Good practices sub-merchants

Payment institutions and Electronic money institutions

DeNederlandscheBank

EUROSYSTEEM

Disclaimer

Good practices set out suggestions or recommendations for entities. They are examples of possible applications that, in DNB's opinion, provide a good interpretation of the obligations laid down in legislation and regulations. Good practices are indicative and entities are free to take a different approach, as long as they otherwise comply with the laws and regulations and are able to demonstrate and substantiate their compliance. To read more about the status of our policy statements, go to the Explanatory guide to DNB's policy statements on Open Book on Supervision.

Contents

Introduction

De Nederlandsche Bank N.V. (DNB) has prepared this good practices document to provide payment institutions and electronic money institutions[1] (hereafter: PIs and EMIs or *institutions*) with guidance on how to manage risks related to the provision of services (directly or indirectly) to sub-merchants. This good practices document contains guidance on the SIRA as well as policy and procedures regarding customer due diligence and transaction monitoring in relation to sub-merchants. DNB observed that the institutions have been increasingly setting up different constructions with their clients in order to provide services to sub-merchants. Therefore, in 2022, we conducted a thematic examination into selected PIs and EMIs that use different partnership constructions to offer payment services to sub-merchants to gain insight into the integrity risks associated with this practice. In addition, we investigated which control measures the selected institutions had implemented in order to mitigate the associated integrity risks. Risk management always requires customisation. This also applies to the risks associated with sub-merchants. The examples presented in this good practices document will not always be directly applicable to every institution.

Definitions

- *Sub-merchant:* Neither the Anti-Money Laundering and Anti-Terrorist Financing Act (*Wet ter voorkoming van witwassen en financieren van terrorisme - Wwft*) nor other statutory obligations provide a definition of a sub-merchant. During our examination, we encountered different definitions and interpretations. A sub-merchant in this document is defined as a provider of goods or services that has a business relationship with a client of a PI or EMI such as a platform, marketplace, payment facilitator, payment aggregator etc. and whose transactions for the goods/services sold are processed via that client by a PI or EMI. Sub-merchants are also often referred to as sellers, especially in the marketplace/platform context.
- *Partnership construction with sub-merchants:* a relationship that a PI or EMI has with a client e.g. a platform, marketplace, payment facilitator or another PSP, in order to process payments for the underlying merchants of that client (referred to as sub-merchants).

Examples of different types of partnership constructions with sub-merchants are described in Appendix 1 of this document: 'Types of partnership constructions with sub-merchants'.

Several institutions were selected in this examination to gain insights into the integrity risks associated with sub-merchants. In addition, DNB investigated which control measures the selected institutions have implemented in order to mitigate these integrity risks. Risk management always requires customization. This also applies to the risks associated with sub-merchants. The examples presented in this good practices document will often, but not always, be directly applicable to every single institution.

1 This good practices document could also be relevant for other payment service providers

Relevant laws and regulations

PIs and EMIs must comply, among other requirements, with the following statutory obligations to mitigate money laundering and terrorist financing risks. This good practices document provides non-binding suggestions for meeting these obligations.

- Sound and ethical operational management (Section 3:10 read in conjunction with Section 3:17 of the Financial Supervision Act (*Wet op het financieel toezicht – Wft*) and with Sections 10 and 17 of the Decree on Prudential Rules for Financial Undertakings (*Besluit prudentiële regels Wft – Bpr*);
- Measures to identify and assess money laundering and terrorist financing risks through the SIRA (Section 2b of the Anti-Money Laundering and Anti-Terrorist Financing Act (*Wet ter voorkoming van witwassen en financieren van terrorisme – Wwft*)
- Policies, procedures and measures to minimise and effectively manage the risks of money laundering and terrorist financing, as well as the risks identified in the most recent versions of the supranational and national risk assessments (SNRA and NRA) (Section 2c of the *Wwft*)
- Customer due diligence (Sections 3, 8 and 9 of the *Wwft*)
- Transaction monitoring (Sections 2a and 3(2), opening words and under d, of the *Wwft*)
- Reporting unusual transactions (Section 16 of the *Wwft*)

Integrity risks related to provision of services to sub-merchants

In our examination, we established that providing payment services to sub-merchants may result in an increased inherent risk of money laundering and terrorist financing. The following are examples of risks related to the nature of the services:

