Non-paper on a supervisory framework for payment processing service providers

Ministry of Finance of The Netherlands

1. *Introduction*

In its Retail Payments Strategy of September 2020, the European Commission announced new policy actions relating to the EU payments ecosystem in order to ensure a high level of security for retail payments in Europe, and to future-proof supervision and oversight of the payments system. Furthermore, a political agreement on the Digital Operational Resilience Act (DORA) was reached in the first half of 2022. In article 51 (Review Clause) of DORA, the Commission is tasked with an assessment of the need for increased cyber resilience of payment systems and payment-processing activities, and the appropriateness of extending the scope of DORA to include operators of payment systems and entities involved in payment-processing activities.

On 1 January 2014, The Netherlands introduced a national supervisory framework for payment processing service providers (PPSPs), including a licensing regime. Given, the DORA review clause and the proposals in the field of payments the Commission is working on, but also the questions raised by a large number of Member States and the EP on the (lack of) regulation and supervision on PPSPs, we would like to bring under attention our national framework for PPSPs. Our regime deals with many of the issues that are included in the DORA review clause and is based on the same international and European standards that underpin DORA. That said, the national regime goes beyond the requirements as laid down in DORA and is more detailed on certain aspects. We feel that it could serve as a blueprint for a more ambitious harmonized regime at the EU-level, especially as the negotiations on DORA showed that there is demand for a legal framework for payment systems and processors among certain Member States and the EP. However, if the Commission would decide to (only) extend the scope of DORA to payment systems and payment processors, we would strongly urge the Commission to leave room for Member States to impose additional or more detailed requirements on operational resilience.

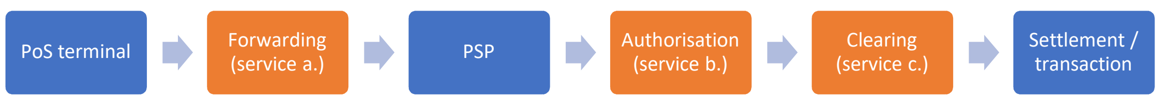
Our current national framework only covers card payments. We are currently assessing the need to expand the framework to also cover online payments, as they have become a very important part of the payment infrastructure in the past years. If it is not possible to come to an EU-level framework for PPSPs that also includes online processors, the most likely outcome is that we will have to expand our national framework.

2. *Goals and scope of the national framework*

The national framework for PPSPs (in Dutch: *afwikkelondernemingen*) was included in the Financial Supervision Act in 2014. PPSPs provide crucial services for the proper functioning of the payments system. Before 2014, a national (informal) oversight framework had existed since 2007. However, this framework was deemed unsuitable for the proper supervision and mitigation of systemic risks in the payments ecosystem. The Dutch government, acting on advice of De Nederlandsche Bank (DNB), therefore decided to introduce a national regime, with which existing oversight frameworks and standards, specifically the CPMI-IOSCO Principles for Financial Market Infrastructures (PFMI), were hard-coded into national law via a supervisory framework with a licensing requirement.

The current framework identifies three types of activities offered by PPSPs:

a) The forwarding by a (legal) person other than a communication network provider of requests made by payers by electronic means to their payment service providers for immediate confirmation that the payment orders initiated by the payers comply with the conditions set by the payment service providers
b) Authorising those requests on behalf of a payment service provider
c) Clearing, insofar that this involves determining monetary claims or obligations of payment service providers, in keeping with the payment instructions of payment service users.



A payment service user uses its card at a point-of-sale (PoS) terminal. The (provider of the) terminal then sends an authorisation and payment request to the payment service provider of the user. This falls under the definition of service a). The payment service provider then needs to check whether the user has enough funds on its account to effectuate the payment. In some instances, third parties perform this check instead of the user's bank. These third parties fall under the definition of service b). If the user has enough funds and the payment request is authorised, the payment needs to be effectuated. When the payer and payee use different payment service providers, transaction needs to be settled. Third parties (e.g. automated clearing houses) offer services to determine the monetary claims and obligations that the services providers have on each other. These services fall under the definition of service c).

In order to ensure that the framework only covers the most important PPSPs, it only applies to entities that process more than 120 million payments per year. There are currently four PPSPs licensed by DNB, with a further two that are active in The Netherlands but do not (yet) reach the threshold for the licensing requirement.[1]

3. Requirements for PPSPs

As mentioned before, the main focus of the national framework is on good governance and sound operational management. PPSPs perform crucial and fundamental activities for the proper functioning of the payments infrastructure. The national framework tries to mitigate several risks.

