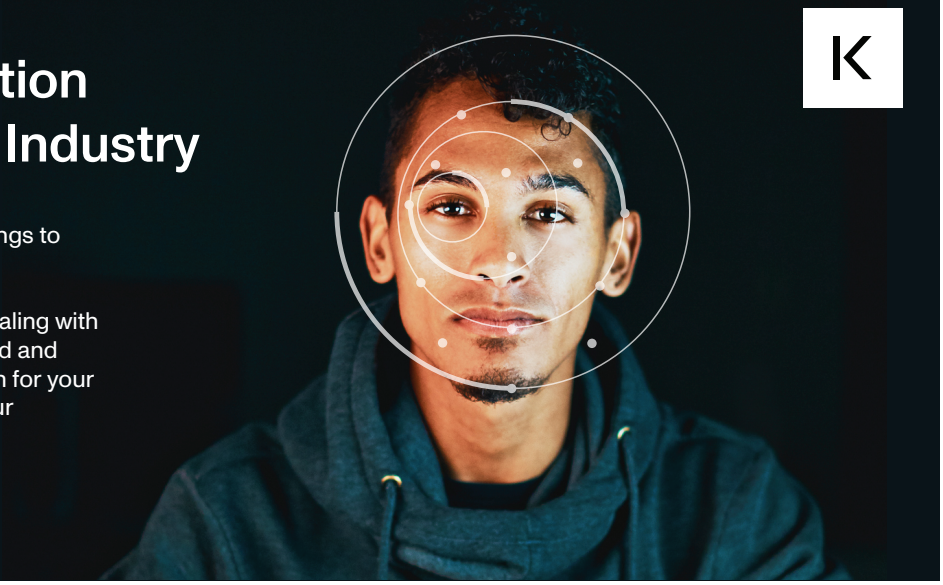
Consumer Authentication

Passwordless Authentication for the Financial Services Industry



For banks and financial platforms, there are countless things to consider when modernizing authentication security.

From balancing evolving compliance requirements, to dealing with rising customer expectations and mounting cases of fraud and account takeover threats, the right authentication solution for your organization will depend on what is most important to your business.

Here are five key things to consider when selecting a new authentication solution.

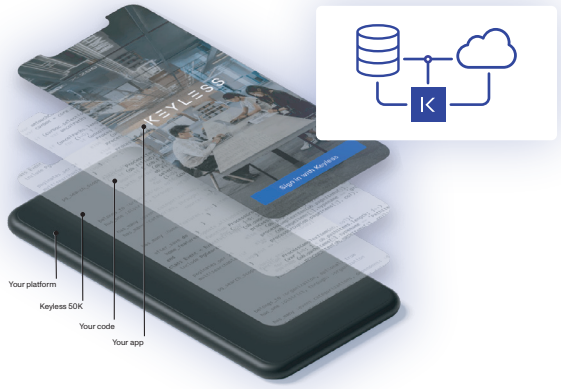
- Infastructure
- Competitiveness
- Compliance
- ROI
- Scalability

→ Cloud, On-premise, or Both?

Complementing your existing infrastructure

With institutional banks using incumbent technologies, and high-growth digital challengers using cloud-based systems, security models in the financial services industry are highly varied.

Your authentication provider should complement your organization's existing infrastructure, and be flexible enough to adapt to your digital transformation strategy – enabling long-term, continuous innovation and scalability. Vendors that can support you in either an on-premise or cloud environment will best future-proof your business.