- Providing payment services to sub-merchants without performing client due diligence on them could mean that malicious parties remain under the radar and could potentially launder money via the payment institution. The Anti-Money Laundering Centre refers to similar risks related to sub-merchants.[2]
- Also, if an institution has no insight into the underlying sub-merchants of their client and is not able to draw up a transaction profile for each specific sub-merchant, it becomes more difficult to detect a potentially unusual transaction (or transaction pattern). The transaction monitoring system only relies on one general transaction profile where anomalies will be difficult to identify in the large volumes of transactions.
- Finally, counterfeit products are often sold via marketplaces. According to the investigations conducted by national and international enforcement agencies such as Interpol, Europol, and the World Customs Organisation, as well as the United Nations Interregional Crime and Justice Research Institute (UNICRI), the proceeds from selling counterfeit goods feed into transnational criminal gangs and terrorist organisations.[3]

In some cases there is more than one PI/EMI active in the payment chain. It is important to be aware that each of these licenced institutions has its own gatekeeper responsibility. The fact that a client with sub-merchants is a licenced institution itself, and is thus subject to supervision, does not relieve the PI or EMI of its independent obligations as a gatekeeper to adequately identify and manage the associated risks. Below, we provide examples of how these risks can be managed.

2 Kwetsbaarheden voor witwassen bij PSP's - AMLC
3 IPO counterfeit goods research - GOV.UK (www.gov.uk) and Counterfeiting and Product Piracy | Europol (europa.eu)

Good practices

Given the different risks associated with provision of services to sub-merchants, we observed that those institutions which analyse and identify the specific risks for their own business associated with sub-merchants are better able to define the control measures appropriate to mitigate those risks. Going forward, the institutions are better able to implement these control measures in their policies and procedures. Following these observations, we decided to provide the following good practices.

SIRA

Pursuant to Section 2b of the *Wwft*, PIs and EMIs must take measures to identify and assess money laundering and terrorist financing risks. PIs and EMIs serving clients with sub-merchants should consider providing insight into the risks associated with sub-merchants in their systemic integrity risk analysis (SIRA), for example by including scenarios that address sub-merchants' specific risks. Examples of different risks are provided in the section about integrity risks related to sub-merchants. Institutions can use these examples in their analyses to identify the specific risks related to their client portfolio. It is important for institutions to conduct the analysis tailored to their own business and determine which risks can actually materialise.

Good practices:
When conducting the risk analysis, an institution answers the following questions to identify the specific risks related to their client portfolio:

- What types of partnership constructions with sub-merchants does my institution serve?
- What (high-risk) products/services do the sub-merchants sell?
- How is the CDD and transaction monitoring with regards to sub-merchants handled?
- How is the settlement to the sub-merchant handled?
- In which jurisdiction does the client with sub-merchants hold its financial licence?

The answers to these questions are used in the risk analysis to determine the exposure to integrity risks related to sub-merchants.

Policy and customer due diligence

Pursuant to Section 2c of the *Wwft*, PIs and EMIs must adopt policies to manage money laundering and terrorism financing risks. For the implementation of this policy with regard to sub-merchants, PIs and EMIs could consider the following elements, which relate to customer due diligence pursuant to Sections 3 ,8 and 9 of the *Wwft*. The elements presented will often, but not always, be directly applicable to every single institution and the list of elements mentioned is not exhaustive. It is important for institutions to tailor their policies to their own business.

Good practices:
A PI/EMI has adopted a customer due diligence policy related to clients with sub-merchants. The following elements are included in this policy:

- When establishing a risk profile for a client with underlying sub-merchants, the institution takes the risks of these sub-merchants into account in the client's risk profile. The risk classification cannot sufficiently match the client's actual risks if the risks of the underlying sub-merchants, for which the transactions are being processed,

are not taken into account in the client's profile. After all, the risk profile of the sub-merchant could also influence the client's risk, e.g. in a situation in which a sub-merchant itself would receive a high risk classification due to, for instance, gambling activities, while the client itself would be considered low risk. This helps the institution to determine whether the sub-merchants fall outside of the institution's risk appetite.

