# *TABLE OF CONTENTS*

- Surcharging ban:
- Unauthorized payments:

## Guidelines on fraud reporting under psd2:

- legal basis and background:

## Frequently asked questions:

- General questions
- Key benefits
- Scope of the directive
- Enhanced rules on authorisation and supervision of payment institutions
- Security of payments:
- Rules for new types of payment service providers
- Transitional period
- Rationale, objectives and process
- Strong customer authentication (SCA);
- Common and secure communication:
- Protection of personal data:

## Conclusion:

## *Glossary:*

## *References:*

## *Articles:*

# *"Payment Services Directive"*

## *A Catalyst for New Growth Strategies in Payments and Digital Banking*

## OVERVIEW:

The payment services industry has undergone profound change since the landmark Payment Services Directive ("PSD 1") was introduced in 2007. Developments in technology and the emergence of new payment services providers have fundamentally altered the market landscape. The new Payment Services Directive II ("PSD 2") is designed to update the rules in respect of payment services, to reflect and regulate aspects of these recent developments.

PSD 2 must be transposed into Irish law by 13 January 2018. From a practical viewpoint, PSD 2 widens the scope of the original rules, covering new services and market operators. While much of the framework of PSD 1 has been retained, an additional layer of obligations will be placed on Payment Service Providers ("PSPs") under the new legislation. This will require PSPs to review their internal procedures and systems to take account of and ensure compliance with PSD 2. With the arrival of Payment Services Directive II (PSD2), the new services and their providers will be registered, licensed and regulated, increasing competition, providing more choices for customers, and encouraging lower prices for payments.

The second Payment Services Directive (PSD2) is part of a global trend in bank regulation emphasizing security, innovation, and market competition. By requiring banks to provide other qualified payment-service providers (PSPs) connectivity to access customer account data and to initiate payments, PSD2 represents a significant step toward commoditization in the EU banking sector.

## HISTORY: (Revision of EU legislation)

On October 8, 2015, the European Parliament adopted the European Commission proposal to create safer and more innovative European payments (PSD2, Directive (EU) 2015/2366). The new rules aim to better protect consumers when they pay online, promote the development and use of innovative online and mobile payments such as through open banking, and make cross-border European payment services safer.

On November 16, 2015, the Council of the European Union passed PSD2. Member states will have two years to incorporate the directive into their national laws and regulations.[10]

The EU and many banks are pushing this development with the new Payments Service Directive 2 (PSD2), which has come into force on 13 January 2018. Banks need to adapt to these changes that open many technical challenges, but also many strategic opportunities, such as collaborating with fintech providers, for the future.

# DEFINITION:

The Payment Services Directive[1] (PSD, Directive 2007/64/EC, replaced by PSD 2, Directive (EU) 2015/2366) is an EU Directive, administered by the European Commission (Directorate General Internal Market) to regulate payment services and payment service providers throughout the European Union (EU) and European Economic Area (EEA). The Directive's purpose was to increase pan-European competition and participation in the payments industry also from non-banks, and to provide for a level playing field by harmonizing consumer protection and the rights and obligations for payment providers and users

# IMPLEMENTATION AND LAW DETAILS:

## Full title

Directive 2015/2366/EU of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC

**Date of entry into force**

12 January 2016

**Date that the rules apply**

13 January 2018

A revised Payment Services Directive (PSD2) was implemented on 13 January 2018. The original directive (PSD) was adopted in 2007, creating a single market for payments and thus the legal foundation for a Single Euro Payments Area (SEPA). Technological innovation and digitalization has led to new entrants in the field offering new services online and on mobile. The problem was that most of these new players were outside of the scope of the PSD and, therefore, not regulated by the EU. The PSD2

aims to improve security and fraud prevention, but also to “foster innovation and competition” by ensuring a healthy playing field for old, new and prospective players.

# KEY DATES:

- March 2000: Lisbon Agenda to make Europe “the world’s most competitive and dynamic knowledge-driven economy” by 2010
- December 2001: regulation EC 2560/2001 on cross-border payments in Euro
- 2002: European Payments Council created by the banking industry, driving the Single Euro Payments Area initiative to harmonize the main non-cash payment instruments across the Euro area (by end 2010)
- 2001–2004: consultation period and preparation of PSD
- December 2005: proposal for PSD by DG Internal Market Commissioner McCreevy
- 25 December 2007: PSD entered into force
- 1 November 2009: deadline for transposition in national legislation
- 2009 update: eliminated differences in charges for cross-border and national payments in euro (EC Regulation 924/2009)
- 2012 update: Regulation on cross-border payments, 'multilateral interchange fees' (EU Regulation 260/2012)
- July 2013: report on implementation of PSD and its two updates[8]
- 16 November 2015: The Council of the European Union passes PSD2, giving member states two years to incorporate the directive into their national laws and regulations.[10]
- 13 January 2018: Directive 2007/64/EC is repealed and replaced by Directive (EU) 2015/2366
- September 2019: all companies within the EU must comply with the national laws and regulations pertaining to directive (EU) 2015/2366 (PSD2).

# OBJECTIVES OF PSD2:

The objective of the Directive is to extend the scope of regulation to the various types of payment services and to update payment services regulation in line with market developments. In short, it is a transformation from a European Single Market to a Digital European Single Market.

**The Financial Conduct Authority (FCA) summarizes the aims of the directive:**

- Standardizing, integrating and improving payment efficiency in the European Union
- Offering better consumer protection

- Promoting innovation in the payments space and reducing costs
- Incorporating and providing clarity on the use of emerging payment methods such as mobile payments and online payments
- Create a equal playing field for payment service providers – enabling new companies to get into the payments space
- Harmonize pricing and improve security of payment processing across the European Union
- Incorporate new and emerging payment services into the regulation
- contribute to a more integrated and efficient European payments market
- promote the development and use of innovative online and mobile payments
- protect consumers
- encourage lower prices for payments

Below are the main and most important changes taking place with the new legislation, as revealed by the European Payments Council.

At the same time, it will introduce higher security standards for online payments. This will make consumers more confident when buying online. PSD2 scope extends to innovative payment services and new providers in the market, such as FinTechs. These players are also called third party payment services providers (TPPs). TPPs include:

- Payment initiation services providers (PISPs): these initiate payments on behalf of customers. They give assurance to retailers that the money is on its way.
- Aggregators and account information service providers (AISPs): these give an overview of available accounts and balances to their customers

# Who work with European Commission?

The commission works with the EBA and three advisory bodies on Directive(EU) 2015/2366 on payment services

## European Banking Authority (EBA):

In the area of payment services the Commission works with the European Banking Authority. The EBA contributes to the regulatory work of the Commission by providing technical advice and drafting technical standards. It also publishes guidelines and recommendations to ensure the consistent and effective application of EU rules.

### Expert groups and comitology committee:

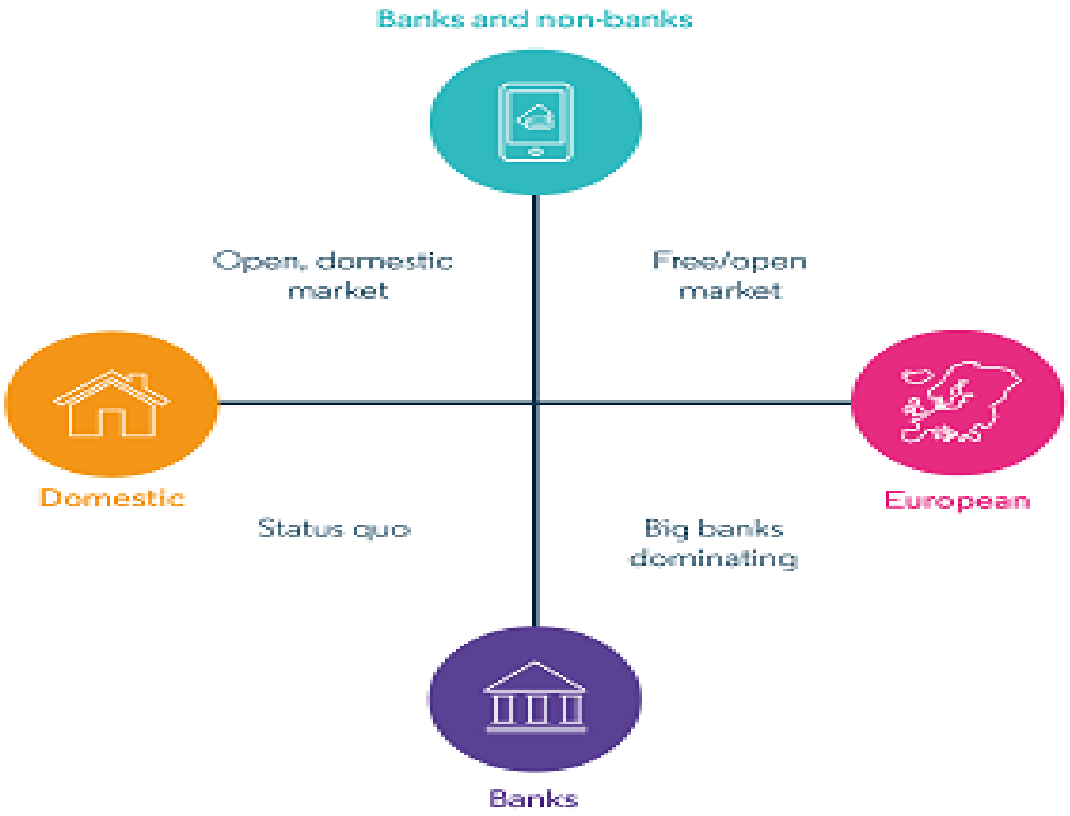
In this area the Commission is also assisted by the Expert Group on Banking, Payments and Insurance (EGBPI), the Payment Systems Market Expert Group (PSMEG), and the Payments Committee.

