KEYLESS

8 Considerations for Banks Implementing Biometric Authentication

Contents

Introduction

Strong and user-friendly customer authentication is a critical aspect of any secure system. It represents the first line of defense against account compromise, data exfiltration, and identity theft.

For banks, two-factor authentication (2FA) is a universally-used approach to mitigate several of the issues associated with passwords. It is a core element of Strong Customer Authentication (SCA), a requirement under the Payment Services Directive 2 (PSD2) in Europe that mandates the use of multi-factor authentication to increase the security of electronic payments. Done well, a multi-factor authentication system prevents the attacker from authenticating even when one of the factors has been compromised.

Today, passwords are the most common authentication method. Unfortunately, they also represent a significant source of vulnerabilities. Thankfully, they are now vanishingly rare as a single authentication factor in the banking industry. However, many commonly-used possession factors in use today are phishable. For instance, a security code sent to the user via email can be forwarded to the attacker, and a 6-digit code can be read to a scammer over the phone. Similarly, text messages can be captured by a fraudster as part of a SIM-swap attack, where the fraudster “steals” the user’s cell phone number via a social engineering attack against the user’s cell phone operator.

The good news is that harder-to-phish authentication factors exist. Among these, biometrics stand out as secure, usable, and convenient. Modern biometric authentication systems have exceedingly low error rates, can authenticate the user in a fraction of a second, and require little to no user training. They are exceedingly popular in the banking industry, with more than half of credit cardholders saying they would switch banks if their current bank doesn’t offer biometric authentication options.[1]

Biometrics also incorporate identity assurance, a key concept that is crucial to understand and will be referenced several times in this whitepaper. Identity assurance ensures that a person's claimed identity is their real identity at all times. In other words, that you can trust that they are really who they say they are. Take an SMS OTP for example—if someone enters a code that does not prove they are the account holder, the genuine person that enrolled. The ability to prove the genuine identity of the person authenticating or, in other words, making sure that the person holding the device is who they say they are, is integral to biometric authentication.

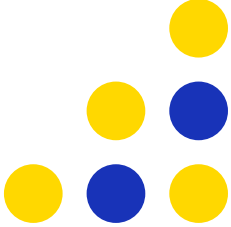
[1] https://usa.visa.com/visa-everywhere/blog/bdp/2020/01/02/banking-on-biometrics-1578003687083.html...

The 5 Primary Authentication Factors

Not all authentication methods are created equal. Each has their advantages and disadvantages but the combination of inherence and possession avoids many of the pitfalls associated with knowledge factors. This is becoming widely acknowledged, but the market has not followed as swiftly as some would like. As recently as 2022, 85% of US banks rely on username-password as the primary way to authenticate returning customers.[2]

Authentication Method	Description	Advantages	Disadvantages
Passwords and PINs	User-created string of characters or personal identification number.	Simple and widely understood; easy to implement across various platforms.	Can be forgotten or shared. Vulnerable to phishing, brute force attacks, and leaks. Do not prove identity.
Email and SMS OTPs	One-time codes or login links sent via email or text. Common for customer password resets.	User friendly, accessible, and widespread.	Prone to phishing. A compromised email can be used to access multiple accounts. Does not prove identity.
Hardware and FIDO Tokens	Physical devices generating unique codes.	Immune to malware and distinct from devices.	No identity assurance, easily lost, and costly. Inconvenience of needing to carry it. Does not prove identity.
App-Based Authentication e.g. Google Authenticator	Uses smartphone apps for QR code scanning or push notifications.	Convenient as users are familiar with apps.	Device is single point of failure. Lost device requires account recovery, does not prove identity.
Biometrics	Uses unique traits like fingerprints or facial features.	Offers high security due to difficulty of replication. Proves genuine identity assurance and cannot be lost or forgotten.	Can raise privacy concerns. Some biometrics require re-enrollment; local biometrics do not provide genuine identity assurance (see "The 3 Biometric Authentication Systems").

One of the biggest advantages of traditional authentication systems such as passwords, PINs, email, and SMS OTPs is that they are well known. Users and customers are comfortable with them, which reduces friction during adoption. However, a significant similarity across these methods is the lack of identity assurance—even some biometrics do not prove identity.



[2] https://www.celent.com/insights/438986014...

The 3 Biometric Authentication Systems

Biometrics offer the best combination of security and usability when compared to passwords, PINs, SMS OTPs, and hard tokens. By authenticating someone using their biometric traits, there's nothing that can be forgotten and nothing that can be lost.

