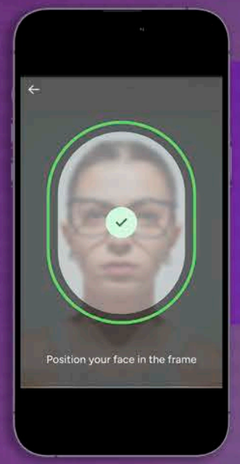


PREVENT FRAUD AND ACCOUNT TAKEOVER

Build Digital Trust With Biometric Authentication

ENTRUST

SECURING A WORLD IN MOTION

Introduction

Unlocking a phone with a face scan. Verifying identity with a selfie. Approving access without a password. These interactions are no longer novel – they're routine. Biometric authentication has reshaped how people expect security to work: instant, invisible, and effortless.

But familiarity alone does not equal trust. To understand how consumers truly feel, Entrust conducted a survey examining perceptions of biometric authentication across age groups and financial institutions.

The results point to a clear shift. Consumers no longer view biometrics as experimental or intrusive. Instead, they associate biometric verification with confidence, ease, reliability, and security – qualities that matter most when accessing sensitive accounts or services.

Drawing on insights from a recent Entrust survey, this ebook examines how identity verification shapes digital experiences and what these perceptions mean for financial institutions looking to strengthen security while meeting rising customer expectations. These insights impact how organizations can view authentication methods as they become easier for the user, and fraud becomes more sophisticated.

How Consumers View Identity Verification

Identity verification plays a visible role in how consumers experience financial institutions, particularly during account opening. This survey shows that while many consumers are satisfied with today's verification processes, expectations continue to rise as more interactions move online.

52%
of consumers now prefer to open accounts online.

A significant 35% are not satisfied with current verification processes. This signals a clear opportunity for financial institutions to improve. The dissatisfaction is amplified by the fact that 52% of consumers now prefer to open accounts online, a trend that spans across age groups.

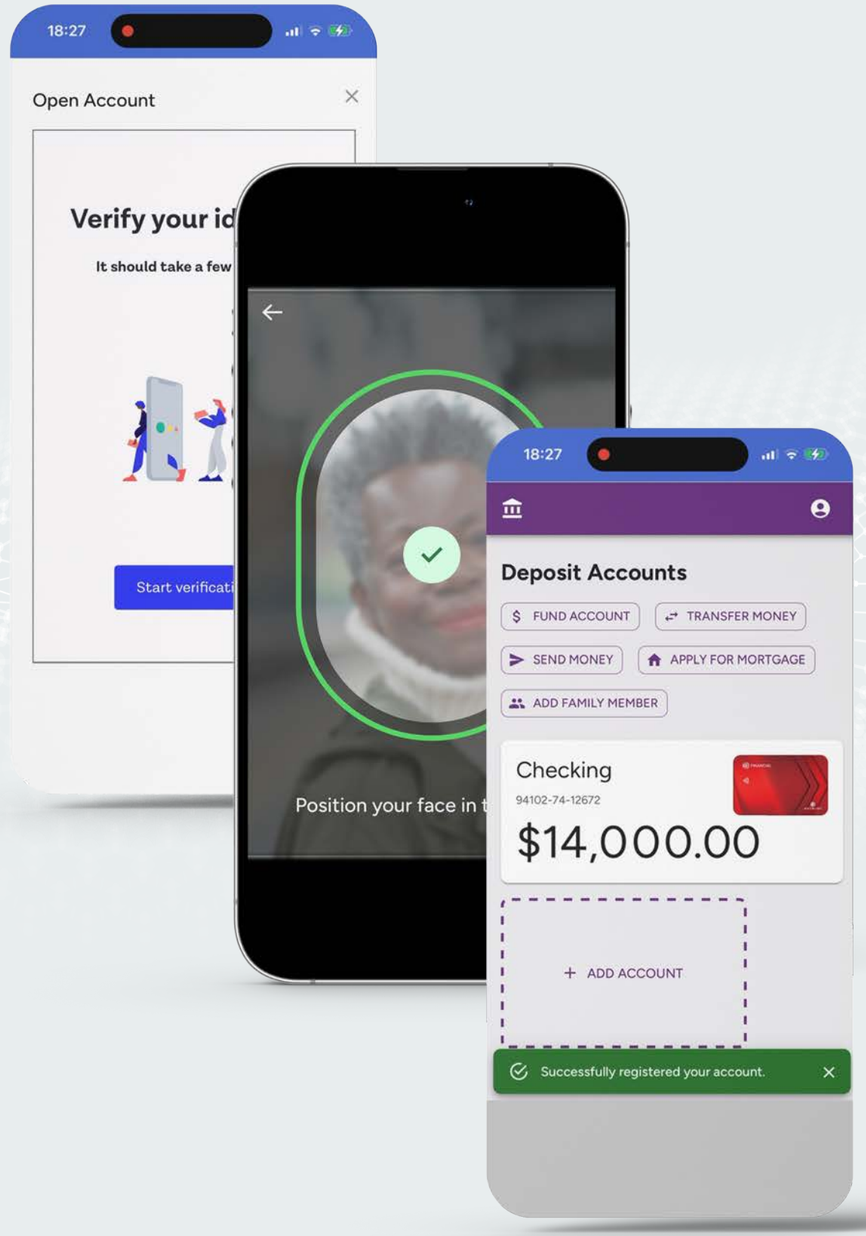
When selecting a financial institution, consumers prioritize experiences that feel:

Easy to use online

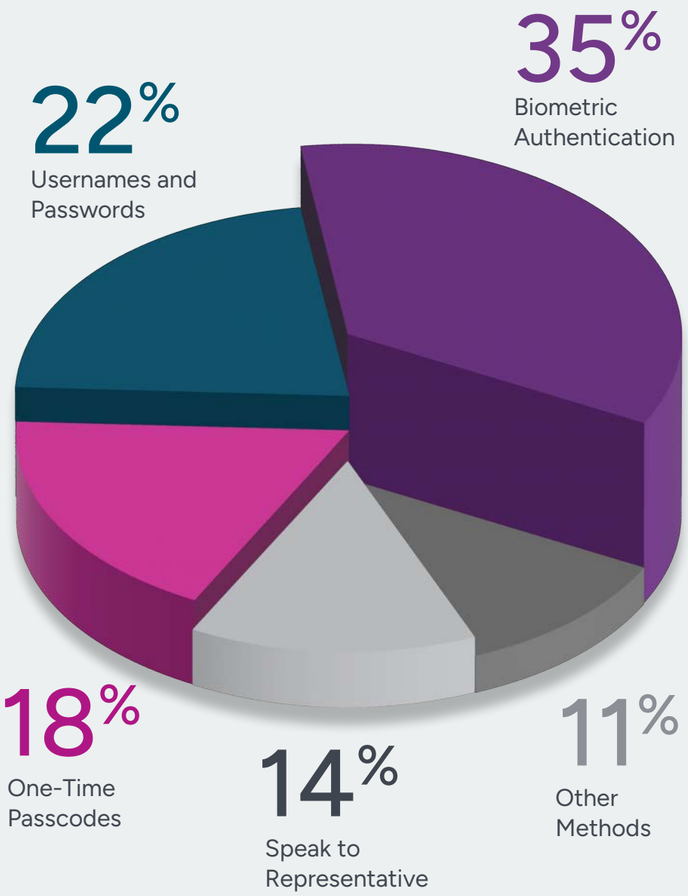
Convenient

Secure and trustworthy

Yet today's authentication landscape hasn't fully caught up with those expectations. Usernames and passwords remain the most commonly used login method (74%), followed by one-time passcodes (46%) and biometric authentication (43%). However, nearly as many consumers say they prefer biometrics as those who prefer traditional passwords – highlighting a growing gap between the methods most widely deployed and the experiences consumers increasingly value. This gap between expectations and reality is especially problematic as fraud attacks increasingly target authentication flows.



Consumers' Preferred Authentication Method:



Biometrics Lead the Conversation in Trust

Trust emerged as one of the strongest signals among survey respondents. Notably, trust is not a consumer preference – it's a business imperative because trust matters when money, accounts, and personal data are at risk. Authentication methods that inspire this feeling drive adoption, loyalty, and long-term customer relationships.

