FSUG opinion on the Commission's Payment Services Directive 2 (PSD2) review

General Remarks

The Financial Services User Group welcomes the European Commission's ongoing work on the PSD2 review, because payments are one of the most common and in the same time important financial instruments used by consumers on a day-to-day basis.

The forthcoming PSD3 should put consumers at the centre and set up a legal framework which allows consumers to be protected no matter the payment service provider used, allow for secure and inclusive transactions offline and online and provide a sound liability framework in case something goes wrong.

In this opinion, the FSUG is making some judgements and coming with some suggestions on some topics to further improve the Directive in the benefit of consumers.

Competition of payments

Even if the EU payment markets are more competitive than 5 years ago, PSD2 alone failed to generate lower fees for payments and to lower the costs of remittances. It was necessary another piece of legislation – Regulation EU 2019/518 as regards certain charges on cross-border payments to improve costs of cross-border payments and to set up better rules for currency conversion. Even so, detrimental practices for consumers like DCC (Dynamic Currency Conversion) are still present on the EU payment markets.

The FSUG is asking for a provision to prevent PSPs to use the Payment Services Directive to avoid competition and to limit the possibility of unilaterally terminate the framework contracts concluded for indefinite periods without a strong and reliable motivation. For example, terminating framework contracts when the consumer is transferring funds to FinTech providers is totally unacceptable.

Scope exclusions

The FSUG strongly opposes against any attempt to use the process of the PSD2 review to increase the list of exclusions mentioned in Article 3 and to reduce the level of consumer protection. On the contrary, the review should reduce some of the existing exclusions and generate a high-level degree of consumer protection.

Telecom operators, independent ATM providers and limited networks exclusions should be addressed in a way which will allow a better consumer protection.

In practice, there are many cases when the mobile phone bill includes costs of subscriptions to games, videos, magazines, parking services and consumers discovered their real costs just when they receive their phone bill. To avoid such things happening and to be sure that consumers are better protected against potential misleading services via their phone bill, we are recommending the deletion of the exclusion of telecom operators from the scope of the Directive.

In case of independent ATM providers, redesigning their business models with charging extra fees directly to the consumers isn't acceptable from our point of view. Also, the European Banking Authority (EBA), in its response to the Call for advice on the review of PSD2 mentioned that there are problems with the application of this exclusion and this makes difficult the supervision of the independent ATM

providers. In the interest of a better consumer protection, the FSUG recommends the removing of this exclusion, too.

The exclusion of limited networks is another point which needs more attention for an efficient consumer protection. In practice, under this exclusion are hidden a high number of shops, massive payment volumes and thousands of different products and services, which is very different than the initial intention of the co-legislators. A better definition of what is a "limited network" and a "limited range of products/services" is very important to avoid the increasing risks for consumers using such payment instruments.

Supervision and complaints handling

A very important issue for consumers is represented by the possibility to address a complaint to the national competent authority (NCA) at local level, in case of a potential detriment. The EU passporting regime allows payment services providers (PSPs) to apply for a license in a Member State and then to provide services in all other Member States. And if the payment services are provided by a "passported" PSPs, without a local agent or branch, it will be very difficult for a consumer to send the complaint to the NCA from the home Member State of the PSP, having instead to send it to the NCA on local level.

A natural development, for the benefit of consumers, is to empower the NCA from the host Member State to supervise the activity of the PSPs and to be responsible also for the complaints addressed by the consumers and to modify Art. 100 (4) accordingly.

The FSUG is of the opinion that consumers should have the possibility to address the complaint to the NCA of their Member State, in their own language. The NCA of the host Member States should be able to take action on that basis without being reliant on the home Member State where the PSP received its passport.

Irrevocability of a payment order

Payments are becoming, day after day, more digital, but until instant payments represent the "new normal" of payments, it is important to allow consumers to be able to revoke their consent on a credit transfer until it is executed. This is important not just to protect them for potential errors they made, but also because, in a digital world, it could be possible to find new offers and opportunities just minutes after a purchase decision was taken.

Like for direct debits, if a credit transfer was not executed, the consumer should have the right to revoke its consent and to cancel the payment. We are suggesting the same regime to be applied for credit transfers and for direct debits, both being able to be cancelled until the execution.

In the same time, we consider important to introduce a provision in the Directive to allow consumers to claim back the amount in case of errors, because at this moment it is very difficult to recover the money sent by mistake to someone. Consumers should receive the same rights for refund for credit transfers as they have for direct debits.

Strong customer authentication (SCA) – art.97-98 and liability in case of fraud

Despite the introduction of the SCA, fraud continues to exist and, even more important, fraudsters are now using new techniques to cheat consumers involving SCA, which complicates very much the refund of affected consumers, because PSPs invoke the "gross negligence" of consumers.

One common method is to introduce fraud via second-hand sales: Consumers selling products on some of the most popular websites are contacted by fraudsters through social media networks (WhatsApp, Facebook Messenger, etc) pretending to be interested in buying them. The crooks send a link to a false website, but with the name of the original one included or very close to it. Sellers are then asked to introduce the data of their cards and Card Verification Value number (CVV), to wait for an SMS or push notification from the PSP and approve it with their credentials/passwords when receiving it, to get the money from them.

