Frequently Asked Questions: Making electronic payments and online banking safer and easier for consumers

1. Payment Services Directive

What is the Payment Services Directive 2 (PSD2)?

The revised Payment Services Directive (PSD2) aims to further modernise Europe's payment services for the benefit of consumers and businesses. It promotes the development of innovative online and mobile payments, more secure payments and better consumer protection. At the same time, the directive aims to improve the level-playing field for payment service providers – including new players or FinTechs – and contribute to a more integrated and efficient European payments market. Overall, the updated rules will help to facilitate innovation, competition and efficiency in the EU online payments market. PSD2 also marks another step towards the completion of the digital single market in the EU andgives consumers more and better choices when it comes to retail payments

Many elements of the PSD2 already entered into application across the EU on 13 January 2018 and more improvements come into application on September 14.

PSD2 brings several major consumer benefits, such as:

- **PSD2 tackles fraud in online payments**: PSD2 introduces strong security requirements for electronic payments and for the protection of consumers' financial data to ensure their privacy is respected by all market operators. These rules should boost consumer confidence when buying online (as of September 2019);
- **PSD2 opens the EU payment market to competition**: PSD2 sets the stage for the future. With online financial services constantly evolving, the new rules will apply equally to traditional banks and to innovative payment services and new providers, such as FinTechs. These players, also called third party payment service providers (TPPs), will now be regulated under EU rules. They will be able to bring a wealth of consumer benefits. For instance, they can initiate payments on behalf of customers. They give assurance to retailers that the money is on its way, or give an overview of available accounts and balances to their customers (as of September 2019);
- **PSD2 increases consumers' rights** in numerous areas. These include reducing consumers' liability for unauthorised payments and introducing an unconditional ("no questions asked") refund right for direct debits in euro (in application since January 2018);
- **PSD2 prohibits surcharging**, which is additional charges for payments with consumer credit or debit cards, both in shops or online. These

rules are applicable since January 2018;

- **PSD2 improves complaints procedure** – PSD2 obliges Member States to designate competent authorities to handle complaints from payment service users and other interested parties, such as consumer associations, if they consider their rights established by the Directive have not been respected. Payment service providers should put in place a complaints procedure for consumers which can be used before seeking out-of-court redress or before launching court proceedings. Payment service providers are obliged to respond in written form to any complaint within 15 business days (since January 2018).

2. Fighting online fraud

What is strong customer authentication?

PSD2 introduces strict security requirements for the initiation and processing of electronic payments. PSD2 obliges payment service providers to apply so-called "strong customer authentication" (SCA) when a payer initiates an electronic payment transaction. Payment service providers include banks and other payment service providers.

SCA is an authentication process that validates the identity of the user of a payment service or of the payment transaction. More specifically, the SCA indicates whether the use of a payment instrument is authorised. Some EU Member States, such as Belgium, the Netherlands and Sweden, already use SCAs for electronic remote payment transactions, be it a card payment or a credit transfer from an online bank. In some other EU countries, some payment service providers apply SCA on a voluntary basis.

The requirements of strong customer authentication across the EU will help reduce the risk of fraud for online payments and online banking, and protect the confidentiality of the user's financial data, including personal data. This means that European consumers will benefit from safer electronic payments. In terms of how it works in practice, customers will receive advice from their banks or payment providers. They will have to provide two or more of the following elements when making payments, which can be categorised as:

- Knowledge: something only the user knows, e.g. a password or a PIN code
- Possession: something only the user possesses, e.g. a mobile phone, and
- Inherence: something the user is, e.g. the use of a fingerprint or voice recognition.

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. Merchants will have to be equipped to be able to operate in a SCA environment.

Whenever a payer initiates an online transaction above €30, the SCA will be applicable, unless one of the nine exemptions apply (e.g. low value transactions, trusted beneficiaries, etc).

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

Strong customer authentication rulescover payment accounts in the scope of PSD2, i.e. all accounts where the holder can place and withdraw funds without any additional intervention or agreement of their payment service provider (such as a current account). As regards the types of payments, as a matter of principle, all electronic payments are subject to strong customer authentication.

Exemptions include low value payments for remote (online) transactions below €30, as well as contactless payments at point of sale – whereby the amount of a single transaction must not exceed €50 and the cumulative amount of previous contactless payments since the last time SCA was performed (e.g. by inputting the card PIN) does not exceed €150. Other categories of exemptions concern corporate payments (see the question below).

Further exemptions may apply, which are set in the **Commission Delegated Regulation (EU) 2018/389**and take account of the risks involved, the value of transactions and the channels used for the payment. 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, and must report certain data on fraudulent transactions to competent authorities and to the EBA. 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 for initiating another transaction. This procedure is already in application in some Member States and has led to significant fraud reduction for online payments.

What about the security of corporate payments?

The **Commission Delegated Regulation (EU) 2018/389** 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 these types of communication systems (corporate and host-to-host) 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.

When will strong customer authentication become mandatory?

The new SCA requirements are applicable as of 14 September 2019, and are being gradually introduced in line with migration plans designed under the authority of national and European supervisors. Some Member States are more advanced than others. We encourage all stakeholders to speed up their efforts to ensure that the new requirements are rapidly and fully in place across the

whole EU.

The European banking authority (EBA) acknowledged the challenges experienced by some stakeholders to introduce SCA fully by 14 September. The EBA therefore adopted an Opinion on 21 June 2019 allowing national supervisors to enforce the new SCA rules on online payments by cards with a degree of flexibility, granting where necessary 'limited additional time' to migrate to compliant authentication methods. Consumers should continue to pay as normal in Member States that decide to avail of this flexibility. At the end of this period of time, consumers will be asked to perform the two-factor strong customer authentication, unless an exemption applies.

3. More choice in the EU payment market

How does PSD2 change the payments markets?

PSD2 also introduces more competition in the payments market by allowing non-bank companies to offer new innovative services to their customers.

Since the adoption of PSD1 in 2007, new services emerged in the area of internet payments, where innovative players – known as FinTechs or 'Third Party Providers (TTPs)' – offer specific payment solutions or services to customers. Until now, these FinTech companies faced difficulties when entering new markets, as they were operating outside of the financial services legal framework. PSD2 requires that these FinTechs follow the same rules as the traditional payment service providers: registration, licensing and supervision by the competent authorities, and PSD2 ensures that they can offer their services across the EU.

Consumers who want to use such new services cannot be prevented by their banks from doing so. Any bank that offers online access to accounts must cooperate with FinTech companies or with other banks providing such services. Consumers and companies using these services will have to grant access to their payment data to third parties providing payments-related services (TPPs). These are, for example, payment initiation service providers (PISPs) and account information service providers (AISPs), or other banks. Consumers will be able to manage their personal finances more efficiently through applications that, for instance, aggregate information from their accounts held with different banks. In order to make that possible, banks must establish secure communication channels to transmit data and initiate payments.

How will common and secure communication work?

The **Commission Delegated Regulation (EU) 2018/389** specifies the requirements for common and secure standards of communication between banks and FinTech companies. Customers will have to give their consent to the access, use and processing of their data. TPPs will not be able to access any other data from the payment account beyond those explicitly authorised by the customer. In other words, previous practices such as unregulated 'screen scraping' will no longer be allowed. Banks will now 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.

How is personal data protected?

In accordance with data protection rules under both PSD2 and the General Data Protection Regulation, account holders can exercise control over the transmission of their personal data under both PSD2 and 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 explicitly request such services 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.