The EGBPI is composed of experts appointed by the EU countries. It provides advice and expertise in the preparation of draft delegated acts to the Commission and its services, in the area of banking, payments and insurance.

The PSMEG helps the Commission prepare legislative acts or policy initiatives on payment issues, including fraud prevention.

The PC is composed of representatives of EU countries and observers from the European Economic Area (EEA). It helps the European Commission adopt implementing measures of the payment services directive, and other issues linked to payments.

## INTRODUCTION TO FRAMEWORK



The entry of PSD2 requires that banks take a number of strategic choices. This is not an easy task, as the choices partly depend on how the payment landscape will evolve after PSD2. We envision four possible scenarios, based on two variables: 1) how domestic or European the financial market will be (horizontal line), and 2) whether the consumers will stick to traditional banks or trust non-banks for making payments (vertical line).

A unified European market has been one of the desired outcomes for both the first and the revised Payments Services Directive for the European Commission. When the Commission wanted to broaden the scope of the first directive, it tried again with the PSD2, and it is likely that the Commission will keep improving this through a PSD3 in the future.

# BENEFITS TO CUSTOMERS:

**Payment services: Consumers to benefit from cheaper, safer and more innovative electronic payments**

**European consumers will be able to reap the full benefits of paying online for goods and services, thanks to new rules that will it make it cheaper, easier and safer to make electronic payments.**

The revised Payment Services Directive (PSD2), aims to modernize Europe's payment services to the benefit of both consumers and businesses, so as to keep pace with this rapidly evolving market.

Valdis **Dombrovskis**, Vice-President responsible for Financial Stability, Financial Services and Capital Markets Union said. *"This legislation is another step towards a digital single market in the EU. It will promote the development of innovative online and mobile payments, which will benefit the economy and growth. With PSD2 becoming applicable, we are banning surcharges for consumer debit and credit card payments. This could save more than €550 million per year for EU consumers. Consumers will also be better protected when they make payments."*

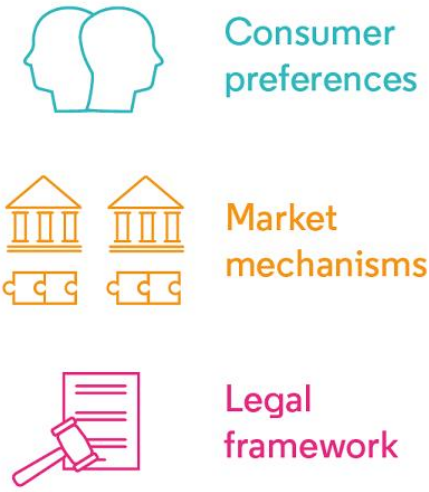
The new rules will:

- Prohibit surcharging, which are additional charges for payments with consumer credit or debit cards, both in shops or online;
- Open the EU payment market to companies offering payment services, based on them gaining access to information about the payment account;
- Introduce strict security requirements for electronic payments and for the protection of consumers' financial data;

- Enhance consumers' rights in numerous areas. These include reducing the liability for non-authorized payments and introducing an unconditional ("no questions asked") refund right for direct debits in euro.
- These rules are applicable as of 13 January 2018 through provisions that Member States have introduced in their national laws in compliance with the EU legislation. The Commission is concerned that many Member States have not yet transposed the Directive and it calls on them to do so as a matter of urgency.

## So why IT means for customer?

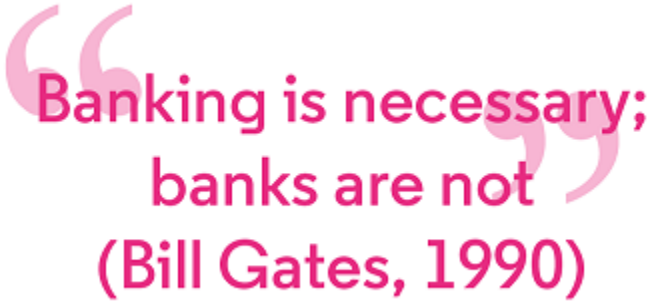
A survey conducted by the European Commission revealed that 80 % said they would not consider buying a financial product in another EU Member State in the future because “they can purchase all the financial products they need in their own country, or they prefer to do so”. This shows how far from a unified market the EU really is. We view this as a consequence of the European market lacking effective mechanisms supporting cross-border banking, such as communication of its benefits, smooth on-boarding processes and harmonized regulations. Regarding the latter, differentiated domestic legal frameworks is identified as the main barrier for both providers and consumers to enter a foreign market by the European think tank CEPS. The costs related to regulatory understanding and compliance might be seen by banks as too large compared to the market’s potential revenues, making the bank’s investment into a new country unattractive.




## Consumer preferences and trust


with the consumer becoming more digital and mobile in their approach to companies, the banks as well as non-banks will need to follow this trend. These tech savvy consumers are asking for financial service offerings that are faster, less formal,

more personalized, easy accessible and cheap . So far, non-banks have proven to meet these requirements in a more innovative and human-centric way than many traditional banks.
Consumers are slowly getting used to using non-banks for financial tasks and it seems like this trend is only continuing. PayPal has already existed in close to 15 years and has gained great consumer trust. Swedish Tink and the Danish Billy are companies that have also gained a great market share without a banking license. And every fifth European consumer say they would use by financial products from challengers such as Google, Facebook and Amazon.




## CHALLENGES AND OPPORTUNITIES FOR BANKS:

PSD2 enables bank customers, both consumers and businesses, to use third-party providers to manage their finances. In the near future, you may be using Facebook or Google to pay your bills, making P2P transfers and analyze your spending, while still having your money safely placed in your current bank account. Banks, however, are obligated to provide these third-party providers access to their customers' accounts through open APIs (application program interface). This will enable third-parties to build financial services on top of banks' data and infrastructure.

Banks will no longer only be competing against banks, but everyone offering financial services. PSD2 will fundamentally change the payments value chain, what business models are profitable, and customer expectations. Through the directive, the European Commission aims to improve innovation, reinforce consumer protection and improve the security of internet payments and account access within the EU and EEA. It introduces two new types of players to the financial landscape: PISP and AISP. AISP (Account Information Service Provider) are the service providers with access to the account information of bank customers. Such services could analyze a user's spending behavior or aggregate a user's account information from several banks into one overview. PISP (Payment Initiation Service Provider) are the service providers initiating

a payment on behalf of the user. P2P transfer and bill payment are PISP services we are likely to see when PSD2 is implemented.

For banks, PSD2 poses substantial economic challenges. IT costs are expected to increase due to new security requirements and the opening of APIs. In addition, 9 percent of retail payments revenues are predicted to be lost to PISP services by 2020. And, as non-banks take over the customer interaction, banks may find it increasingly difficult to differentiate themselves in the market for offering loans.

While PSD2 poses serious threats to current business models, it also creates opportunities for banks to compete as technology innovators, wielding powerful analytical tools to extract valuable insights from their vast stores of proprietary data. Market dynamics and customer attitudes may favor banks that can capture opportunities quickly and effectively. If third parties do not gain the full trust of customers, banks could retain their role as trusted financial anchor, as customers would not find it attractive to provide third parties access to their data or accounts (unless recommended by banks). But there are no guarantees that banks will be able to defend their status as secure trusted advisors. In the worst-case scenario, closed-loop ecosystems could emerge and reduce banks to the role of balance-sheet provider. Customer interactions would be reduced significantly, with current account transactions limited primarily to incoming salary deposits and outgoing payments to fund transaction accounts at another PSP. Third parties would handle all transactions and accumulate the associated customer data

## Approaches to new regulations:

We are seeing a few common approaches to meeting the new requirements:

| | |
|---|---|
| **Challengers** | These are new entrants the market who do not have an existing technology estate to tie them to a particular solution. Typically, they are selecting fit-for-purpose platforms to quickly build capability and products. They're embracing and defining the opportunity for change and transformation, centered on providing a better customer experience in banking. Their biggest challenge is in scaling their innovation, but if they can overcome this, they look to be very successful |
| **Transformers** | These are the banks which have been around for a while, who have the scale, but are trying to grasp the innovation that Open Banking presents, as well as reeling from the new competition posed by the Challengers. They may decide to embrace existing technology investments and selectively transform these to compete effectively. The biggest challenge for Transformers might be to overcome their own siloes. This approach may be costly as well as risky, but may well leverage the reach and scale they already have. |

| | |
|---|---|
| **Modernizers** | Companies which have started embarking on a modernization project before the new regulations came into play, may find themselves having to reconsider their plans. This may count in their favor, as they have already committed to updating or replacing some of their legacy systems. Their challenge might be to continue their plans and investments as well as changing to meet new requirements at the same time |
| **Revivers** | This is a hybrid approach, where some of the most established banks find that their legacy systems are not going to meet the new requirements, and they decide to create a challenger bank outside the walls of the current institution. They develop their new operations and brands in parallel, which means they could potentially shift everything across in future. |

## Our API Management Solutions:

We're working with organizations that might be investigating API management solutions at present – those looking into new API solutions, or if they're using one but need more advice. This is especially key for those looking to comply with Open Banking and PSD2.

We're partners to some of the top players in this area, and we can help by:

- Setting up an API Strategy
- Selecting the right API Management platform
- Providing demos on the right software
- Advising on how to discount the license
- Setting up API Standards and best practices
- Enabling the Dev community running Hackathons etc
- Building / managing APIs

Clearly there is a lot of work to do, but also many opportunities to be had. We are keen to help banks in any of these scenarios. Please contact us for a free consultation and impartial advice.

## A Decision Point has arrived for European Banks:

PSD2 presents significant opportunities to grow new revenue streams, capture customer ownership and progress towards an extended ecosystem centered on the 'Everyday Bank'. However the largest share of the spoils will go to those banks that move first to capitalize on these opportunities

The imperative for banks is to leverage API integration and their existing customer relationships in order to develop a customer value ecosystem centered around their own banking portals. Accenture believes four primary strategic options are available to banks in order to respond effectively to the threats and opportunities of PSD2— while deciding whether to become a banking ‘utility’, or to continue to play a central role at the heart of their customer’s daily lives.

