entersekt

The Financial Authentication Company.

The state of digital banking security

How banks and credit unions can address growing security threats while meeting modern consumer expectations



Executive summary

Trust, once broken, is difficult to repair. Just ask the dozens of industries currently experiencing record lows of consumer trust.

In financial services, as customer preferences continue to evolve at a rapid pace, the industry must find a way to adapt alongside them if they want to keep that trust. But, in addition to a resistance to change, the industry must also contend with consumer demands that sometimes conflict with best practices.

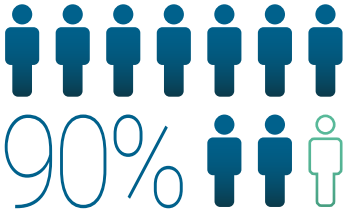
To examine these dynamics further, Entersekt launched a survey of over 400 banking and credit union consumers in May 2026, inquiring about their experience with their primary provider, their preferences, and their expectations. The findings highlight a conflicting picture between what customers expect and what they receive, emphasizing the need for modern solutions that prioritize security without impeding convenience. Moreover, they highlight customer willingness to change financial institutions should their expectations not be met, particularly around security.



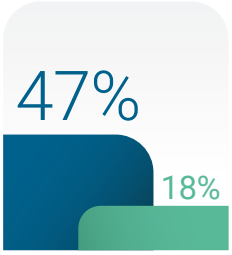
Read on to learn about the current state of consumer trust, obstacles the industry faces in meeting modern consumer preferences, and how FIs are looking for new solutions.



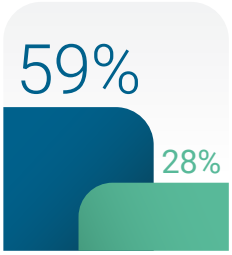
Would consider leaving an institution based on authentication methods alone.



Of consumers rate security as a top factor when choosing a financial institution.



47% of FIs utilize OTP via text for authentication, despite only 18% of consumers considering it secure.



59% of consumers trust their FI to flag suspicious transactions without the need for their review, but 28% still want an active role in what transactions are flagged.

Introduction

It's no secret that consumer trust has been in free fall over the past few decades. Growing global political and economic instability has only accelerated this erosion. But while some industries struggle to keep heads above water, the financial services industry is managing better than most.

A recent survey by the American Bankers Association found that 45% of consumers trust financial institutions (FIs) five times more than the next-most-trusted industry, healthcare (9%). According to the 2026 Edelman Trust Barometer, financial institutions have a positive trust score in 16 of 28 countries.

But trust is not a given. It needs to be earned and maintained. And the grace period for FIs is closing.

As consumer preferences and the threat of fraud continue to evolve, it is imperative that FIs, particularly those small and mid-sized, change alongside them. By exploring consumer preferences regarding authentication and fraud prevention, *"The State of Digital Banking Security"* aims to define the current state of trust, outline the expectations of modern digital banking, and identify steps FIs can take to stay ahead.

Our findings reveal critical insights that highlight the precarious balance of convenience and security FIs must navigate in order to deliver a trustworthy digital experience.



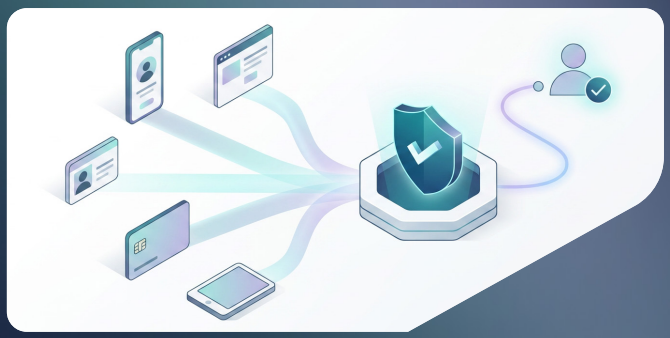
Fraud is top of mind for consumers, and they are willing to look elsewhere if they feel their FIs aren't doing enough.



Consumers expect FIs to use the most secure verification methods available, but there's a huge gap between expectation and reality.



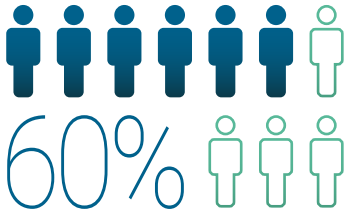
Just because consumers trust FIs doesn't mean they want to give up control, especially when it comes to security.



Unsiloed data and comprehensive analytics offer a secure solution in a world of frictionless experiences.

Where we are now: The current state of trust

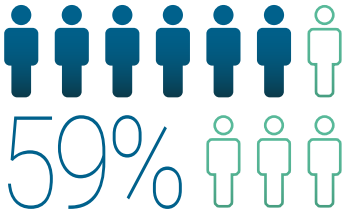
When it comes to security, customers look to FIs as the security experts. Authentication and fraud prevention are two of the largest elements of security, with consumer trust spread almost equally:



of respondents trust FIs to choose the most secure authentication methods.

