Open banking in Portugal: the European Union framework

Maria Lúcia Leitão • Head of the Banking Conduct Supervision Department

8 November 2018

OPEN BANKING: A challenge to ensure consent from consumers concerning data collection, use and sharing is informed and adequate

BANCO DE PORTUGAL
EUROSISTEMA


We are an innovative, customer-centric digital bank
Digital Bank
Cool! Let's build an app on the top of your API. How can we connect?

What is open banking?

Is open banking a new jargon?

Should market conduct supervisors include open banking in their agenda?

What is an API?

Open banking is closely linked to financial innovation and is a complex topic

Open banking raises several challenges to market conduct supervisors, mainly on security and privacy

"Perhaps the most complex of these is educating end users on data permission and privacy"
(McKinsey&Company)

Open banking is also known as “open bank data”

- Consumers may make financial transactions (e.g. payments) and obtain information on their bank accounts through third party providers
- Those third party providers can access to consumers’ financial data (with their permission) through the use of application programming interfaces (APIs)

Open banking – a new point in the EU agenda

- The provision of payment services (payment initiation services and account information services) through APIs is within the scope of the **new Payments Services Directive (PSD2)**

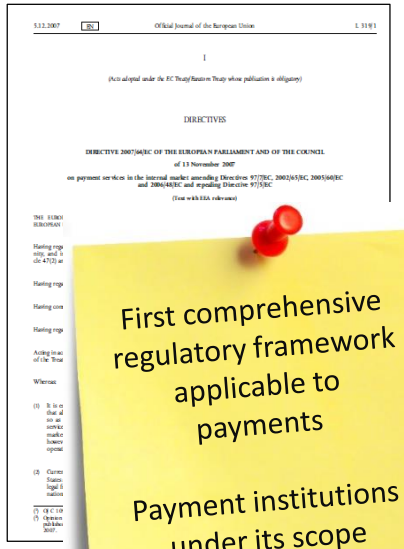
- **Specific standards** to ensure the security of communication will enter into force in **2019**

- The **European Banking Authority** is working on the implementation of these **standards** in close cooperation with national competent authorities

The evolution of the legal framework applicable to payments in the European Union

2007

Directive 2007/64/EC (PSD1)


DIRECTIVES

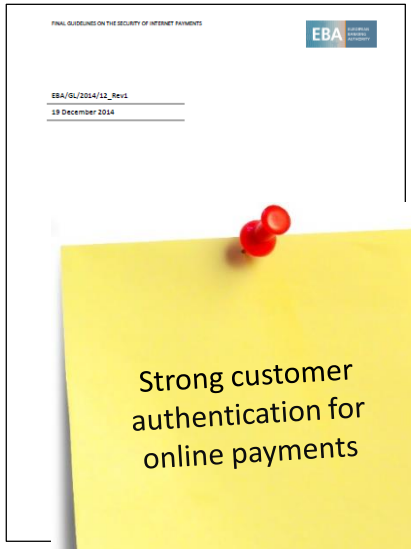
DIRECTIVE 2007/64/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 13 November 2007

First comprehensive regulatory framework applicable to payments

Payment institutions under its scope

2014

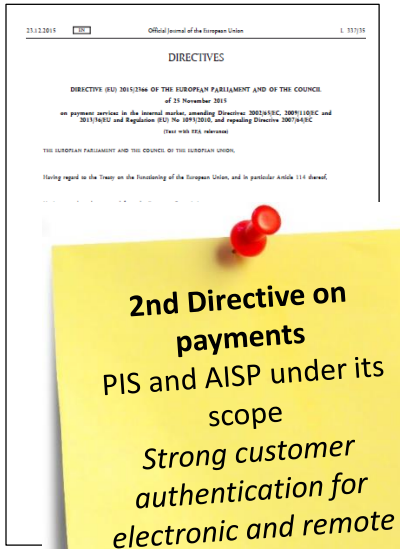
Guidelines on the security of internet payments


EBA/GL/2014/12_Rev1
19 December 2014

Strong customer authentication for online payments

2015

Directive (EU) 2015/2366 (PSD2)


DIRECTIVES

DIRECTIVE (EU) 2015/2366 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 25 November 2015

