Payment Services Directive (PSD2): Regulatory Technical Standards (RTS) enabling consumers to benefit from safer and more innovative electronic payments

1. 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.

2. Strong Customer Authentication (SCA)

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.

3. 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.

4. 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.

5. Transition period

Can TPPs continue to use screen scraping during the transition period?

There will be transition period between the application date of PSD2 (13 January 2018) and the application date of the RTS (18 months after publication of the delegated act in the Official Journal of the EU). Payment market players need this transition period to upgrade their payments security systems so that they meet the RTS requirements.

This means that the PSD2 provisions on strong customer authentication and on secure communication, which are directly specified in the RTS, will not apply immediately. In other words, the application of security measures in Articles 65, 67 and 97 of PSD2 is postponed until the RTS becomes applicable. However, those parts of Articles 65, 67 and 97 that are not dependent on the RTS will

apply as of 13 January 2018.

The delayed application of the RTS 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.

New payment initiation service providers and account information service providers willing to provide these services must obtain the relevant authorisation to enter the market during the transition period.