MEMO
N°08

PSD2 AND SECURITY ISSUES

FÉDÉRATION
BANCAIRE
FRANÇAISE

- What is PSD2?

- What issues does it raise for the security of customer data and payment systems?

- Which solutions can guarantee security?

- What are the procedures for moving to strong authentication?

01

WHAT IS PSD2?

A new regulatory framework

Directive EU 2015/2366 on payment services in the internal market, known as PSD2, updates the regulatory framework governing payments in Europe. It aims to incorporate technology changes, allowing the emergence of **"innovative, safe and easy-to-use digital payment services".**

54.8

BILLION
CARD PAYMENTS
IN EUROPE

Source: ECB, Payment Statistics, 2018
(excluding UK, Slovakia, Malta and Ireland)

PSD2 came into force on **13 January 2018**. It requires customers' account payment data to be freely available for two new activities:

- **account information services:** a data aggregation service that means customers with accounts in one or more banks or other institutions can get all their information in one place;
- **payment initiation service:** this allows a payment service provider to send a payment order in the customer's name to their account keeping bank or other entity.

Innovation and security

PSD2 has two ambitions: to encourage innovation in a competitive European payments market and to strengthen payment security and customer protection.

It will therefore require aggregators to register and payment initiators to be licensed.

It is the home member states of the new players (the country where they have their registered office) that are responsible for regulating them.

In France, this means the Autorité de contrôle prudentiel et de résolution (ACPR).

From the customer's point of view, the big change is that the account-keeper (bank or payment institution where the customer has their account) will have to reimburse the customer in the event of a fraud taking place after a payment initiation. This **new liability regime** places the cost of fraud, whatever its source, on the shoulders of the account-keeper, who must seek redress from the payment initiator who is obliged, in turn, to take out insurance.

02

DATA AND SYSTEMS PROTECTION: A KEY ISSUE

A background of rising risks

The Directive itself emphasises the new risks that innovation and the multiplication of market operators will bring. As it says **“In recent years, the security risks relating to electronic payments have increased. This is due to the growing technical complexity of electronic payments, the continuously growing volumes of electronic payments worldwide and emerging types of payment services”.**[1]

It goes on to add **“ Safe and secure payment services constitute a vital condition for a well-functioning payment services market. Users of payment services should therefore be adequately protected against such risks. Payment services are essential for the functioning of vital economic and social activities”.**[1]

Since work on the Directive began, the number of cyber-attacks has exploded. This is a major concern for both banks and regulators.

32%

ANNUAL INCREASE IN CYBER-ATTACKS IN FRANCE IN 2018

Source : F-Secure, March 2019

[1] Recital 7 of the Directive

A vital need for security

The question is how to simultaneously protect data and the funds that everyone entrusts to their bank while also guaranteeing the safety of payment transactions. The directive notes the absence of rules governing payment initiation services and the lack of control which raise a **“series of legal issues, such as consumer protection, security and liability as well as competition and data protection issues, in particular regarding protection of the payment service users’ data in accordance with Union data protection rules.”** concluding that **“ The new rules should therefore respond to those issues”**[2].

It goes on to say that, **“Security of electronic payments is fundamental for ensuring the protection of users and the development of a sound environment for e-commerce. All payment services offered electronically should be carried out in a secure manner, adopting technologies able to guarantee the safe authentication of the user and to reduce, to the maximum extent possible, the risk of fraud”**[3].

The Directive thus makes it clear that security is a major concern of Europe's lawmakers. At stake is the maintenance of public confidence in payment systems, without which economic life grinds to a halt.

Each year, banks invest heavily to maintain a high level of security in the systems and infrastructures.

[2] Recital 29 of the Directive
[3] Recital 95 of the Directive

03

THE CHOICE OF SECURITY

New security standards

Since security is a crucial issue, PSD2's article 98 entrusted the European Banking Authority's (EBA) experts with defining Regulatory Technical Standards (RTS) for **strong customer authentication (SCA)** for payment transactions and access to online payment accounts. These standards, published in the Official Journal of the EU on 13 March 2018[1], have been applicable as of **14 September 2019**, 18 months after their publication, as stipulated in the directive.

API: A shared solution

These security standards (RTS) are based **on a standardised, secure access mode open to all operators**. Custodian banks must provide payment aggregators and initiators with a standardised, secure interface. This interface replaces web scraping techniques based on payment aggregators' and initiators' use of customers' user IDs and passwords, which customers are solely responsible for sending.

An **Application Programming Interface** (API), which is well known in the digital marketing and online world, is a suitable response to the requirements of the directive and RTS, in terms of both equal access for all and security for customer data. Across Europe, banks and consumers (through the European Consumers' Organisation - BEUC), as well as a number of new fintechs that are coming onto the payment market, support this solution.

For four years, French banks have worked on defining, developing, and deploying APIs that comply with the requirements set by the RTS. **These solutions are available for customer account access by third-party payment services (TPP)**.

[1] Commission Delegated Regulation (EU) 2018/389 of 27 November 2017.

Phasing in strong authentication

14 September 2019 marks t**he start of adoption of strong authentication for payment transactions and payment account access procedures**. As experts in the security of funds and their customers' data, banks are prepared for this deadline. They have moved into high gear to ensure optimal roll-out for their customers and online merchants.