But as with other authentication methods, biometric systems are also not all equal. They differ in how a user's biometric data is processed and stored. When an enrollment or authentication image is taken, that biometric data has to be stored somewhere in order to be used to authenticate the person. Each system deals with this data differently, and can be evaluated on three different aspects.

Security: The system's ability to reduce the risk of account takeovers.

Privacy: Protecting the biometric data needed to authenticate users.

User Experience: Making the authentication process as effortless as possible for the customer.

Biometric System	Description	Security	Privacy	User Experience
Local / Device-Native	Biometric data never leaves the device.	Weak. Remote services cannot confirm if the user truly provided their biometric input.	Strong. Biometric data never leaves the device.	Moderate. Can be used offline but biometrics are tied to the device.
Centralized / Server-Side	Biometric data leaves the device in encrypted form. Server has access to the user's biometric data.	Strong. Can authenticate users to remote services such as online banking.	Weak. Matching a fresh biometric sample requires the server to decrypt user data, risking full data disclosure if the server is compromised.	Strong. Biometrics are not tied to the operating system.
Decentralized	Biometric data leaves the device in encrypted form. Server does not have access to the user's biometric data.	Strong. Can authenticate users to remote services such as online banking.	Strong. Biometric leaves the device in encrypted form.	Strong. Biometrics are not tied to the operating system.

[2] https://www.celent.com/insights/438986014...

Local Biometrics

Also known as device-native or platform authentication, local biometric matching is commonly used by smartphone, tablet, and laptop vendors—a classic example being FaceID. With this approach, the user's biometric template is stored on the device, never leaving it. This offers strong privacy benefits as data is not sent over the cloud, but comes with security and usability drawbacks.

Only local authentication events, such as unlocking your phone or accessing apps on your device, can verify biometric authentication. Remote services, like online banking or cloud-based applications, cannot confirm if the user truly provided their biometric input. Therefore, local biometrics are often considered a possession factor, not a biometric factor, for remote services.

Further, if a device is lost or stolen, the biometric template becomes unavailable and the user will need to re-enroll. As a result, the new device and all its applications cannot determine whether the newly-enrolled user is the same as the user on the old device. This opens the door to various attacks where a fraudster can claim that the user lost their device and then enroll their own biometric data. It can also prove costly for companies that use call-center and SMS-based authentication for account recovery.

Local authentication also does not support identity portability, meaning a user cannot enroll on one device and then use their biometrics to authenticate on another.

Centralized Biometrics

A centralized, or server-side system stores biometric data on a cloud server. Biometric data is captured on the device and then stored on a server. This approach provides security and usability benefits but reduces privacy and data confidentiality.

Here, no biometric data is stored on the user's device. Instead, the user's template is stored on a server, often in encrypted form. When the user wants to authenticate, they send a new biometric sample to the server. The server decrypts the template and matches it against the sample. This method is used by almost all cloud-based biometric systems today.

Server-side matching is better for authenticating users to remote services such as online banking. The server can confirm that biometric authentication occurred and communicate this to third parties securely. Additionally, the same server-side biometric template can be used across multiple devices, improving portability and security if a user's device is lost, stolen, or replaced.

However, this method significantly reduces biometric privacy compared to local matching. While data can be encrypted during transit and storage, traditional server-side systems don't protect it during use. To match a new biometric sample with the stored template, both must be unencrypted on the server. This means the server must have the ability to decrypt the user's template. As a result, if the server is compromised all biometric data can be exposed, leading to potential identity theft, unauthorized tracking, and other abuses.

Decentralized Biometrics

The decentralized approach has emerged as a way to address the privacy issues associated with server-side biometric authentication. In its 2023 Innovation Insight for Biometric Authentication,[3] Gartner defines decentralized systems as biometric authentication systems that are neither local nor centralized. This approach is still nascent, and its exact definition within the biometric authentication space is yet to be fully agreed on.

Biometric systems offering a decentralized approach are built with the intention of preserving privacy. A successful decentralized system not only addresses privacy issues associated with centralized biometrics, but the security and usability drawbacks of local systems too. In the decentralized model used by several commercial solutions, multiple servers store and process pieces, or "shares," of a user's biometric data. Each server matches only its part of the biometric template during authentication. While this method aims to enhance privacy, it is flawed since vendors often control enough shares to reconstruct the full biometric data. This setup is vulnerable to attacks, as compromising a few servers can expose all biometric data. Moreover, such systems struggle with compliance issues, especially under GDPR, which treats any reconstructible biometric data as highly sensitive. This has led to regulatory scrutiny and fines for companies using server-side biometrics.

