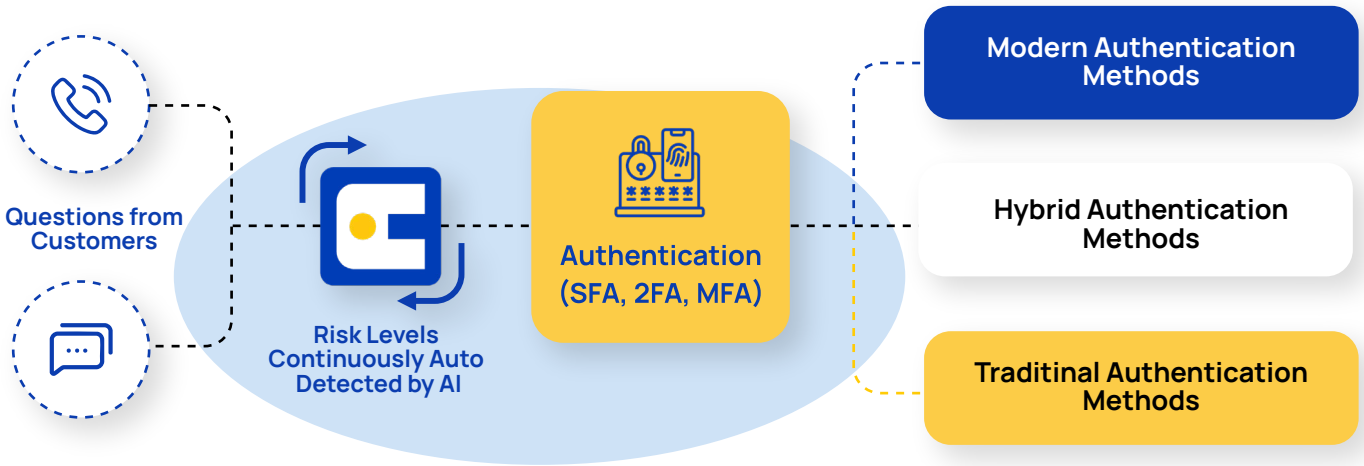
interface.ai

FRAUD PREVENTION AI

Prevent Fraud with Biometric Authentication and Caller ID Forensics

Enhance **authentication** and **fraud prevention** with a layered approach combining traditional authentication (in/out of wallet questions with OTP) with secure device-based biometrics and advanced Caller ID Forensics. interface.ai's intelligent, risk-based framework ensures the right level of authentication is applied at every step—maximizing security while minimizing friction for members and always on Caller ID forensics prevents spoofed-number attacks, SIM-swap scams, and other caller-ID–manipulation tricks from ever reaching your IVR or agents—shutting down social-engineering threats before they even start.



Context-Aware Adaptive Authentication with Seamless Experience

interface.ai Voice AI and Chat AI leverages an adaptive, risk-based authentication framework that intelligently balances user convenience with security. By assessing the context and sensitivity of each interaction, AI Voice and AI Chat apply the appropriate level of authentication—ensuring low-friction access for everyday tasks and stronger protection for high-risk actions.

The system follows a progressive, context-aware approach to authentication:

- **No-Risk Interactions**
  For informational requests (e.g., branch hours or routing numbers), no authentication is needed, delivering a frictionless, self-service experience

- **Low-risk interactions**
  For actions like checking balances or recent transactions, the IVA initiates lightweight knowledge-based authentication (e.g., in-wallet or out-of-wallet questions). This is enhanced by passive phone number verification and Caller ID Forensics for Voice calls, which silently check for spoofed numbers or fraud indicators—providing an added layer of security without disrupting the user

- **High-risk interactions**
  For high-risk interactions such as fund transfers or profile updates, the system initiates two-step authentication to ensure maximum security. This includes Caller ID Forensics, which performs real-time fraud detection by analyzing caller behavior and phone attributes, and Device Biometrics, which provides secure and private identity verification using Face ID or fingerprint on the user's device. This method ensures compliance and user privacy, as no biometric data is stored or shared. If device biometrics are unavailable for the user or the scenario, the system automatically falls back to a one-time passcode (OTP) to secure the transaction and maintain high-risk security standards.