## Strategic options for banks to respond to the threats and opportunities of PSD2

**Strategic Option 1:** Comply with PSD2 Accenture’s view is that banks which seek to achieve minimum compliance with PSD2 risk disintermediation and a loss in volume and quality of customer interactions. However, as competition intensifies in the financial services industry, banks must prioritize their investment and have a clear strategy for developing and maintaining their core business. For some banks, a valid decision may be to narrow the focus of their business model towards the provision of liquidity and infrastructure services. In such cases, the bank becomes a ‘utility’ managing underlying customer accounts, processing payment transactions, and providing liquidity and credit services which are offered to the customer through a TPP who owns the customer experience

**Strategic Option 2:** Facilitate & Monetize Access Although PSD2 mandates the opening of certain bank APIs, these are restricted to payment account transaction and balance data, Credit Transfer initiation and account identity verification. Access via APIs to additional customer data in relation to non-payment accounts, customer demographics, identity documentation and direct debit mandates is entirely optional.

This means banks have a choice over whether to extend their API development beyond the minimum requirements and enable a customer to retrieve additional data sets as described above. Banks could also extend development to enable the creation of Standing Orders and Direct Debit Mandates or the completion of product applications via API. By taking this step, banks gain opportunities to monetize these additional APIs as well as to collaborate with third parties to create new products and services based on these data sets and niche customer needs. An example of such a service would be the sharing of a customer’s mortgage data and identity documents with a home insurance provider (with the customer’s consent).

**Strategic Option 3:** Provide Advice & New Services—Monetize Insight Leveraging customer insight empowers the bank to provide a highly customer centric, digital banking portal, and create a customer value ecosystem consisting of symbiotic or mutually beneficial relationships between the bank and TPP that create value for the

customer. Such services can enhance customer loyalty as well as open new revenue opportunities for both bank and TPP.

A bank could significantly improve its ability to sell customer insight by offering PISP and AISP services as well, due to the increased availability of customer data and touch points. However API integration is not strictly necessary with referral based partners.

**Strategic Option 4:** Expand the Ecosystem & Aggregate Value Beyond the monetization of APIs and customer insight, investment in open APIs could present opportunities for more integrated partnerships between banks and third party companies within and outside of the financial services industry. Such partnerships could manifest themselves in two ways:

- **Consolidation of services**—new products/services owned by third parties but offered via the bank's online portal
- **Consolidation of data**—customer data owned on third party systems but presented on the bank's online portal

An open API infrastructure and the consolidation of customer data from multiple third party sources transform the online banking portal into a platform reflecting the customer's everyday needs and transactions. By establishing itself at the center of this ecosystem of both financial and non-financial services, the bank can become a pivotal part of a customer's daily life, acting as:

- **Advice Provider**: Providing specific buying suggestions, based on deep customer knowledge and purchasing algorithms
- **Value Aggregator**: Assembling components (financial and non-financial, own and third parties') to create an integrated solution for 'real world' customer needs
- **Access Facilitator**: Supporting the customer in 'everyday/everywhere' buying processes (shopping, access to daily services)

## Recommendations for banks:

Banks should look broadly at the evolution of customer journeys (in both retail and corporate environments) and at the changes in how participants interact in diverse ecosystems. What value is at risk? Which pieces of the value chain must the bank support to increase value under PSD2? No bank can deliver all use cases to all customer segments. Depending on the markets they serve, some banks will emphasize consumer-oriented "lifestyle" use cases, and others will focus on new use cases for corporate clients. Staying focused on the markets and use cases where they can beat the competition on a sustained basis, banks should follow the steps below as they build a strategy for PSD2:

- ***Define the bank's ambition, and be prepared either to lead or to execute a fast-follower approach.*** It is critical to establish a mechanism to identify, test, and, if successful, scale up use cases faster than the competition.
- ***Conduct a comprehensive use-case evaluation.*** Banks should weigh carefully the strategic impact of potential business opportunities arising from PSD2. What is the potential of each use case to augment customer touch points and data stores, increase revenue, and expand market share? In addition to gains and losses in revenue and the cost of technology upgrades, the use case should also consider the necessary changes in bank culture and talent pool.
- ***Evaluate the potential of data (and customer touch points) as a core asset.*** Recognizing the potential to apply advanced analytics to internal data reserves to enhance fraud detection, customer relationship management, and credit scoring, several banks are already leveraging existing customer data to jump ahead of the competition. Over the next 18 months, banks should act aggressively to optimize the use of proprietary data, particularly for cross-selling and loan pricing, in retail as well as corporate banking.
- ***Consider building a finance-based ecosystem or leveraging an existing one.*** While requiring significant management attention and potentially capital investments as well, ecosystems offer the opportunity to co-opt some third-party organizations, retain customer touch points, generate additional data on customers, increase pricing power, and tap new sources of revenue. Developing an ecosystem strategy is particularly relevant for larger, primarily branch-based incumbents.
- ***Define the group wide strategy for opening up under API banking.*** Banks should assess the IT implications of PSD2 both for transaction platforms and group wide systems and architecture. Winning under PSD2 is not simply a matter of maintaining connectivity for account queries and transaction initiation, but also seizing the opportunity to reduce costs and improve response times by streamlining the IT architecture, from account servicing to group wide data management. IT design should be flexible to accommodate fast-evolving fraud controls and regulatory standards.
- ***Identify potential technology partners.*** How can a bank attract the right PSPs to their solutions-development "sandbox"? Banks should leverage the strengths of fintech innovators, established technology providers, and even other banks that can deliver flexible technology solutions for customer use cases to support continual innovation.

# KEY CHANGES FROM THE PREVIOUS DIRECTIVE

PSD2 reflects significant changes to the payments market. These changes include:

## Extended coverage:

PSD2 will cover both intra-EEA (European Economic Area) payments, as well as 'One Leg Out' payments – such as when the beneficiary or originator is located outside the EEA.

## Transaction charges:

Payments in currencies where the originator and beneficiary are in EEA countries will use charge option 'SHA'. This means that transaction charges will be shared between the payer and payee.

## New entrants & competition:

The EU is removing barriers for new entrants to the finance industry and, thus, is welcoming competition between new tech services and the established banks. The objective is that in the near future consumers will be able to view all of their bank accounts, payments' accounts and bills in one place, such as an Application Programming Interface (API), through third-party providers. Of course, the payment account holder will have to give prior consent for this to take place. Furthermore, new players will be able to access the aforementioned accounts (with prior consent) to make payments via credit transfers on behalf of their customers.

This could be revolutionary. Until now, a new entrant had to obtain near-to-impossible licenses, which are mostly held by credit institutions, such as banks. PSD2 is meant to streamline this process for new companies, allow them to compete with each other and with the established institutions.

## Increased customer protection:

Strong Customer Authentication (SCA) will be implemented in order to reduce the risk of fraud. This means that when accessing their data or accounts, users will have to take two or more independent actions in order to enhance protection. These include:

- Knowledge – something only the user knows (password, PIN, etc.)
- Possession – something only the user possesses (card or other material)
- Inherence – something the user is (fingerprint, voice or facial recognition)
- For remote transactions (internet, mobile), a unique authentication code will dynamically link transactions to the respective amount and payee

These elements will have to be applied each time a user makes a payment above a certain amount (unless the beneficiary is already identified). These will apply only the first time a user accesses their payment account, and then every 90 days.

## Regulation of Third Party Payment Providers (TPPs):

TPPs are Payment Service Providers who do not hold customer payment accounts. Under PSD2 there are two main types: Payment Initiation Service Providers (PISPs) and Account Information Service Providers (AISPs). PISPs will initiate a payment from a customer's bank account on their behalf, and AISPs will provide account aggregation services to customers. Under PSD2, banks are responsible for giving PISPs and AISPs access to a customer's account upon their consent.

## EU-wide and beyond:

If one of the parties processing a transaction is located outside the EU, the transaction is still under the scope of PSD2. This includes all official currencies (excluding crypto currencies) and aims to offer more information for the consumer and more protection for the European part of the transaction.

## Refunds:

The unconditional right of refund for Direct Debit until up to 8 weeks after payment will become a formal legal requirement. This already applies to the European Payments Council Debit scheme (EPC SDD).

## Surcharging ban:

Surcharging for card payments will be banned. This applies to card payments that are subject to interchange fee caps under the Interchange Fee Regulation.

## Unauthorized payments:

Consumers will not pay more than €50 (compared to €150 previously) for unauthorised payments, except in situations such as fraud or gross negligence.

These are the main changes and impacts that are taking place under PSD2. Reach out to the following sources if you would like to dig in deeper into PSD2 literature: European Payments Council, FCA and Payments UK.

# GUIDELINES ON FRAUD REPORTING UNDER PSD2:

The Guidelines, which are addressed to payment service providers and competent authorities, are aimed at contributing to the objective of PSD2 to increase the security of retail payments in the EU.

**The European Banking Authority (EBA) published today its final Guidelines on fraud reporting under the revised Payment Services Directive (PSD2). These Guidelines, which the EBA developed in close cooperation with the European Central Bank (ECB) and which are addressed to payment service providers and competent authorities, are aimed at contributing to the objective of PSD2 of enhancing the security of retail payments in the EU.**

These Guidelines require payment service providers across the 28 EU Member States to collect and report data on payment transactions and fraudulent payment transactions using a consistent methodology, definitions and data breakdowns.

Having assessed the responses received to the consultation paper (CP) it had published in August 2017, the EBA decided to make a number of changes to the Guidelines and related annexes. In particular, the final Guidelines now no longer require quarterly reporting of high-level data and a more detailed set of data on a yearly basis, but the reporting of a uniform set of data on a semi-annual basis instead.

