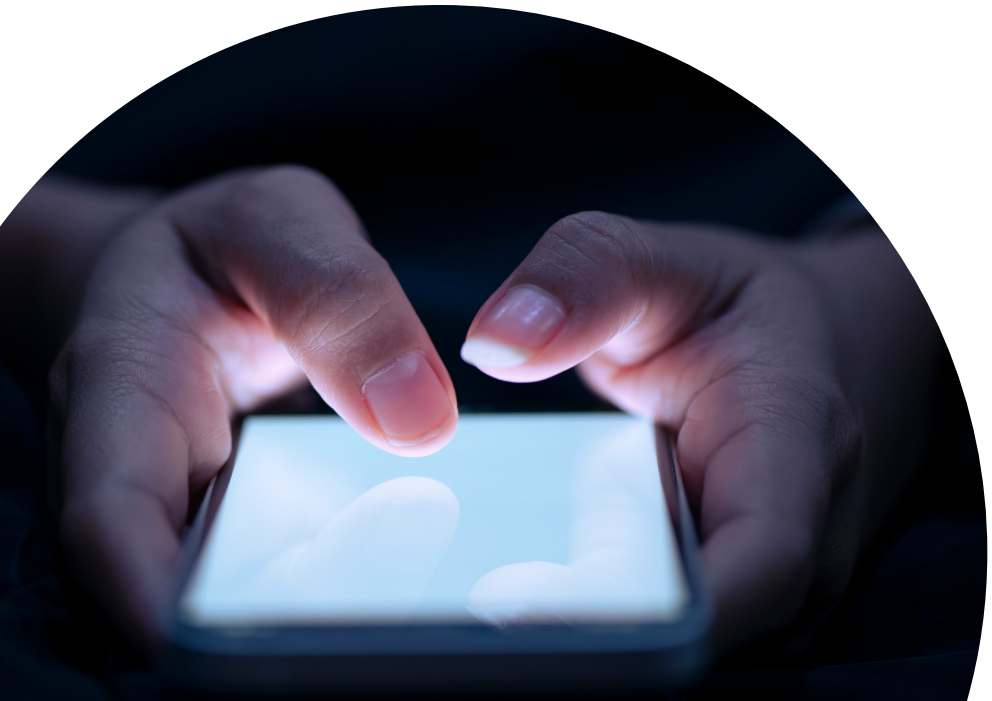
A practical guide for fraud, authentication and call center leaders

Fraudsters exploit low-friction phone channel experiences

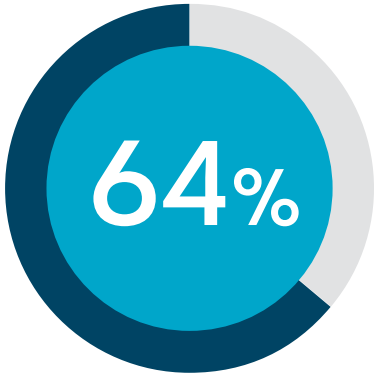
Caller authentication is no longer reducing fraud. Instead, it's driving up operational costs while allowing attacks to succeed.

Organizations are investing more time and effort into verifying customers on every call, yet fraudsters are increasingly bypassing those controls using compromised identity data and scalable, automated methods. The result is a growing imbalance: higher cost, greater friction and persistent fraud losses.

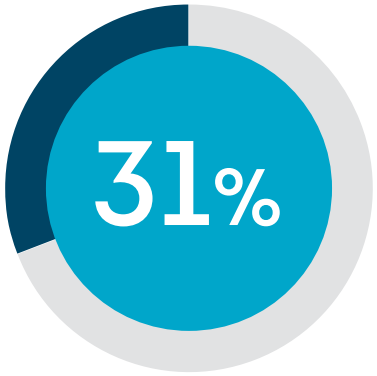
This guide is designed to help fraud, authentication and call center leaders understand the reasons behind these challenges and how to address them. It outlines how phone channel fraud has evolved, highlights the shortcomings of traditional authentication approaches, and examines how these gaps contribute to both increased risk and operational inefficiency.



