THE PASSWORDLESS SOLUTION TO PSD2

STRONG CUSTOMER AUTHENTICATION

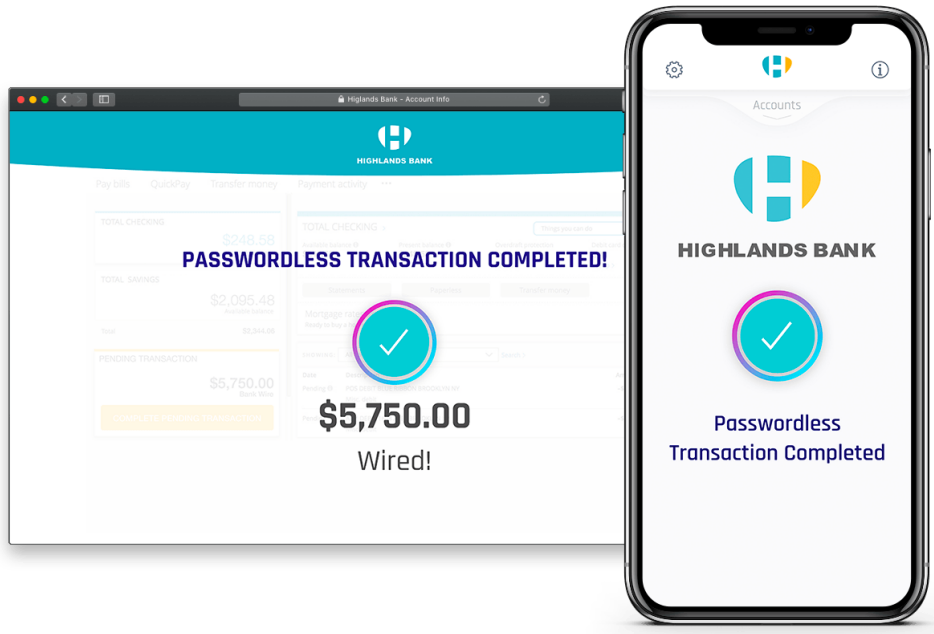
Are YOU Ready for SCA Requirements?

As of January 1st, 2021, companies doing business in the European Union must comply with Payment Services Directive (PSD2) requirements. One of those requirements is SCA, or "Strong Customer Authentication", which requires that all customer-facing applications must now utilize multi-factor authentication.

PSD2 contains significant guidelines for how MFA should be implemented. For example, Section 9.3 of the Regulatory Technical Standards (RTS) describes the use of "separated software execution environments" for enabling Strong Customer Authentication. At a high level this implies that passwords and legacy 2-Factor Authentication (2FA) have become insufficient for securing consumer transactions. For example, password-based authentication takes place on the server-side and relies on shared secrets. It does not make use of a "separated software execution environment."

The above example is just one instance of the many technical nuances of PSD2 that have caused friction for business leaders and application developers. Another less obvious hurdle? Multi-factor authentication simply isn't widely adopted by customers.

This guide explains why True Passwordless Authentication is being adopted as the optimal solution for SCA, and how it is enabling industry leaders such as Mastercard, Rakuten, and CVS Health to achieve PSD2-Compliant authentication while providing users a pristine customer experience.

