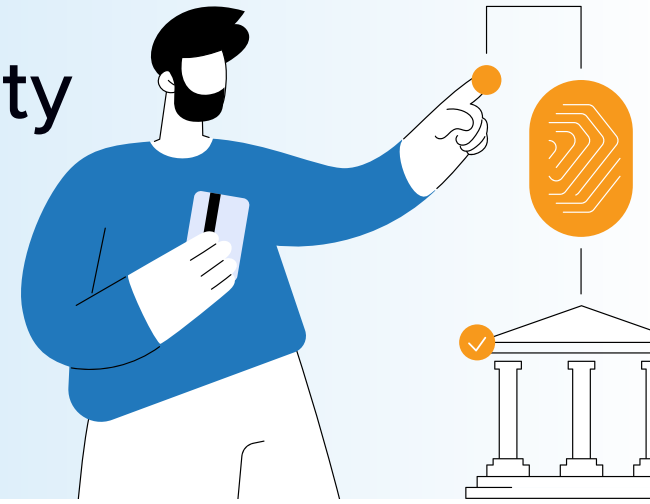
Improving Customer Experience and Security in the Finance Sector with Passwordless Authentication



Ensuring security is one of the biggest challenges in the digital business era, and for financial institutions it is even more acute. Digital banking still relies on traditional means of authentication, like passwords or PINs, which are neither convenient to use nor secure. Even Bill Burr, the former National Institute of Standards and Technology (NIST) manager known as the father of the modern password, today admits: "Much of what I did I now regret." Solutions that are better than passwords are now available, and consumers are opening up to new approaches such as biometrics. But the reality remains that more than 70% of consumers use usernames/passwords most frequently, followed by biometrics with around 25%, according to a 2021 PYMNTS report .

Trust is key for financial institutions, but the financial sector is among the sectors most targeted by cybercriminals. Breaches can cause massive damage to an organization's reputation, to customer trust, and financially. The average cost of a data breach for financial organizations was $5.97 million in 2022, the second highest average among all verticals (after healthcare)[1].

According to the IBM/Ponemon study, **multifactor authentication mitigates the cost of breaches by an average of $187,000**

Consumers demand top-notch security, but also look for simplicity and convenience. Not surprisingly, security is therefore also a key priority for regulators, which have introduced and tightened measures such as the new rules on Strong Customer Authentication (SCA). This has reduced online fraud but added friction to ecommerce checkout processes. Friction, of course, negatively impacts customer experiences (CX) and has increased shopping cart abandonment for merchants and impacted transaction revenues for financial institutions. This calls for a difficult balance of security and convenience. Technology can move the needle towards frictionless security, but requires a concerted effort by all stakeholders, including consumers, FSIs, merchants, payment providers, and technology providers.

The Fast Identity Online (FIDO) Alliance is a collaborative effort that has evolved over the past decade to develop strong authentication standards that enable organizations to reduce their dependence on password-based authentication. The FIDO2 standards, announced in 2019, significantly expanded the capabilities that FIDO-based authentication offered, as well as incorporating an open web standard (WebAuthn). Significantly, FIDO2 also gained the support of one of the technology industry's most important players, Apple, which joined Google and Microsoft (and many others) in the alliance. This means that FIDO2-based authentication is now supported by the three main providers of operating systems for mobile and desktop devices as well as platforms that organizations and end users worldwide depend upon.

What is clear is that there is no quick fix, but the financial industry is moving towards a risk-based, data-driven authentication strategy. This means differentiating between high- and low-risk transactions with different authentication levels, using various authentication methods in parallel, and to using behavioral patterns to detect suspicious transactions to deliver the most convenient and secure customer experience possible.

[1] IBM and Ponemon Institute, Cost of a Data Breach Report 2022
[2] Mastercard New Payments Index 2022

[1] https://www.pymnts.com/wp-content/uploads/2021/07/PYMNTS-Generation-Connected-July-2021.pdf

Building the Future of Authentication and Payments

Advanced Authentication Challenges

- 89% of finance organizations still use a username/password combination to log on to some of their corporate applications. This represents a significant security risk.
- A 2021 IDC survey found that at 85% of finance companies, senior management or the board had requested an identity security technology review to assess exposures.
- Password/username still dominates the authentication of online banking, with 65% of consumers having used it in the past 30 days, but biometric authentication is gaining ground with 47%.
- Finance companies need to adopt a clear strategy for the use of advanced MFA. This needs to cover the technology platform, the definition and optimization of security policies, and the implementation of risk-based authentication mechanisms to ensure robust security controls that do not impact customer experience.