After receiving the information from their victims, the fraudsters are using it to generate the request for the SCA and the confused seller is performing the SCA for the false transaction, authorising in fact the stealing of the amount introduced by fraudsters. After that, the communication through social media channels is blocked by fraudsters and the messages deleted by the crooks to protect themselves from future investigations.

What it is also very important here is that, in most cases, consumers immediately realise that they were victims of a fraud they urgently contact their PSPs to block the payment card used and to inform about the fraud, and asking PSPs to block the fraudulent transaction. In many cases, the amount blocked in their accounts is released by PSPs to fraudsters after few days, because the SCA was performed.

In such cases, consumers usually do not receive compensation as the PSP claim that the consumer authorised the payment or acted with gross negligence. EBA shares this observation in the Call for advice for PSD2 review (page 68-69). The FSUG is of the view that becoming victim of social engineering should not be qualified as gross negligence and compensation should be foreseen also for authorised transactions involving fraud. All resulting losses should be immediately reimbursed by PSPs.

The current liability regime leads to a moral hazard situation: PSPs do not need to compensate consumers in case of fraud and have as a consequence little incentive to adequately protect consumers against fraud. The EBA considers that such approaches are undesirable because PSPs are also required under Article 2 of the RTS on SCA&CSC to carry out transaction monitoring mechanisms, including cases of well-known fraud scenarios; and are expected to raise PSUs' awareness and provide assistance and guidance in light of new threats and vulnerabilities under Guideline 3.8 of the Guidelines on ICT and security risk management (EBA/GL/2019/04).

The PSD3 should introduce a reform of the liability framework including the following elements:

- PSPs should be asked to not make funds available or to execute the payment when there is a suspicion or evidence of fraud and to not release the blocked amounts if there is a formal complaint of fraud by the consumer.
- PSPs should immediately compensate consumers. To incentivise the beneficiary PSP to contribute to the recovery of funds, a shared liability between the sending and receiving PSP should be introduced.
- PSPs should be only in exceptional cases be able to claim the money back from the consumer in case of gross negligence. Gross negligence must be defined in the context of digitalisation and effectively prevent that consumers are held liable in case of sophisticated technological attacks.
- The burden of proof should be on the PSP to prove that they did everything possible to protect the consumers' funds and to prove that the consumer acted with gross negligence.

The FSUG would like to emphasise that it is highly unlikely that a consumer-proof liability regime will lead to a more negligent behaviour among consumers. Fraud cases, no matter the outcome, lead to a significant level of stress and administrative hassle which will naturally prevent a negligent behaviour among consumers.

SCA methods and potential financial exclusion

The options implemented for performing SCA should be imposed via regulation and should not be based on one or few solutions that rely on technologies, such as app-based, which very often are involving the use of a smartphone.

In the current state of play, many consumers are not comfortable/able/willing to use app-based solutions. Regulation and delegated acts must require firms to allow for different options and based on technologies that are easy to use, known by the widest possible array of population, secure and cost free and that consumers are able to choose one of the options offered.

Contactless payments and the EUR 50 limit

Consumers have adopted contactless payments more rapidly due to the pandemic. And there are many consumers that are welcoming this option, for the economy of time and for the convenience of using it.

Nevertheless, there are also many consumers that show mistrust and concerns about contactless payments. To address these concerns, it is important to introduce a possibility of setting own limits to the contactless payment features, from zero (complete deactivation) to EUR 50 (maximum that should be allowed).

The FSUG considers that a higher limit, as it was requested by the industry, is too risky for consumers. First of all, because the card could be stolen and then used by thieves, raising the amount at risk. Second, because a too convenient way of payment facilitates overspending and increases the risk of losing the control of their personal spending for consumers.

Using the commercial trade name and ex-ante IBAN verification

It is in the best interest of consumers to have access to as many tools possible to be sure that they are sending money to those intended to receive them. Any potential measure to diminish the risk for mistaken payments is welcomed, because the potential consequences for some mistakes could be very serious, especially in case of a big amount payment.

Using the commercial trade name with the ex-ante IBAN verification will allow consumers to easily identify to whom a payment was made. Introducing such requirements in the PSD2 review will make sure that it will become mandatory for all players.

Amount to be blocked on the payer's payment account when the exact transaction amount is not known in advance

There are many cases when merchants are blocking disproportionately high amounts when the exact transaction amount is not known in advance. This is in the very big disadvantage of consumers, who cannot use their own resources for other spendings.

The principle supported by the FSUG is that the amount blocked in these cases should be proportionate, transparently determined, and represent a true estimate of the final transaction

amount. To that end, the provision under the relevant Article should specify the way the additional amount is determined, strictly limiting excessive amounts.

Another important point here, which was also mentioned by the EBA in its response to the Call for advice for PSD2 review, are the divergent practices in relation to the time of release of blocked funds. Funds often have not been immediately released after the execution of payment transaction or the receipt of the payment order, or even, at times, have required an additional action in the form of explicit request from the payer. The revised text should indicate that the release of those funds should be immediately after the determination of the full amount.