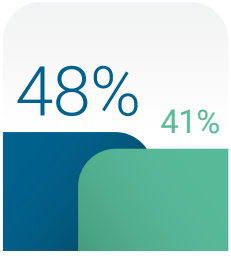


of respondents report that FIs correctly identify fraudulent transactions.

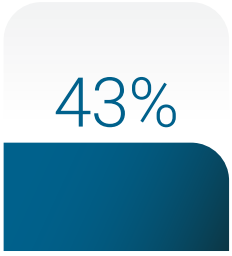


of customers trust their FIs to flag suspicious transactions without their review.

However, cracks are starting to show:



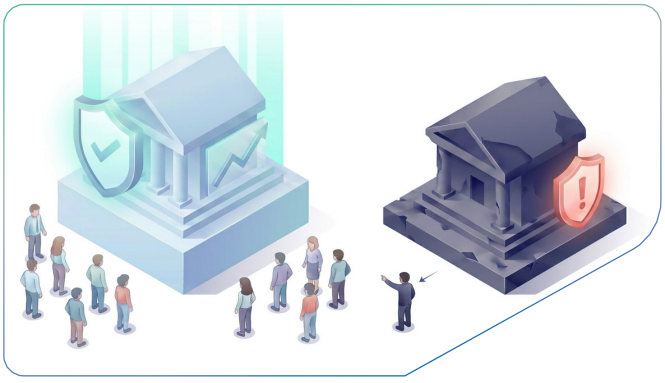
48% of consumers blame retailers for a lack of security when it comes to fraudulent transactions. But blaming FIs isn't far behind at 41%.



of consumers would consider leaving their FI based on the provided authentication methods.

Why it matters

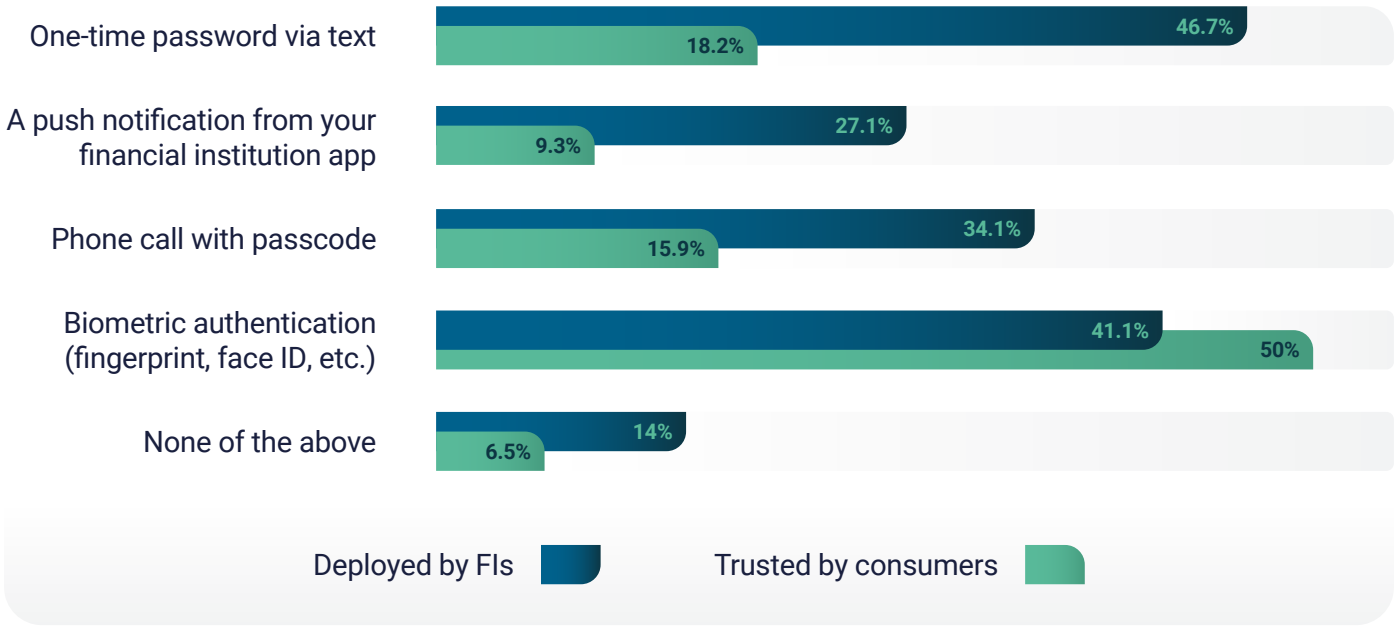
When asked what factors were most important when choosing an FI, over 90% of respondents cited security, indicating that fraud is top-of-mind for most consumers. And, with this heightened awareness, comes heightened scrutiny around best practices. FIs that fail to keep pace will be left behind by those that do. Rather than viewing security as a compliance issue, FIs should approach it as a competitive differentiator.