This risk-based, multi-layered model ensures robust protection where it matters most—while keeping routine interactions fast and effortless for members.

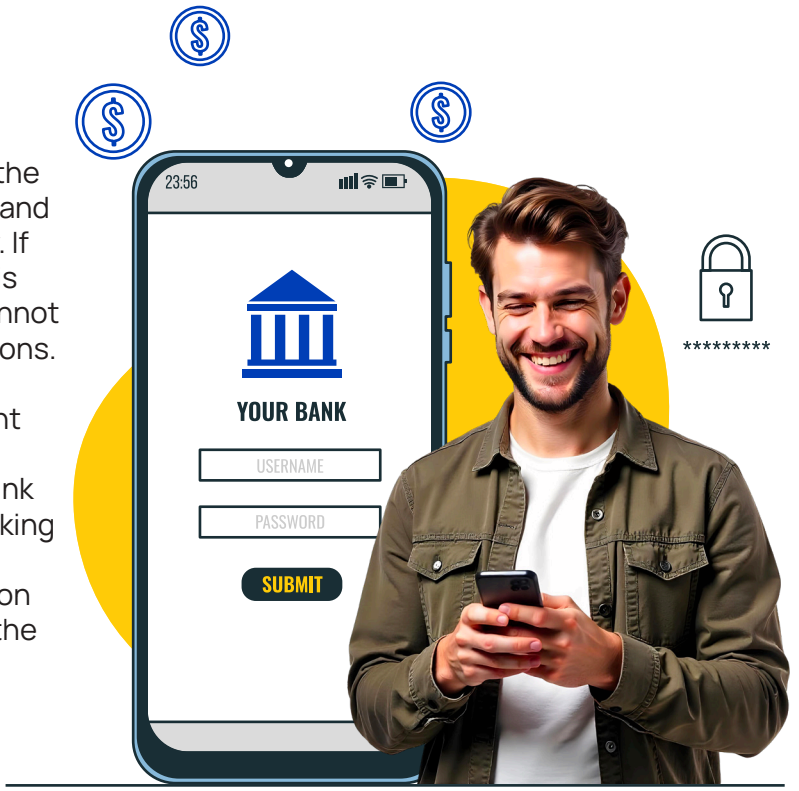
Device Biometrics: Seamless, Secure Authentication

Device biometrics enables secure, low-friction authentication using fingerprint or facial recognition stored on a user's mobile device. This method ensures high security without requiring users to share or store personal biometric data externally.

Registration

When a user calls from a mobile number, the system checks if the number is registered in the core system. Caller ID forensics is performed and shown to agents but does not affect the flow. If the number is eligible, an authentication link is sent via SMS to the calling number—users cannot choose alternative numbers for security reasons.

To begin, the user provides a member/account number and the last four digits of their SSN. Upon successful verification, they receive a link to initiate biometric authentication. After clicking the link, they enter their SSN, proceed to the biometric prompt, complete the authentication using their device, and return to the call and the user is registered to device biometrics.