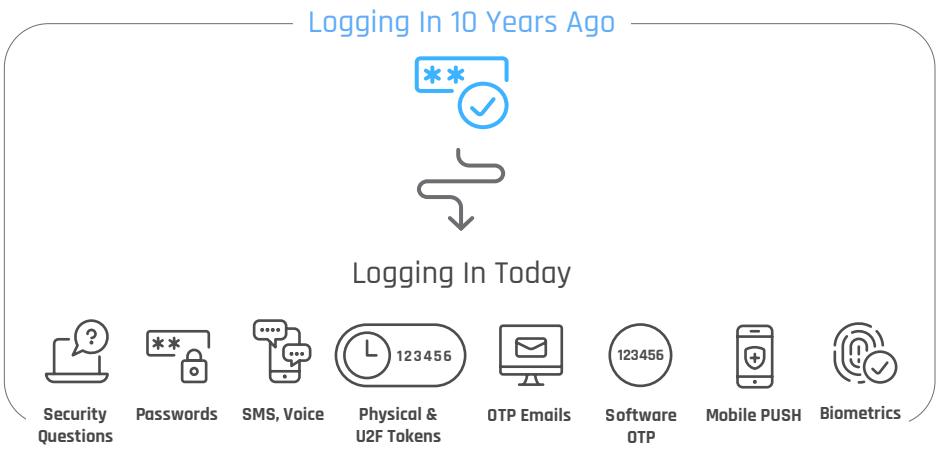


Why is Customer MFA Not Widely Adopted?

It's the friction factor. Simply put, customer-facing MFA is too difficult to use. Your customers have more login options than ever before, yet there remains a major gap in MFA adoption. According to Mary Meeker's 2019 Internet Trends Report, the number of websites supporting Two-Factor Authentication (2FA) had *dropped* to 52% - with many of them citing user friction as a blocker.

In a sense, the SCA requirement is a way to make Multi-factor security mandatory for the customer. Unfortunately, forcing more friction onto users with a regulatory requirement is not a winning strategy.

So how can we make people actually *want* to use a stronger MFA?



Some definitions in case you get acronym fatigue:

PSD2 - The Payment Services Directive is a payment regulation system that is governed by the European Commission aimed at contributing to the development of a single payment market in the European Union.

SCA - Strong Customer Authentication is a requirement of the PSD2 that ensures electronic payments are performed with multi-factor authentication, to increase the security of electronic payments.

RTS - The Regulatory Technical Standards on strong customer authentication provide a guideline for achieving the objective of the PSD2 of enhancing consumer protection and improving the security of payment services across the European Union.

Passwordless Technology Has Made MFA Enjoyable

Your customers expect a fast, easy digital experience, one that password-based MFA is unable to provide. And while PSD2 requirements aim to reduce fraud and make online payments more secure, the only way ensure adoption this time is to deploy a method that actually improves usability.

That's why businesses such as Mastercard, CVS Health, and Rakuten are deploying *Passwordless* customer Authentication with HYPR to deliver a better, more secure customer experience. By taking passwords out of the MFA process, businesses can finally eliminate password reuse, fraud and phishing – all while providing a lightning-fast user experience that's easy to use and easy to deploy.

Most importantly, they are able to satisfy 3 key requirements of the PSD2

1 The authentication shall be based on two or more elements which are categorised as knowledge, possession and inherence and shall result in the generation of an authentication code. - *Article 4.1*

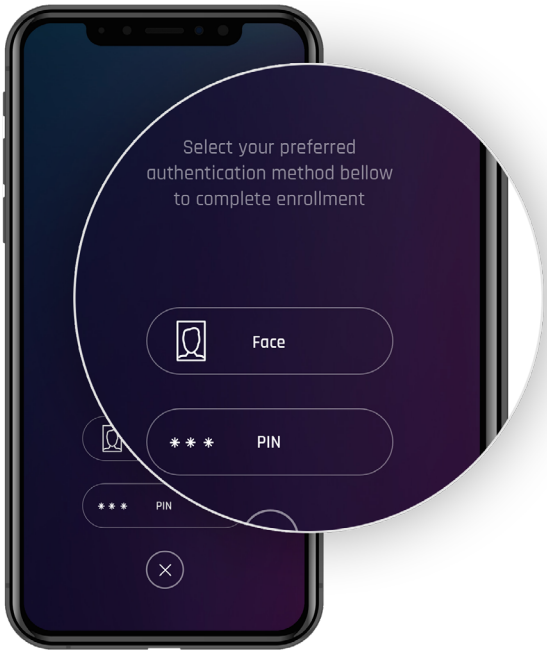
How You Meet this Requirement with HYPR:
Businesses must use multi-factor authentication for all transactions that require SCA. This requirement describes the need for multiple authentication factors - including but not limited to - Something You Have (Possession i.e. Smartphone), Something You Are (Inherence i.e. Biometrics), and Something You Know (Knowledge i.e. PIN).