The great authentication debate

Security awareness isn't the only threat to consumer trust. There are also significant gaps between what consumers expect from their FIs and what they actually get, especially when it comes to identity authentication. From biometric data to one-time passwords (OTP), there are many methods for consumers to prove they are who they say they are. But some methods are more secure than others.

Authentication methods





OTP: Outdated and over-deployed

In the 2010s, OTP was considered the gold standard of authentication. Still, vulnerabilities around phishing and interception led it to fall out of favor with security experts, with consumer trust soon following suit. In our findings, only 18.2% of respondents believed it to be the most secure verification method. Despite this, OTP continues to be the most deployed method by FIs, with 46.7% of respondents reporting their institution uses it.

The main reason is legacy tech. FIs spent billions upgrading their systems in the early years of smartphones to accommodate surging mobile device use. Unfortunately, rising costs and shrinking budgets have left many FIs, especially community and regional institutions, locked into outdated systems with little room to upgrade.

However, newer security methods are becoming more affordable, like passkeys. Passkeys use FIDO2 (Fast IDentity Online) standards to generate a pair of linked keys. One, the public key, is freely shared with services, while the other, the private key, is securely stored on a specific device, making it resistant to interception. FIDO2 standards are also open-source, making the framework free-to-use, and therefore more affordable for smaller businesses.



Bring on the biometrics

While FIs' authentication methods have stagnated, consumers' have continued to evolve, with 50% placing their trust in biometrics. Since these methods rely on physical attributes, consumers perceive them as harder to steal and easier to use since they're always with you.

But biometrics have their own vulnerabilities, particularly in the age of AI. Voice cloning and deepfakes are now good enough to fool many security systems, while AI-enabled attacks allow scammers to inject malicious code to bypass live biometric checks using virtual cameras and deepfakes.

Social engineering is an equally significant, and growing, threat. Tactics like bank impersonation, investment scams, and romance scams manipulate consumers into authorizing fraudulent transactions themselves—a category referred to as authorized push payment (APP) fraud. Because these transactions look legitimate to the system, they can slip past authentication methods that only confirm identity rather than transaction intent.

A layered approach

As convenient as it would be, there is no single, foolproof method when it comes to authentication. Fraudsters are quick to adapt, even quicker with AI, and over-reliance on one method leaves accounts vulnerable. That's why cybersecurity experts are increasingly leaning toward layered approaches to authentication.





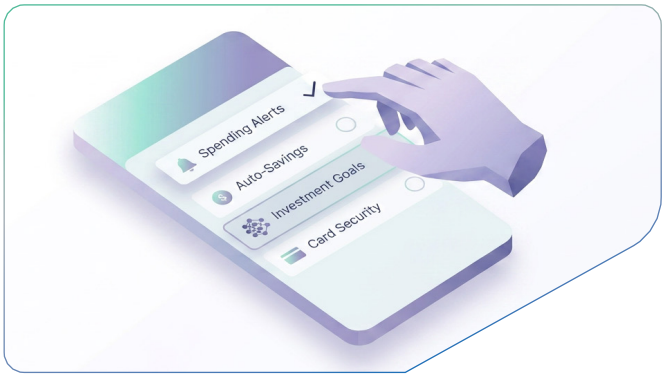
Why it matters

By using a mix of authentication methods, such as biometrics and passkeys, in conjunction with device signals, customer behavior and real-time fraud analysis, layered authentication creates a network of multiple security checkpoints and ongoing threat surveillance to make it harder for criminals to gain access without introducing more friction to the customer experience.



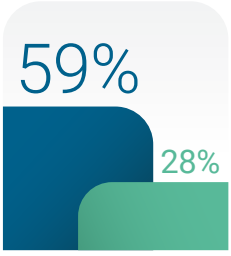
Preferences point to personal

One of the defining marks of the modern customer experience is personalization. Starting in the late 1990s with the popularization of the internet, there's been growing consumer demand for businesses to demonstrate that they know their customers as people. This demand has only increased as digital experiences and smartphones become more pervasive in everyday life.

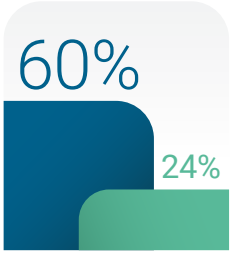


Control and choice

But there's more nuance to personalization than likes and dislikes; it's also about choice and control. While personal data and predictive algorithms have come a long way in delivering tailored experiences, customers still desire a level of fine-tuning for themselves even when there are high levels of trust.