- If the client holds a financial licence, the institution requests the client's AML/CFT policy and procedures and checks whether the client has implemented controls to manage ML/TF risks.
- Depending on the type of partnership construction, the institution either conducts client due diligence on the sub-merchants itself or requires the client with sub-merchants to perform client due diligence on sub-merchants. This allows the institution to mitigate the risk that malicious parties remain under the radar and potentially launder money via the institution.
- The institution investigates and performs ongoing monitoring of the website(s) where the products/services provided by the sub-merchants are sold. This allows the institution to mitigate the risk associated with illegal or counterfeit products, while also ensuring that the products/services sold fall within the institution's risk appetite.
- The institution requests a client with sub-merchants to provide a proof of holding a financial licence in order to ensure that the settlement is handled by a licenced institution. However, please note that the fact that a client with sub-merchants has a licence and is subject to supervision does not relieve the institution of its independent obligations as a gatekeeper to identify and manage risks in its own risk classification.
- Depending on the type of partnership construction and the risk classification, the institution conducts annual reviews of clients with sub-merchants. In case the client with sub-merchants is responsible for conducting client due diligence on the sub-merchants, the annual reviews include a sample review of selected sub-merchants file.
- The institution performs audits or checks on the client with sub-merchants for compliance with the *Wwft*.
- Approval is obtained from senior management upon client acceptance and after each review for a client with sub-merchants.[4]

We also provide general guidance on customer due diligence in our Guideline on the Anti-Money Laundering and Anti-Terrorist Financing Act and the Sanction Act.[5]

4 Approval from senior management must be obtained in circumstances described under Section 9 of the Wwft.
5 dnb-guidance-anti-money-laundering-and-anti-terrorist-financing-act-and-the-sanctions-act-december-2019.pdf

Transaction monitoring

Pursuant to Sections 2a and 3(2), opening words and under (d), of the *Wwft*, institutions that, among other things, serve clients with sub-merchants must adequately monitor the processed transactions. During the examination, we observed that transaction monitoring is more challenging for partnership constructions with sub-merchants where all transactions are processed on one account (e.g. the account of the marketplace or a payment facilitator) and /or the transactions are processed in bulk. The reason for this is that the transaction monitoring system only relies on a single transaction profile instead of the separate transaction profiles of the underlying sub-merchants. This makes it more difficult to identify potentially unusual transactions.

The good practices regarding the transaction monitoring system will often, but not always, be directly applicable to every single institution and the list of possible adjustments mentioned is not exhaustive. It is important for institutions to tailor their transaction monitoring system to their own business.

Good practices:

For transactions with sub-merchants, the institution makes the following adjustments to the transaction monitoring system:

- The institution develops specific business rules to distinguish and therefore better monitor transactions from different sub-merchants. In this way, any unusual transactions of individual sub-merchants are more likely to be detected.
- When establishing the transaction profile, the institution includes the expected transaction profile of the underlying sub-merchants in the transaction profile of the client with sub-merchants. This is done by requesting the client with sub-merchants to share data about the sub-merchants (for example in a aggregated overview). This information can then be factored into the expected transaction profile of the client with sub-merchants. This enhanced transaction profile will serve as input for dynamic business rules specifically for the relevant client with sub-merchants.
- The institution requests the client with sub-merchants to periodically share information on their sub-merchants portfolio. This input, as well as any potential alerts or observations during the previous processing period, is being used to ensure that the transaction profile and associated business rules remain current and accurate.

Appendix 1: Types of partnership constructions with sub-merchants

During the examination, we identified different types of constructions with sub-merchants. The most common types of constructions are: marketplaces, platforms, payment facilitators, referral partners and resellers. We divided the different types into three groups based on their similarities.