The geographical scope of the data, too, has been reduced in size and complexity compared to the draft Guidelines that had been proposed in the CP, as the Guidelines do no longer require country-by-country data breakdowns and there is now a uniform geographical breakdown (instead of three different ones). In addition, fraudulent transactions where the payer is the fraudster are no longer within the scope of the Guidelines. Furthermore, jointly with the ECB, the EBA has made particular efforts further to align the Guidelines with related reporting requirements, in particular with the ECB Regulation on payment statistics (ECB/2013/43).

## Legal basis and background:

These Guidelines have been drafted in accordance with Article 96(6) of Directive (EU) 2015/2366 on payment services in the internal market (PSD2), which states that "Member States shall ensure that payment service providers provide, at least on an annual basis, statistical data on fraud relating to different means of payment to their competent authorities. Those competent authorities shall provide EBA and the ECB with such data in an aggregated form".

**Press contacts:** Franca Rosa Congiu

**E-mail:** press@eba.europa.eu

**Tel:** +44 (0) 207 382 1772

# FREQUENTLY ASKED QUESTIONS:

## GENERAL QUESTIONS

### What is the Payment Services Directive?

The first Payment Services Directive (PSD1) was adopted in 2007. This legislation provides the legal foundation for an EU single market for payments, to establish safer and more innovative payment services across the EU. The objective was to make cross-border payments as easy, efficient and secure as 'national' payments within a Member State.

Since 2007, this Directive has brought substantial benefits to the European economy, easing access for new market entrants and payment institutions, and so offering more competition and choice to consumers. It offered economies of scale and helped the Single Euro Payments Area (SEPA) in practice. The first PSD has meant more transparency and information for consumers, for example about execution time and fees; and it has cut execution times, strengthened refund rights, and clarified the liability of consumers and payment institutions. A very tangible benefit is that payments are now easier and quicker throughout the whole EU: payments are usually credited to the payment receiver's account within the next day.

### Why did the Commission propose to review this Directive?

The Commission proposed to review PSD1 to modernise it to take account of new types of payment services, such as payment initiation services (see question 18). These service providers have brought innovation and competition, providing more, and often cheaper, alternatives for internet payments; but were previously unregulated. Bringing them within the scope of the PSD has boosted transparency, innovation and security in the single market and created a level playing field between different payment service providers.

At the same time, certain rules set out in the first PSD, such as the exemptions of a number of payment-related activities from the scope of the Directive (payment services

provided within a “limited network” or through mobile phones or other IT devices) have been transposed or applied by Member States in different ways, leading to regulatory arbitrage and legal uncertainty. In a number of areas, it has also led to impaired consumer protection and competitive distortions. Updated definitions ensure a level playing field between different providers and address in a more efficient way the consumer protection needed in the context of payments.

The Commission proposed to revise the Payment Services Directive (PSD1) in July 2013. The proposal was part of a package of legislative measures on payment services, which included a proposal for a Regulation on interchange fees for card-based payment transactions (the Interchange Fee Regulation). The Interchange Fee Regulation 2015/751 entered into force on 9 June 2015.

## What are the main objectives of the revised Directive?

The revised Payment Services Directive (PSD2) updates and complements the EU rules put in place by the Payment Services Directive (PSD1, 2007/64/EC). Its main objectives are to:

- Contribute to a more integrated and efficient European payments market
- Improve the level playing field for payment service providers (including new players)
- Make payments safer and more secure
- Protect consumers

## WHAT IS PSD 1?

Adopted in 2007 and implemented in 2009, the Payment Services Directive (PSD1) aimed to create a single market for payments in the European Union, as well as provide a foundation for the Single Euro Payments Area (SEPA). Its main objective was to make cross-border payments as easy, inexpensive and secure as domestic payments.

However, as the digital economy developed, new services began to appear – services that lay outside of the scope of PSD1.

## What are the main differences between PSD1 and PSD2?

PSD2 widens the scope of PSD1 by covering new services and players as well as by extending the scope of existing services (payment instruments issued by payment service providers that do not manage the account of the payment service user), enabling their access to payment accounts.

PSD2 also updates the telecom exemption by limiting it mainly to micro-payments for digital services (see question 9), and includes transactions with third countries when

only one of the payment service providers is located within the EU ("one-leg transactions"). It also enhances cooperation and information exchange between authorities in the context of authorisation and supervision of payment institutions. The European Banking Authority (EBA) will develop a central register of authorised and registered payment institutions.

To make electronic payments safer and more secure, PSD2 introduces enhanced security measures to be implemented by all payment service providers, including banks. In particular, PSD2 requires payment service providers to apply strong customer authentication (SCA) for electronic payment transactions as a general rule. To that end, the Commission adopted rules that spell out how strong customer authentication (SCA) is to be applied.

## What is a PISP?

A PISP will be able to initiate payments on behalf of a customer from the customer's account with a bank (the ASPSP).

For example, someone making a purchase online can initiate a credit transfer via a PISP instead of using a debit or credit card. When customers choose this option, they agree to share their bank credentials with the PISP. The PISP then initiates a payment for the customer and the ASPSP will then execute the payment and debit the customer's account.

Under PSD2, a PISP must:

- Have a PISP licence in their home country, and get passporting rights to operate in other European host countries.
- Not hold the payer's funds at any time, but only initiate payments in connection with the provision of the payment initiation service.
- Ensure that the personalised security credentials of the customer are not accessible to any other parties, and that they are transmitted by the PISP through safe and efficient channels.
- Ensure that any other information about the customer, obtained when providing payment initiation service, is only provided to the payee and only with the customer's explicit consent.
- Ensure that every time a payment is initiated, communications between all parties are conducted in a secure way.
- Not store sensitive payment data of the customer. Not request from the customer any data other than that which is necessary to provide the payment initiation service.
- Not use, access or store any data for purposes other than for the provision of the payment initiation service as explicitly requested by the payer.

- Not modify the amount, the recipient or any other feature of the transaction.

## What is an AISP?

An AISP provides details on transactions and balances, and accesses account information.

With a customer's consent, AISPs will provide account aggregation services across different banks within the EEA to a customer, offering a view of multiple accounts in a single place. This means customers can have access to a comprehensive, aggregated view of their payment accounts via a single portal.

Under PSD2, an AISP must:

- Have an AISP licence in their home country, and get passporting rights to operate in other European host countries.
- Provide services only based on the customer's explicit consent.
- Ensure that the personalised security credentials of the customer are not accessible to other parties, and that, when they are transmitted by the AISP, that it is done through safe and efficient channels.
- Identify itself at each session to the ASPSP (ie bank) of the customer and securely communicate with the ASPSP and the customer.
- Access only the information from the designated payment accounts and associated payment transactions.
- Not request sensitive payment data linked to the payment accounts.
- Not use, access or store any data for purposes other than for performing the account information service explicitly requested by the customer, in accordance with data protection rules.

## What is open banking?

As the name suggests, open banking is all about opening up banking data, to help consumers make the right financial choices.

For the longest time, banks have sat on some of the most valuable data in the world: the details of all our transactions. Banks know how much we spend on food and rent, where we travel, and how we spend our leisure time – but they've never made it easy for us to share that data, *our data*, with other people or companies.

Banks also hold onto other important data, such as the locations of every cash machine in the country, and the exact details of overdrafts, credit cards, loans and mortgages – financial products that impact the lives of millions of people.

# KEY BENEFITS

## What are the benefits for consumers under this Directive?

### A. Economic benefits

The new EU rules should help stimulate competition in the electronic payments market, by providing the necessary legal certainty for companies to enter or continue in the market. This would then allow consumers to benefit from more and better choices between different types of payment services and service providers.

During the past years, new players have emerged in the area of internet payments offering consumers the possibility to pay instantly for their internet bookings or online shopping without the need for a credit card (around 60% of the EU population does not have a credit card). These services establish a payment link between the payer and the online merchant via the payer's online banking module. These innovative and low cost payment solutions are called “payment initiation services” and are already offered in a number of Member States (e.g. Sofort in Germany, IDeal in the Netherlands, and Trustly in Sweden). Until now, these new providers were not regulated at EU level. The new Directive will cover these new payment providers (“payment initiation services”), addressing issues which may arise with respect to confidentiality, liability or security of such transactions.

Furthermore, PSD2 will help lower charges for consumers and ban "surcharging" for card payments in the vast majority of cases (including all popular consumer debit and credit cards), both online and in shops. The practice of surcharging is common in some Member States, notably for online payments and specific sectors, such as the travel and hospitality industry. In all cases where card charges imposed on merchants are capped, in accordance with the complementary regulation on interchange fees for card-based payment transactions (the Interchange Fee Regulation), merchants will no longer be allowed to surcharge consumers for using their payment card. This will apply to domestic as well as cross-border payments. In practice, the prohibition of surcharging will cover some 95% of all card payments in the EU and consumers would be able to save more than €550 million annually. The new rules will contribute to a better consumer experience when paying with a card throughout the European Union.

Consumers will be better protected against fraud and other abuses and payment incidents, with improved security measures in place. As regards losses that consumers may face, the new rules streamline and further harmonise the liability rules in case of unauthorised transactions, ensuring enhanced protection of the legitimate interests of payment users. Except in cases of fraud or gross negligence by the payer, the

maximum amount a payer could, under any circumstances, be obliged to pay in the case of an unauthorised payment transaction will decrease from €150 to €50.

**B. Consumers' rights:**

PSD1 and PSD2 protect consumer rights in the event of unauthorised debits from an account under certain conditions. A direct debit is a payment that is not initiated by the payer, but by the payee on the basis of consent of the payer to the payee. It is based on the following concept: "I request money from someone else with their prior approval and credit it to myself". The payer and the biller must each hold an account with a payment service provider and the transfer of funds (money) takes place between the payer's bank and the biller's bank. However, since the biller can collect funds from a payer's account, provided that a mandate has been granted by the payer to the biller, the payer should also have a right to get the money refunded. Member States have applied different rules with regard to this issue.