While 59% of consumers trust their FIs to flag suspicious transactions without their review, 28% want an active role in what types of transactions are flagged for their approval.



While 60% of consumers trust their FIs to use the most secure authentication methods, 24% want to actively choose what methods they use.

The price of privacy

Part of this dissonance between trust and control comes from growing concerns around the access and use of personal data. According to PWC's Consumer Intelligence series, only 25% of Americans believe that companies handle their data responsibly. Another driver of this anxiety is the lack of transparency in how data is collected and used, not to mention the eventual fatigue many consumers experience after being overwhelmed with long, complex privacy agreements.





Why it matters

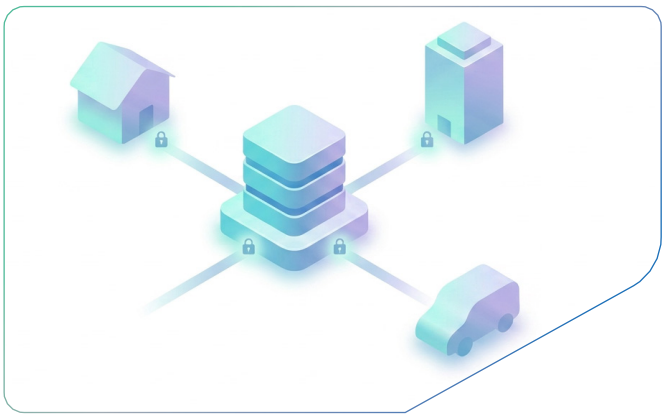
When consumers experience a lack of control in one area, they often try to make up for it elsewhere, hence a continued demand for a controlled user experience. Meeting this need and affording customers choices when it comes to security and privacy is one of the easiest ways FIs can reinforce trust.



Friction in a frictionless world

In addition to personalization, another must-have for the modern consumer is a frictionless customer experience. Today, one in three transactions are abandoned because consumers found the process too inconvenient. But when it comes to security, friction is essential, leaving FIs in a tough spot.

How can they add more security without taking away from convenience?



Lessons from a pandemic

Digital transformation projects were accelerated due to the new normal created by the COVID-19 pandemic. Faced with a fragmented, remote workforce, businesses needed data infrastructure that was centralized, but flexible, with users being able to access the data they needed no matter where they were. Adoption of these centralized data platforms led to surges in productivity across dozens of industries; however, not all industries complied.

"For too long, the industry has approached security from a siloed perspective, with authentication on one side and fraud identification on the other. This leaves them with a fragmented view that is at odds with the digitally integrated landscape of today. We need comprehensive solutions that look at fraud as a whole, not separate parts."

– Entersekt Chief Strategy Officer, Dewald Nolte

Two sides of the same coin

Concerns around data security and privacy, in addition to exorbitant costs and legacy systems, held the industry back from adopting centralized solutions in the past. But now, with advances in AI and real-time data analysis, these solutions aren't as out of reach as they once were.

FIs already collect data around customers' purchase behavior and monitor authentication events across multiple devices. By centralizing these elements and layering machine learning and AI on top, FIs could monitor and learn about fraud not just on an individual basis, but across institutions, without ever introducing another step to their consumers.



Building a trustworthy future

Both consumer preferences and fraud will continue to evolve as advances in technology reshape the digital landscape. While consumer trust in FIs remains high for now, that is not a guarantee if the industry is unable or unwilling to adapt alongside them.

43% of your customers are one authentication experience away from considering the competition—and the methods most institutions rely on today are the ones consumers trust least. Closing that gap doesn't mean choosing between security and convenience; it means deploying intelligent, adaptive authentication that layers protection behind the scenes while the customer experience stays effortless.

That is the work Entersekt does every day for financial institutions around the world, from community banks and credit unions to global brands. To see what your customers' authentication experience could look like—and to benchmark your current approach against the expectations documented in this report—visit entersekt.com or talk to our team.

The institutions that treat authentication as a competitive experience, not a compliance checkbox, will be the ones that keep the trust everyone else is losing.



entersekt
The Financial Authentication Company.

Appendix

Methodology: This report analyzes data from a May 2026 survey of 483 U.S. adults ages 18 and older with a focus on their current experience with their primary financial services provider. It explores consumer preferences and expectations regarding bank security, primarily around authentication and fraud prevention. Insights from this survey will help financial services providers identify what consumers are looking for in a digital banking experience and how new, modern security solutions can help meet demands without compromising security.

Participant demographics: Participants were based in the United States and all identified relationships with small financial institutions, such as regional and community banks and credit unions. The majority of participants (35.7%) identified as 55 and older, with a nearly even split between male (49.8%) and female (50.0%). 44.2% hold a high school diploma or equivalent, while 30.6% have a bachelor's degree. 45.6% are employed full-time, and 21.7% are retired. The largest bracket (33.4%) reports an annual household income of less than $50,000.