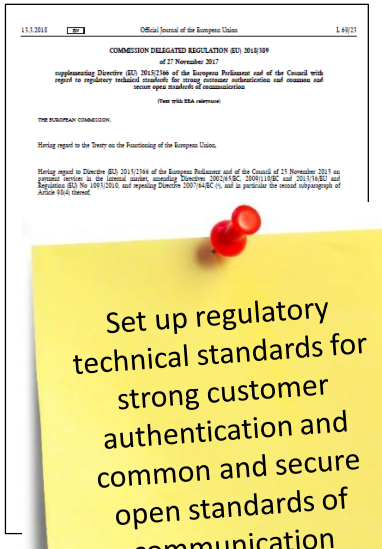
2nd Directive on payments

PIS and AISP under its scope

Strong customer authentication for electronic and remote payments

2018

Commission Delegated Regulation (EU) 2018/389


COMMISSION DELEGATED REGULATION (EU) 2018/389
of 27 November 2017

Set up regulatory technical standards for strong customer authentication and common and secure open standards of communication

Opinion of the EBA on the implementation of the RTS on SCA and CSC


EBA-Op-2018-04
13 June 2018

Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC

Guidance on regulatory technical standards for strong customer authentication and common and secure open standards of communication

Main goals of Payment Services Directive 2 (PSD2), in force since January 2018

Main goals of Payment Services Directive 2 (PSD2), in force since January 2018

- New payment services and new payment service providers under its scope:

  ✓ Payment initiation service (Payment initiation service provider – PISP)

  ✓ Account information service (Account information service provider – AISP)

  Exclusively provided via digital channels

Main goals of Payment Services Directive 2 (PSD2), in force since January 2018

- ✓ Transparency conditions and information requirements
- ✓ Protection in case of unauthorised transactions
- ✓ Complaints handling
- ✓ ADR procedures

