"Payments tomorrow" annual conference
by the Payments Association EU

Madrid, 14 October 2022

The future regulation of the European payments industry

I am delighted to join you for this year's conference related to the future of payments and to share the EBA's view on how the future regulatory framework in the area can be shaped. The discussion is very timely, taking into account the ongoing review of the Payment Services Directive (PSD2), which is an integral part of the Commission's Retail Payment Strategy from September 2020 aiming at developing innovative and competitive retail payments, supporting digital and instant payment solutions, ensuring consumer protection and improving access to the payment ecosystem.

In my remarks, I will cover:

- First, the EBA's recent advice to the European Commission in the context of the review of PSD2, which indicated some key areas that can be addressed in the revision of the legal framework, such as the impact of new types of fraud, the unintended consequences for consumers stemming from compliance with the legal requirements and others.
- Second, the opportunities and challenges in the move from Open Banking to Open Finance.

I will also cover the expected impact of a future PSD3 and a framework on Open Finance on the European financial services, which should help in enhancing competition further by removing impediments to access to the market, providing more choice and convenience for customers with the rollout of new services, while ensuring more secure and efficient financial services, and promoting the development of new and innovative financial and non-financial services and products.

The EBA's response to the Call for advice on the review of PSD2

The EBA published in the summer a response to the Commission's Call for advice on the review of PSD2. It was an important effort where we tried to assess our experience in the implementation of PSD2 and we hope it would an important building block of the review of PSD2. We covered in this response more than 200 proposals on how to develop and strengthen the payments' legal framework in the future.

Let me first highlight that the ultimate objectives of PSD2 have started materialising in the market. We see evidence in the decrease of fraud, we see a large number of new market entrants. In that context our overall view is that PSD2 has succeeded in pursuing its overall objectives and we proposed changes to PSD2 that are evolutionary, rather than revolutionary. Accordingly, I think that PSD3 should build on the strengths of PSD2, while addressing new threats and some of the challenges payment service providers (PSPs) and competent authorities faced in the application of the requirements, such as the rollout of strong customer authentication (SCA) and the removal of obstacles to the provision of account information and payment initiation services.

In particular, some of the key areas the EBA sees merit in adjusting in PSD3 relate to:

- enhancing the security requirements and addressing new types of fraud;
- ensuring consumers are properly protected and their needs taken into account;
- enhancing the enforcement of the legal requirements and the scope of supervision;
- streamlining and simplifying the legal framework by merging PSD2 and the Electronic Money Directive; and
- ensuring easy access to payment systems and avoid de-risking practices.

I will touch upon all these topics in more detail now starting with the security requirements.

Security requirements

Fraud levels have decreased significantly after the implementation of SCA. This means that the legal requirements set out in PSD2 and the EBA legal instruments have been fit for purpose and the approach taken should not be fundamentally changed.

However, fraud methods and techniques evolve and this evolution requires the payments' industry and the legal framework to adapt. In particular, as you are all aware, new types of fraud, such as social engineering fraud, are on the rise. This type of fraud relates to cases where fraudsters manipulate payers into initiating a payment transaction to a fraudster. While SCA and the complementary security requirements in the EBA Regulatory technical standard on strong customer authentication and common and secure communication (RTS on SCA) mitigate to some extent this type of fraud, I think more needs to be done. This is why we propose a combination of additional measures, such as enhanced educational and awareness programs to payment service users, investing in more efficient transaction monitoring mechanisms and increasing cooperation between payment service providers (PSPs) in relation to known cases of fraud and specific fraudsters.

Another area for improvement relates to the scope of transactions subject to the security requirements. We are aware that the industry struggled in the past few years with the interpretation of the requirements to some of the transactions falling outside the scope of SCA, such as merchant initiated transactions (MIT) and mail order and telephone order (MOTO) transactions, and that some actors used these transactions to circumvent the requirement to apply SCA. To avoid this scenario going forward, I think PSD3 will be a good opportunity to set clearly the regulatory approach and applicable requirements to the transactions not subject to SCA.

We have also observed that more and more payments leverage on new technologies and services provided by third parties, such as digital wallets or authentication solutions integrated in smartphones. Such innovations are welcomed and should be encouraged since they provide more payment options and greater choice for the payment service user.

However, these innovations should not pose a risk to the security of the payment transactions. That is why it is imperative for PSPs to continue being responsible for the security of transactions and, subsequently, the authentication of their customers.

