WAVESTONE

THE FINANCIAL SECURITY OF ONLINE TRANSACTIONS IN 2020:

WHAT WILL THE EFFECT OF PSD2 BE?

In an ever-more connected world, online financial transactions, from viewing bank accounts to making payments, are increasing at a steady rate: in 2017, more than 1.5bn people globally made an online payment, and over 2bn are expected to do so in 2019. In France, six out of ten people regularly make mobile payments.

This appetite for services is encouraging both traditional players and fintechs to take positions in the online banking market. Many solutions are now being deployed at large scale, something that requires appropriate regulation.

CONTACT

Michel GIRIER
michel.girier@wavestone.com

Jean DIEDERICH
jean.diederich@wavestone.com

PSD2 AND FINANCIAL PLAYERS

PSD2, the revised EU Directive on Payment Services, is part of the picture in developing electronic transactions. It represents a new step in standardizing financial exchanges, and follows PSD1 and the recent OpenBanking UK work.

As the number of players in the market grows, the number of solutions being deployed for user authentication and the security of financial operations is increasing. Such solutions may draw on means of exchange already recognized as secure (for example, EBICS and SWIFT)—but these are not well placed to meet the growing need for real-time access to data.

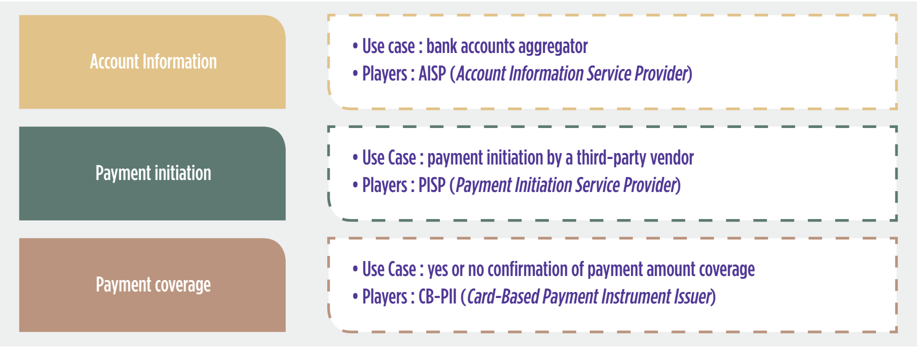
The purpose of the directive is to provide a regulatory framework for both banking and non-banking players, while also promoting competition.

To do this, the directive defines three types of services carried out by payment service providers:

- Account Information Services (AISs), which display and aggregate balance data and effect transactions in accounts used for payment.
- Payment Initiation Services (PISs), which involve a payment order being transmitted, on behalf of a payer, to their bank.
- Card-based Payment Instrument Issuers (CB-PIIs), which provide users with a means of payment.

Each provider of these types of services must accept a set of obligations under the directive's provisions. As long as they meet the obligations, the providers, known as AISPs, PISPs, and CB-PIIs, can access a user's bank account data free-of-charge via the user's Account Servicing Payment Service Provider (ASPSP).

Services within the scope of PSD2



Account Information	• Use case : bank accounts aggregator • Players : AISP (*Account Information Service Provider*)
Payment initiation	• Use Case : payment initiation by a third-party vendor • Players : PISP (*Payment Initiation Service Provider*)
Payment coverage	• Use Case : yes or no confirmation of payment amount coverage • Players : CB-PII (*Card-Based Payment Instrument Issuer*)

WHAT PSD2 BRINGS TO SECURITY

As a condition of allowing banks to access data via their ASPSP, the directive requires them to deploy a new interface which incorporates a set of security measures that enables the services to be offered securely .

As a result of the efforts of a number of working groups (in particular STET and the Berlin Group), the chosen solution has been the construction of APIs to deploy the ASPSPs' services; these use the Open API standards adopted by the major internet players. The associated security standards that have been selected are OAuth2 and OpenID Connect.

Identification and authentication of players

In response to the way aggregators currently function, one of the directive's most important measures is the obligation on banking players to mutually identify and authenticate when carrying out any transaction involving accounts used to make payments.

In the absence of suitable interfaces, aggregators currently use «web scraping," which consists of simulating a user's online banking navigation by replaying their authentication secrets. This method has three main flaws:

- the customer aggregator is not formally identified, which prevents the ASPSP from verifying whether or not they are a legitimate player
- the login secrets of the user are transmitted and known by a third party ; they don't remain confidential to the user
- the traceability of operations cannot be assured because it's impossible to prove the origin of a request.

Therefore, the directive (in Articles 66 and 67) obliges all players, including AISPs and PIISPs, to identify and authenticate themselves in order to have access to the services. A consensus has emerged around mutual, certificate-based authentication for all communications between Third Party Providers (TPPs) and ASPSPs.

