iProov

Biometric Adoption Navigator Report

Biometric authentication is revolutionizing how businesses protect identities and streamline user interactions. By offering more secure and user-friendly alternatives to knowledge and possession authentication factors, biometric authentication is helping companies reduce fraud, meet compliance, and enhance the user experience.

Authentication Factors

Knowledge

Knowledge factors are something you know, like a password or PIN. They're commonplace due to their ease of implementation but provide a poor user experience and are vulnerable to phishing, social engineering, and data breaches.

Passwords

PIN

Secret Question

Possession

Possession factors, such as physical tokens or one-time passcodes (OTPs) sent to devices, are often used to bolster passwords in multi-factor authentication (MFA). While adding an extra layer of security, these factors are vulnerable to loss, theft, and phishing.

One-time Passcode

Magic Link

Hardware Token

Inherence

Inherence factors offer a uniquely human way to authenticate. Device-native biometrics are a popular UX feature but are only as secure as a PIN. However, third-party biometric solutions offer anti-spoofing and identity verification for high assurance throughout the identity lifecycle.

Device-native Biometrics

Third-party Voice Biometrics

Third-party Face Biometrics

iProov

Passwords

Passwords are ubiquitous yet insecure and provide a poor user experience with costly overheads.

34% of all login attempts are credential stuffing attacks[1].

PIN

Numeric codes typically used as a second factor for devices and apps.

Pen testers broke a 5-digit PIN in 5 minutes[2].

Secret Question

Questions about personal information typically used as a second factor or step-up authentication.

19.7% chance of guessing the answer to "What is your favorite food?" within 1 guess[3].

One-time Passcode

Unique codes sent via SMS, email, or authenticator app. Easy to implement but vulnerable to SIM swapping and phishing.

83% of organizations are concerned about OTPs' susceptibility to account takeover.

Magic Link

One-time use link sent via email for passwordless login. Easy to use but vulnerable to interception and phishing.

Found to have a day zero vulnerability[4].

Hardware Token

Physical devices that generate codes or can be plugged into a device. While they offer higher security, they lack convenience and can be easily lost, forgotten, or stolen.

Device-native Biometrics (eg: FaceID)

Commonly used to unlock devices or as an alternative to an OTP. Can be bypassed by a PIN code.

40% of on-device biometrics can be bypassed with 2D images[5]

Third-party Voice Biometrics

Creates a voiceprint for re-authentication. Commonly used for remote banking or call center authentication but easily spoofed.

99% failure rate at detecting voice clones[6].

Third-party Face Biometrics

Leverages anti-spoofing liveness detection and identity verification for high assurance.

Able to achieve 0.0002 attack error rate depending on provider

1. BleepingComputer, "Okta: Credential Stuffing Accounts for 34 Percent of All Login Attempts," published June 15, 2023.
2. CTDefense, "PIN Code Authentication Bypass," published February 28, 2022
3. ACM Digital Library, "Secrets, Lies, and Account Recovery: Lessons from the Use of Personal Knowledge Questions at Google", published May, 2015
4. Dfns, "Magic Links Suffer from Zero-Day Vulnerability, Industry-Wide Debate on Web3 Wallet Security Sparked", February 2023
5. Which?, "Smartphones have face recognition that can be easily spoofed with 2D photo", May 2023,
6. University of Waterloo, "How Secure Are Voice Authentication Systems Really?", June 2023

Key Use Cases

Low Risk — **High Risk**

Account Login

Traditional methods such as passwords are vulnerable to interception and prime targets for account takeover (ATO) attacks. Verizon's 2022 Data Breach Investigations Report (DBIR) found that 80% of attacks against web applications can be attributed to the use of stolen credentials, typically passwords[7]. Biometrics offer increased resistance to such attacks. For everyday account login, device-native biometrics can provide a sufficient level of security. However, it's crucial to note that these methods shouldn't be relied upon for higher-risk use cases due to lack of anti-spoofing capabilities.

Step-up Authentication

Step-up authentication is essential for high-risk actions such as transaction authorization, sensitive data access, or requesting new services. Biometrics serve as an effective additional layer of security in these scenarios without adding friction to the user journey. When integrated with identity verification processes, biometrics can offer high assurance it's the right person, a real person, and they're authenticating in real time. Adaptable solutions like iProov tailor the level of identity assurance to the use case and risk profile, ensuring seamless self-service for users while mitigating the need for costly and time-consuming staff assistance.

Account Recovery

Gartner identifies account recovery as the highest-risk event in the identity management lifecycle[8]. Forgotten passwords or lost credentials open the door for fraudsters to exploit vulnerable processes. In 2023 alone, account takeover fraud (ATO) resulted in losses of nearly $13 billion (Javelin Strategy & Research, 2024)[9]. Third-party biometrics verified against a real-world identity offer a powerful defense against ATO during account recovery. This ensures high assurance that the person attempting to regain access is the right person and a real person, minimizing the risk of unauthorized account access and enhancing the user experience. For the highest assurance, iProov delivers a passive challenge response to confirm the individual is authenticating in real time, not a deepfake.

7. Verizon, "Data Breach Investigations Report 2024", published 2024
8. Gartner, "Innovation Insight for Biometric Authentication", published December 2003, restricted.
9. Javelin, "Resolving the Shattered Identity Crisis", published April 2024

How to Deploy iProov Face Biometrics Throughout the Identity Lifecycle

Face Capture

Verify it's a real person, not a spoof, with presentation attack detection and injection attack detection.

Use Cases: Account Login

+ Flashmark Challenge Response

Verify it's a real person and they're **authenticating in real time** with a passive challenge response built for security and accessibility.

Use Cases: Device Binding, Step-up Authentication, Account Recovery

+ ID Capture

Verify it's the right person, a real person and they're **authenticating in real time.**

Use Cases: First-time Onboarding

Customer Spotlight

Knab Bank - Strong Customer Authentication

Knab replaced their banking card readers with iProov Face Biometrics for Strong Customer Authentication (SCA). This saved them €5+ million in issuing card readers and provided a device-independent authentication solution for ID verification, step-up authentication, and device binding.

"Our customers really are everything to Knab. That's why we chose iProov – like us, they are clear leaders in delivering the very best customer experience without compromising on the highest standards of security and compliance."

Marcel Kalse, Co-founder
Knab

Watch Now

Raffeisen Bank - Device Binding

With a simple face scan, customers can quickly recover their account when they're locked out or change devices. This eliminates cumbersome, manual recovery processes and reduces the risk of account takeover (ATO).

"iProov has been successfully deployed by leading global banks and has achieved the industry's highest completion rates."

Tomáš Rosa, Ph.D. Cryptology and Biometrics Competence Centre Lead, Mathematical Security Architect
Raiffeisen Bank

Speak to an Expert

To learn more about how biometric authentication can benefit your organization, contact us for a personalized consultation. We'll discuss your specific needs, recommend the most suitable biometric solutions, and outline a tailored implementation plan.

Embrace the future of identity verification with biometrics. Contact us today to get started.