Consumer protection

I will now move to the other aspects related to the protection of consumers and how their needs could be better met. When monitoring the implementation of the security requirements, we observed that the application of the legal requirements by some PSPs led to undesirable outcomes for consumers, such as consumers covering losses for unauthorised transactions and financial exclusion.

First, in some jurisdictions, PSPs have introduced a practice of transferring liability for unauthorised and fraudulent transactions predominantly on the customer who bore the ultimate losses. This goes against the harmonised application of the Directive and its spirit. Therefore, it is key to clarify key requirements and terms in PSD3 related to the distribution of liability, such as 'fraudulent act', 'gross negligence' and 'reasonable grounds for suspecting fraud'.

The second undesirable outcome for consumers relates to the unintended consequence of using innovative solutions and devices for initiating payment transactions. In particular, some of the authentication approaches chosen by PSPs, mainly those reliant on smartphones, led to the exclusion of certain groups of society, such as vulnerable consumers, from using remote electronic payment transactions and online access to payment accounts as fundamental financial services. To address this issue, we propose that alternative authentication solutions or approaches should be considered for these groups of society to meet their needs and to avoid excluding them from the financial sector.

Enforcement and supervision

The third set of proposals I would touch upon relate to enforcement and supervision of the legal requirements. As I alluded previously, the implementation of SCA has been challenging both for the industry and supervisors, thus requiring additional time and guidance. Therefore, to ensure a robust legal framework that is applied consistently by all market

participants, more effective supervisory tools and enforcement measures and slight adjustment of scope are needed.

To avoid a situation where the industry is not ready for the rollout of future security requirements, a key point for supervisors is to have the necessary tools to ensure that all actors in the payment chain implement the necessary changes in a timely manner and that non-regulated actors, such as payment gateways or payment schemes, who are responsible for the implementation of the security requirements, bear some responsibility or liability for potential incompliance with the legal requirements by introducing specific requirements to them. By doing so, such intermediaries holding a crucial point in the payment chain will fall partly within the scope of supervision and enforcement in case of incompliance.

A lesson learnt also for us as regulators is that such novel and wide-scale initiatives as the rollout of SCA take time, require a staged and EU-wide coordinated approach, and careful consideration of the impact on all involved actors.

Merger of PSD2 and EMD

Another important aspect in the revision of PSD2 relates to the overall complexity of the legal framework. I believe that streamlining and simplifying the legal requirements is crucial to ensure effective regulation and compliance. It should also decrease the cost for the industry due to the decrease in administrative burden.

In that regard, we strongly support the merger between PSD2 and EMD2. We have observed that the differences between payment and e-money services are negligible and often pose issues in the treatment of innovative business models and payment solutions. Moreover, payment and electronic money institutions rely on the same systems for processing payment services and e-money services and for bookkeeping. Therefore, following the principle ‘same activity, same risk, same rules’, there is a strong case to be made to merge PSD2 and EMD.

Such a merger will contribute to avoiding regulatory arbitrage, ensuring technological and business model neutrality, ensuring a level-playing field between different PSPs and a future-proof legal framework.

Access to payment infrastructure

I will move to the next key point related to access to the payment infrastructure by payment and e-money institutions. Participation in payment systems and obtaining easy access to accounts maintained with credit institutions is crucial for the operation of payment and e-money institutions. Payment and e-money institutions rely on such accounts to settle transactions executed by them and for safeguarding clients' funds.

However, we have identified unwarranted de-risking practices by some banks where they had refused opening accounts to payment and e-money institutions or terminated existing business relationships. These banks associated some business models of payment and e-money institutions with high level of money laundering and terrorist financing risks. Such practices, when unjustified, can potentially lead to competitive advantage for banks and give rise to general level-playing field and regulatory arbitrage concerns.

In that regard, I think it is crucial for PSD3 to clarify the reasons for refusing access to accounts with banks and for terminating existing business relationships and to introduce specific criteria that banks can take into account in their assessment. This will be beneficial for enhancing competition in the market but also fostering innovation, which is often led by payment and e-money institutions.

Move from Open Banking to Open finance

Now, I would like to reflect on the opportunities and challenges that lay ahead of us in the move from Open Banking to Open Finance, or otherwise expansion from access to payment accounts data towards access to other types of financial data, such as insurance, investment, savings and others. Open finance is seen as having the potential to spur further innovations in the financial sector, to the benefit of consumers and the overall financial ecosystem. I would agree with that view.