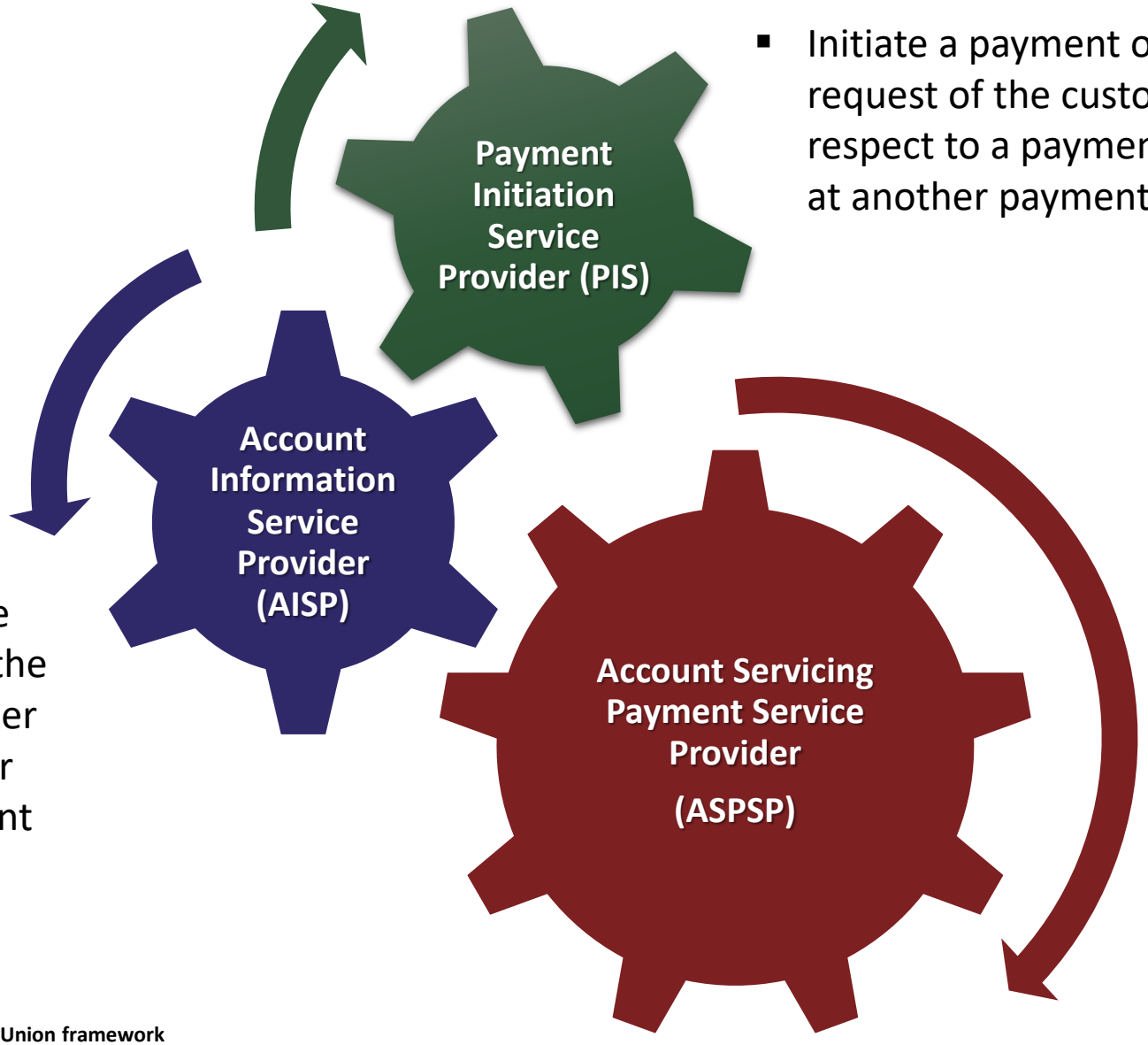
…

Main goals of Payment Services Directive 2 (PSD2), in force since January 2018

- ✓ Strong customer authentication (SCA)
- ✓ Security incident reporting obligations apply to payment service providers
- ✓ Framework with appropriate mitigation measures and control mechanisms to manage the operational and security risks
- ✓ Monitoring mechanisms to detect unauthorised or fraudulent payment transactions
  (Commission Delegated Regulation (EU) 2018/389)

Since 2015 payment service providers should comply with SCA under the EBA Guidelines on the security of internet payments. PSD2 makes this requirement binding