Under PSD1, payers had the right to a refund from their payment service provider in case of a direct debit from their account, but only under certain conditions. In order to enhance consumer protection and promote legal certainty further, PSD2 provides a legislative basis for an unconditional refund right in case of a SEPA direct debit during an 8 week period from the date the funds are debited form the account. The right to a refund after the payee has initiated the payment still allows the payer to remain in control of his payment. In such cases, payers can request a refund even in the case of a disputed payment transaction.

As far as the direct debit schemes for non-euro payments are concerned, where they offer the protection as set out under PSD1, they can continue to function as they do today. However, Member States may require that for such direct debit schemes refund rights are offered that are more advantageous to payers.

Consumers will also be better protected when the transaction amount is not known in advance. This situation can occur in the case of car rentals, hotel bookings, or at petrol stations. The payee will only be allowed to block funds on the account of the payer if the payer has approved the exact amount that can be blocked. The payer's bank shall immediately release the blocked funds after having received the information about the exact amount and at the latest after having received the payment order.

Furthermore, the new Directive will increase consumer rights when sending transfers and money remittances outside the EU or paying in non-EU currencies. PSD1 only addresses transfers inside the EU and is limited to the currencies of the Member States. PSD2 will extend the application of PSD1 rules on transparency to "one-leg transactions", hence covering payment transactions to persons outside the EU as regards the “EU part” of the transaction. This should contribute to better information of

money remitters, and lower the cost of money remittances as a result of higher transparency on the market.

Finally, the new Directive will oblige Member States to designate competent authorities to handle complaints of payment service users and other interested parties, such as consumer associations, concerning an alleged infringement of the directive. Payment service providers that are covered by the Directive on their side should put in place a complaints procedure for consumers that they can use before seeking out-of-court redress or before launching court proceedings. The new rules will oblige payment service providers to answer in written form to any complaint within 15 business days.

**C. Payment security:**

The new rules also provide for a high level of payment security. This is a key issue for many payment users and notably consumers when paying via the internet. All payment service providers, including banks, payment institutions or third party providers (TPPs), will need to prove that they have certain security measures in place ensuring safe and secure payments. The payment service provider will have to carry out an assessment of the operational and security risks at stake and the measures taken on a yearly basis.

## How will PSD2 benefit potential market entrants and contribute to the Single Market?

**Market entrants:**

Since the adoption of PSD1, new services emerged in the area of internet payments, where so called third party providers (TPPs) offer specific payment solutions or services to customers. For example, there are services which collect and consolidate information on the different bank accounts of a consumer in a single place ("account information services - AIS"). These services will typically allow consumers to have a global view on their financial situation and to analyse their spending patterns, expenses, financial needs in a user-friendly manner. Other third party providers facilitate the use of online banking to make internet payments (so-called "payment initiation services - PIS"). They help to initiate a payment from the user account to the merchant account by creating a software “bridge” between these accounts, fill-in the information necessary for a transfer (amount of the transaction, account number, message) and inform the merchant once the transaction has been initiated.

Until now, entering the market of payments was complicated for TPPs, as many barriers were preventing them from offering their solutions on a large scale and in different Member States. With these barriers removed, more competition is expected with new players entering new markets and offering cheaper solutions for payments to more and more consumers throughout Europe. The TPPs will have to follow the same rules as the

traditional payment service providers: registration, licensing and supervision by the competent authorities. In addition, new security requirements included in the text of the PSD2 will oblige all payment service providers to step up the security around online payments.

**Single Market**

PSD2 will allow consumers and merchants to benefit fully from the internal market, particularly in terms of e-commerce. The Directive aims to help develop the EU market for electronic payments, which will enable consumers, retailers and other market players to enjoy the full benefits of the EU internal market, in line with the digital single market. Such further integration is becoming increasingly important as the world moves beyond bricks-and-mortar trade towards a digital economy.

# SCOPE OF THE DIRECTIVE

## What is the scope of the Directive?

The Directive applies to payment services in the European Union. The Directive focuses on electronic payments, which are more cost-efficient than cash and which also stimulate consumption and economic growth.

There are a number of payment means (including cash and cheques) not falling within the scope of this Directive.

## Will the new rules also apply to international payments?

While PSD1 only applies to intra-EU payments, PSD2 extends a number of obligations, notably information obligations, to payments to and from third countries, where one of the payment service providers is located in the European Union.

The extension of the scope has implications primarily for the banks and other payment service providers that are located in the EU. In practice, this means that these financial services providers shall provide information and transparency on the costs and conditions of these international payments, at least in respect of their part of the transaction. They can also be held liable for their part of the payment transaction if something goes wrong that is attributable to them.

Moreover, the extension in scope will also have as an effect that the same rules will apply to payments that are made in a currency that is not denominated in Euro or another Member State's currency.

This will be an important improvement for consumer protection in particular in the area of global money remittances.

### To what extent will payments through telecom operators be covered by this Directive?

Under PSD1, payments made through a telecom operator were not covered, where the telecom operator acts as an intermediary between the consumer and the payment service provider (by operator billing or direct to phone-bill purchases). Under PSD2, the purchase of physical goods and services through a telecom operator now falls within the scope of the Directive.

Under the new rules, the exclusion for payments through telecom operators has also been further specified and narrowed down. The exclusion now covers only payments made through telecom operators for the purchase of digital services such as music and digital newspapers that are downloaded on a digital device or of electronic tickets or donations to charities.

## ENHANCED RULES ON AUTHORISATION AND SUPERVISION OF PAYMENT INSTITUTIONS

### Will there be changes in the authorisation requirements for payment institutions?

Under PSD2, payment institutions are required to fulfill a variety of requirements in order to obtain an authorisation to provide payment services. These requirements are largely the same as under PSD1.

The main changes relate to the enhanced levels of payment security under PSD2. Entities that wish to be authorised as a payment institution shall provide with their application a security policy document, as well as a description of security incident management procedure, contingency procedures etc.

Capital requirements which aim to ensure financial stability have largely remained the same under PSD2 as they were set out in PSD1. Specific capital requirements have been defined for third party service providers in relation to their respective activities and the risks these represent. Third party service providers are not subject to own fund requirements. However, they need to hold a professional indemnity insurance covering the territories in which they offer services.

### Will the rules change for waived payment institutions?

Under PSD1, entities with an average volume of monthly payment transactions below €3 million can benefit from a lighter authorisation regime, if their Member State of establishment makes use of that option.

This so-called "waiver" regime will be maintained under PSD2 as an option for Member States, albeit with this difference, that Member States making use of the option can decide to define a lower threshold under which such "waivers" can be granted.

Payment institutions that have obtained a waiver under PSD1 may need to re-assess their status under PSD2, depending on whether the Member State that has made use of the option under PSD1 decides to continue to make use of the option and/or to lower the threshold under which the waiver is granted.

## What are the changes for limited networks under this Directive?

As under PSD1, payment transactions based on a specific payment instrument within a limited network - for instance a chain of department stores or a network of petrol stations under the same brand offering a dedicated payment instrument to their customers - are outside the scope of the Directive. In order to ensure a more coherent supervision of such networks across the Union, the Directive provides that networks, when their activities reach a certain value, shall notify these activities to competent authorities, so that these can assess whether or not the network shall apply for a licence as a payment institution. This is to ensure that the financial risks for consumers are minimised.

## Will this Directive strengthen the supervision of payment institutions that provide services cross-border?

As a main principle, payment institutions are supervised by the Member State where they are authorised to provide the defined payment services (the so-called 'home Member State').However, if the payment institution provides these services through established agents or branches in the other Member State (the host Member State), that Member State can act in case of an infringement or a suspected infringement of EU rules under the Directive.

In this respect, the supervision under PSD2 has not changed. However, to reinforce the investigative and supervisory powers of the host Member State, PSD2 has introduced a more detailed pass porting procedure. This procedure will ensure better cooperation and information exchange between the national competent authorities. Furthermore, the host Member State can ask payment institutions operating with agents and branches in its territory to regularly report on their activities. To that end, the payment institution can be requested to set up a central contact point in the host territory (see question 15 below). In emergency situations, requiring immediate action, the host Member State is allowed to take precautionary measures with regard to the payment institution concerned, in parallel to the host's duties of cooperation with the home Member State to find a remedy.

The European Banking Authority has been mandated to draft regulatory technical standards on the cooperation and information exchange between authorities.

### Is there a need to set up a central contact point in a Member State if they are providing payments services cross border?

PSD2 contains an option for Member States to require a payment institution that provides cross-border payment services to set up a central contact point if it operates with agents or branches that are established in their territory. The central contact point shall ensure adequate communication and information with regard to the activities of the payment institution in the host territory. The European Banking Authority is mandated to draft regulatory technical standards on the criteria under which a central contact point can be requested, and the functions of such contact point.

The fourth Anti-Money Laundering Directive (Directive EU/2015/849) also contains an option for Member States to request a central contact point in its territory. The set-up of such a contact point, however, can only be requested for the purpose of ensuring compliance with the money laundering and anti-terrorist financing rules. This provision should be distinguished from the Member States option under PSD2, which can only be invoked for the purpose of adequate communication and information by the payment institution on compliance with the rules under PSD2.

### Will payment institutions be able to access accounts maintained by credit institutions?

For payment institutions, access to a payment account maintained by a credit institution is vital for the operation of their business. PSD2 provides specifically that Member States will have to ensure that credit institutions do not block or hinder access to payment accounts and that payment institutions have access to credit institutions' payment accounts services in an objective, non-discriminatory and proportionate manner. This aspect is very relevant for money remittance services as many of them have lost access to the banking system in the recent years.

## SECURITY OF PAYMENTS:

### What is strong customer authentication?

The PSD2 text introduces strict security requirements for the initiation and processing of electronic payments, which apply to all payment service providers, including newly regulated payment service providers. This stricter approach on security should contribute to reducing the risk of fraud for all new and more traditional means of

payment, especially online payments, and to protecting the confidentiality of the user's financial data (including personal data).