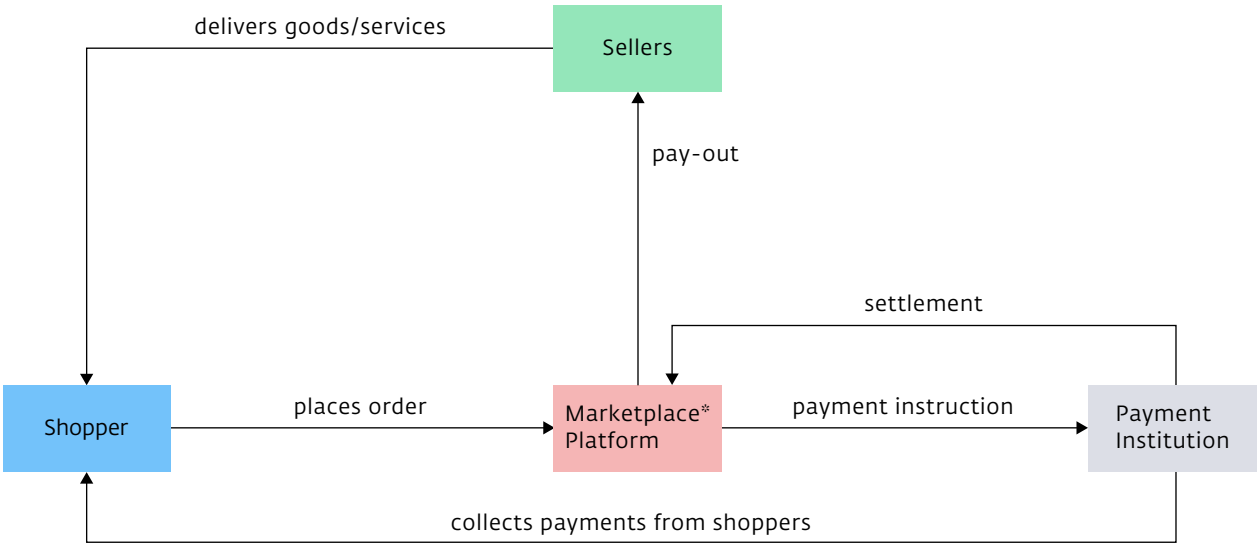
1. Marketplaces and platforms

A marketplace is an ecommerce website or a mobile app that enables sellers (referred to as sub-merchants) to provide their products or services to the users of a marketplace/platform. Payments are processed by a PI or EMI through the website of a marketplace/platform and are often split between the marketplace/platform and sub-merchants. Examples of online marketplaces are peer-to-peer marketplaces, ride sharing services, crowdfunding platforms and so on.

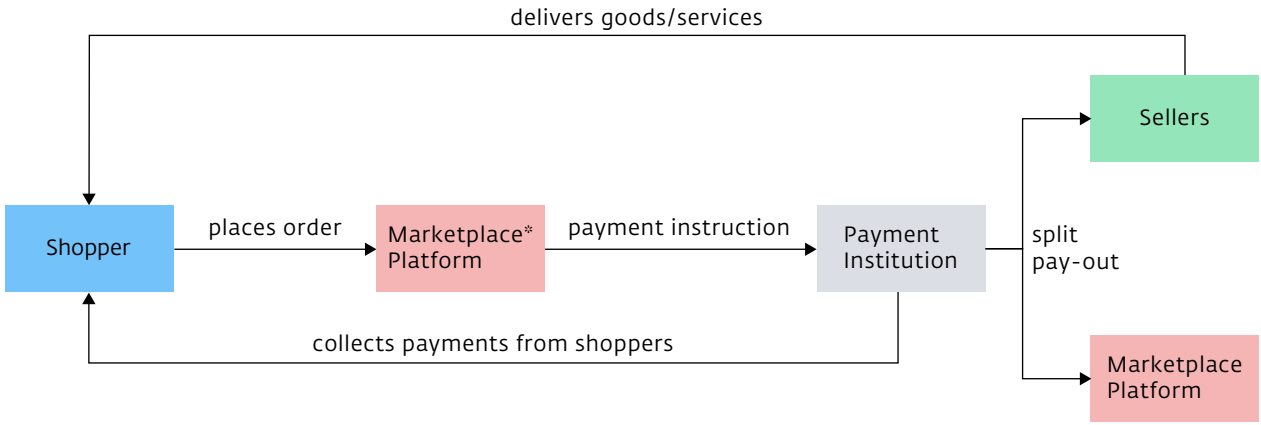
In this construction, the PI or EMI classifies the marketplace as its client and often refers to the marketplace or platform as the merchant or the *merchant of record*. Depending on the chosen construction the sub-merchant is either the client of both the PI/EMI and the marketplace/platform (rare cases) or only of the marketplace/platform (most commonly).