Third party providers under the scope of PSD2

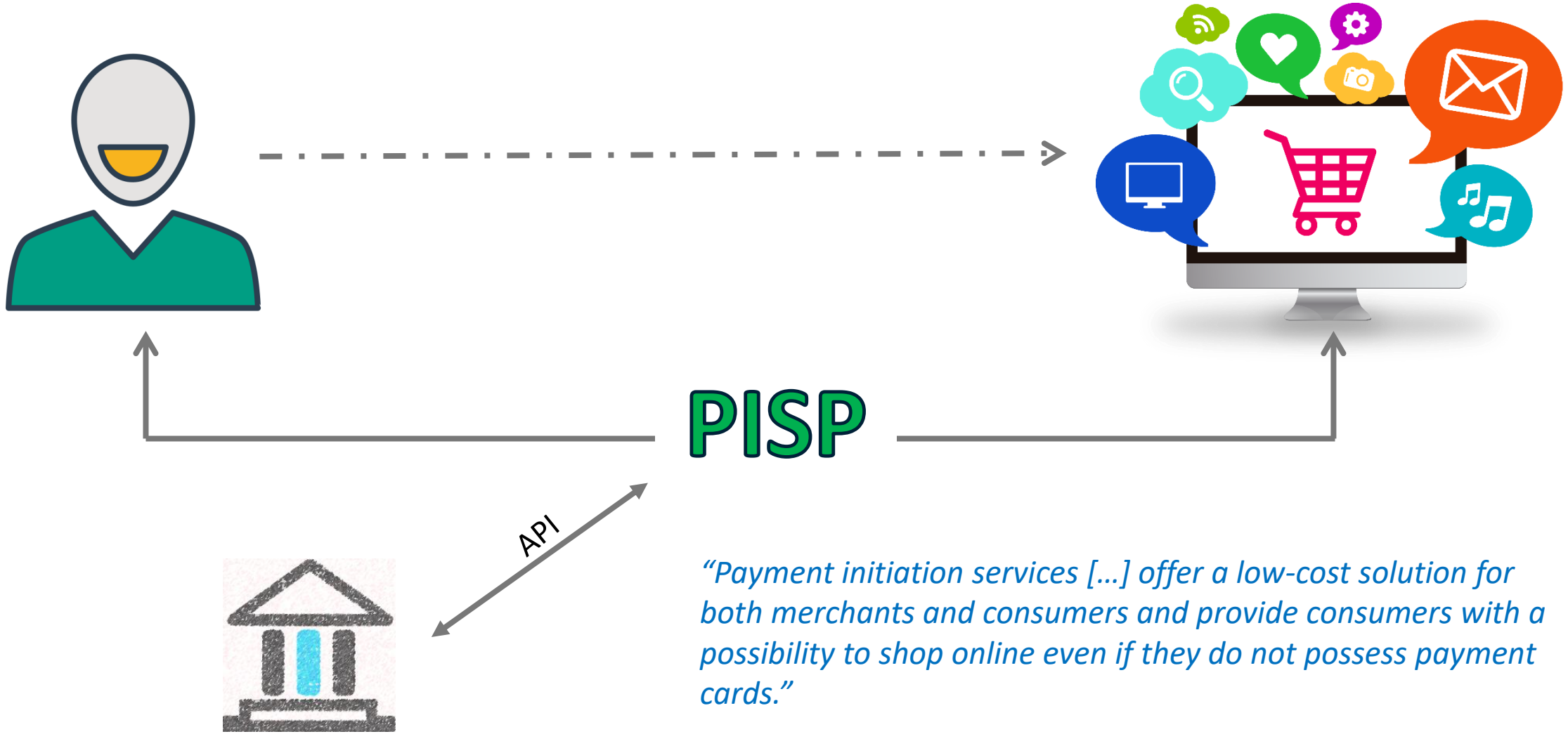


- Initiate a payment order at the request of the customer with respect to a payment account held at another payment service provider

- Provide consolidated information on one or more payment accounts held by the customer with either another payment service provider or with more than one payment service provider

- Provide and maintain a payment account for a payer

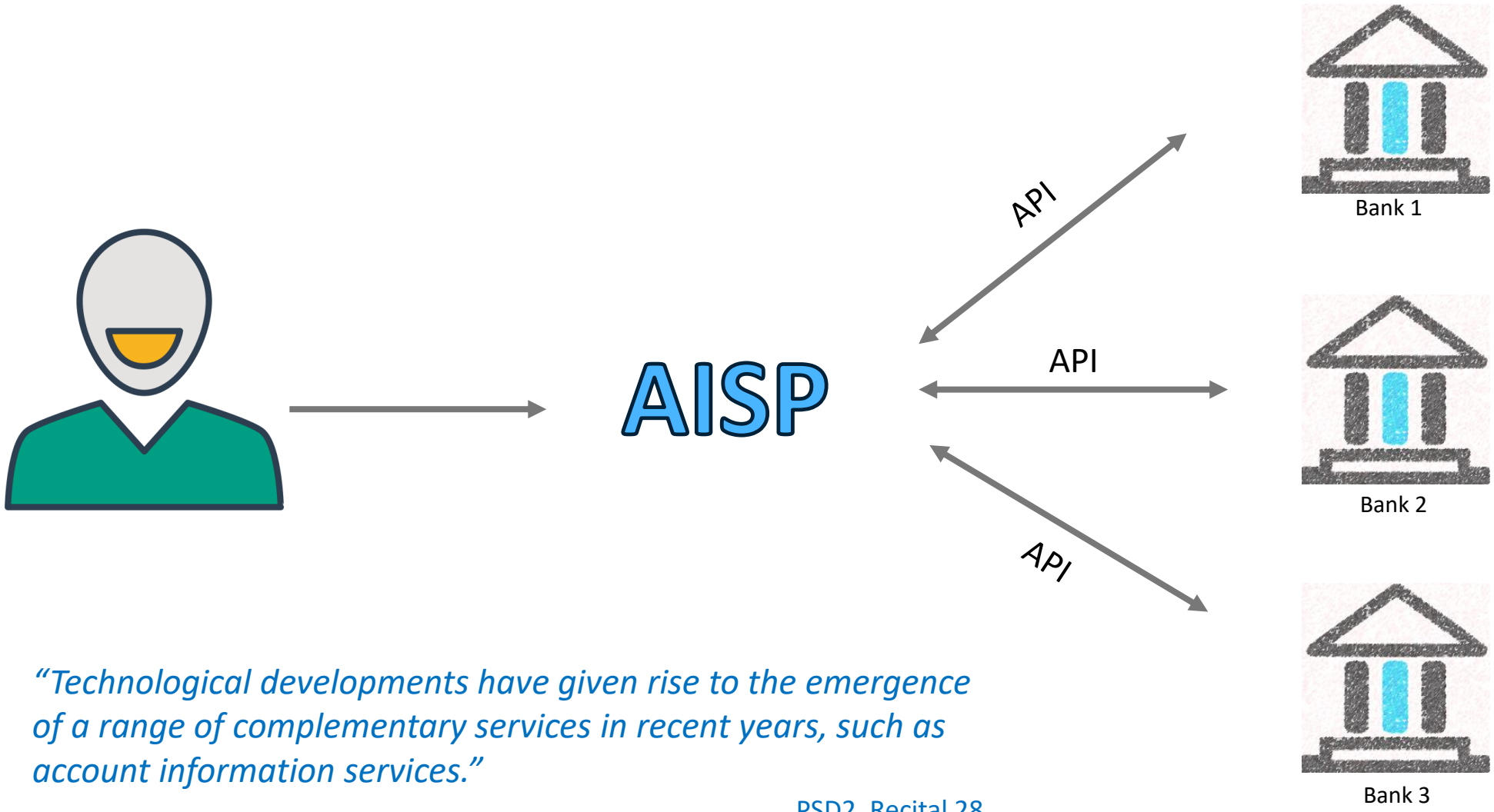
Payment Initiation Service Provider makes the payment on behalf of the customer



"Payment initiation services […] offer a low-cost solution for both merchants and consumers and provide consumers with a possibility to shop online even if they do not possess payment cards."