True Passwordless Authentication is inherently multi-factor. It combines in a strong possession factor and local user-inherent factors. To perform a transaction, the user requires possession of their smartphone, and their biometric and/or PIN.

Businesses can even offer the user a choice in their preferred authentication method, as well as enforcing step-up authentication policies based on a combination of factors such as Face ID and Decentralized PIN.

How is HYPR Different from Legacy MFA?
Passwords and shared secrets are the most vulnerable part of legacy authentication processes; and yet they are also the foundation for most MFA methods. If your MFA process is built on top of a password you are unlikely to satisfy SCA requirements under the PSD2.

A passwordless schema replaces the use of shared secrets with Public-Key Cryptography (PKC), enabling a much stronger authentication mechanism. That makes it much safer than legacy, password-based MFA, while being faster and easier to use.



Rakuten

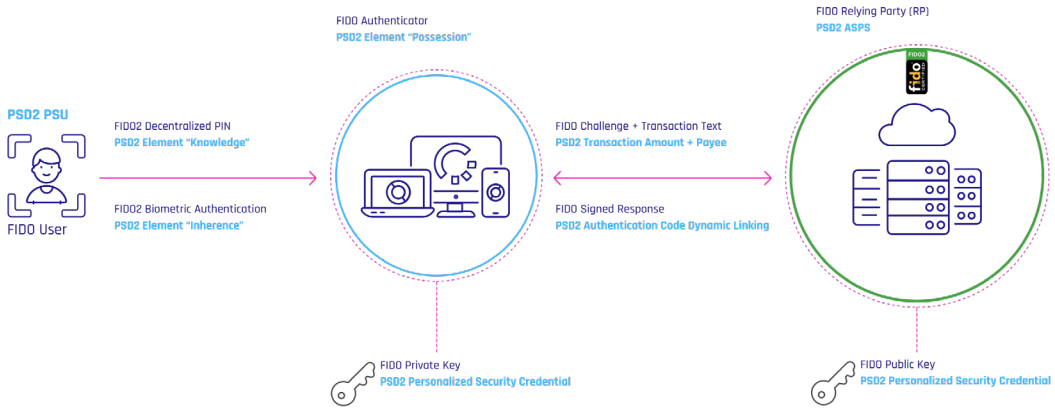
Enabling Faster Payments
The eCommerce giant deployed HYPR to eliminate payment fraud and accelerate transactions across mobile and web. "HYPR's passwordless authentication SDK provides a strong alternative to phishable and inconvenient passwords – and it works across devices customers already use in their daily lives already." - Arshal Ameen, Rakuten

2 The payer is made aware of the amount of the payment transaction and of the payee; - *Article 5.1*

How You Meet this Requirement with HYPR:
All transactions above 30 Euros mandate the use of Strong Customer Authentication (SCA). However, in addition to SCA there are also "dynamic linking" requirements needed that introduce further caveats.

At a high level this requirement means businesses must use cryptographic signatures to authorize online transactions. Dynamic linking requires a unique authentication code for each transaction. It can only be used once, is specific to the transaction amount and payee, and both amount and payee are made clear to the payer when authenticating.

True Passwordless authentication is powered by advanced Public-Key Cryptography and open standards such as Fast Identity Online (FIDO). At its core, this approach removes the hackers' primary target: the password. By forcing hackers to pursue each device individually, the risk of large-scale credential reuse and password spraying attacks drops significantly. Using a FIDO-Certified architecture enables you to authorize transactions in accordance with PSD2 RTS, fulfilling the "dynamic linking" requirements.