Firstly, it addresses operational risks. When a PPSP malfunctions, many payments cannot take place, even if PPSPs are only one link in the larger payment chain. It is therefore important that PPSPs manage these risks properly. The requirements related to this risk are based on the PFMI and are in line with the DORA-requirements.

A second risk has to do with the integrity and reliability of payment instructions, and the confidentiality of payments. In other words, PPSPs play an important role in making sure that payment instructions are not corrupted or altered during the process, nor that sensitive payment information is leaked. Both the operational and integrity risks could lead to systemic risks for the provision of payment services if not handled properly: operational incidents can lead to major disruption, while integrity issues can lead to a loss of confidence in the payments markets, and in the worst case in the financial sector as a whole.

International standards, most notably the PFMI, have been drafted in order to mitigate these risks. Our national framework has hard-coded these standards in national law (primarily in level 2 and 3 legislation). The benefit of this approach is that NCAs have formal powers to enforce the application of these standards, thus ensuring good governance and sound operational management in PPSPs and preventing risks from materialising. The requirements also include fit and proper tests for senior management, but also more detailed requirements regarding up-time of systems.[2]

The national framework currently does not require entities to be located in The Netherlands or in the Union. Two of the four entities that currently fall inside the framework are located outside The Netherlands, one of which even outside the EU. Nevertheless, it is illegal to offer payment processing services without the proper notifications with and authorisations by DNB. The national framework does provide for an equivalence regime, where PPSPs would not require a license if they operate from a country with similar legal and supervisory requirements. However, the equivalence regime has not been used yet.

---

[1] https://www.dnb.nl/en/public-register/register-of-payment-processing-service-providers/?p=1&l=10&rc=V0ZUQUY – NB: Alipay Connect PTE Ltd. and JCB International have notified DNB that they offer payment processing services, but they do not reach the threshold. They are therefore not required to be licensed in The Netherlands, but they have to inform DNB on a yearly basis about the amount of transaction they process. The four entities that fall under the full licensing regime are CCV Group, EquensWorldine (both based in The Netherlands), Mastercard Europe and Visa Europe (both based outside The Netherlands).

[2] For example, PPSPs that offer service a) or b) should ensure that they are operational for 99,88% of the time during 06.00h-00.30h, and outside this timeframe 98,50% of the time. PPSPs that offer service c) should ensure that their maximum downtime after an incident does not exceed two hours.

4. Relationship with DORA and existing oversight frameworks
The review clause in art. 51 only covers the need to expand the scope of the DORA regime, which is limited to digital operational resilience, to also include payment systems and payment processors. The national framework would not clash with the DORA requirements. We do note that the national framework has a broader range of requirements and that it is more detailed on certain aspects than DORA. As mentioned before, the national regime includes specific up-time requirements, for example.

We do strongly advise the Commission that, if it were to only decide to include payment systems and processors in DORA, it leaves room to Member States to impose further and more detailed requirements on operational resilience.

In July 2014, the Regulation on oversight requirements for systemically important payment systems (SIPS-regulation) was introduced by the ECB. This regulation provides for an oversight regime for payment systems that play an important role at the EU-level and is also based on the PFMI. Nevertheless, the SIPS-regulation has a different scope than the national regime, insofar it does not include service a) and b). Furthermore, the SIPS-regulation does not provide for a licensing regime, which lead to a smaller set of possible sanctions to enforce the requirements on PPSPs and payment systems in general. In our view, our national framework could add to the quality, effectiveness and robustness of the regime as set out in the SIPS-regulation, and could actually bolster the powers of the ECB, NCBs and NCAs. That said, it is obvious that any EU-level regime should of course be designed in such ways that it respects the mandates and powers of the ECB and NCBs as set out in the relevant treaties and legislation.

5. Legal texts and further information
Unfortunately, no official English translation exists of the national law and the explanatory memorandum accompanying the law. Relevant legal texts in Dutch can be found here:

- Financial Supervision Act (FSA) (consolidated): https://wetten.overheid.nl/BWBR0020368/2022-07-08
- Amendment of the FSA of 2014 introducing the national regime: https://wetten.overheid.nl/BWBR0034293/2015-01-01
- Explanatory memorandum accompanying the amendment of the FSA of 2014: https://zoek.officielebekendmakingen.nl/kst-33632-3.html
- Decree on prudential requirements (level 2): https://wetten.overheid.nl/BWBR0020420/2022-07-08
- DNB regulation on PPSPs (level 3): https://wetten.overheid.nl/BWBR0035089/2014-05-03

Further background information on the national regime can be found on the website of DNB: https://www.dnb.nl/en/sector-information/supervision-sectors/clearing-and-settlement-systems/