PSD2, Recital 29

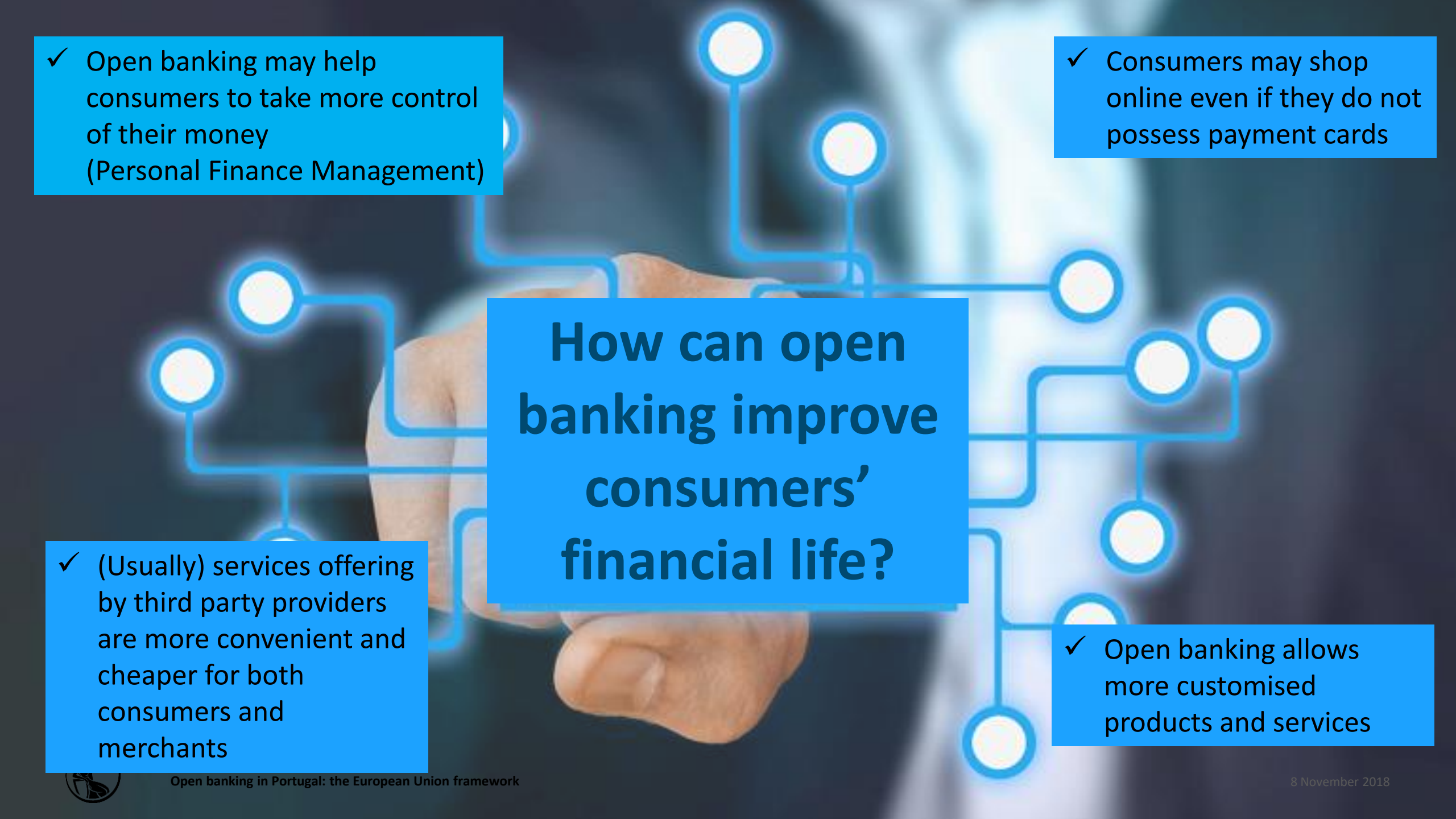
Account Information Service Provider provides the customer with aggregated online information on one or more payments accounts