At the time of registration a user's private key is generated from a biometric such as a fingerprint or face. HYPR ensures this key always remains on their personal device and is used to sign transactions, including the transaction amount, payee ID and other data.

Once a transaction is processed, HYPR responds with a signed response that cryptographically links this data to the authentication code required by SCA. This is a fast and easy way to achieve "dynamic linking" for transactions processed on mobile and web applications.

CVS Health

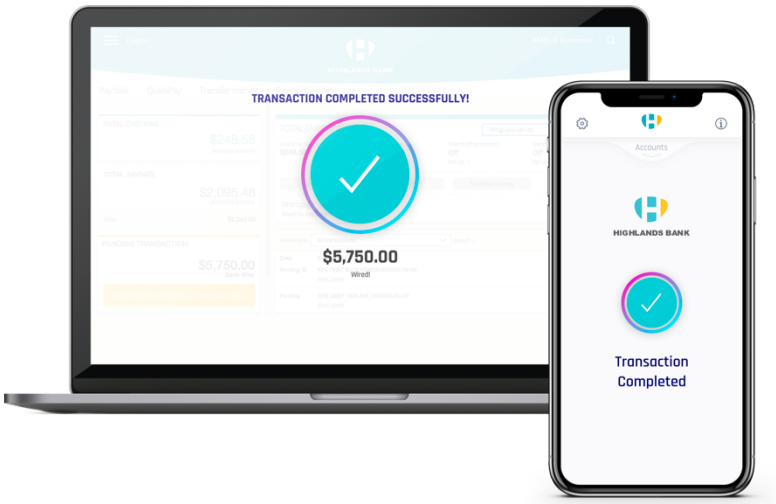
Reducing ATO Fraud by 98%
The Fortune 10 Healthcare Giant Deployed Passwordless Authentication to more than 10 million customers - reducing ATO fraud by a whopping 98.4%. "True Passwordless Security provides not only an ability for me to help drive a strategic vision that addresses security and fraud risk for my enterprise, it also helps me drive a vision, meet the digital engagement goals, and provide users and our customers with a better experience"
- Brian Heemsoth, CVS Health Aetna

3 The use of separated secure execution environments through the software installed inside the multi-purpose device. - *Article 9.2 & 9.3*

How You Meet this Requirement with HYPR:
This requirement describes the need to use an isolated software environment such as a smartphone to process cryptographic signatures for transaction approval.

Unlike password-based authentication, which stores user credentials and shared secrets on the server side, HYPR stores each user's cryptographic material – including authentication keys, PINs, and biometrics – on their smartphone. This approach ensures the protection of users' private keys and payment tokens used to approve transactions on mobile and web applications, as well as adherence to security requirements laid forth by the Regulatory Technical Standards (RTS).

Simply put, HYPR transforms your Smartphone into a Smart Card.



Why can't password-based MFA achieve this requirement?

The simple reason is that password-based authentication takes place server-side and relies on shared secrets. It does not utilize a cryptographic signature stored on a "separated secure software execution environment." This has rendered the ubiquitous password-based MFA insufficient for meeting SCA requirements.

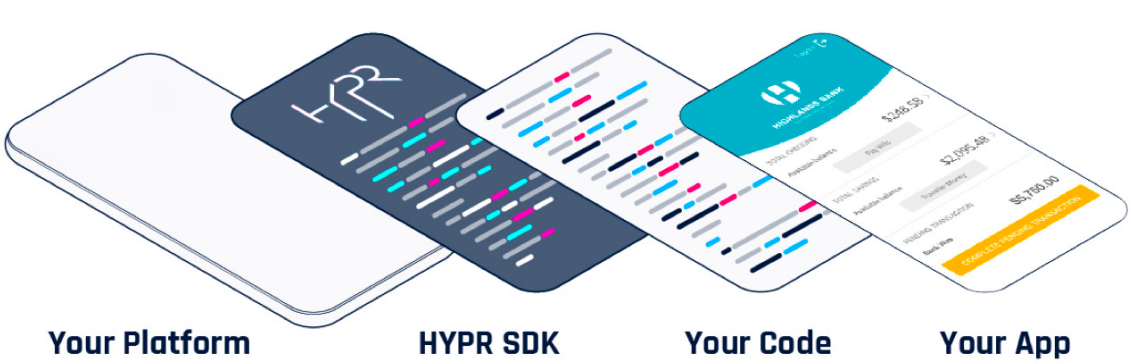
HYPR goes a step further in ensuring that your users' cryptographic material is protected from malware and stored below the mobile operating system level, by utilizing the latest mobile TrustZone® technology available on billions of iOS and Android devices. Additionally, HYPR leverages advanced jailbreak and root detection to prevent compromised devices from being used to perform fraudulent transactions.