Secure Payments Challenges

- As PSD2 took full effect in 2021, conversion rates of online payments dropped due to SCA requirements mandating two factor authentication (2FA) for most online transactions. In September 2021, an average of 29% of transactions failed in Europe, meaning almost a third of online transactions failed due to a 2FA challenge. This resulted in loses that may have reached €90 billion for online merchants in 2021. These opportunity costs are 11 times higher than the actual cost of fraud.
- 2021 clearly was a disruptive year given that SCA was new for many consumers and merchants. EBA data from June 2021 shows a massive surge of adoption, stating that 82% of payment services users are subscribed to a SCA solution and 99% of EU merchants supported SCA. The data also shows a considerable reduction of fraud from 2020 to 2021 .
- SCA allows for exceptions to 2FA, such as low transaction value, recurring payments, trusted beneficiaries and the use of transaction risk analysis. Managing and optimizing exceptions using a data-driven approach will be instrumental in reducing friction and improving security further.

[4] PYMNTS: Consumer Authentication Preferences for Online Banking and Transactions, Jan 2023
[5] https://cmspi.com/eur/en/resources/content/strong-customer-authentication-sca-impact-assessment-september-2021/
[6] EBA Report on Data Provided by PSP on their readiness to apply SCA for E-Commerce card-based Payment Transactions, EBA/REP/2021/16, June 2021

The Future of Authentication

- The work of the FIDO Alliance and all its members has provided the standards basis for the development of robust, interoperable, and easy-to-adopt authentication solutions that are available for all financial and commercial entities to safeguard digital transactions.
- Passwordless authentication based on FIDO2 standards can be implemented in almost any platform and has reached mainstream recognition and adoption.
- Biometric authentication factors continue to be developed, and sensors incorporated into hardware and software platforms provide both biometric and behavioral biometrics, enabling organizations to move away from high-risk username/password authentication.
- Passkeys, based on FIDO standards, are a major advance in the shift away from passwords. Combining strong authentication with a streamlined user experience, these will rapidly become a pervasive authentication option for websites and services worldwide.

The Future of Frictionless Payments

- Although 2FA can be a cause for increased cart abandonment if it introduces friction (like OTPs), moving away from classic 2FA schemes towards modern and frictionless FIDO authentication will certainly improve the user experience and reduce risk combined with consumer familiarity. Smarter use of exemptions and adaptation of exemptions rules to market needs can further improve the user experience. FSIs should invest in both FIDO-based authentication solutions and data-driven capabilities to use exceptions for low-risk transactions:
  - **Transaction risk analysis (TRA)** is based on a dynamic friction strategy to ensure that the experience of legitimate customers is not affected by unnecessary friction. Real-time risk analysis checks for six risk factors to classify transactions.
  - **Risk-based authentication (RBA)** applies similar principles, assessing the probability of account compromise with each login. If a request seems unusual or suspect, the user must take additional steps to gain access.
  - **Passkeys (WebAuthn)** utilize elements of the FIDO standard specific to public/private key design, offering a distinct improvement over a username and password in browsers and mobile apps.
  - **Fully-fledged FIDO certified authentication (FIDO UAF)** provides full control over the authentication stack, transaction signing, and strong device binding for mobile apps.

Key takeaways:

Optimize Customer Authentication to Manage Risk:

Passwordless authentication is a major step toward improving security while minimizing friction. A holistic approach is needed that embeds Passwordless authentication in a holistic, risk-based approach that allows for the orchestration of all the security tools at a bank's disposal to ensure less friction does not come at the cost of fraud.

Deliver Better Customer Experiences:

Banks that take CX seriously should look to eliminate any element of friction and any vulnerability in the authentication process. Biometrics make authentication processes as straightforward for users as unlocking their phone. With FIDO-based technology under the hood, the second factor is invisible to the user, making two-factor authentication feel like one factor.

Deploy Multilayered and Invisible Security:

Authentication will become increasingly frictionless and invisible as banks use a variety of factors checked in the background. Passive factors like location, malware checks, behavioral patterns, and passkeys can be confirmed without any action by the consumer. This will reduce the need for active 2FA as regulation adapts to the rapid evolution of technology.

Message from the Sponsor

For the last 170+ years, our mission has been to create innovative solutions that safeguard critical industrial sectors. With G+D as a partner, banks and financial institutions can concentrate on their core business — without having to constantly worry about how to safeguard their customers.

Partner with the trusted experts at G+D

Convego AUTH-U: Shaping the way you authenticate

Giesecke+Devrient

IDC

Info Snapshot, sponsored by Giesecke+Devrient
May 2023 | IDC #EUR150672323

@idc @idc idc.com