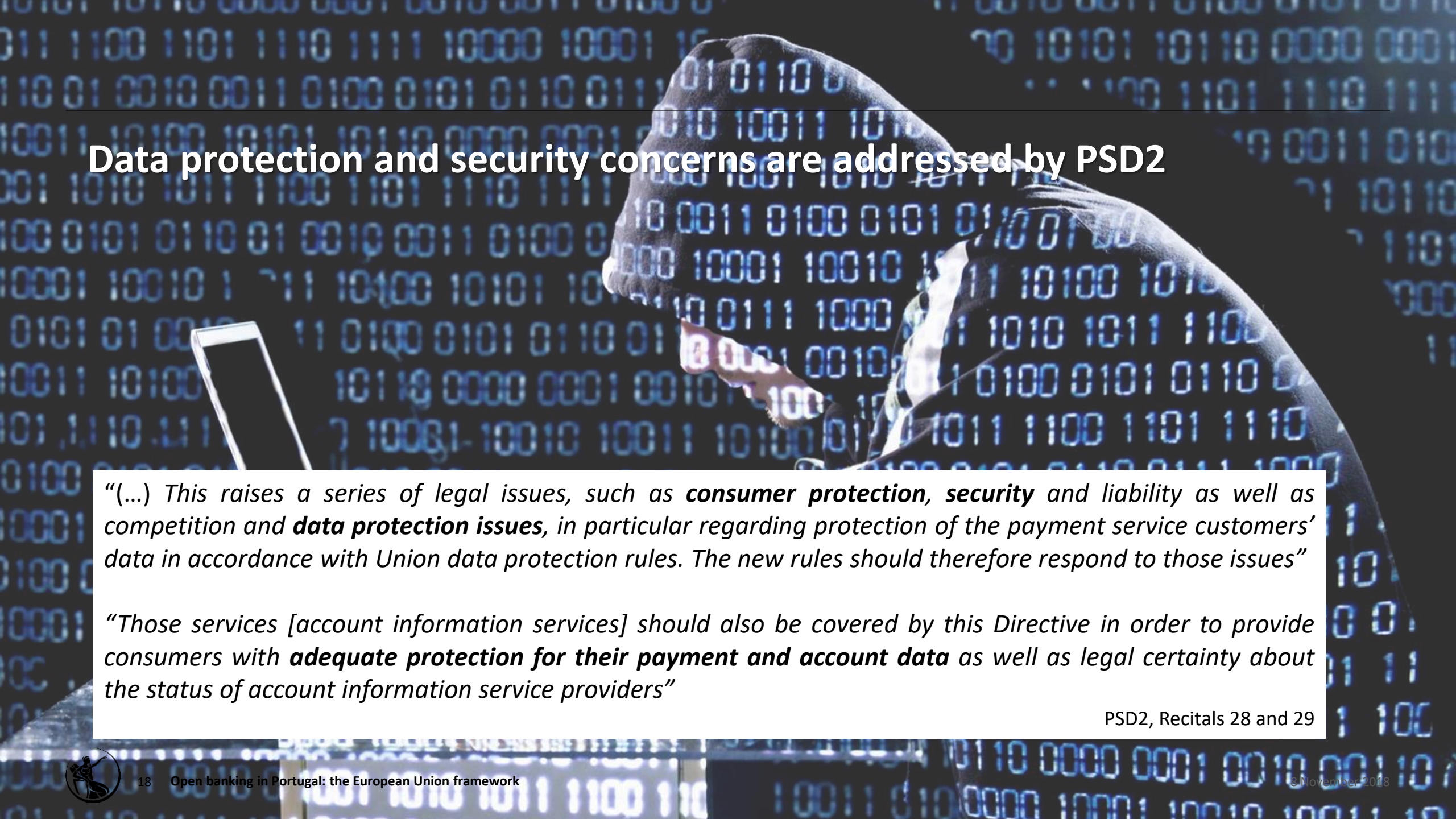
"Technological developments have given rise to the emergence of a range of complementary services in recent years, such as account information services."

