EBOOK

Why One-Time Passcodes Fail: Restoring Trust in OTP Authentication

A practical guide to equip fraud, identity and authentication leaders to protect consumer trust in a familiar step-up authentication method.

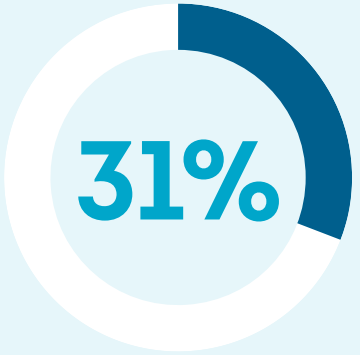
TransUnion

Customer authentication needs a more secure OTP process

Protecting customer accounts is everyone's job. Yet authentication processes are failing to keep accounts secure. Despite a shift toward more robust authentication frameworks, most organizations still rely on one-time passcodes (OTP) — opening the door to phone takeover fraud and OTP interception.

We need a different approach. According to TransUnion®, account takeovers (ATO) were the leading cause of fraud loss cited by companies in 2025.[1] Increasingly, criminals are targeting consumers' phones to pass authentication and access accounts undetected. Last year alone, the FBI IC3 received 971 SIM swap complaints from consumers totaling more than $17 million in losses.

This guide is designed to help fraud, identity and authentication strategists collaborate to better combat fraud attacks and reduce incidences of ATO and new account opening fraud by mitigating phone takeover risk and OTP interception.



of US business leaders cited account takeover as the leading cause of fraud losses in 2025

increase in ATO suspected digital fraud rate from 2024 to 2025

Source: *TransUnion, H1 2026 Update: Top Fraud Trends*

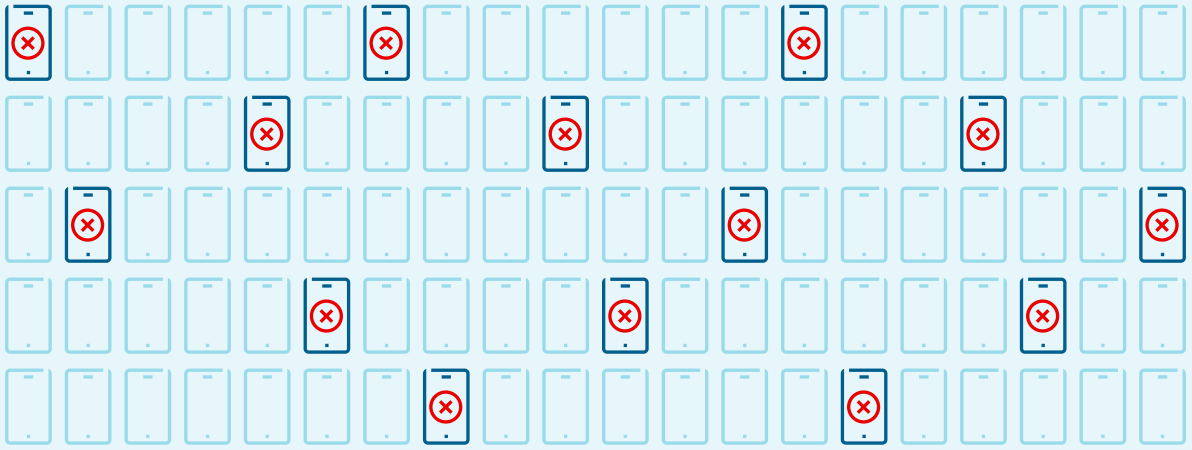
Fraudsters are targeting the weakest link in OTP authentication: *THE PHONE NUMBER*

OTPs are fast, familiar and trusted by consumers. But companies can no longer trust the OTPs they're sending are getting into the right hands. To be clear, OTPs are secure — it's consumers' phones that are vulnerable.

Using techniques like SIM swapping, unauthorized phone number reassignment or call forwarding, fraudsters are redirecting calls and texts to devices they control. When your authentication system sends an OTP, it might be going to a fraudster without you even knowing it — exposing customers to ATO or your organization to new account creation fraud.

14%

of applicant phone numbers failed verification because they were linked to a different consumer



Source: *TransUnion, Internal analysis*

Account takeover is rising as phone-based fraud erodes trust in authentication

The risk of losing consumer trust — and valuable business — is something most organizations understand. It's why protecting customers' online accounts and data is so critical. Fraudsters view attacking customer accounts as the easiest route to a payout — which is why secure authentication is so critical.

Overall, 36% of US business leaders reported biometrics as their primary authentication method, but vulnerabilities are present in ATO attacks, including spoofing, engineering or stolen devices.[2] While passkeys are the future of secure authentication, consumer adoption has lagged. Passkeys are nearly ubiquitous; 93% of accounts are now eligible; however, just 36% of accounts have a passkey enrolled — and only 26% of all sign-ins use passkeys.[3]

OTPs aren't going away anytime soon. Nearly a third (31%) of US business leaders said OTP was their secondary authentication method.[4] Why? Because they're convenient and trusted. More than a quarter of US consumers said OTP was their preferred method of online account authentication, second only to multifactor authentication. The best solution for today's environment is to combine biometrics with additional authentication.