Below are two examples of how the transaction and money flow often take place by marketplaces and platforms.

a) Marketplace in the money flow:[6]



b) Marketplace outside of the money flow:

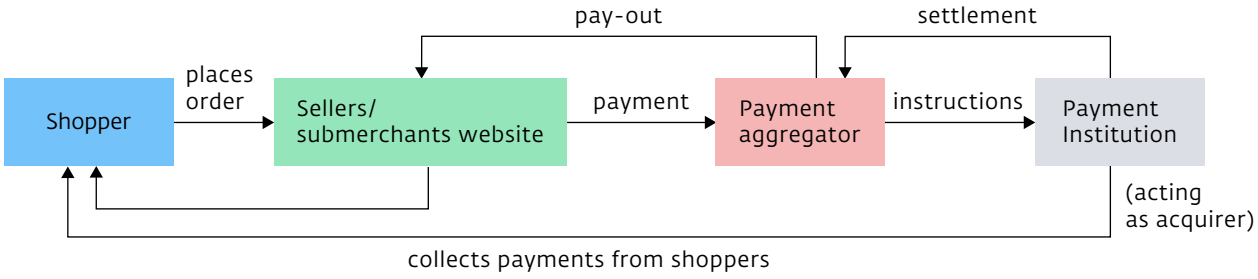


6 Marketplaces/platforms which provide money pay-out to the sellers must hold a (PSD2) licence to do so, Electronic trading platforms (e-commerce platforms) under PSD2 (dnb.nl)

2. Payment facilitators and payment aggregators

Payment facilitators[7] and other payment aggregators are parties which support multiple websites of different sub-merchants in order to provide these sub-merchants with payment services. There is no overarching website such as in the marketplace/platform construction, each sub-merchant has its own website where the goods and services are sold. The payment facilitator/aggregator is a client of a PI or EMI. Depending on the chosen construction, the sub-merchant is either the client of both the PI/EMI and the payment facilitator/aggregator (rare cases) or only of the payment facilitator/ aggregator (most commonly). Payment facilitators/aggregators have their own financial licence. The settlement to the sub-merchant is handled by the payment facilitator/aggregator.

Below is an example of how the transaction and money flow often take place by payment facilitators and payment aggregators.[8,9]



3. Referral partners and other business partners

Referral partners and other business partners refer clients (referred to as sub-merchants or merchants) to a PI or EMI. These partners do not participate in executing the transactions; they either just introduce the sub-merchants to a PI or EMI or participate in the on-boarding of sub-merchants by handling the communication between the PI and EMI. The partners receive commission for the introduction of sub-merchants. Eventually the sub-merchants become direct clients of the PI or EMI. In this construction, the sub-merchant is often considered as a regular merchant of a PI or EMI.

7 The term payment facilitator is used in the acquiring context, particularly by Visa and MasterCard card schemes. In this context, a payment facilitator is a third party that may sign a merchant acceptance agreement on behalf of an acquirer and receive settlement of transaction proceeds from an acquirer on behalf of a sub-merchant. A sub-merchant in the payment facilitator construction is a merchant whose payment services are provided by a payment facilitator

8 Electronic trading platforms (e-commerce platforms) under PSD2 (dnb.nl)

9 The role in the transaction of the payment facilitator and other payment aggregators is different depending on the services provided and agreements singed with the payment institution and sub-merchants. This flowchart is an example and does not apply directly to every type of payment facilitator/ payment aggregator.

The table below presents an overview of the most common set-up per type of partnership construction with sub-merchants:

	Marketplace/ Platform	Payment facilitator/ Payment aggregator	Referral partners/ Other partners
Role	Provide individual sellers with possibility to sell products/ services	Provide payment services to sub-merchants	Provide PI/EMI with new merchant
Website	Website per marketplace/ platform	Website per sub-merchant	Website per sub-merchant
Financial license	Payment license if the marketplace settles to sub-merchants	Payment license	n/a
Business relation PI/ EMI	Either with client and sub-merchants or only with the client	Either with client and sub-merchants or only with the client	Either with client and sub-merchants
Settlement to sub-merchant	Either by PI/EMI or by marketplace/platform	By payment aggregator	By PI/EMI

De Nederlandsche Bank N.V.
Postbus 98, 1000 AB Amsterdam
020 524 91 11
dnb.nl

Volg ons op:

DeNederlandscheBank
EUROSYSTEEM