PSD2, Recital 28


OPEN
BANKING


✓ Open banking may help consumers to take more control of their money (Personal Finance Management)
✓ Consumers may shop online even if they do not possess payment cards
How can open banking improve consumers' financial life?
✓ (Usually) services offering by third party providers are more convenient and cheaper for both consumers and merchants
✓ Open banking allows more customised products and services

Data protection and security concerns are addressed by PSD2

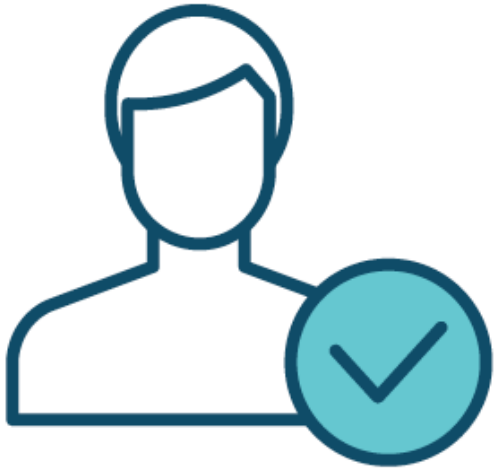


"(…) *This raises a series of legal issues, such as* ***consumer protection****,* ***security*** *and liability as well as competition and* ***data protection issues****, in particular regarding protection of the payment service customers' data in accordance with Union data protection rules. The new rules should therefore respond to those issues"*

"Those services [account information services] should also be covered by this Directive in order to provide consumers with ***adequate protection for their payment and account data*** *as well as legal certainty about the status of account information service providers"*

PSD2, Recitals 28 and 29

ASPSPs do not check the customer's consent… PISPs and AISPs should comply with several regulatory requirements



- ASPSPs do not have to check the customer's consent, if account information services and payment initiation services are provided following a contract

- AISPs and PISPs can rely on the authentication procedures provided by ASPSPs to the customer, when it comes to expressing explicit consent

PISPs and AISPs should comply with a set of rules on data protection

- PISPs shall ensure that information about the customer is only provided to the payee and only with the customer's explicit consent
- The information requested from the customer shall only be that necessary to provide the services
- PISPs and AISPs shall not use, access or store any data for other purposes
- The scope of data to be shared with AISPs and PISPs by the ASPSP does not include the customer's identity (e.g. address, date of birth, etc.)

PISPs and AISPs should comply with a set of rules regarding data protection

- The AISP accesses only the information from designated payment accounts and associated payment transactions
- RTS places a limit of four times a day on the AISP's access to payment account data without the customer being directly involved
- However, an ASPSP may contractually agree with the AISP that the AISP can access the account without the customer's involvement at 'a higher frequency', with the payment service customer's consent

Security is one of the biggest challenges to open banking

Security is crucial to ensuring customers' protection and confidence

'Security of electronic payments is fundamental for ensuring the protection of customers and the development of a sound environment for e-commerce. A solid growth of internet payments and mobile payments should be accompanied by a generalised enhancement of security measures.'

(PSD2, Recital 95)

'A virtue of central bankers is that they are, by nature, worried about risks and security. And one concern that is very closely linked to innovation and digitalisation is that of cyber risks.'

Speech by Yves Mersch, Member of the Executive Board of the ECB, at the Second Annual Conference on "Fintech and Digital Innovation: Regulation at the European level and beyond", Brussels, 27 February 2018

Payment Service Providers must comply with strong customer authentication (SCA)

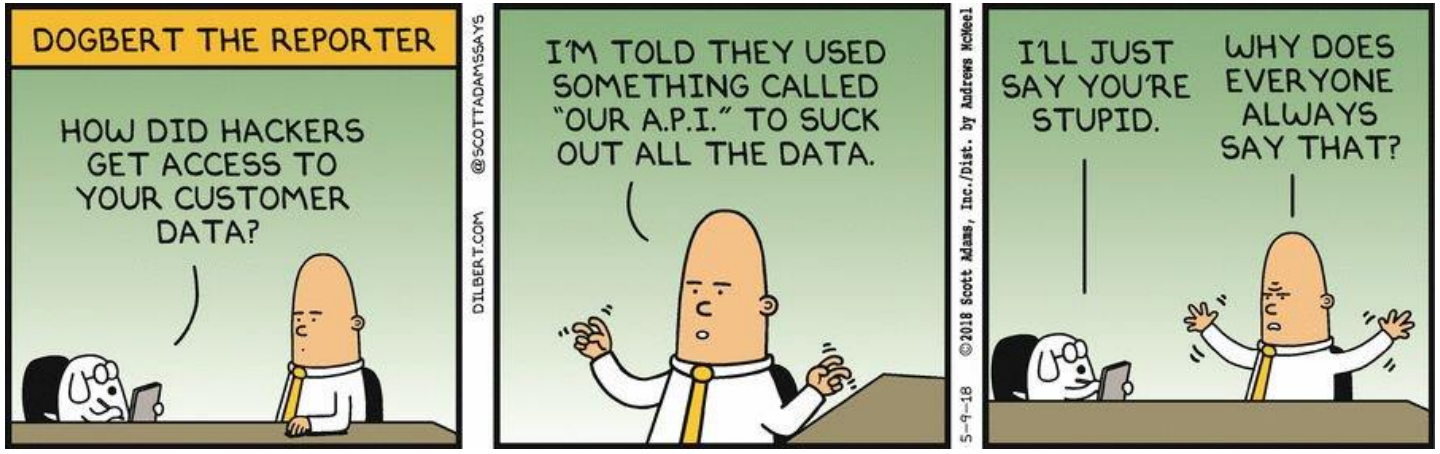
SCA is an authentication based on the use of two or more elements categorised as