In that regard I see that Open Finance has the potential to contribute to:

- the development of tailor-made services to consumers and businesses;

- the development of new and innovative financial and non-financial services and products;
- facilitate access for consumers to a wider range of financial products and services;
- allow consumers to better access their information thus leading to easier comparison between the features and prices of various products, and therefore help them make better informed decisions,;
- bring about further competition in the market.

However, it needs to be done right. That is why it is crucial to leverage and build on the experience accrued during the implementation of Open banking under PSD2. It is an opportunity to benefit and expand on the parts that worked well and to address the challenges faced when implementing PSD2, such as API fragmentation, deficiencies in the quality of some APIs and others.

Leveraging on the experience of PSD2, I see four pillars of the Open Finance framework were experiences can be drawn: namely the scope of data, consent management, security requirements, and communication and interface requirements.

In relation to the scope of the data, it should be clear which types of data can be accessed and which types not, what data should be accessible free of charge and what data to be monetised, as well as whether the framework will cover online access to data only or access through other protocols and interfaces. Another related aspect is to set out clearly in level-1 the interplay with the requirements of GDPR to avoid overlapping requirements and uncertainty for market participants.

When it comes to the consent management, the future framework should allow consumers to be in control of their data. The requirements should be precise on the process of provision and revocation of consent and envisaging consumers to be able to revoke consent from their data providers. However, general opt-out of the new services should be avoided since this may hinder competition.

Another key aspect relates to the security requirements for Open Finance, which will be the building block for consumers' trust in Open Finance. Since we are already reaping the

benefits of PSD2, it will be appropriate to apply similar security requirements for the communication between third party providers and data providers, as well as the identification of customers.

The new framework can also address one of the biggest issues in PSD2 – the authentication of the payment service users when using third party providers. Since third party providers are authorised entities and subject to the legal framework, it will be opportune to allow them to apply and be responsible for the long-term authentication of their customers. This will reduce friction in the customer journey and improve customer convenience, while maintaining the same level of security.

The fourth pillar relates to access interfaces. We see a strong case in considering mechanisms for ensuring further harmonisation of the implementation and application of the legal requirements, including a centralised oversight. This may or may not include developing a single EU API. If that were to be the choice, I believe it should be an industry-led initiative but with a mechanism for supervisory authorities to provide steer. Such a standard will be beneficial for the technical uniformity, to facilitate technical implementation and integration by stakeholders, as well as consistent application of the requirements and the assessment of compliance by competent authorities. The legal requirements on access interfaces, in turn, should incentivise the industry to focus on delivering high-performing APIs and be clear, in particular in the delineation between mandatory and premium functionalities.

Conclusion

To conclude my remarks, I would stress that PSD3 and the establishment of an Open Finance framework can be a great opportunity that could bring significant benefits for the consumers and businesses in the EU and it will influence how the European financial services are shaped. Both initiatives are expected to foster innovation, enhance competition, improve transparency, enhance security and consumer protection, and provide greater choice of service and products for customers. PSD3, in particular, will be a great opportunity to ensure further harmonisation on the payments market and avoid regulatory arbitrage and unlevel-playing field.

A future PSD3 and an Open Finance framework are just one piece of a future regulatory landscape affecting payment services. The Commission has set a very ambitious agenda for the digital transformation of the EU economy and the financial sector. Starting with the recently agreed Digital operational resilience act (DORA) and the Regulation on markets in crypto-assets (MiCA), where the EBA is already preparing for delivering the significant workload that lies ahead of us, but also with the work done on instant payments, the initiative to establish and regulate essential aspects of a digital euro as a new form of central bank money, and the potential revision of the Settlement Finality Directive to improve access to payment systems. All these initiatives will shape the future of the retail payments sector and we should ensure that it continues to provide the best possible service, with the highest level of convenience and security at the lowest cost to consumers.

The EBA looks forward to the decision of the Commission on whether or not to propose PSD3 and/or a framework on Open Finance and we stay ready to support the delivery of the tasks that that may be conferred on the EBA. I will also look forward to engaging with you on all these topics in the future when shaping the future of the EU payments legal framework.

Thank you very much for your attention.