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

FBF.FR/EN/HOME

Draft completed 2017

FÉDÉRATION
BANCAIRE
FRANÇAISE

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?

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 ".**

59.6
BILLION
CARD PAYMENTS
IN EUROPE

source: ECB, Payment Statistics, 2016

PSD2 will take effect as from **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. Both groups currently operate through a technique called "web scraping" free from any regulatory control and answerable only to the customers who give them access to their accounts by communicating their login credentials and passwords.

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

New activities, new 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 ".**

A background of rising risks

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

35%

ANNUAL INCREASE IN CYBER-ATTACKS IN FRANCE

Source : Global Security Mag - October 2017- Baromètre RGPD

(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 current absence of rules governing payment initiation services and the lack of control which raises 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 infrastructure.

(2) Recital 29 of the Directive
(3) Recital 95 of the Directive

03

THE CHOICE OF SECURITY

Essential security standards

Since security is a crucial issue, PSD2's article 98 charges the European Banking Authority (EBA) to use its expertise to define regulatory technical standards for strong customer authentication (SCA) and secure communications between payment services providers.
The EBA delivered its security recommendations to the European Commission on 23 February 2017.

The Commission adopted the RTS on 27 November 2017. They are now pending ratification by the European Parliament and Council.

These standards are based on a standardised and secure open access model for all participants. Account-keeping banks must make available an interface for the use of account aggregators and payment initiators. This standardised and secure interface should replace the current web-scraping techniques, in which aggregators and payment initiators use customers' login details and passwords.

Strong customer authentication, or two-factor authentication, uses two of three types of identification: something you know (password, PIN), something you own (computer, mobile), something you are (digital fingerprint, retina, voice).

API: a shared solution

APIs (Application Programming Interfaces) are a familiar tool in the world of digital marketing and the internet and so represent an appropriate response to the demands of the Directive and the technical regulatory standards, offering both equal access for all players and security for customer data. This solution has the support not only of banks but also of European consumers (represented by BEUC, the European Consumers' Organisation) and a good number of FinTechs breaking into the payments market.

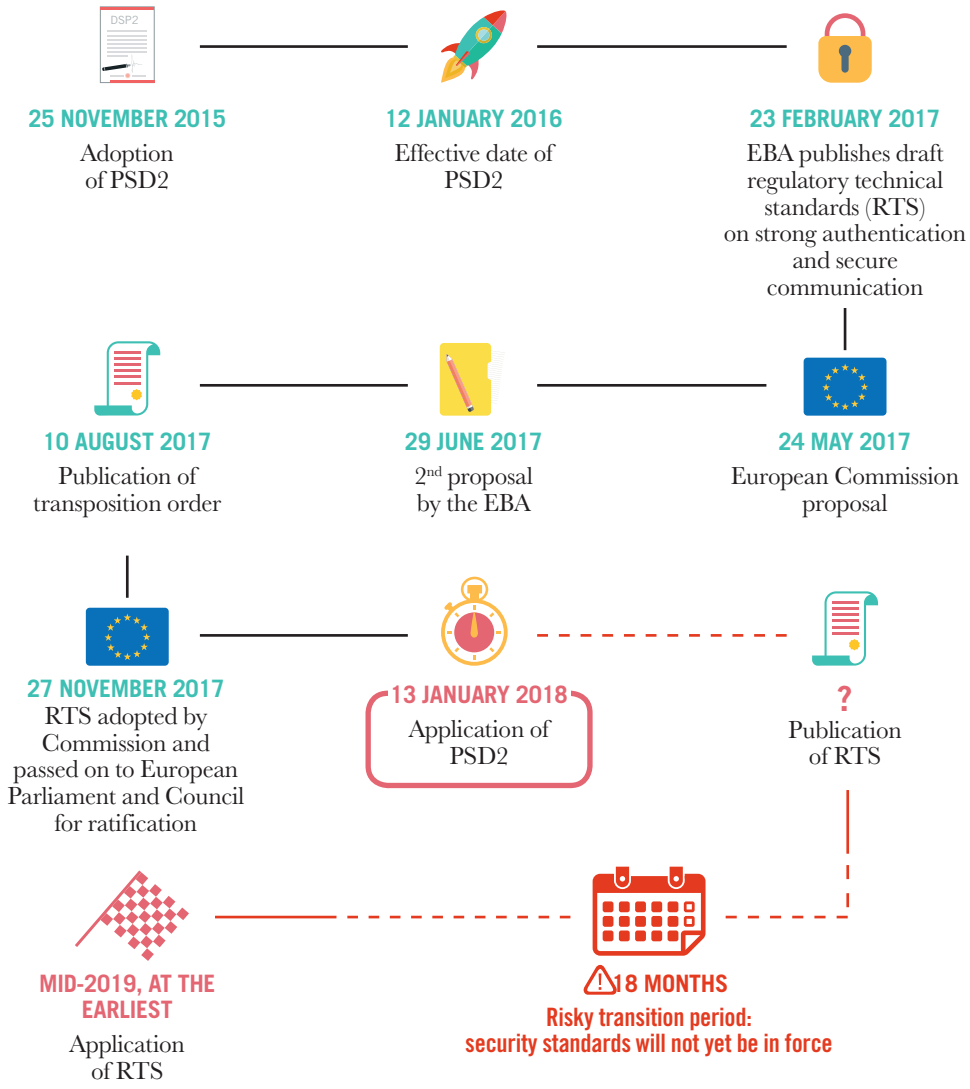
However, the European Commission, under pressure from some already well-established business in the aggregation and payment initiation market who are looking to protect their share, has proposed allowing the insecure web-scraping method to continue in certain cases. Banks oppose this, even as a fall-back solution.

Security standards cannot be brought in at the same time as the Directive in January 2018.

RTS will only come into force 18 months after their publication as the Directive states.

AN INCONSISTENT CALENDAR

A Directive coming into force on 13 January 2018 but security standards that will only apply from mid-2019 at the earliest.



04

OUR KEY ISSUES

The French Banking Federation (FBF) welcomes the European Commission's publication of regulatory technical standards (RTS) for the Payment Services Directive PSD2.

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.

> Events of recent months have reminded us that cyber-attacks are becoming ever more common and more powerful. APIs offer a secure response and their recognition by the European Commission is good news for all of us. French banks will be rolling out this solution in 2018.

MARIE-ANNE BARBAT-LAYANI
FBF CHIEF EXECUTIVE OFFICER
Press release
28 November 2017

Glossary

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

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.

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).

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.

TPP Third Party Provider: account aggregators or payment initiators.

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