That said, a groundbreaking approach that uses secure Multi-Party Computation (sMPC), a privacy-preserving cryptographic technique, has been established to overcome the flaws of previous decentralized models.

This method involves two steps:

1. During enrollment, a biometric profile is captured, transformed on the user's device using sMPC, and stored on the cloud. No biometric information can be extracted from this profile, ensuring that neither the cloud service provider nor even the vendor can link it to the user's face.

2. During authentication, another sample is captured, transformed, and compared with the stored profile using the sMPC protocol. By comparing two encrypted profiles, biometric data is protected in use, at rest, and in transit, offering the privacy benefits of local authentication with the security and portability of server-side biometrics.

[3] https://www.gartner.com/en/documents/5048531...

The Most Common Account Takeover Fraud Types Affecting Banks

Banking fraud is as old as banks themselves. From counterfeit coins in ancient Mesopotamia to forged documents in Roman banking, financial institutions have always faced deceit.

Account takeovers, a fraud attack where a third party gains unauthorized access to a user's account and takes control of it, are the modern plague affecting banks. A 2024 report by the Federal Trade Commission (FTC) reported a 14% increase in reported losses from 2022 to 2023.[4]

The most common account takeover fraud types are split between the below 7 threat vectors:

Account Selling and Monetization: Hackers use compromised accounts to transfer money, make purchases, or sell credentials on the dark web, especially targeting accounts with valuable data.

Credential Stuffing: Attackers exploit stolen login credentials to access multiple accounts across different platforms, relying on users' tendency to reuse passwords.

Deepfakes: Attackers use AI-generated images to spoof identity verification processes that require users to take a selfie.

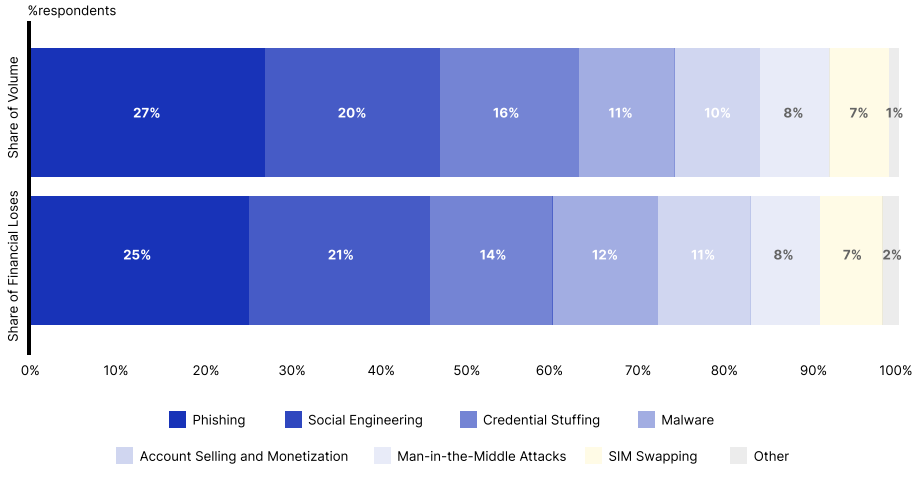
Malware: Malicious software like Trojans and spyware can capture login credentials by recording keystrokes or manipulating legitimate banking apps, and hijack banking sessions by stealing session cookies.

Man-in-the-Middle (MitM) Attacks: Attackers can set up fake websites to trick users into paying for items that won't ever arrive or intercept SMS communications between two parties, capturing sensitive information such as OTPs to access their accounts.

Phishing: Scammers use emails, texts, or fake websites to trick individuals into revealing login credentials by pretending to be trustworthy entities.

SIM Swapping: Fraudsters convince mobile carriers to transfer a victim's phone number to their own SIM card, allowing them to intercept SMS authentication codes and access secured accounts.

Social Engineering: Exploiting human psychology, attackers extract sensitive information through methods like pretexting, baiting, and quid pro quo schemes.