Payment service providers will be obliged to apply so-called strong customer authentication (SCA) when a payer initiates an electronic payment transaction. Strong customer authentication is an authentication process that validates the identity of the user of a payment service or of the payment transaction (more specifically, whether the use of a payment instrument is authorised). Strong customer authentication is based on the use of two or more elements categorised as knowledge (something only the user knows, e.g. a password or a PIN), possession (something only the user possesses, e.g. the card or an authentication code generating device) and inherence (something the user is, e.g. the use of a fingerprint or voice recognition) to validate the user or the transaction. These elements are independent (the breach of one element does not compromise the reliability of the others) and designed in such a way as to protect the confidentiality of the authentication data. On 27 November 2017, the Commission adopted rules that spell out how strong customer authentication (SCA) is to be applied."

For remote transactions, such as online payments, the security requirements go even further, requiring a dynamic link to the amount of the transaction and the account of the payee, to further protect the user by minimizing the risks in case of mistakes or fraudulent attacks.

## Will all payments have to apply strong customer authentication? Are exemptions possible?

As a matter of principle, all electronic means of payment are subject to strong customer authentication. However, exemptions to the principle of strong customer authentication (SCA) are possible, as it is not always necessary and convenient to request the same level of security from all payment transactions.

These exemptions have been defined by the European Banking Authority (EBA) and adopted by the European Commission, taking account of the risk involved, the value of transactions and the channels used for the payment.

Such exemptions include low value payments at the point of sale (to facilitate the use of mobile and contactless payments) and also for remote (online) transactions. The exemptions from strong customer authentication seek to avoid disrupting the ways consumers, merchants and payment service providers operate today. They are also based on the fact that there are alternative authentication mechanisms that are equally safe and secure.

# RULES FOR NEW TYPES OF PAYMENT SERVICE PROVIDERS

## What are payment initiation services?

The PSD2 opens the EU payment market for companies offering consumer or business-oriented payment services based on the access to the information from the payment account – so called "payment initiation services providers" and "account information services providers". Payment initiation services providers typically help consumers to make online credit transfers and inform the merchant immediately of the payment initiation, allowing for the immediate dispatch of goods or immediate access to services purchased online. For online payments, they constitute a true alternative to credit card payments as they offer an easily accessible payment service, as the consumer only needs to possess an online payment account.

## What are account information services?

Account information services allow consumers and businesses to have a global view on their financial situation, for instance, by enabling consumers to consolidate the different payment accounts they may have with one or more banks and to categorize their spending according to different typologies (food, energy, rent, leisure, etc.), thus helping them with budgeting and financial planning.

## What is payment instrument issuing?

The issuing of a payment instrument is one of the payment services that falls within the scope of PSD1 and of PSD2. Any authorised payment service provider, be it a bank or a payment institution, can issue payment instruments. Payment instruments do not only cover payment cards, such as debit cards and credit cards, but any personalized device or set of rules agreed between the issuer and the user used to initiate a payment.

PSD2 allows payment service providers that do not manage the account of the payment service user to issue card-based payment instruments to that account and to execute card-based payments from that account. Such “third party” payment service provider – which could be a bank not servicing the account of the payer – will be able, after consent of the user, to receive from the financial institution where the account is held a confirmation (a yes/no answer) as to whether there are sufficient funds on the account for the payment to be made.

## What opportunities will these providers offer to consumers and enterprises?

The "payment initiation services providers" allow consumers that shop online to pay for their purchases through a simple credit transfer from their payment account. In some countries, these services are already in use (55% of internet payments in the Netherlands). By providing a proper legal framework in which these services can be offered, PSD2 opens possibilities for providers of these services to operate across the EU and to compete on an equal basis with other regulated players in the market, such as banks.

Account information service providers already exist today and offer tools that allow companies and consumers to have a consolidated view of their financial situation. Nowadays, these services are not regulated, at least at EU level. PSD2 will provide for a common framework with clear conditions under which these providers can access the financial information on behalf of their clients. This will allow these services providers to operate without hindrance and to reach a broader audience which normally does not make use of such account managing services.

Today, account holders are not obliged to use payment instruments offered by the same payment service provider with which they hold their account. For example, credit cards are not only provided by the bank where the user holds its account, but also by third party providers. This does not work, however, in the case of debit cards, where payment service providers have found it very difficult to offer such payment service in connection to accounts not held by them. The source of these difficulties is the fact that these third providers do not have access to feedback information on the availability of funds on the account held by other financial institution. PSD2 lifts this obstacle, which is likely to see consumers benefit from competitive card services offered by third party providers.

## Will these providers be subject to the same rules as other payment institutions i.e. authorisation and security?

The PSD2 requires all that payment services providers be authorised and regulated. The inclusion of new payment providers within the scope of PSD2 will allow competent authorities to better monitor and supervise the activities of these new players.

PSD2 also fully clarifies the liability issues between bank servicing the account of the payer and the payment initiation service. When a payment initiation service provider is used by a payer to initiate a payment, it will be liable for any payment incidents within its sphere. In particular, the bank of the payer shall not be held liable for payment incidents that can be traced back to the initiator.

### To what extent will these providers have access to information on my payment or bank account?

These new providers will only be allowed to provide the services the payer decides to make use of. In order to provide these services they will not have full access to the account of the payer. Those offering payment instruments or payment initiation services will only be able to receive information from the payer's bank on the availability of funds (a yes/no answer) on the account before initiating the payment (with the explicit consent of the payer). Account information service providers will receive the information explicitly agreed by the payer and only to the extent they are necessary for the service provided to the payer.

The security credentials of the payment service user shall not be accessible to other third parties and will have to be transmitted through safe and efficient channels to the bank servicing the account. A dynamically generated code only valid for that specific transaction (linked to the amount and recipient) will have to be used in the authentication process.

## TRANSITIONAL PERIOD

### Is there a different date of application for the security requirements?

Without prejudice to the date of application of PSD2 (13 January 2018), a different date of application is foreseen for the new security measures - strong customer authentication and standards for secure communication - introduced in the PSD2. Their entry into force is subject to the adoption of the regulatory technical standards which have been developed by the European Banking Authority and adopted by the Commission. As a result, the new security measures shall apply 18 months after the publication in the Official Journal of these standards, currently under objection period of the European Parliament and Council.

### Will authorizations under PSD1 keep their validity under this Directive?

The text of PSD2 foresees transitional provisions for payment institutions that are already authorised to provide services under PSD1. These institutions are allowed to continue providing payment services for 30 months (authorised institutions) or 36 months (“small” institutions that benefited from the waiver under Article 26 of PSD) after the entry into force of PSD2.

In order to provide payment services beyond that transitional period, the existing payment institutions would need to submit all relevant information required under PSD2

to the competent authorities that have granted them their existing licenses and fully comply with the relevant PSD2 requirements.

In addition, Member States may provide for the existing payment institutions to be automatically granted PSD2 authorisation if the competent authority already possesses evidence that the payment institution complies with PSD2 requirements. Competent authorities shall make such an assessment on a case-by-case basis. They should inform the payment institution concerned before the authorisation is granted.

## Can existing providers of payment initiation and account information services continue to provide their services after the date of application of PSD2? As of when will they need to apply for a licence?

PSD2 provisions ensure that providers of payment initiation services (PIS) and account information services (AIS) that are already established in the market can continue to perform their activities. More specifically, PSD2 states that Member States shall allow existing PIS or AIS providers in their territories to operate in accordance with the currently applicable regulatory framework.

As the provision of PIS and AIS is a new payment service recognised in PSD2, existing and new providers of such services would need to apply for authorisation under the PSD2 regime from the date of application of the new Directive.

Furthermore, because the new security measures of PSD2 regarding strong customer authentication and standards for secure communication will become applicable later than other provisions (see answer 24), PIS and AIS providers that seek authorisation under PSD2 are not required to submit proof of compliance with these security requirements until that later date. As provision of both types of services is dependent on the authentication procedures provided by banks, upgrades to the security requirements and procedures applied by banks need to be fully implemented by banks before the application of these measures is possible for the PIS and AIS. In case banks do not comply on time with the security requirements and standards for secure communication, they cannot use this non-compliance to hinder or obstruct the use of PIS and AIS.

The delayed application of the security requirements should not create any difficulties for the provision of existing payment-related services by market players that have been operating in Member States before 13 January 2016. Article 115(5) of PSD2 ensures the continuity of these services. These payment services providers should still apply for the relevant authorisation under PSD2 to their national authority as soon as possible.

### What is the role of the Internet Security Guidelines, published by the European Banking Authority in 2014, during the transitional period?

The EBA guidelines on the security of internet payments address the issue of security of internet payments as an interim solution, until the application of the PSD2 and its more comprehensive security requirements.

When the EBA Guidelines are applied by the competent authorities of the Member States, in the transitional period, they must be interpreted in so far as there is any scope to do so, in line with the PSD2's content and objectives. As a consequence, compliance with the EBA Guidelines on the security of internet payments should not be used to justify obstructing or blocking the use of PIS or AIS.

Pending the full application of the PSD2 rules, including the rules on the security of payments, and in accordance with the PSD2 text, “Member States, the Commission, the European Central Bank and the European Banking Authority, should guarantee fair competition in that market avoiding unjustifiable discrimination against any existing player on the market”.

## RATIONALE, OBJECTIVES AND PROCESS

### What are the objectives of PSD2?

The revised Payment Services Directive (PSD2), which enters into application on 13 January 2018, will facilitate innovation, competition and efficiency. It will give consumers more and better choice in the EU retail payment market. At the same time, it will introduce higher security standards for online payments. This will make consumers more confident when buying online. PSD2 scope extends to innovative payment services and new providers in the market, such as FinTechs. These players are also called third party payment services providers (TPPs). TPPs include:

- Payment initiation services providers (PISPs): these initiate payments on behalf of customers. They give assurance to retailers that the money is on its way.
- Aggregators and account information service providers (AISPs): these give an overview of available accounts and balances to their customers.