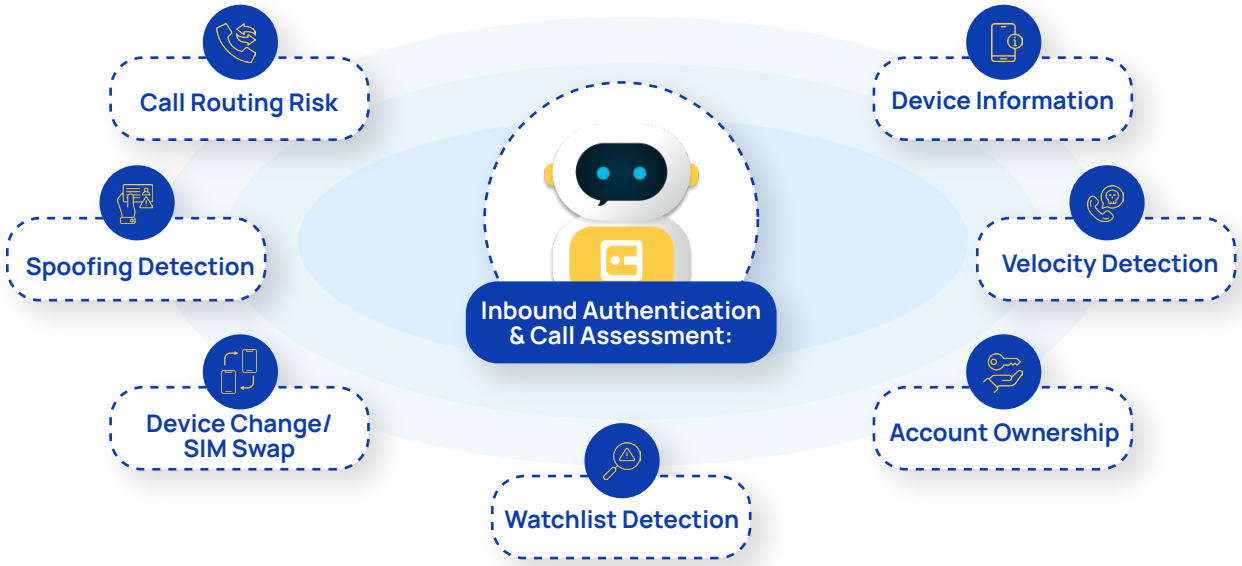


Authentication

When the user calls from a registered mobile number and if the user is registered for device biometrics, the system sends a biometric authentication link via SMS. The user clicks the link, authenticates using their device's finger-print or Face ID, and is prompted to return to the call. Caller ID forensics is again performed and made available to agents during any handoff.

Caller ID Forensics: Fast-Track Identity Verification

Caller ID Forensics accelerates authentication in the contact center, delivering a seamless, high-confidence identity check that keeps every interaction secure—without slowing members down.



When a call hits the contact center, Caller ID Forensics analyzes signaling data and metadata in real time:

Caller-ID-verified number – The system flags the number as genuine and simply asks the caller for a quick secondary proof (e.g., last four of SSN).

Unverified number – The caller remains unverified and must clear higher-security hurdles such as member ID plus a one-time passcode.

This risk-based flow lets trusted members breeze through with minimal effort while forcing spoofed or suspect calls to scale a much higher wall

Benefits

Frictionless Authentication Experience:
Device biometrics offer fast and secure authentication without requiring the customer to share or store any personal biometric data, creating a smooth user experience

Agent Empowerment & Efficiency:
When a handoff is needed, agents receive full context—including authentication steps taken, Caller ID Forensics results, a conversation transcript, and AI-generated resolution suggestions—so they can assist immediately and effectively

Proactive Fraud Detection:
Caller ID Forensics automatically scans for 35–40 risk factors to detect spoofed numbers, SIM swaps, or high-risk call origins—flagging threats before they escalate

Compliance-Friendly Security:
Device biometrics never leave the user's device. This eliminates the need for storing sensitive data or acquiring member consent, significantly reducing compliance and audit overhead

Dynamic Risk-Based Authentication:
Authentication adjusts in real time based on the sensitivity of the customer's request. Low-risk queries require minimal authentication, while high-risk actions prompt stronger verification methods

Industry-First Combination:
The unique combination of real-time Caller ID Forensics with on-device biometrics offers unparalleled fraud prevention—making this solution a clear differentiator in the market

Key Capabilities

Device Biometrics:
Utilizes on-device fingerprint or facial recognition for secure, low-friction authentication. No sensitive data is stored or transmitted, ensuring both user privacy and regulatory compliance

Multi-Layer Authentication Support:
Supports in-wallet and out-of-wallet questions, OTPs, and magic links—layered dynamically based on risk level

Caller ID Forensics:
Automatically analyzes 35–40 caller attributes (e.g., burner phones, SIM swaps, spoofed numbers, location mismatches) to identify potential fraud. High-risk calls are flagged for immediate attention

Intelligent Call Transfer with Context:
Provides agents with a full transcript, authentication summary, Caller ID Forensics results, and an AI-suggested resolution during handoff

Risk-Based Authentication Engine:
Continuously evaluates the risk of each customer interaction and applies the appropriate level of authentication—from no-auth for basic FAQs to multi-step verification for sensitive transactions

Seamlessly Integrated with Voice AI & Chat AI:
Instantly feeds authentication results and risk scores into your conversational agents, enabling secure, personalized interactions across phone and digital channels—no extra development or context hand-offs required