It also provides a practical framework for moving forward — one that helps organizations reduce fraud exposure, contain authentication costs and enhance the customer experience through risk-based, adaptive approaches across the phone channel.



of US business leaders reported increased fraud attacks targeting call centers[1]



of US business leaders reported account takeover (ATO) was the leading cause of fraud losses for their organizations[2]

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

Authentication is driving cost and not reducing risk

Organizations are paying more to verify customers on every call with no guarantee of better protection

Phone fraud is often framed as a security issue. In reality, it's an operational cost problem at scale. Authentication happens on every call and small inefficiencies multiply quickly across millions of interactions.

Phone fraud doesn't just cause financial loss; it creates system-wide inefficiency. Even failed fraud attack attempts increase cost. And with AI-driven fraud, call centers face:

- **Rising call volume as attacks are automated**
- **More calls successfully navigating IVR**
- **Higher call handling times**
- **Added friction that increases escalations**
- **Higher fraud rates and losses**
- **More manual reviews from false negatives**
- **Increased agent strain**

Bottom line: Authentication is adding cost faster than it's improving protection.

The cost of authentication is a problem of scale

Estimated cost of authentication for a typical organization handling 10 million calls annually[3]

[3] *Forrester, The Total Economic Impact™ of TruValidate Inbound Authentication*

Phone fraud has shifted from effort to efficiency

Automated and data-driven attacks are allowing fraudsters to repeatedly pass authentication at scale

Phone fraud has evolved from isolated social engineering attempts into coordinated attacks aimed at accessing customer accounts. This escalated threat shows no signs of slowing down. TransUnion documented a 13% increase in the percentage of high-risk calls into US call centers from 2024 to 2025, reaching 6.8% of all calls.[4]

Phone fraud attacks operate within expected workflows until they succeed. At scale, this leads to:

- **More attempts at passing authentication**
- **Increased downstream fraud**
- **Higher operational costs**

Phone fraud is no longer constrained by effort or skill — it has become a scalable, repeatable process that will continue to grow.

What's changed in the last 18 months

AI-driven interaction
Fraudsters can generate high call volumes and adapt in real time

Compromised identity data availability
Verification questions are easier to answer

Cross-channel orchestration
Phone is now a vector for cross-channel ATO attacks

[4] *TransUnion, H1 2026 Update: Top Fraud Trends Report*

Fraud is passing authentication

Attackers are exploiting normal service workflows to gain access after successful verification

Modern fraud doesn't rely on avoiding controls, it succeeds by behaving like legitimate customers. Phone channel fraud often starts upstream with data breaches or direct consumers scams — or both. With compromised consumer data in hand, fraudsters use every level of the phone channel (carriers, consumers and call centers) to get the upper hand in ATO attacks in any channel.

Fraudsters exploit routine interactions with knowledge to perpetrate ATO:

- **Password resets**
- **Contact updates**
- **Phone number network transfers**
- **One-time passcode (OTP) requests**

Trust is under attack – and it's working

Gaming your system to pass authentication...

Fraudsters enabled by automation and AI-assisted workflows:

- **IVR can be mapped**
- **Responses can be rehearsed**
- **Scripts adapt to agent behavior**
- **OTPs can be intercepted**
- **Attempts can be repeated at scale**

leads to more bad outcomes

The system says "verified," the outcome says otherwise:

- **Authentication passed; fraud still happens**
- **Fraud teams investigate activity that appeared legitimate**
- **Multiple teams engage after ATO to recover customer**
- **Fraud loss and reputational damage**

Traditional authentication is being outpaced

Predictable authentication methods are being learned, replicated and passed by modern fraud tactics

Most phone authentication relies on consistency: same questions, same flows, same assumptions. This process isn't valid in our current environment of compromised consumer data and AI-enabled attacks. In fact, 79% of US business leaders cited an increase in use of stolen personal information to pass KBA.[5] Yet, fraudsters rely on that predictability to execute attacks.

Why static authentication leads to more fraud

Attack surface	Static authentication failure points
Telephony	Caller ID and known numbers are spoofable and rotated
IVR	PINs and menu paths can be mapped, tested and optimized at scale
Live agent	Fixed KBAs and scripts are easily rehearsed or recovered by callers
Identity verification	One time data match treats identity as static
Impersonation	Correct answers assumed to equal real speaker
OTP	Compromised devices and phone numbers send authentication codes to fraudsters
Policy & exceptions	Predictable rules are learned and exploited
ATO	Pass/fail decisioning allows learning across attempts