### What are the objectives of the Regulatory Technical Standard?

Market players need specific requirements to comply with the new obligations in PSD2. To this end, PSD2 empowers the Commission to adopt regulatory technical standards (RTS) on the basis of the draft submitted by the European Banking Authority (EBA).

The security measures outlined in the RTS stem from two key objectives of PSD2: ensuring consumer protection and enhancing competition and level playing field in a rapidly changing market environment.

Consumer protection is achieved through increasing the level of security of electronic payments. This is why the RTS introduces security requirements that payment service providers must observe when they process payments or providing payment-related services. Payment services providers include banks and other payment institutions. These standards define the requirements for strong customer authentication and the instances when payment service providers can be exempted from such authentication.

Another key objective is bringing more competition and innovation in the retail payment market. In this context, the RTS includes two new types of payment services, the so-called payment initiation services and the account information services.

### Has the Commission amended the RTS submitted by the EBA?

The Commission made some limited substantive amendments to the draft RTS submitted by the EBA. This was done to better reflect the mandate of PSD2 and to provide further clarity and certainty to all interested parties.

### When will the new rules become applicable?

PSD2 will become applicable as of 13 January 2018, except for the security measures outlined in the RTS. These will become applicable 18 months after the date of entry into force of the RTS. Subject to the agreement of the Council and the European Parliament the RTS is due to become applicable around September 2019.

### To what type of accounts will this RTS apply to?

The RTS only covers payment accounts in the scope of PSD2, i.e. accounts held by one or more payment service users which can be used for the execution of payment transactions. While this definition has not changed with the adoption of PSD2, the list of payment services has evolved. It includes payment initiation services and account information services.

## STRONG CUSTOMER AUTHENTICATION (SCA);

### What does “stronger identity checks” mean in practicality?

“When customers access their payment accounts online, initiate electronic payment transactions, or carry out any other actions through remote channels that may imply a risk of payment fraud or other abuses, so called strong authentication will be required.

“Very simply, strong authentication is a procedure based on the use of two or more elements from the categories knowledge, ownership and inherence.

## How will the new RTS enhance security for electronic payments?

Thanks to PSD2 consumers will be better protected when they make electronic payments or transactions (such as using their online banking or buying online). The RTS makes strong customer authentication (SCA) the basis for accessing one's payment account, as well as for making payments online.

This means that to prove their identity users will have to provide at least two separate elements out of these three:

- something they know (a password or PIN code);
- something they own (a card, a mobile phone); and
- Something they are (biometrics, e.g. fingerprint or iris scan).

Strong customer authentication is already commonly used throughout the EU. For example, when customers pay with a card at brick-and-mortar shops they are required to validate a transaction by typing their PIN codes on card readers. However, this is not the case for electronic remote payment transactions, be it a card payment or a credit transfer from an online bank. For these transactions, SCA already is applied in some EU countries only (including Belgium, the Netherlands and Sweden). In other EU countries some payment service providers apply SCA on a voluntary basis.

The RTS sets out that strong customer authentication must be used to access one's payment account and to make online payments. Banks and other payment service providers will have to put in place the necessary infrastructure for SCA. They will also have to improve fraud management. Consumers and merchants will have to be equipped and trained to be able to operate in a SCA environment.

The RTS also allows for exemptions from strong customer authentication. This is to avoid disrupting the ways consumers, merchants and payment service providers operate today. It is also because there may be alternative authentication mechanisms that are equally safe and secure. However, payment service providers that wish to be exempted from SCA must first apply mechanisms for monitoring transactions to assess if the risk of fraud is low.

All payment service providers will need to prove the implementation, testing and auditing of the security measures. In case of a fraudulent payment, consumers will be entitled to a full reimbursement.

For online payments, security will be further enhanced by linking, via a one-time password, the online transaction to its amount and to the beneficiary of the payment.

This practice ensures that in case of hacking, the information obtained by a potential fraudster cannot be re-used by for initiating another transaction. This procedure is already in application in countries such as Belgium and has led to significant fraud reduction for online payments.

## When will strong customer authentication become mandatory?

The use of SCA will become mandatory 18 months after the entry into force of the RTS, i.e. once the RTS is published in the Official Journal of the EU, scheduled for September, 2019.

This will allow payment service providers, including banks, sufficient time to adapt their security systems to the increased security requirements defined in PSD2.

## What about security of corporate payments?

The RTS also caters for the security of payments that are carried out in batches. This is the way most corporates make payments, rather than one by one. The new rules also take into account host-to-host machine communication, where for example the IT system of a company communicates with the IT system of a bank to send messages for paying invoices. Security mechanisms for this type of communication systems can be as effective as strong customer authentication. Therefore, they can benefit from an exemption from the SCA, if this is approved by national supervisors.

## Could SCA have a negative impact on e-commerce?

The Commission wants to foster the development of e-commerce by building consumer trust. At the same time, the Commission wants to reduce fraud affecting online payments, which are particularly at risk. This entails a higher level of security and may require e-commerce market players to adapt their IT systems or their business models so that they are more secure.

Merchants will still be able to apply risk analysis to transactions with their customers. This method is often applied to card payments. The RTS does not prevent merchants from continuing to do so. Both PSD2 and today's RTS are addressed only to payment service providers, including the banks of the consumers and those of the merchants. Merchants are not in the scope of the RTS. It will be for merchants and their payment service providers to agree on how to meet the objective of reducing fraud.

# COMMON AND SECURE COMMUNICATION:

## How will common and secure communication work?

PSD2 establishes a framework for new services linked to consumer payment accounts, such as the so-called payment initiation services and account information services. In this context, the RTS specify the requirements for common and secure standards of communication between banks and FinTech companies.

Consumers and companies will be able to grant access to their payment data to third parties providing payments-related services (TPPs). These are, for example, payment initiation services providers (PISPs) and account information service providers (AISPs). TPPs are sometimes FinTech companies, but could also be other banks.

Customers will have to give their consent to the access, use and processing of their data. TPP will not be able to access any other data from the payment account beyond those explicitly authorised by the customer.

Banks will have to put in place a communication channel that allows TPPs to access the data that they need. This communication channel will also enable banks and TPPs to identify each other when accessing customer data and communicate through secure messaging at all times.

Banks may establish this communication channel by adapting their customer online banking interface. They can also create a new dedicated interface that will include all necessary information for the payment service providers.

The rules also specify the contingency safeguards that banks have to put in place when they decide to develop a dedicated interface (the so-called "fall back mechanisms"). The objective of such contingency measures is to ensure continuity of service as well as fair competition in this market.

## What makes a good dedicated communication interface?

According to the RTS, all communication interfaces, whether dedicated or not, will be subject to a 3-month 'prototype' test and a 3-month 'live' test in market conditions. The test will allow market players to assess the quality of the interfaces put in place by account servicing payment service providers, including banks.

A quality dedicated communication interface should offer at all times the same level of availability and performance the interfaces made available to a consumer or a company for directly accessing their payment account online. In addition, a quality dedicated

interface should not create obstacles to the provision of payment initiation or account information services.

Payment service providers, including banks, will have to define transparent key performance indicators and service level targets for the dedicated communication interfaces, if they decided to set them up. These performance indicators should be at least as stringent as those set for the online payment and banking platforms used by the customers.

The Commission is promoting the set-up of a market group, composed of representatives from banks, payment initiation and account information service providers and payment service users. This group will review the quality of dedicated communication interfaces. This follows up on the work carried out by the Euro Retail Payments Board on payment initiation services.

### Can banks be exempted from setting up a fall-back mechanism?

Yes. They can be exempted if they put in place a fully functional dedicated communication interface responding to the quality criteria defined by the regulatory technical standards. National authorities will grant the exemption to individual banks by national authorities, after having consulted the EBA. The role of the EBA is to ensure that national authorities have similar interpretations when they assess of the quality of dedicated interfaces. Divergences of interpretation would be detrimental to the good functioning of the Single Market for retail payments.

A national authority can revoke the exemption where a dedicated communication interface no longer meets the quality criteria defined under the RTS, for more than two consecutive calendar weeks. In this case, the national authority also informs EBA. The national authority also ensures that the bank establishes an automated fall-back mechanism. This must happen in the shortest time possible, and within 2 months at the latest.

## PROTECTION OF PERSONAL DATA:

### How is personal data protected?

Account holders can exercise control over the transmission of their personal data under both PSD2 and the Data Protection Directive (under the General Data Protection Regulation or GDPR as from May 25 of 2018). No data processing can take place without the express agreement of the consumer. In addition, payment service providers can only access and process the personal data necessary for the provision of the services the consumer has agreed to.

PSD2 regulates the provision of new payment services which require access to the payment service user´s data. For instance, this could mean initiating a payment from the customer's account or aggregating the information on one or multiple payment accounts held with one or more payment service providers for personal finance management. When a consumer seeks to benefit from these new payment services, she or he will have to request such service explicitly from the relevant provider.

Payment service providers must inform their customers about how their data will be processed. They will also have to comply with other customers' rights under data protection rules, such as the right of access or the right to be forgotten. All payment service providers (banks, payment institutions or new providers) must comply with the data protection rules when they process personal data for payment services.

### What data can TPPs access and use via "screen scraping"?

PSD2 prohibits TPPs from accessing any other data from the customer payment account beyond those explicitly authorised by the customer. Customers will have to agree on the access, use and processing of these data.

With these new rules, it will no longer be allowed to access the customer's data through the use of the techniques of "screen scraping". Screen scraping means accessing the data through the customer interface with the use of the customer's security credentials. Through screen scraping, TPPs can access customer data without any further identification vis-à-vis the banks.

Banks will have to put in place a communication channel that allows TPPs to access the data that they need in accordance with PSD2. The channel will also be used to enable banks and TPPs to identify each other when accessing these data. It will also allow them to communicate through secure messaging at all times.

