Non-paper on payment services and open finance

Ministry of Finance of The Netherlands

1. Introduction

In 2022, the Ministry of Finance of the Netherlands conducted a national evaluation of the implementation of the revised Payment Services Directive (PSD2). The evaluation was focused on the effects of PSD2 on the Netherlands' payments market, with a particular focus on how PSD2 affected consumer protection (including privacy and data protection), innovation and competition, and the security and robustness of the payments sector.

In its Retail Payments Strategy of September 2020, the European Commission announced a "comprehensive review" of the revised Payment Services Directive (PSD2). In the Digital Finance Strategy, the Commission also announced its intention to propose an Open Finance legal framework. This non-paper, based on the outcomes of the national evaluation of PSD2, serves as input for the PSD2-review, with the view of potential future proposals by the Commission for a revision of the PSD2-framework and the introduction of a framework for Open Finance.

2. Outcomes of the evaluation of the implementation of PSD2 in The Netherlands

The national evaluation of PSD2 led to the following general observations:

- **PSD2 has contributed positively to competition in the payments market and to a more unified single European payments market.** Nevertheless, consumers are hesitant to actively use services where payments data are processed, because they do not always see the added benefit of these services or are not inclined to share their payments data because of privacy concerns. Furthermore, payment services providers would prefer a more harmonized legal and supervisory framework.
- **PSD2 has contributed positively to innovation in the payments market.** PSD2 has led to a broader adoption of the use of application programming interfaces (APIs), which has led to more efficient services. However, the lack of a common API standard has led to a plethora of different API propositions. It has also led to the rise of data aggregation services, where PSD2-licensed entities offer their license as a service. As PSD2 was not drafted with these types of aggregation services in mind, it raises the question whether the existing framework is adequate.
- **PSD2 has contributed positively to the security of the payments chain.** The use of APIs and Strong Customer Authentication (SCA) led to a decrease of security risks. The requirements regarding fraud have been effective, although a significant move towards new types of fraud (phishing, spoofing, etc.) has been identified.
- **PSD2 has contributed positively to consumer protection.** The requirements regarding liability in cases of bank fraud increases the protection of consumers. The fear of consumers being excluded from payment services because they did not want to use data-related services has not materialised. Nevertheless, there are signals that a significant group of payment service users, especially vulnerable people, feel that SCA-methods are burdensome and lead to a decrease in the accessibility of the payments system.
- **PSD2, in combination with the General Data Protection Regulation (GDPR), offers adequate protection of privacy.** Nevertheless, the surge in data aggregators (see above) and small misalignments between PSD2 and GDPR do leave room for potential improvements. Furthermore, some PSD2-requirements that are meant to ensure the relationship between Account Servicing Payment Service Providers (ASPSPs) and Third-Party Providers (TPPs) block or prohibit tools and functions that enable consumers to easily rescind their given data sharing authorisations, such as a consent dashboard.

3. Lessons learned for an open finance framework

Based on the beforementioned results of the evaluation, we see potential improvements to the existing requirements on the payment data sharing provisions of the PSD2-framework and/or as input for an effective general framework for open finance, in random order:

- **Further increase in the protection of payment service users.** Some aspects of PSD2, while well intentioned, lead to barriers for payment users, especially those that are less digitally skilled. The SCA requirements have benefitted the overall security of payment services, but they complicate doing payments for some vulnerable user groups. Furthermore, the legal framework should not prohibit users to have access to tools where they have a

complete overview of the authorisations that they have given (provided by their ASPSP, for example), and which they can use to directly rescind these authorisations. We recommend the Commission to assess to what extent the requirements on SCA can better take into account usability by vulnerable groups. Furthermore, we recommend the Commission to identify and remove barriers for tools that enhance the control and protection of payment service users as much as possible.

- **Standardisation of APIs.** While during the drafting of PSD2 and the underlying Regulatory Technical Standards the private sector indicated that they wanted to have the freedom to come up with their own APIs, they now indicate that a general API standard at the EU-level would be welcomed and would lead to a more efficient application of PSD2. We recommend the Commission to explore whether common EU API-standards (either a single standard, or a limited set of different standards) would benefit the payments market and could contribute to a more effective general framework for Open Finance.
- **Review of the prohibition for compensation for access to the account.** PSD2 requires ASPSPs to provide access to the payments account without monetary compensation. The goal of this prohibition was to remove barriers for TPPs to use payments data. Furthermore, this approach adds to the general view that payments data belong to the consumer, and not to the ASPSP. However, it is possible that without the possibility for any compensation at all, ASPSP are only doing the bare minimum to comply with PSD2, leading to suboptimal solutions. We recommend the Commission to investigate whether the prohibition of a monetary compensation for providing access to payments accounts is problematic, and if so, what remedies would be proportionate and effective, with the interests of payment services users and market competition in mind.
- **Further alignment of PSD2 and GDPR.** The private sector has indicated that, although relevant national and EU institutions have proved guidance over the years, there are still overlaps and misalignments between PSD2 and GDPR. Furthermore, more general data related EU regulations are being developed at this moment, such as the European Data Act. We recommend the Commission to thoroughly check the alignment of the existing PSD2-framework and a potential future Open Finance framework with the GDPR and other general data related EU legal frameworks.
- **Emergence of data aggregators.** As mentioned in section 2 of this non-paper, PSD2 has led to new types of service providers that provide data aggregation services. In other words, these entities offer their PSD2 license to other entities so that the latter can have access to payments data. Although the combination of PSD2 and GDPR should minimize any potential risks to consumer protection (and data protection in particular), PSD2 has not been drafted with these types of services in mind. We recommend the Commission to examine and investigate the rise of these (and similar) business models and asses the need for any additional requirements to mitigate any new risks stemming from these business models.
- **Expand the scope of access to the account to also include savings and credit-card accounts (and other types of relevant accounts).** PSD2 currently only regulates for access to information on payments accounts. However, it could be beneficial for consumers to use the legal framework as set out in PSD2 for other types of accounts, especially if they want to make use of account information services. The risks of the access to the account provisions in PSD2 do not differ significantly between payment accounts, and savings or credit card accounts, for example. We recommend the Commission to assess the need to broaden the scope of access to the account to also include other types of accounts.
- **Further harmonisation of legal requirements and supervisory practices.** While PSD2 has led to more unified single market for payments services, private sector parties still see differences in the implementation and application of the PSD2 requirements. We recommend the Commission to assess the need, and the benefits and drawbacks of further harmonisation of legal requirements and supervisory practices, such as by proposing a regulation instead of a directive and by expanding the mandate of the European Supervisory Authorities.