Over a third of consumers (35%) ranked biometric authentication highest for trust compared to other authentication methods, and that perception remained consistent across age groups. This was significantly higher than the next two most trusted methods – usernames and passwords (22%) and one-time passcodes (18%). That gap reflects broader industry challenges with legacy authentication. Compromised credentials – including stolen, weak, or reused passwords – remain the most common attack vector in data breaches.[1]

Rather than viewing biometrics as unfamiliar or risky, many consumers see them as a dependable way to verify and reverify identity. As a high-assurance authentication method, biometric tools are often associated with:

- A lower risk of impersonation and account takeover
- Greater confidence in account privacy
- Fewer disruptions caused by forgotten credentials

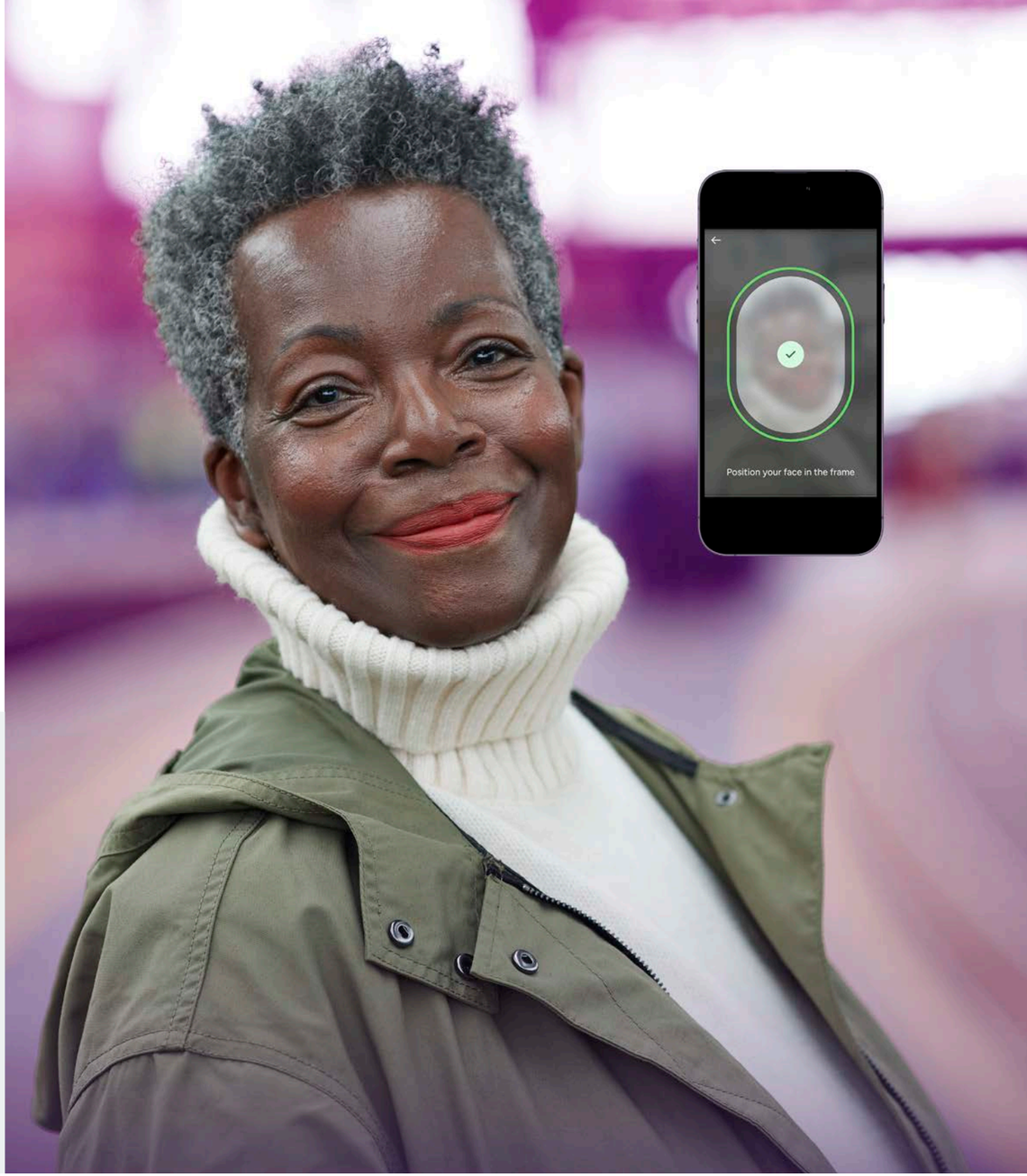
For organizations, this matters because trust is foundational. Authentication methods that consumers already trust reduce resistance, support adoption, and help create secure experiences that feel familiar rather than disruptive.

