Identity in Banking: Securing Access

Across the digital corridors of global banking, a transformation is taking place. While most headlines focus on customer-facing innovations, such as faster payments, AI-driven investment tools, frictionless onboarding and engagement, or mobile-first platforms, the foundational question of who gets access to what—and importantly, how they are verified to enable that access—is not discussed as much.

Access controls, once a matter of physical credentials and perimeter defense, are now at the heart of a complex balancing act between secure access and protecting privacy in the digital domain. For banks and financial institutions, the stakes have never been higher: security threats grow more sophisticated by the day, threat vectors related to fraud, account takeover, synthetic identities and more abound, and yet the demand for seamless, real-time user experiences only seems to grow.

At the core lies a question of trust and identity.

The Growing Challenge of Verifying “Who's there”

For Chief Information Security and Compliance Officers and technology leaders, the task is no longer just about building stronger walls. It's about verifying every entry, action, and user, without interrupting operations or repeatedly compromising customers' personal data.

In large institutions, employees frequently need to access sensitive systems, from core banking platforms and risk engines to treasury and payments. Customers, too, access increasingly complex digital services, often initiating high-risk transactions from personal devices in unmonitored environments. As agentic AI tools come to market, these challenges are only exacerbated.

Traditional authentication methods, such as passwords, one-time passcodes (OTPs), and security questions, are now not so much a safeguard as they are a liability: easily forgotten, frequently reused, and notoriously vulnerable to phishing and social engineering. They fail to provide the certainty that modern banking demands.

Biometrics and Person-centric Access

As the need for reliable identity grows, many institutions are turning to biometrics, a method that ties access directly to the individual.

Unlike a password, your fingerprints cannot be fabricated, and your face cannot be convincingly forged. A biometric signature anchors access to the individual in a way that no static credential can. And in an era of deepfakes and synthetic images, IDEMIA's advanced solutions stand apart, robust enough to discern the genuine from the generated, ensuring that even the most sophisticated imitations cannot slip through.

In practice, biometric authentication offers a unique mix of security and ease: a fingerprint at the branch, a facial scan at a remote terminal, or a biometric login into the core banking system or risk dashboard. These interactions are faster and more intuitive than any token or code and ensure the actual customer is accessing their critical and sensitive services.

Some global banks are already seeing the benefits: fewer authentication failures, reduction in fraud, reduced credential-related support calls, improved auditability across systems, and perhaps most importantly, stronger trust in the integrity of every login.

Where Identity Begins: Onboarding

But the issue of identity doesn't begin at login, it begins at onboarding. For banks operating across regions and regulatory regimes, the Know Your Customer (KYC) process is an operational and compliance cornerstone. Increasingly, it's also a vulnerability, and in too many cases raises challenges to privacy when performed in remote or digital environments. Document-based verification, historically the standard in eKYC, is no longer sufficient. It is easy for scans to be manipulated, data to be stolen, and static checks cannot always guarantee authenticity. What's required today is proof of personhood.

Modern onboarding technologies now integrate biometric checks at the very first step. They authenticate government-issued IDs using optical and digital verification techniques, and match the document's photo with a real-time selfie. The inclusion of liveness detection embeds anti-spoofing measure that helps guard against the use of photos, masks, and even synthetic deepfakes. Importantly, these elements can be securely bound to the user's device and underlying personal identifying information can be secured and protected.

This approach doesn't just satisfy regulators. It creates faster, more secure onboarding experiences for customers, especially for digital-first users entering through mobile channels. The reusable verifiable credentials add yet another layer of trust, enabling individuals to permission their credential for instant KYC verification. Bound to biometrics, this fusion becomes exceptionally powerful, delivering both the regulatory assurance institutions require, and the speed, control, and confidence consumers seek at the very start of their digital journey. In today's digitally-native and cross-border financial services environment, this type of application is becoming increasingly relevant, and enables a more seamless customer experience while providing enhanced protective measures on sensitive customer data.

Securing Access Across Systems and Contexts

What makes biometric authentication particularly versatile is its adaptability. It works across platforms, whether it's a teller logging into a branch terminal, a remote risk analyst accessing Citrix, or a customer approving a wire transfer through a mobile app. It works in different configurations: in-band, embedded directly into a banking system's access flow, as well as out-of-band, through a companion mobile app or secondary verification channel.

For organizations with hybrid workforces or geographically dispersed branches, this flexibility means authentication can continue even when internet connections are unreliable or infrastructure varies. While multi-factor authentication (MFA) continues to be widely adopted, biometrics add a layer of confidence and simplicity that strengthens, rather than complicates, the security model.

Lessons Beyond Banking

Though the financial sector has some of the strictest compliance and security demands of any industry, the questions it faces around identity and access are not unique. All kinds of enterprises, particularly highly regulated sectors that handle confidential client personal data (e.g. education certifications, health records, etc.) or financial assets, are grappling with the same set of challenges: How do we know who is accessing critical systems? Can we verify it in real time, without friction? Is the system resilient enough to adapt as our workforce—and risks—evolve?

From consulting firms managing cross-border deals to finance departments in global multinationals, the need for trusted, scalable identity infrastructure is becoming universal.

A Strategic Shift

What was once considered a back-end IT issue is now recognized as a strategic priority. Access is no longer just a technical problem; it's a business risk, a reputational exposure, and a test of operational maturity. In this environment, biometrics are gaining ground, not because they are futuristic, but because they offer something increasingly rare: a simple, secure answer to the question of trust. As online activity and commerce grow and applications and services are increasingly digitally native, such tooling becomes essential for both reducing friction and enhancing controls.

Powered by IDEMIA Public Security

IDEMIA Public Security's platform enables financial institutions to modernize employee and customer access through a biometric identity layer that seamlessly integrates document authentication, liveness detection, and secure access—all in real time.

With deployments across global banking environments, IDEMIA Public Security's solutions enable seamless login to systems like Windows, Citrix, and core banking platforms, while also powering secure onboarding and compliance-ready eKYC workflows. These capabilities are already in use across some of the world's most security-conscious institutions. With IDEMIA Public Security solutions, banks aren't just prepared for the future—they're equipped to lead it with confidence.

Photo: IDEMIA