4. Recommendations on improving the legal framework for payment services

Additionally, we have identified other aspects which could be further explored as they could improve the existing legal framework for payment services specifically, in random order:

- **Merge PSD2 with the revised Electronic Money Directive (EMD2).** In order to align the framework for payment services and minimize legal loopholes as much as possible, EMD2 could be merged into PSD2. Many concepts in EMD2 are functionally similar to PSD2 services yet are

regulated differently. For example, an e-money wallet is functionally not different from a regular payments account. We recommend the Commission to consider integrating EMD2 into the PSD-framework.

- **Enhance the supervisory framework for PSPs that are part of a larger group.** More and more (big)tech companies are entering the market for payment services. This leads to new risks, as there are fallout risks stemming from decision elsewhere in the group that can affect the licensed PSP. It would be beneficial to impose additional requirements on PSPs *of a significant size* that belong to a non-financial group, among which:
    - Additional supervisory requirements related to intragroup transactions, in line with art. 123(1) of the Capital Requirements Directive 4 (CRD4) for credit institutions, and art. 265 of the revised Solvency Directive (SII) for insurance undertakings.
    - Formalisation of art. 9(3) of PSD2 along the lines of the existing Supervisory Review and Evaluation Process (SREP) for credit institutions.
    - Alignment of the criteria regarding the control of shares and ownership of a PSP, as laid down in art. 6 of PSD2, with the requirements in art. 23 of CRD4.

  We recommend the Commission to investigate the necessity to introduce the abovementioned enhanced requirements for significant PSPs that belong to a non-financial group.
- **Strengthen the ability of payment institutions to gain access to payment account services of credit institutions.** Article 36 of PSD2 already provides that payment institutions should have access to such services on an "objective, non-discriminatory and proportionate basis", and that a refusal by a credit institution to do so should be duly motivated and reported to the competent authority. Nevertheless, a more detailed standard of guidance of what would constitute a proper basis does not exist, leading to grey areas for competent authorities where it is unclear if a refusal by a credit institution is justified or not, especially as credit institutions often refer to AML/CFT requirements to deny access to payment institutions. We recommend the Commission to explore the necessity of further detailing criteria for credit institutions to refuse the access of a payment institution to certain payment services.
- **Create a legal framework for technical service providers in order to ensure fair access to crucial technical solutions.** In order to ensure consumer protection and their freedom to choose the best products, but also to keep the provision of payment services competitive, a framework to ensure access to technical solutions, such as NFC-chips on devices, is necessary. Certain bigtech-companies have become dominant parties in the provision of mobile devices, including smartphones, where they also control certain solutions that can be used to support payments. Access of third parties to these solutions need to be based on objective, non-discriminatory, proportionate and transparent conditions in order to promote innovation and competition in payments. We recommend the Commission to draft requirements for technical service providers in order to ensure the free and fair access to technical solutions that can be used for payment services.
- **Ensure that payment information and transaction overviews are transparent.** As non-bank PSPs have become increasingly important since the introduction of PSD, more and more consumers and merchants use them. However, it is often unclear in transaction overviews who the beneficiary of the transaction was if a PSP was involved. In other words, often PSPs use a general (segregated) account to collect the payment, where the payer can only see on his bank statement that he has done a transaction with a PSP but cannot verify who the exact beneficiary was. This can lead to risks for fraud and unfair commercial practices, but also to uncertainty for consumers as they sometimes do not have a good overview of their transactions. This is especially prevalent with payments for subscriptions. We recommend the Commission to explore whether requirements or standards on payment transaction information could be beneficial.
- **Enhanced measures to counter fraud.** PSD2 introduced new provisions to battle bank fraud. While these types of fraud have diminished since then, new types of fraud have become prevalent, such as phishing and spoofing. A review of the PSD-framework should deal with these new types of fraud. Furthermore, there are few requirements for PSP to check their clients, in particular web shops, with the aim of countering fraud. In many instances fraud could have been prevented if PSPs had done better checks on the reliability of their clients and had signalled unusual patterns earlier. We recommend the Commission to explore new measures to counter new types of fraud, and to enhance the role of PSPs in identifying malicious fraudulent actors and preventing them from being able to perform illegal activities.