> **With the ubiquity of OTPs a reality, it's more important than ever to ensure they're not a successful attack vector for fraudsters to pursue ATO.**

Organizations risk losing customers when authentication fails to protect accounts

Business impact

49%

of consumers said personal data security was the top attribute they look for when selecting an online company to do business with[5]

42%

of consumers who experienced account takeover closed their accounts[6]

Consumer impact

75%

of scam victims provided personal information to scammers, with emails and phone numbers provided most frequently[7]

$15 billion

in consumer losses attributed to account takeover fraud in 2025[8]

Identity compromise undermining OTP effectiveness

Organizations that recognize OTP risk often reach for solutions that don't address the real problem: Consumer identities can't always be trusted. Personal information fraudsters need to pull off a phone takeover — such as Social Security number, address, phone number, date of birth — are frequently the target of data breaches and consumer scams. And the problem is only getting worse as breach volumes increased 47% from 2024 to 2025.[9]

Common OTP alternatives do not address phone-level risk

Sending OTPs to a backup email
The same data breaches that give fraudsters what they need to execute a SIM swap also compromise email accounts. And forcing customers to switch apps for a time-sensitive code drives abandonment and higher call center volume.

Requiring a secondary phone number
Once fraudsters know a business collects secondary numbers, they may simply target an attack to register a number they control as the backup.

Routing OTP requests to a call center
All inbound callers must be verified before service is delivered, increasing costs and exposing call center agents to social engineering techniques. This can frustrate customers and ultimately doesn't stop account takeover fraud.

With limited options, organizations are in a difficult position, especially as fraud tactics become increasingly sophisticated all while consumers continue to expect safe, friction-right service. Fraud and authentication leaders need innovative authentication strategies that match the ease and convenience of sending SMS text messages or placing phone calls to deliver OTPs securely.

Real-time phone risk signals strengthen OTP authentication without adding friction

The most effective way to protect your OTPs is to evaluate phone number risk before codes are sent. Real-time risk signals from the telephony network can tell you if a number is safe without any customer engagement or added friction.

A three-step approach to identifying compromised phone numbers

1. **Determine phone number to individual linkage**
   A person using a phone number not linked to their identity should be considered suspect.

2. **Identify fraud attributes associated with the phone**
   Attributes like carrier changes, phone usage or number status indicate elevated risk.

3. **Evaluate mobile network operator (MNO) data**
   SIM swap, unauthorized reassignment, call forwarding, caller ID change all indicate heightened risk.

If the signals look clean, send the OTP. If they indicate risk, withhold the code, cancel the transaction or initiate an alternative verification method controlled by your fraud team. Most of your customers will never notice — and fraudsters who've compromised legitimate numbers will be stopped before damage is done.

Steps to strengthen OTP authentication and reduce takeover risk

As OTP-related fraud shifts from code interception to phone-level compromise, strengthening authentication requires a more disciplined, data-driven approach. The goal is not to replace OTPs but to ensure they're used at the right moments and delivered to the right individuals. That starts with understanding where your current controls are failing, focusing protection where fraud risk is highest and consistently extending safeguards across channels.

The following actions provide a practical framework to help you reduce account takeover risk while maintaining seamless customer experiences.

1 Assess where OTPs are failing in your current environment

Review your data from the past 60 days to identify OTPs that were sent in cases that later resulted in fraud. Conduct a proof of concept with a trusted service provider using authoritative phone data to assess risk in customer records and determine if those transactions could have been prevented. Assess the dollar amount that could have been saved and prioritize use cases with the biggest losses.

2 Focus OTP protections on high-risk transactions

Not all transactions carry the same risk. Password resets, contact detail changes and money movement are interactions fraudsters target most often because they open the door to broader account takeover. New account setup, enrollment or credit card applications are also areas where fraudsters target OTP interception to open new accounts they control.

3 Extend OTP safeguards across digital and call center channels

Digital channels are critical, but OTP security checks should be applied to interactive voice response (IVR) and call centers to ensure the legitimacy of those interactions. This can help call center managers contain high-risk calls within IVR, allowing agents to avoid ATO attacks and possible social engineering.

4 Measure authentication effectiveness and customer impact

In addition to the number of fraud incidents, track IVR containment rates, authentication abandonment and customer satisfaction scores. If your OTP controls are working, fraud drops without impacting customer experience.

Your OTPs are worth protecting

Consumers trust OTPs because they're simple and familiar. That trust is an asset — and the goal is to preserve it.

The good news is protecting OTPs doesn't require replacing them or adding friction for your customers. Ensuring OTP effectiveness requires knowing whether the phone about to receive a code is still in your customer's hand. When that question is answered before the code is sent, positive things happen: fraud drops, your customer experience stays intact and a trusted authentication method remains viable.

Learn how phone risk intelligence can strengthen your OTP authentication strategy.

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

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

[3] FIDO Alliance, FIDO Alliance Launches Passkey Index, Revealing Significant Passkey Uptake and Business Benefits, October 14, 2025.

[7] Javelin Strategy & Research, Multi-Layered Fraud Defense, Strategies for Evolving Threats, 2025.

[6, 8] Javelin Strategy & Research, 2026 Identity Fraud Study: The Illusion of Progress, 2026.

TransUnion

ABOUT TRANSUNION (NYSE: TRU)

TransUnion is a global information and insights company with over 12,000 associates operating in more than 30 countries. We make trust possible by ensuring each person is reliably represented in the marketplace. We do this with a Tru™ picture of each person: an actionable view of consumers, stewarded with care. Through our acquisitions and technology investments we have developed innovative solutions that extend beyond our strong foundation in core credit into areas such as marketing, fraud, risk and advanced analytics. As a result, consumers and businesses can transact with confidence and achieve great things. We call this Information for Good® — and it leads to economic opportunity, great experiences and personal empowerment for millions of people around the world.

transunion.com