- ✓ **knowledge** (something only the customer knows) – password or PIN
- ✓ **possession** (something only the customer possesses) – token, smart card, mobile phone
- ✓ **inherence** (something the customer is) – fingerprints or voice recognition

that are **independent**, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data

Payment Service Providers must comply with strong customer authentication (SCA)

- Payment Service Providers apply SCA where the customer:
  - ✓ accesses his/her payment account online
  - ✓ initiates an electronic payment transaction
  - ✓ carries out any action through a remote channel which may imply a risk of payment fraud or other abuses



SCA is the rule and customers' security credentials must not be shared

- Only the ASPSP can apply SCA or decide whether or not an exemption (e.g. unattended terminals for transport fares and parking fees or trusted beneficiaries) applies to a customer's payment account in the context of the account and payment initiation services
- Payees can never decide whether or not to use an exemption
- PISPs and AISPs must ensure that the personalised security credentials of the customer are not, with the exception of the customer and the issuer of the personalised security credentials, accessible to other parties and that they are transmitted through safe and efficient channels

Payment Service Providers must comply with strong customer authentication (SCA)

- **Banco de Portugal** is working with merchants' associations to increase security and confidence of payment card customers in the digital channels (card not present), through the awareness and knowledge of security protocols and measures (such as 3D-secure)

- Most banks in **Portugal** are using password + SMS token [One Time Password] to comply with SCA when customers access homebanking

Financial literacy initiatives should focus security procedures

- **Banco de Portugal** takes initiatives regarding security and strong customer authentication to encourage the adoption of security precautions by customers

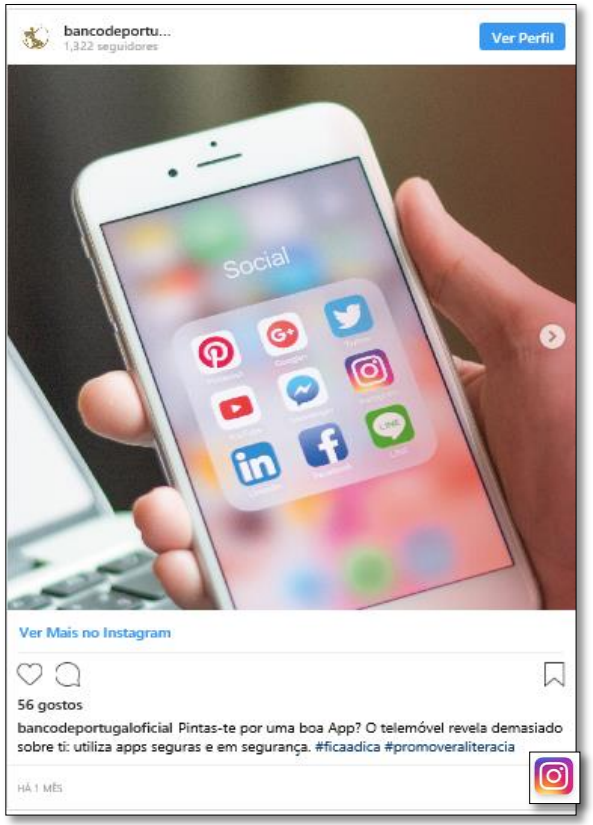
Leaflets and other materials

Training sessions

Awareness campaigns on the Bank Customer Website

#ficaadica - #toptip – 5 TIPS for staying safer online

- Banco de Portugal has in place a **digital financial literacy strategy**, included in its Strategic Plan for 2017-2020, aiming to:
  - ✓ Empower bank customers on digital financial services
  - ✓ Enlighten bank customers on the secure use of digital channels
  - ✓ Raise awareness on digital financial products' features and risks



THANK YOU!

mlleitao@bportugal.pt

Maria Lúcia Leitão • Head of the Banking Conduct Supervision Department

8 November 2018

OPEN BANKING: A challenge to ensure informed and adequate consent from consumers concerning data collection, use and sharing

BANCO DE PORTUGAL
EUROSISTEMA