→ Competitiveness

Supporting and scaling UX

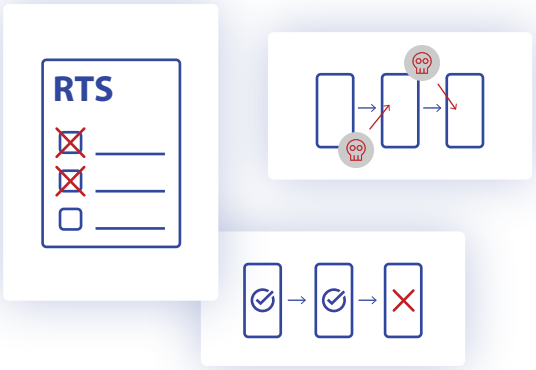
When it comes to banking, protecting customers' private data and accounts from fraud and security risks is paramount to your reputation. But that doesn't mean you need to settle for frustrating authentication journeys that ultimately drive customers away. Ideally, your authentication provider should help you provide consistent, stand-out experiences that keep your customers happy while simultaneously protecting them.

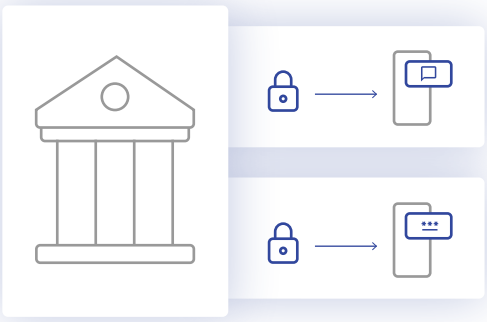
→ Compliance Readiness

Exceeding compliance requirements

Banks and fintechs have unique considerations when choosing an authentication solution. Regulations that are designed to protect customers from growing fraud and security threats, like GDPR, CCPA, and PDS2, must remain a priority.

Though it's necessary to adopt a platform that helps meet those criteria now, privacy-first solutions that combine advanced data encryption with standardization and scalability will help you stay ahead of the constantly evolving regulatory landscape.





→ Measuring Time-to-Value Metrics

Identifying and collecting ROI metrics to build your business case

Building a business case driven by ROI metrics will ensure that whatever solution you choose aligns with your organization's roadmap. Banks dedicate a significant amount of time and money every year to managing expensive, outdated authentication methods.

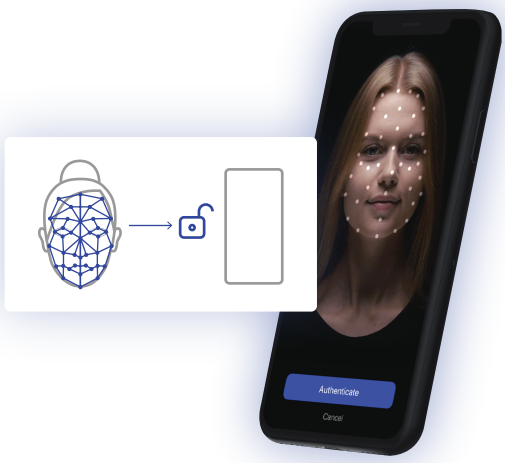
Performing password resets, sending one-time SMS codes to thousands of customers every day, and answering avoidable helpdesk calls (40% of which are customers looking for help with account access) burns a lot of budget. By calculating the productivity benefits and cost savings associated with phasing out old technology, you'll be able to clearly demonstrate the ROI of implementing a future-proof authentication solution.

→ Scalability

Scaling with your digital ecosystem as it grows

The authentication platform you choose must support the users, devices, and applications you rely on right now. But what about as your business scales?

Thanks to digital onboarding, banks and fintechs are experiencing hyper-growth, and need an authentication vendor to scale with them as they launch new services, shift strategies, and enter different markets. The right solution should be flexible, making it easy for you to deploy passwordless authentication where you need it most.



About Sift & Keyless

Sift is the leader in Digital Trust & Safety, empowering companies of every size to unlock new revenue without risk. Sift recently acquired Keyless, the pioneer in digital trust through patented privacy-preserving biometric technology. Together both companies now deliver frictionless authentication and payments experiences that eliminate account takeover (ATO) fraud and increase the security posture, while making it easy to comply with ever-changing regulatory requirements such as the GDPR or PSD2.