Strengthening user authentication

Enhanced user authentication is one of the directive's fundamental measures—a theme that occurs repeatedly throughout its text and one that is core to the Regulatory Technical Standards (RTS) developed by the European Banking Authority (the EBA).

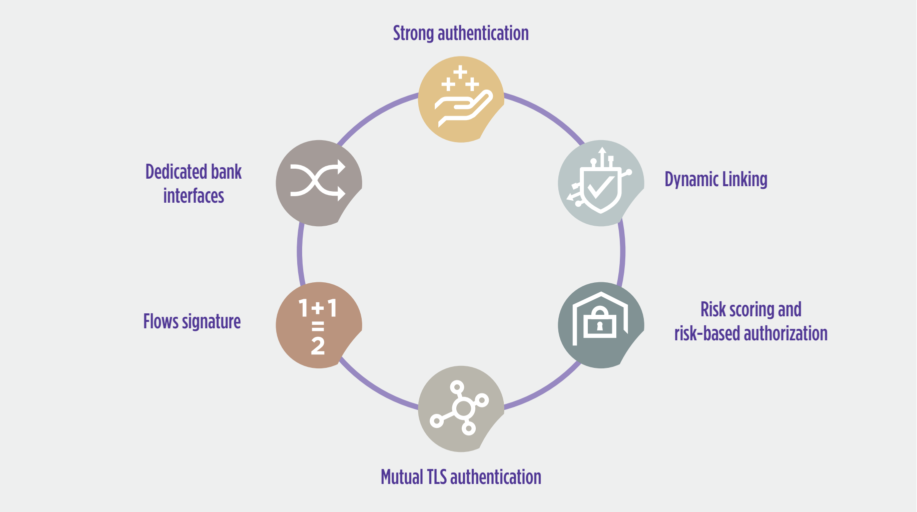
Today's enhanced authentication solutions rely mainly on the use of passwords (which can be replayed and are subject to phishing) and SMS OTP (which introduces the risk of interception). Both methods are widely used, but they have security vulnerabilities and can be expensive. The new mobile payment services also allow identification using an email address or mobile phone number that is unknown to the bank.

The purpose of the RTS is to make this user authentication secure by defining standards for Strong Customer Authentication (SCA), using two independent factors such that, if one factor is compromised the other is not affected. The directive requires the ASPSP to put in place the means of achieving this enhanced authentication, and to ensure that both factors remain secure throughout the chain of transmission.

A few solution are being considered to implement such authentication factors:

- Passwords remain the factor of choice, provided they are accompanied by a second factor that secures the enhanced authentication.
- Hardware solutions, although more secure, have the disadvantage of additional cost: the need for physical authentication tokens, keys, FIDO U2F devices, etc.
- Smartphone software is constantly being developed: in-app notifications, software authentication tokens, biometrics using device sensors, Mobile-Connect, etc.

Security requirements under PSD2


Strong authentication
Dynamic Linking
Risk scoring and risk-based authorization
Mutual TLS authentication
Flows signature
Dedicated bank interfaces
1+1
=
2

Dynamic linking

On the subject of payment transactions, the directive requires a unique code to be generated that enables the parties to the transaction to recover its characteristics at any point in the authentication and authorization process. In particular, throughout the process, the user must be aware of the amount and beneficiary of the transaction that they are authorizing.

This measure is similar to the current state of the art being applied for some types of online payment. Here, users receive an OTP code by SMS, accompanied by the transaction details: its amount, and the beneficiary of the payment. The directive makes this method universal by introducing it as a requirement for all payment transactions.

Exemptions from strong authentication

When defining the need for strong authentication and the specific requirements for Strong Customer Authentication, PSD2 tries to balance them with user navigation ergonomics. To do this, it details cases where payment service providers can choose to exempt their users from strong authentication.

The conditions that must be in place to make use of these exemptions are described precisely in the relevant RTS ; these are, in particular, related to the place and the system used for the payment. It's then the responsibility of the PSP to determine, using a risk assessment, whether an exemption can be applied or not.

THE LIMITS OF PSD2

PSD2 represents a milestone in strengthening the security of payment services. It puts in place measures that take into account the needs of the increasing number of digital players. As we stand, however, it contains limitations that constrain what the security mechanisms can offer.

PSD2's limited scope: accounts used for payments only

PSD2, as a directive about payment services, governs the online operations of players involved in such services only as far as they come within its scope: i.e. to the extent that they relate to accounts used for payment transactions.

In reality, however, the players, in particular aggregators, carry out operations on all user accounts—including savings accounts. One of the challenges these aggregators face is to ensure that they can provide value-added services that cover all types of user account activity—whether it relates to current accounts, savings accounts, checks, cards, credit, shareholding plans, etc.

