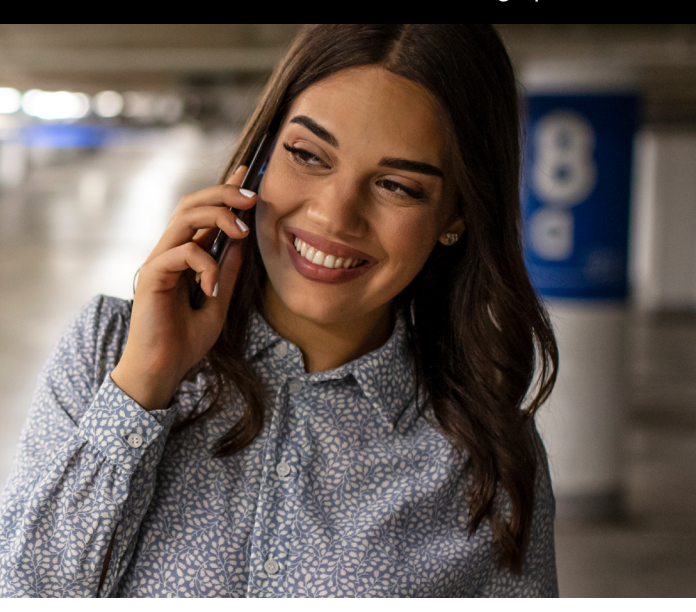# Don't let great customer service compromise your enterprise

Increased instances of contact center fraud in recent years have led to critical questions about balancing security with customer experience.

> How do we protect the enterprise from fraud, maintain customer's privacy and improve CX?

> What is our fraud and authentication strategy, tools and processes?

> How do we reduce the risk of fraud in our voice channels?

> What is the solution to frictionless authentication?

> How do we increase self-service capabilities?

> How do we increase call center operational efficiency and increase agent productivity?

> How do we manage transaction risks without treating legitimate customers like fraudsters?

> How do we manage regulatory compliance?

1-in-106
In 2024, 1 out of every 106 calls to a contact center were deepfakes. This represents a 6.8x increase.[1]

$12.7B
Spent on ineffective authentication.[2]

1-in-599
In 2024, 1 out of every 599 calls to a contact center were fraudulent. This represents a 100% increase over the past 4 years.[3]

89%
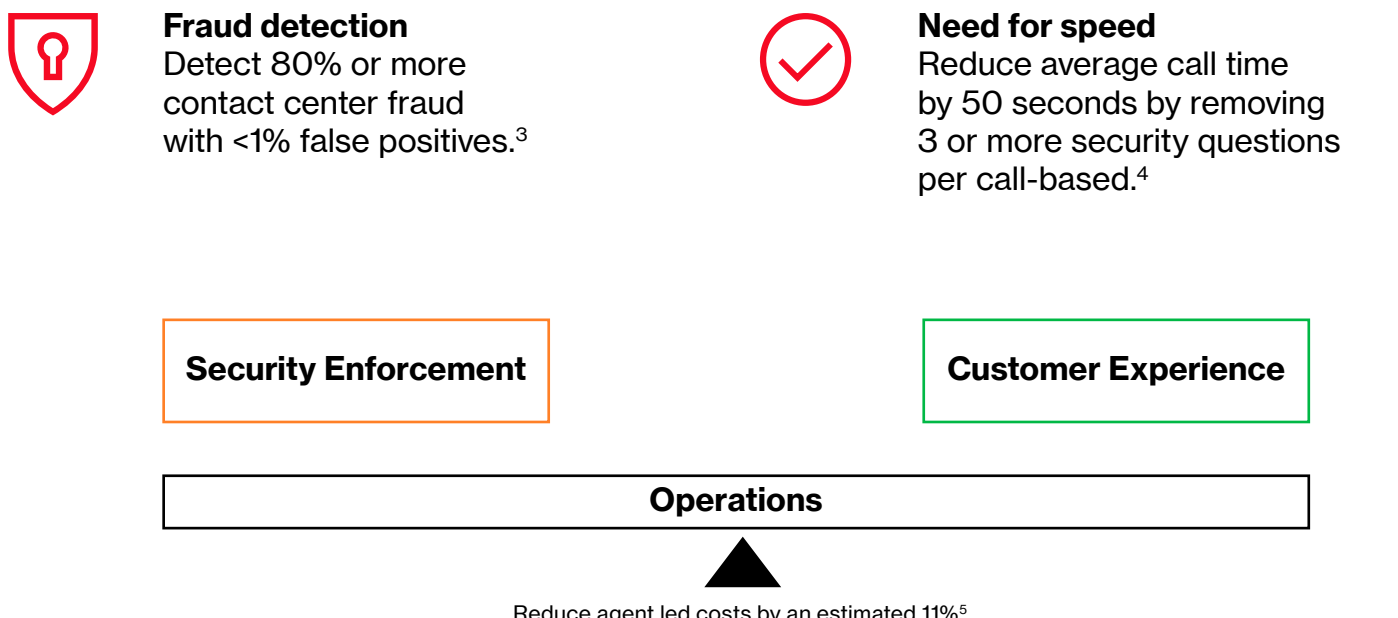Percentage of calls that use a live agent for authentication.[2]