[5] *TransUnion, H2 2025 Update: Top Fraud Trends Report*

The phone is the weak link – not the OTP

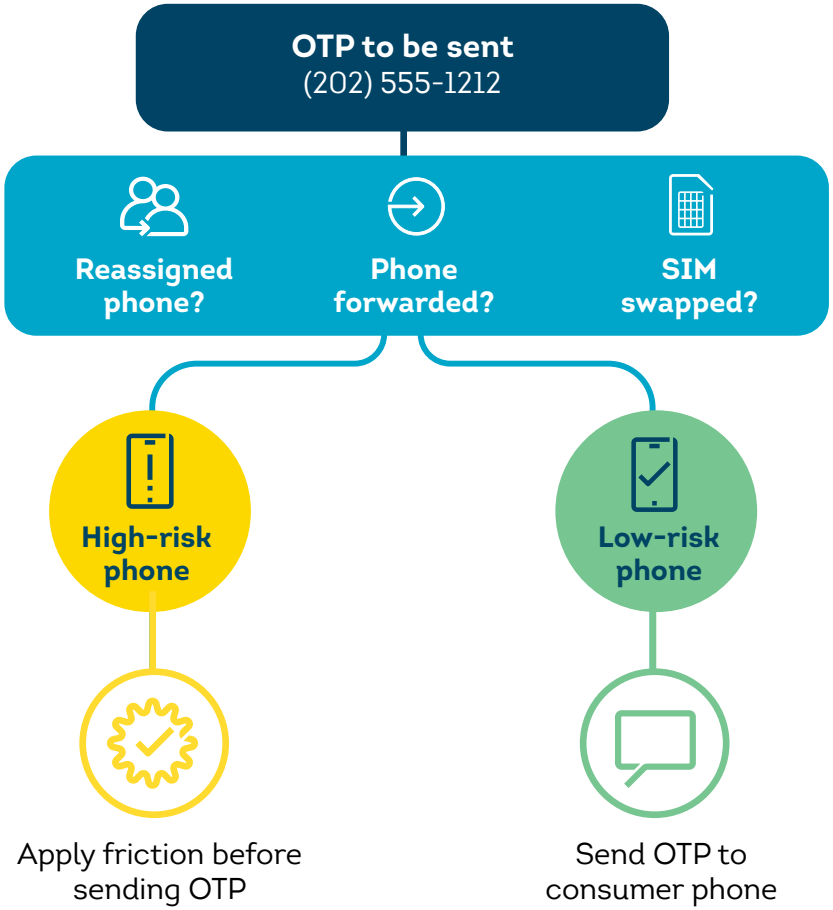
When phone control is compromised, authentication can succeed for the wrong person

One-time passcodes are widely used, but their effectiveness depends on one key assumption: The phone receiving the code is still controlled by the customer. This assumption increasingly breaks down; 85% of US business leaders cited being very concerned about the security of phone numbers before sending an OTP.[6]

Modern fraud combines phone control, identity data and automated execution. If the phone is compromised, authentication can silently fail. This is an increasingly common attack method that starts with mobile phone carriers:

- **Phone number is ported, reassigned or SIM swapped to a new device**
- **OTP is sent to the new device**
- **Authentication succeeds — for the wrong party**