Banks may establish this communication channel by adapting their customer online banking interface. They may also create a new dedicated interface that will include all necessary information for the relevant payment service providers.

The RTS specifies the contingency safeguards that banks shall put in place if they decide to develop a dedicated interface. This will ensure fair competition and business continuity for TPPs.

## CONCLUSION:

Many in the industry believe PSD2 – along with Open Application Programming Interfaces (API) – will accelerate the digital economy in banking services.

Banks will need to open up legacy systems with APIs and, through the use of Open APIs, third-party developers will be able to build applications and services around the financial institution's systems. These applications and services will provide access to the traditional banking infrastructure. For customers, this will enable them to see and manage their finances through a portal not set up or maintained by their bank(s). Customers will also be able to move money between accounts when viewed in an aggregated format.

Implementing the directive doesn't mean customers and merchants will be able to take advantage of the benefits. Compelling propositions that help all parties do what they need to in a 'frictionless' way will make all the difference and that is where HSBC will be focusing its attention.

PSD2 should increase competition with new value propositions, services and solutions with the increase of online shopping and e-procurement.

## *GLOSSARY:*

| terms | abbreviations | definitions |
|---|---|---|
| Payment Services Directive 2007/64/EC | PSD1 | Adopted in 2007 and implemented in 2009, the Payment Services Directive (PSD1) aimed to create a single market for payments in the European Union, as well as provide a foundation for the Single Euro Payments Area (SEPA). Its main objective was to make cross-border payments as easy, inexpensive and secure as domestic payments. However, as the digital economy developed, new services began to appear – services that lay outside of the scope of PSD1. |
| Revised Payment Services Directive (EU) 2015/2366 | PSD2 | The Payment Services Directive[1] (PSD, Directive 2007/64/EC, replaced by PSD 2, Directive (EU) 2015/2366) is an EU Directive, administered by the European Commission (Directorate General Internal Market) to regulate payment services and payment service providers throughout the European Union (EU) and European Economic Area (EEA). The Directive's purpose was to increase pan-European competition and participation in the payments industry also from non-banks, and to provide for a level playing field by harmonizing consumer protection and the rights and obligations for |

| | | |
|---|---|---|
| | | payment providers and users |
| Payment Service Provider | PSP | A payment service provider (PSP) offers shops online services for accepting electronic payments by a variety of payment methods including credit card, bank-based payments such as direct debit, bank transfer, and real-time bank transfer based on online banking. Typically, they use a software as a service model and form a single payment gateway for their clients (*merchants*) to multiple payment methods. |
| Payment Service User | PSU | Payment Service User is the consumer or retailer who is the user of services provided by payment service providers like banks or TPPs. |
| Two-factor authentication | 2FA | Two-factor authentication (2FA), sometimes referred to as two-step verification or dual factor authentication, is a security process in which the user provides two different authentication factors to verify themselves to better protect both the user's credentials and the resources the user can access. Two-factor authentication provides a higher level of assurance than authentication methods that depend on single-factor authentication (SFA), in which the user provides only one factor -- typically a password or passcode. Two-factor authentication methods rely on users providing a password as well as a second factor, usually either a security token or a biometric factor like a fingerprint or facial scan. |
| Account Information Service Provider | AISP | Account Information Service Providers will have to be given access to account information by the AS PSP when granted permission of the account holder. Information given by the AS PSP can subsequently be used by the AISP in order to render its service such as aggregating data relating to PSU (consumer) accounts held across one or many AS PSPs. |
| Application Programming | API | An *application program interface* (API) is a set of routines, protocols, and tools for |

| | | |
|---|---|---|
| Interface | | building software applications. Basically, an API specifies how software components should interact. Additionally, APIs are used when programming graphical user interface (GUI) components. A good API makes it easier to develop a program by providing all the building blocks. A programmer then puts the blocks together. |
| Account Servicing Payment Service Provider | ASPSP | Account Servicing Payment Service Providers are traditional financial institutions (e.g., banks) which provide accounts to consumers and from or to which the consumer issues payments |
| European Banking Authority | EBA | To build a single regulatory and supervisory framework for the entire EU banking sector |
| Payment Initiation Service Provider | PISP | Payment Initiation Service Providers will be allowed to initiate payments issued by the account owner between the AS PSP (bank) and PSU (consumer). This allows them to use the information from AS PSPs to facilitate online banking payments |
| Regulatory Technical Standards (to be issued by the EBA) | RTS | The European Commission adopted the Delegated Regulation on Regulatory Technical Standards (RTS) in November 2017. These standards provide detailed specifications to achieve the strict security requirements for payment service providers in the EU |
| Strong Customer Authentication | SCA | Strong Customer Authentication is a new *mandatory* requirement for authenticating online payments that will be introduced in Europe on September 14, 2019. It will require payments to be authenticated using at least two of the following three elements:<br>• something that only the customer *knows*<br>• something that the customer *is*<br>• something that only the customer *has* or possesses |
| Third Party Provider | TPP | Third Party Payment Service Providers is the generic term for the Third Party Account Information Service Providers (AISP) and Third Party Payment Initiation Service Providers (PISP). A TPP does not hold a |

| | | |
|---|---|---|
| | | payment account nor does it enter into possession of the funds being transferred |

## *REFERENCES:*


- ✓ https://ec.europa.eu/info/business-economy-euro/banking-and-finance/consumer-finance-and-payments/payment-services/payment-services_en
- ✓ https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366/law-details_en
- ✓ https://en.wikipedia.org/wiki/Payment_Services_Directive
- ✓ https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366/who-we-work_en
- ✓ http://europa.eu/rapid/press-release_IP-18-141_en.htm?locale=en
- ✓ http://www.finanssivalvonta.fi/en/Regulation/International_Projects/psd2/Pages/Default.aspx
- ✓ http://www.sepaforcorporates.com/single-euro-payments-area/5-things-need-know-psd2-payment-services-directive/
- ✓ https://eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-fraud-reporting-under-psd2
- ✓ http://europa.eu/rapid/press-release_MEMO-15-5793_en.htm?locale=en
- ✓ http://europa.eu/rapid/press-release_MEMO-17-4961_en.htm
- ✓ https://www.bankrate.com/uk/open-banking/what-is-open-banking/
- ✓ http://europa.eu/rapid/press-release_MEMO-15-5793_en.pdf
- ✓ http://europa.eu/rapid/press-release_MEMO-15-5793_en.pdf
- ✓ https://www.ey.com/Publication/vwLUAssets/Regulatory_agenda_updates_PSDII_Luxembourg/$FILE/Regulatory%20agenda%20updates_PSDII_Lux.pdf
- ✓ http://www.ey.com/Publication/vwLUAssets/EY-payment-services-directive-2/$FILE/EY-payment-services-directive-2.pdf
- ✓ https://www.jpmorgan.com/cm/BlobServer?blobkey=id&blobnocache=true&blobwhere=1320744067467&blobheader=application%2Fpdf&blobcol=urldata&blobtable=MungoBlobs&blobheadername1=Content-disposition&blobheadervalue1=attachment;filename=Payment%20Services%20Directive%202%20-%20What%20You%20Should%20Know%20-%202017-10-17.pdf
- ✓ http://www.matheson.com/images/uploads/documents/Payment_Services_Directive_II.pdf
- ✓ https://en.wikipedia.org/wiki/Payment_service_provider

- ✓ https://searchsecurity.techtarget.com/definition/two-factor-authentication
- ✓ https://www.cryptomathic.com/news-events/blog/an-introduction-to-the-regulatory-technical-standards
- ✓ https://europa.eu/european-union/about-eu/agencies/eba_en
- ✓ https://stripe.com/guides/strong-customer-authentication


## *ARTICLES:*


- ✓ https://www.accenture.com/t00010101T000000Z__w__/gb-en/_acnmedia/PDF-15/PSD2-Seizing-Opportunities-EU-Payment-Services-Directive-(1)-(1).pdf#zoom=50
- ✓ https://www.evry.com/en/news/articles/psd2-the-directive-that-will-change-banking-as-we-know-it/
- ✓ https://www.accenture.com/gb-en/insight-psd2-opportunities-banks
- ✓ https://www.gbm.hsbc.com/insights/technology/payment-services-directive-ii-psd2
- ✓ http://www.sepaforcorporates.com/single-euro-payments-area/5-things-need-know-psd2-payment-services-directive/
- ✓ https://www.europeanpaymentscouncil.eu/news-insights/insight/psd2-almost-final-state-play https://www.lexology.com/library/detail.aspx?g=db45d79e-9d1c-4440-9995-445f3ec67ac1
- ✓ https://smartpayments.com/banking/open-banking-and-psd2-history-european-payments/
- ✓ https://www.mckinsey.com/industries/financial-services/our-insights/psd2-taking-advantage-of-open-banking-disruption
- ✓ https://www.finextra.com/blogposting/13520/psd2-challenges-and-promises-for-the-future-of-banking
- ✓ https://www2.deloitte.com/cy/en/pages/financial-services/articles/anticipating-challenges-opportunities-psd2.html
- ✓ https://fdwconsult-be02.webnode.com/l/psd-2-the-implementation-of-psd-2-a-lot-of-opportunities-but-also-big-challenges-part-ii/
- ✓ https://www.integrella.com/2017/11/23/open-banking-and-psd2/
- ✓ https://openbankinghub.com/how-open-banking-and-psd2-create-opportunities-for-small-businesses-17383af71dd6
- ✓ https://www.worldpay.com/global/blog/2018-04/psd2-changes-and-opportunities-explained
- ✓ https://worldline.com/en/home/blog/2017/july/psd2-what-behind.html
- ✓ https://www.smartdebit.co.uk/psd2-april-2017-changes-info/
- ✓ https://www.finextra.com/blogposting/12668/psd2---what-changes


***PREPARED BY SARA ZEB AFRIDI***