1. https://www.verizon.com/business/resources/reports/dbir/

Convenience Without Compromise

Convenience strongly influences how consumers evaluate identity verification and authentication methods. According to 36% of survey respondents, biometric authentication is the most convenient option available today. We expect that number to continue to grow as people's comfort with biometrics in their everyday lives extends into every aspect of their lives.

Consumers increasingly expect verification processes to be quick and easy to complete. Lengthy steps, repeated inputs, or interruptions can negatively affect how the experience is perceived. But comfort shouldn't come at the expense of protection. Biometric verification aligns with these expectations by streamlining authentication and reducing manual effort – all without sacrificing security.



Survey responses indicate that consumers value verification methods that:

- Minimize friction during onboarding and access, leading to increased conversions
- Reduce the need to remember or retrieve credentials
- Fit naturally into mobile and digital workflows
- Protect against identity fraud, impersonation, and account takeover

Biometrics deliver on all four. When verification feels convenient, users are more likely to complete processes without frustration or delay. Convenience, in this sense, supports both usability and acquisition, making it a critical enabler of business growth.

Consumers Prefer the Selfie Method

Facial biometric authentication, or the selfie method, stands out clearly for consumers. Nearly half of respondents (42%) believe it's a better, more traditional authentication method than what they currently use. And they're right, because this method helps to support fraud-resistant authentication.

Among those respondents, preference is driven primarily by experience. Consumers who prefer selfie-based authentication say:

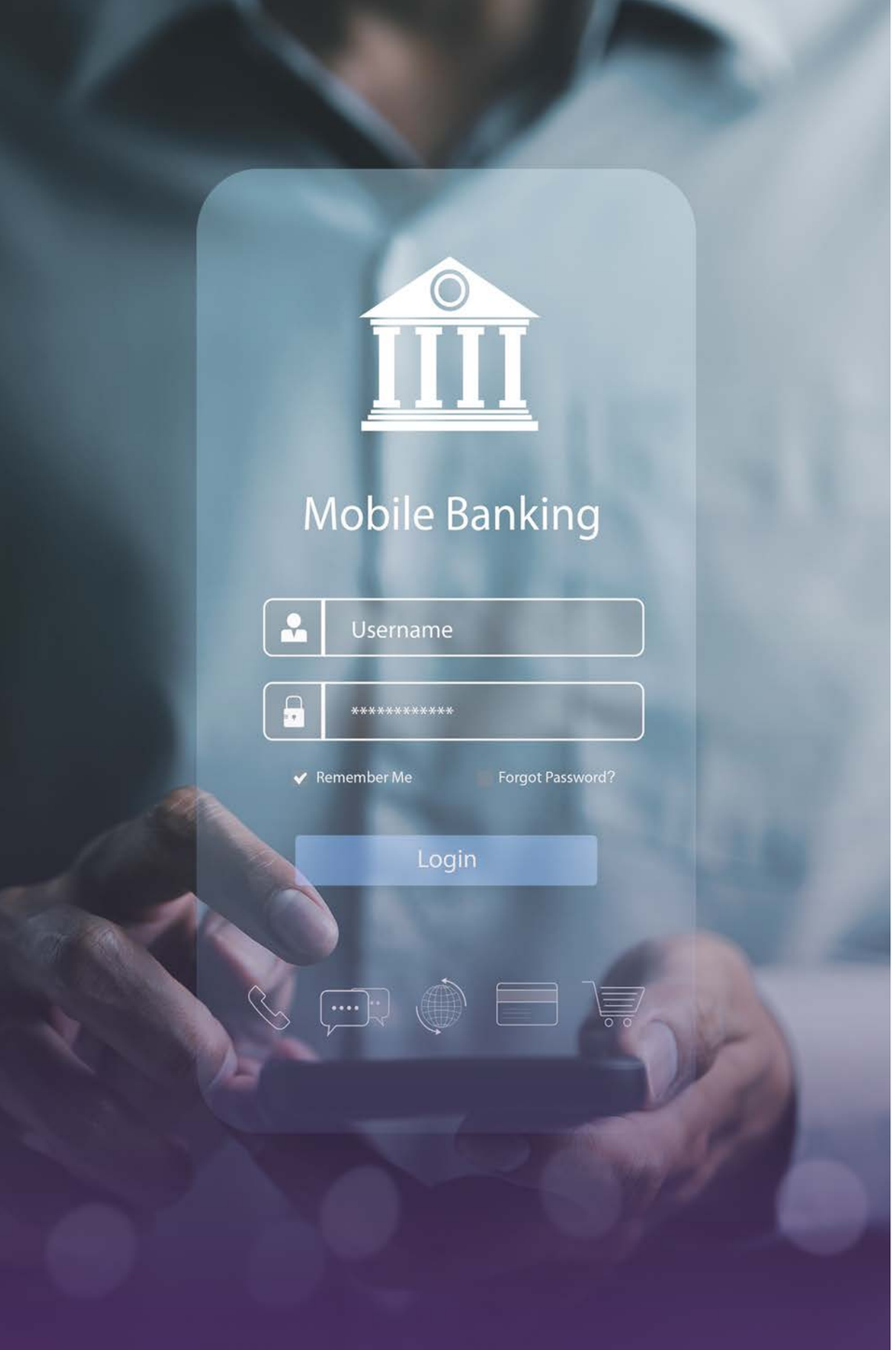
It has a better UX

It's simple and easy to use

It reduces the need to manage multiple passwords or codes

Critically, security also contributes to this preference. More than half (53%) of these respondents believe facial biometrics offer better security than other methods. Together, these factors help explain why biometrics continue to gain traction as a preferred form of identity verification.

53%
of respondents believe facial biometrics offer better security than traditional methods.



How Fraud Shapes Consumer Expectations

Fraud has a significant impact on how consumers evaluate financial institutions. Entrust's survey shows that fraud is closely tied to trust and loyalty, even when the experience is indirect.

More than half of respondents (56%) say they would switch banks if they or someone they know experiences fraud. This finding highlights how quickly confidence can erode when consumers believe their accounts or identities are at risk.

At the same time, many consumers feel their current protections fall short. 55% believe there is room for improvement in how well their bank protects them from fraud. As fraud becomes more sophisticated, expectations for stronger safeguards continue to rise. Financial institutions should consider the high cost of new customer acquisition versus retaining existing customers when looking to combat fraud, impersonation, and account takeovers.

Importantly, consumers do not view better fraud protection as a burden:

84% say better fraud protection represents a better service experience

63% want more fraud protection whenever possible

79% are willing to complete additional security steps if it improves long-term safety

68% are happy to use biometric authentication if it offers better protection

The Power of Biometric Fraud Protection

As fraud tactics evolve, traditional authentication methods are increasingly challenged by sophisticated attacks. Biometric authentication helps address these risks by verifying not only that a real person is present but also that the individual attempting to access or transact is the same person who originally opened the account. The original biometric becomes a “trusted anchor” throughout future transactions. This continuity of identity is critical for confirming that legitimate account holders, not bad actors, are initiating sensitive actions.

Modern biometric systems incorporate capabilities such as liveness detection, which help distinguish genuine users from fraudulent attempts involving photos, videos, deepfakes, or injection attacks. These protections are especially important as AI-powered fraud techniques become more accessible and more difficult to detect. Together, they strengthen security during onboarding, login, and high-risk transactions.

Biometric authentication also supports layered security strategies. When combined with other signals and controls, biometrics add assurance without requiring users to manage additional credentials or remember complex passwords.

By focusing on who is accessing an account rather than what they know, biometric authentication helps organizations stay ahead of emerging fraud techniques, such as account takeovers and impersonation attempts. When implemented thoughtfully, it delivers stronger protection while supporting the seamless experiences consumers increasingly expect. Entrust authentication solutions strengthen this process further through adaptive risk decisioning, AI-powered fraud detection, and a fraud lab that is dedicated to identifying emerging fraud techniques like deepfakes and injection attacks.

ABOUT ENTRUST

Entrust fights fraud and cyber threats with identity-centric security that protects people, devices, and data. Our comprehensive solutions help organizations secure every step of the identity lifecycle, from verifying identity at onboarding to securing connections and fighting fraud in everyday transactions. Ongoing monitoring supports compliance and safeguards keys, secrets, and certificates. With a foundation of identity-centric security, our customers can transact and grow with confidence. Entrust has a global partner network and supports customers in over 150 countries.

For more information, visit entrust.com.

entrust.com | Toll-Free: 888.690.2424 | International: +1.952.933.1223 | sales@entrust.com

ENTRUST
SECURING A WORLD IN MOTION