The OTP risk decision many organizations skip



[6] *TransUnion, H2 2025 Update: Top Fraud Trends Report*

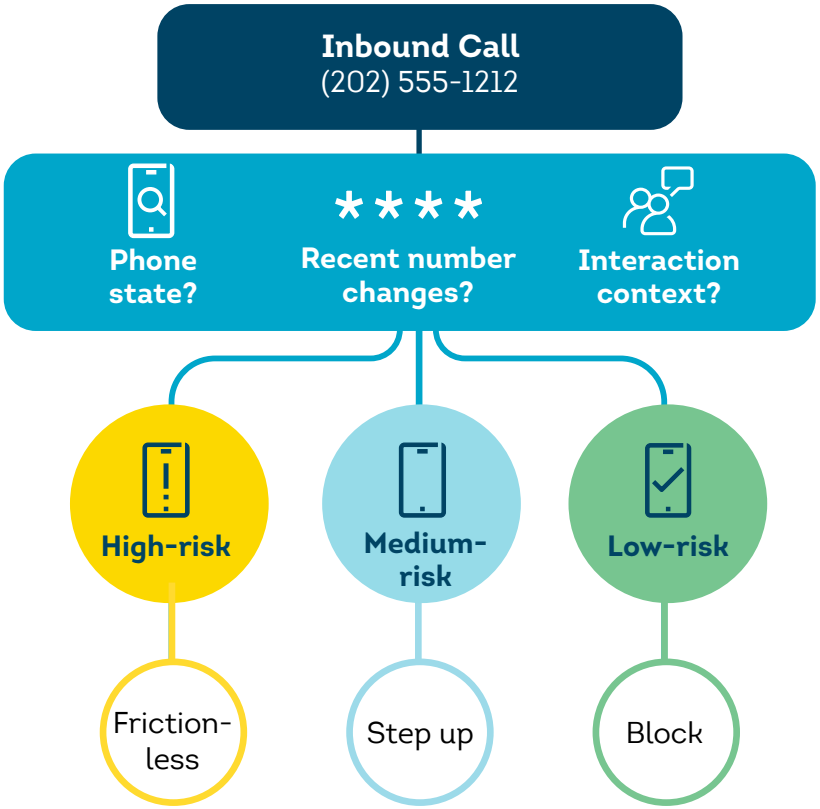
Stop treating phone numbers as identity

Trust should be based on real-time risk, not a static phone number tied to an account

Phone numbers are not fixed identifiers. Yet, many organizations evaluate phone number integrity and identity in silos. A different mindset is needed: A phone number is not an identity — it's a signal. Since numbers can be spoofed, transferred, reassigned or SIM-swapped, they require real-time risk evaluation.

Organizations are seeing their risk exposure grow: 83% of US business leaders reported an increase in call spoofing and 81% virtualized calls in 2025.[7]

Call trust signals many organizations don't evaluate



[7] *TransUnion, H2 2025 Update: Top Fraud Trends Report*

Adopt a risk-based decisioning approach to fraud prevention

Reducing fraud and cost requires shifting from uniform authentication to risk-based decisioning

You don't need to replace systems; you need to apply risk intelligence where it matters. Here's what you should be doing now:

- **Prioritize risk reduction** — Identify top three high-risk calls
- **Determine cost exposure** — Measure authentication time
- **Apply layered authentication model** — Determine best method for each use case
- **Align teams and goals** — Fraud, authentication and contact center
- **Complete proof of concept** — Pilot risk-based assessment

1 Phase 1: Define and quantify your cost of trust (0-30 days)

Determine use cases that drive friction and fraud risk associated to your call population. Identify high-risk call flows that are creating outsized costs or fraud for your call center

Outcome: Clear business case for change, prioritized call flows, plan differentiated caller treatment

A roadmap to fraud and cost reduction with risk-based decisioning

2 Phase 2: Implement risk-based authentication to reduce fraud (30–120 days)

Apply phone risk signals to inbound calls and outbound OTP process. Implement differentiated call flows.

Outcome: Automate step-up early, improve risk decisioning, stop fraud passing authentication

3 Phase 3: Streamline low-risk calls to reduce cost (120–180 days)

Integrate real-time signals into IVR and call routing

Outcome: Reduce friction, increase IVR containment, , shorten call handling time, enhance customer satisfaction

4 Phase 4: Adopt adaptive authentication (180–360 days)

Align phone and digital signals into a holistic authentication model applied in all channels.

Outcome: Improve risk decisioning, lower false positives, increase fraud capture rate, reduce manual reviews

Rethinking phone authentication: Lower costs, better protection, happier customers

Organizations that evaluate risk earlier can reduce fraud exposure without increasing customer friction

The phone remains essential because it promotes human engagement and is trusted. However, today's authentication model often adds friction, increases costs and fails to prevent fraud. Leading organizations will seek to:

- **Move from static to adaptive authentication**
- **Evaluate risk earlier in the interaction**
- **Apply intelligence across channels**

Risk-based authentication requires a clear picture of identity

Risk-based identity insight allows organizations to preserve trust while staying resilient. Increasing dynamic and adaptive risk evaluation accuracy is critical to capturing more phone-based fraud and reducing authentication friction for trusted customers.

Moving forward, organizations should look for a holistic way of leveraging a single, unified view of customers — one that consolidates risk signals from every channel over time. This provides a clear picture of identity, enabling smarter risk decisions in the phone channel for you and your customers.

Protect the phone channel with TransUnion®

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

HOW CAN WE HELP?

Learn more about our solutions, visit:
https://www.transunion.com/solution/truvalidate/omnichannel-authentication/inbound-authentication-solutions