- **Online payment account access** (online banking, mobile banking apps): the law stipulates that strong customer authentication be required at least once every 90 days. It is implemented **simply and gradually, with a roll-out specific to each bank**. Customers are notified of the changes by their banks.
- **Online purchase payments**: the current customer authentication mechanism is still used, but it is **gradually replaced by new strong authentication solutions** offered by the banks to their customers. This transition is part of a market schedule developed by all participants in the ecosystem (card networks, online merchants, banks, etc.) in connection with national authorities and is published by the French Observatory for the Security of Payment Methods (OSMP).

04

OUR KEY ISSUES

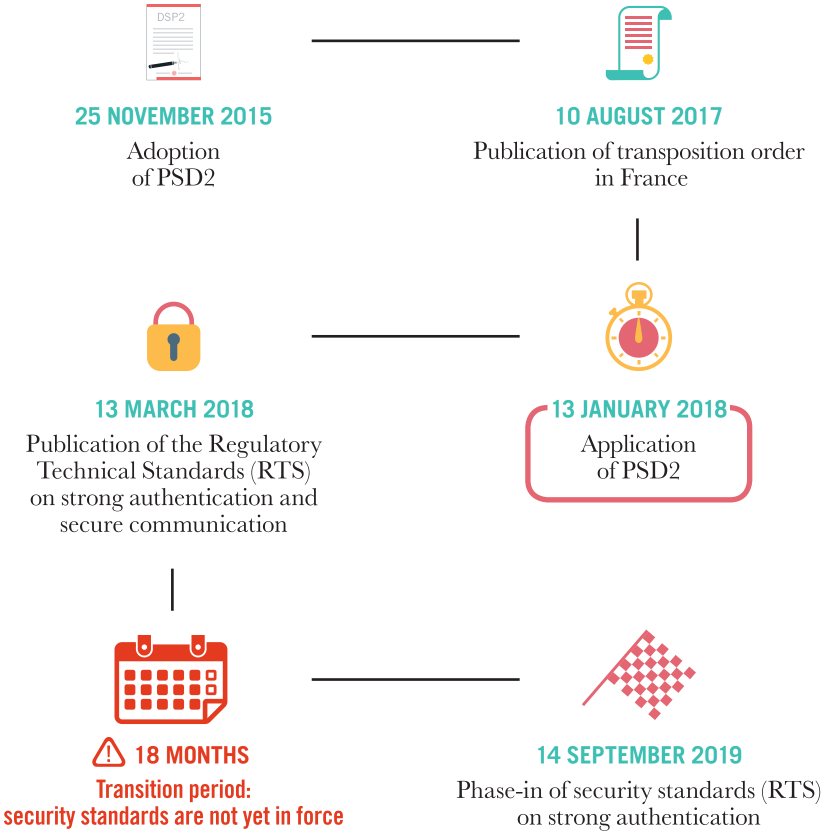
By requiring account aggregators and payment initiators to use standardised, open and secure application programming interfaces (APIs) when accessing accounts in the EU the Commission has put security first.

The FBF, like other bodies such as the European Banking Authority (EBA), European Consumer Organisation (BEUC), cyber-security authorities, European banking associations and FinTechs looking to break into the market, have always supported APIs as the only solution that can deliver real security in the current climate of increasingly frequent cyber-attacks.

Faithful to their values of innovation in security and support for their customers, banks have developed APIs for access to customer payment accounts by payment aggregators and initiators (TPP). These interfaces have been in testing for many months and are available in production. They are ready, they meet PSD2 and security standards, and they can be used by TPPs. They guarantee the security of customer data and funds.

CALENDAR

PSD2 has been applicable since 13 January 2018, and security standards from 14 September 2019.



25 NOVEMBER 2015
Adoption
of PSD2

10 AUGUST 2017
Publication of transposition order
in France

13 JANUARY 2018
Application
of PSD2

13 MARCH 2018
Publication of the Regulatory
Technical Standards (RTS)
on strong authentication and
secure communication

⚠ **18 MONTHS**
Transition period:
security standards are not yet in force

14 SEPTEMBER 2019
Phase-in of security standards (RTS)
on strong authentication

Glossary

ACCOUNT AGGREGATOR Data aggregation means that customers with multiple payment accounts, in one or more institutions, can get all the information they need in one place.

API Application Programming Interface. The API is an effective, standardised and secure method of communication between two applications.

PAYMENT INITIATOR Payment initiation services mean a payment service provider can send a payment order, in the name of the customer, to the account-keeping institution.

RTS Regulatory Technical Standards: technical standards for strong customer authentication and secure communication.

STRONG AUTHENTICATION or two-factor authentication uses two out of three types of ID information: something you know (password, PIN), something you own (computer, mobile), something you are (digital fingerprint, retina, voice).

TPP Third Party Provider: account aggregators or payment initiators.

WEB SCRAPING Technique for capturing website content in order to re-use the content.

© Freepik

18, RUE LA FAYETTE
75440 PARIS CEDEX 09
FRANCE
TEL. : +33 (0)1 48 00 52 52

FBF.FR/EN/HOME

September 2019

FÉDÉRATION
BANCAIRE
FRANÇAISE