By regulating access to accounts used for payments only, the European Commission and the EBA have put aggregators' ways of working under the spotlight (for example, the fact that they replay user login secrets); yet they have not provided solutions to all the issues associated with their exchanges with banks.

To allow these aggregators to develop their services further, the regulatory framework will need to be broadened. Moreover, given the work done by banks to comply with PSD2, which has required the construction of the architecture needed to use these services on the internet, further development to cover a broader range of accounts and other user services is very likely. A workgroup "API Scheme" is indeed working on extending the API standards to cover a larger scope.

Incompatibility with existing standards

Unlike the OpenBanking UK initiative, which was based on a recognized standard developed by the OpenID Foundation's Financial API Working Group, the new services offered by banks under PSD2 are based on regulatory requirements, not established security standards.

User consent

User consent is a good example of the gap between standards, in this case OpenID Connect, and regulation.

The directive implies that the user's consent for an aggregator to use one or more of their accounts:

- must be collected by the TPP (i.e. for the application that uses the APIs),
- must be applied and verified by the ASPSP (which hosts the APIs).

This is in contrast to the OpenID Connect standard (implemented as part of OpenBanking UK), in which consent must be collected by the service hosting the data and the APIs.

The authorization code flow

Implemented for the use of AISPs, the authorization code process requires the user to be redirected from the AISP to the ASPSP's authentication and consent service, and then returned by being redirected to the AISP's application.

This redirection can be considered as an obstacle to the use of services, as Article 32 of the RTS sets out by way of an example. It may, therefore, be deemed illegal and ASPSP would have to implement other communication flows.

The acceptability of that flow under PSD2 then becomes a question for each national regulatory authority, which has the effect of limiting the standardization of these interfaces across Europe. At present in France, the ACPR (the French financial regulator) has accepted the use of this redirection process.

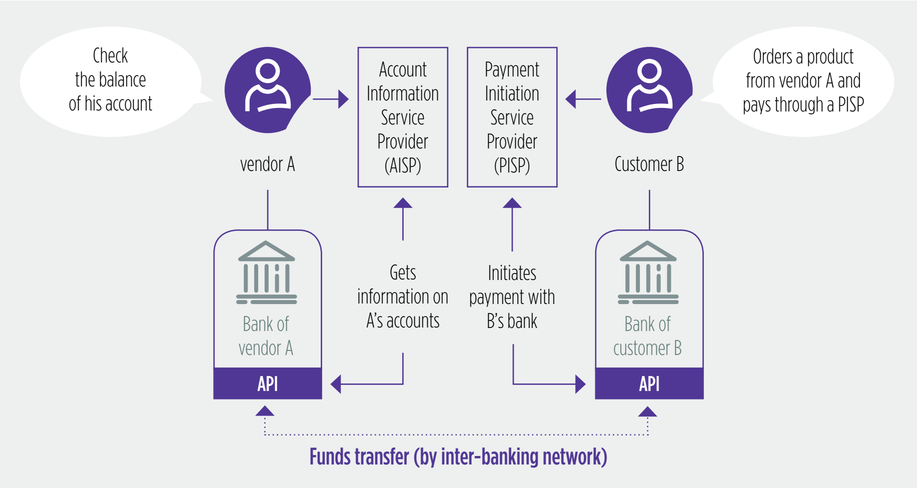
CONCLUSION

In a digital environment that's constantly changing, PSD2 supports the development of intermediary players in payment services by standardizing exchanges and introducing better user-navigation ergonomics and transaction security.

It contains important security provisions which are forcing banking ISs to develop—the opening up of internet-based services and changes to authentication methods are particularly complex areas for the traditional banks.

Nevertheless, it leaves other uses untouched, which means further legislation will be required. A particular area of interest is accounts outside the scope of PSD2, for which the work begun here offers an opportunity to make access to these services secure.

Players on the PSD2 stage


Check the balance of his account
vendor A
Account Information Service Provider (AISP)
Payment Initiation Service Provider (PISP)
Customer B
Orders a product from vendor A and pays through a PISP
Bank of vendor A
API
Gets information on A's accounts
Initiates payment with B's bank
Bank of customer B
API
Funds transfer (by inter-banking network)

WAVESTONE

www.wavestone.com

In a world where knowing how to drive transformation is the key to success, Wavestone's mission is to guide large companies and organizations in their most critical transformation projects, with the ambition of a positive outcome for all stakeholders. That's what we call "The Positive Way".

Wavestone brings together 3000 employees across 8 countries. It is a leading independent player in the european consulting market.

Wavestone is listed on Euronext Paris, and recognized as a Great Place To Work®.