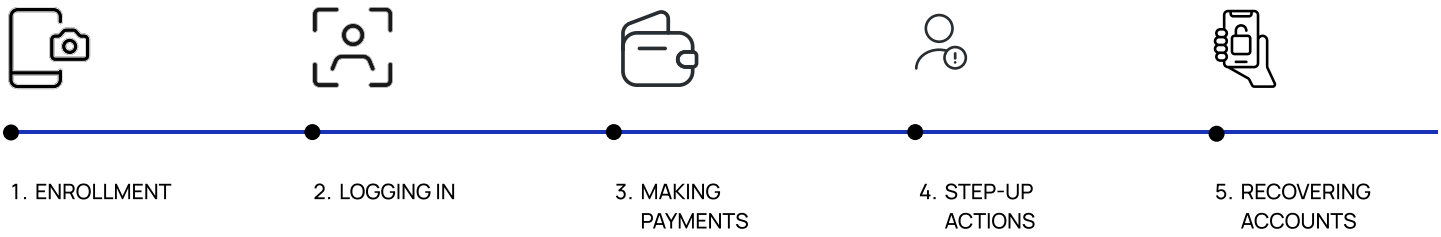


The table to your left ranks the most significant ATO threat vectors by total share of both volume and financial losses according to Liminal Research. Phishing is the most common method attackers use to access user accounts, underlining the market need for phishing-resistant authentication methods. This is closely followed by credential stuffing and social engineering.

[4] FTC (February 2024), "As Nationwide Fraud Losses Top $10 Billion in 2023, FTC Steps Up Efforts to Protect the Public."...

Key Use Cases for Biometrics in Banking (Recovery, Step-Up)

There are five core use cases for biometrics within the banking sphere:



Digital Onboarding via IDV Provider: Biometrics are used by IDV providers by capturing a user's face and then comparing it with a government-issued ID - an integral part of any KYC check. But users don't want to re-upload their identity document each time. This is where authentication comes into play. Some IDV providers also offer biometric authentication, but the majority do not, and those that do not offer the privacy-preserving capabilities of a decentralized model. As a result, IDVs will often partner with an authentication provider to sell a combined solution.

Login: Biometric logins replace traditional methods such as hard tokens. By using biometrics, banks can effectively prevent account takeovers and greatly enhance the user experience by verifying the genuine identity of the person logging in.

Payments: Many banks still use SMS OTPs as a second authentication factor, but this method is prone to fraud. The frequent advisory to "DO NOT SHARE THIS NUMBER WITH ANYONE" that comes with SMS-based codes highlights the risks involved. Since SMS OTPs can be easily intercepted or phished, they are a weak link in the security chain. Switching to more secure methods like biometrics is crucial to improving security and protecting customer accounts from fraud.

Step-Up Authentication: This is used for actions that carry higher risk, such as changing personal details like passwords or addresses. Biometrics can effectively secure these areas.

Account Recovery: Account recovery fraud is a common but often overlooked cyber threat. A gateway to account takeovers, account recovery fraud enjoys particularly high success rates. Account recovery is also costly. According to Forrester, the support costs related to passwords can run into the millions every year.[5] This is often split between SMS OTPs and customer call centers. Biometric authentication can be used at the account recovery step by complementing - or even replacing - customer helpdesks. Instead of using a support center to manually reset passwords, biometrics can be used to enable self-service account recovery.

[5] https://www.keepersecurity.com/assets/pdf/Keeper-White-Paper-Forrester-Report.pdf...

Biometrics as a Cost-Savings Strategy

When considering biometrics as a cost-savings strategy, it's worth looking at how much each authentication method costs to implement and maintain.

The costs of different authentication methods vary significantly:

- Passwords and PINs: Although these do not incur issuance or maintenance costs, recovery and customer support requirements can make these expensive to maintain.
- Email OTPs: Free to send, provided the user has access to data.
- SMS OTPs: These can be expensive to run, with costs varying by provider and country.
- Hard Tokens: These are also costly as they require constant replacing and reissuing hard tokens is costly.
- Biometrics: Generally inexpensive to operate, with costs depending on the provider's pricing model.

Pricing Models for Biometrics:

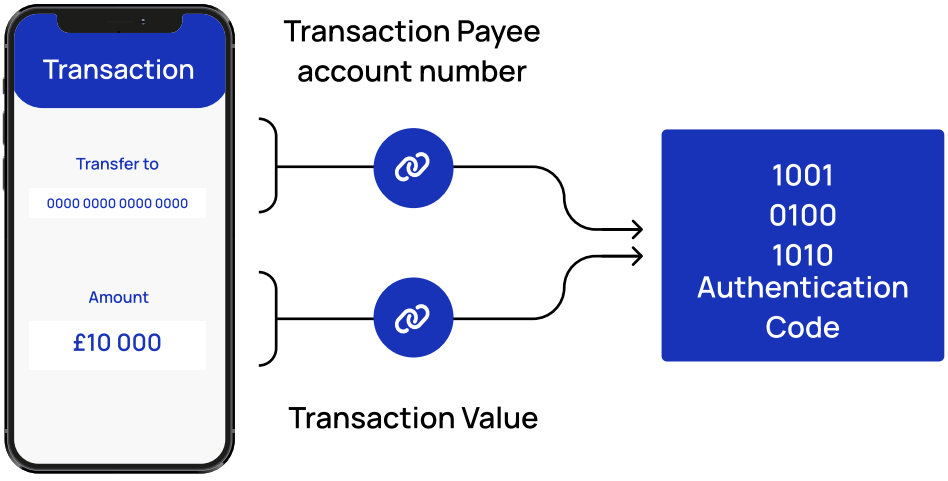
- Per-transaction Pricing: This model involves charging banks for each authentication, similar to customer help desks, where each user action incurs a cost. This can lead to high expenses.
- Per-user Pricing: This model charges based on the number of active users per month, allowing unlimited authentications without additional costs.

Biometrics with PSD2 SCA

In the EU, PSD2/SCA mandates that all EU banks authenticate the identity of their customers by using at least two independent authentication factors and dynamically link transaction amount and account number.

Dynamic Linking

The authentication code generated shall be specific to the amount and the payee agreed to by the payer when initiating the transaction.



In addition, the updated payment regulations also require the creation of a dynamic link – this additional authentication element dynamically links the transaction amount and the account number of the payee in a code to be authenticated. This is typically done by generating a unique and independent one-time code before each successful transaction.

Integrating Identity Verification and Authentication

Identity verification (IDV) and authentication are essential parts of a biometric identity system in banking. Typically, users go through a one-time ID verification using a government-issued ID. For future actions like logging in, making payments, updating sensitive information, or recovering accounts, they use biometric authentication against the initial verification image.

However, users often need to sign up separately for IDV and authentication services, while in other cases identity verification and authentication are not integrated at all. To simplify this process, banks can adopt an integrated approach that lets users authenticate with a third-party provider without additional sign-ups. This ensures that users who have completed the one-time IDV step can authenticate without needing to enroll again.

End-User Benefits

- **Existing Users:** Users already verified with an IDV are passively enrolled through a backend bulk integration.
- **New Users:** Users enrolling with an IDV are automatically enrolled in the biometric authentication system.
- **Other Users**: Those not verified with an IDV can enroll via SDK or web.

There are also benefits for banks and IDVs. Banks can quickly implement biometric multi-factor authentication (MFA) across their entire user base and IDVs can offer integrated biometric authentication services without separate enrollments, making it easier to sell combined solutions.
This integrated approach ensures compatibility across multiple IDVs, streamlining processes and improving overall security, usability, and efficiency in user authentication and verification.

Integrating a Biometric System

This section outlines what an integration overview for a biometric authentication provider would look like if implemented in a banking environment.

Enrollment

Users must enroll their biometric data. Preferably, this involves a connector or feature that allows an authentication provider to work with any number of a bank's existing IDV providers so that users can authenticate without enrolling with an authentication provider. If not, users would need to register their biometric features using an SDK provided by the authentication provider.

Authentication

Users receive a push notification when they try to access a resource. They authenticate using their biometrics, and the result is sent to the mobile application's backend. The backend uses APIs to perform necessary security checks, and upon successful verification, access is granted.

Key Components

- SDK: The relevant SDK would need to support both Android and iOS platforms, and provide methods for enrolling users, authenticating, de-enrolling, and restoring backups.
- Backend Service: The backend service would need to offer APIs for performing security checks through backend-to-backend calls. After the SDK returns a successful authentication response, these APIs can be used to further verify and secure the transaction.

By streamlining the enrollment and authentication processes and leveraging robust backend services, banks can offer a more secure and efficient way for users to access their accounts and perform transactions. This integration minimizes the risks associated with traditional authentication methods and provides a seamless user experience.

Conclusion

Biometric systems, whether local, centralized, or decentralized, offer varying degrees of security, privacy, and user experience. But on the whole, biometric authentication does offer a more secure, user-friendly, and more cost-effective alternative to traditional methods like passwords, PINs, and SMS OTPs, which are susceptible to fraud.

Implementing an integrated approach that combines identity verification with biometric authentication is key to streamlining the enrollment and ongoing authentication processes. Leveraging these technologies also allows banks to better meet regulatory requirements. As the banking industry continues to evolve, adopting biometric authentication will be crucial for reducing account takeover fraud, providing a better customer experience, and saving costs related to account recovery.