Enterprises need a solution that combines fraud detection and automated authentication to manage risk, safeguard their brand, and build consumer trust.

Consumers expect an easy customer experience, and want assurances that their personal identifiable information (PII) is protected.

The role of anti-fraud and authentication

Increase self-service adoption with automated authentication.

Establish call flows with conditional rules based on risk scores.

Increase consumer authentication rate with passive enrollment.

Decrease the risk of fraud before call arrives to agent.

Gain insight into fraud and authentication analytics.

Improve CX with automated authentication.

Balancing the requirement of Enterprise Security and Customer Experience

Fraud detection
Detect 80% or more contact center fraud with <1% false positives.[3]

Need for speed
Reduce average call time by 50 seconds by removing 3 or more security questions per call-based.[4]

Security Enforcement

Customer Experience

Operations

Reduce agent led costs by an estimated 11%[5]

Verizon VoIP Inbound Anti-Fraud and Authentication

Core technologies that drive the solution.

Something you use **Network**	Something you are **Voice**	Something you have **Device**	Something you do **Behavior**	Something you do **Liveness**
Media forking	**Deep Voice™ Biometrics**	**Phoneprinting™ Technology**	**Toneprinting™ Technology**	**Liveness Detection**
• Global network	• Deep learning voice biometrics	• 1380 feature signatures	• Pattern recognition	• Deepfake detection
• Intelligent routing	• Designed for limited speech	• Anomaly detection and whitelisting	• BOT recognition	• Identifies frequency changes
• Duplicate media	• High enrollment rates	• Uses natural caller interactions	• Reconnaissance detection	• Identifies natural vs. synthetic speech
• Passive and secure				
• Enhanced SIP headers				

Verizon
Supplies IP header via media forking

Pindrop
Analysis provides fraud and authenticating scoring to contact center via API[6]

Learn more

Find out how a balanced integrated solution can help you reduce risk and increase customer satisfaction. Contact your account representative today or visit us at:
www.verizon.com/business/products/contact-center-cx/voice-security/voip-inbound-anti-fraud-authentication/

1. Pindrop 2025 Voice Intelligence and Security Report
2. Contact Babel US Decision Makers Guide 2024
3. Pindrop 2025 Voice Intelligence and Security Report
4. Based on analysis of 76 Pindrop Passport customers who were able to remove 3 or more KBAs on annual call volume with ANI validation and full profile authentication
5. Calculated as average handle time reduction by Pindrop (50 seconds or $0.78 per call) compared to the average cost of incoming call ($6.91) as per Contact Babel US DMG 2024
6. Feature availability may be limited in some states

verizon business