200,000+ Passwordless Users
Ireland's largest health insurer is leading the way in passwordless and has reimagined the digital experience. "The ability to deliver strong passwordless authentication to our customer base is critical to our vision for a secure digital health experience. HYPR has empowered us to realize that vision at scale." - Damien Mullan, VHI Healthcare

Easily Deploy SCA Across Mobile and Web with HYPR

HYPR provides a fast and simple way to meet PSD2 compliance by eliminating passwords and shared secrets. This mobile-first approach to SCA is trusted by industry leaders to prevent credential reuse, achieve compliance, and enhance the customer experience.

At HYPR we believe everyone deserves the best possible user experience – including your technical teams. Time is a precious resource and your organization needs internal security agility. The True Passwordless SDK is designed to make life easier for your developers with a fast and easy 1-day integration.



Deliver Lightning-Fast Customer Login Experiences

Deliver a fast and consistent mobile-to-web login experience through passwordless transaction approvals, including step-up authentication. HYPR is scalable to millions of transactions per minute – handling usage spikes as well as growing demand.

Reduce ATO Fraud by up to 99%

Reduce Account Takeover (ATO) Fraud and improve your customer login experience. Increase customer MFA adoption and mobile engagement with lightning-fast security that sparks joy.

Give Your Developers a Break

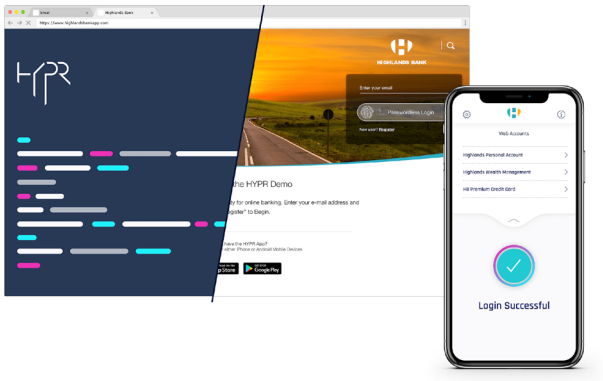
HYPR is built for speed, with mobile and web SDKs that put emphasis on rapid deployment so your team can quickly secure access on any app across all business lines.

Integrate SCA with Your Identity and Risk Engines

Effortlessly connect apps to your existing identity provider, fraud and risk engine. Do more with your existing authentication spend without displacing your favorite tools.

Guarantee Future-Proof Interoperability

Guard your investment by leveraging open standards such as FIDO2. HYPR is the leading provider of FIDO authentication for enterprises and a board member of the FIDO Alliance.



Watch Demo

HYPR is the Passwordless Company backed by Comcast, Samsung, and Mastercard.

Passwords and shared secrets remain the #1 cause of breaches despite billions of dollars invested in cyber security.
The HYPR Passwordless Cloud makes it easy to go Passwordless across the enterprise by combining the convenience of a smartphone with the security of a FIDO token.

With HYPR, businesses are finally able to solve the MFA gap, eliminate customer passwords, and deliver lightning-fast login experiences their users love.

Go Passwordless Now at www.HYPR.com