Guidelines for the reporting of payment data from payment service providers and transmission to the Central Electronic System of Payment information (CESOP)

Table of Contents

Version	Date	Description
1.00	7 July 2022	Version Submitted for publication

1 INTRODUCTION

On 18 February 2020, the Council adopted a legislative package to collect payment data in order to improve the fight against e-commerce VAT fraud. The package is composed of two legal texts:

- Council Directive (EU) 2020/284 of 18 February 2020 amending Directive 2006/112/EC as regards introducing certain requirements for payment service providers[1] and:
- Council Regulation (EU) 2020/283 of 18 February 2020 amending Regulation (EU) No 904/2010 as regards measures to strengthen administrative cooperation in order to combat VAT fraud[2].

The new rules will enter into force on 1st January 2024. The amendments to Directive 2006/112/EC[3] ("the VAT Directive") create a new reporting obligation for payment service providers established in the European Union ("EU") to keep records of the payments they process and their beneficiaries ("payees"), while the amendments to Regulation (EU) 904/2010 focus on the development of the Central Electronic System of Payment information ("CESOP"), where the data collected will be stored and processed before being put at the disposal of Member States anti-fraud experts to fight VAT fraud.

The use of payment data is driven by the need to improve the fight against e-commerce VAT fraud, which is made particularly difficult due to the lack of physical presence of sellers in Member States of consumption. The use of internet and new technologies has allowed companies to sell goods abroad without the need to set-up any kind of physical presence. This in turn can make it difficult for Member States to perform controls as they are dependent on the goodwill of foreign sellers to declare their transactions in order to know that they are being active in their territory. Even in the cases where a Member State is aware that sellers on a website are supplying goods or services in their territory, it can be extremely difficult to identify the actual seller behind the website. This lack of information makes it extremely difficult for Member States to request or exchange information with each other as they do not know with who they should share the information, or to who they should ask for it.

As of 2024, the use of payment data and CESOP will provide anti-fraud experts in Member States with the information needed to identify sellers abroad that supply goods or services on their territory. The system is designed to limit the administrative burden on payment service providers by collecting data via a harmonised standard form and restricting the data collected to what is necessary to identify the sellers and combat e-commerce VAT fraud. No data on the buyer ("payer") shall be collected, apart from the estimated Member State of origin of the payment, and data on the seller shall only be collected if it receives a substantial amount of cross-border payments.

The present guidelines have been drafted in collaboration with experts from the payment sector and Member States and focus on explaining the rules governing the reporting of payment information. They detail the scope of the reporting obligation, present the main payment methods currently used in the European Union to pay for goods and service online, explain what are the triggers of the reporting obligations and attempt to list the data elements used by payment service providers which could be reported to CESOP. They are addressed to both payment service providers who will have to report data under the new reporting obligations, and Member States who will have to collect the data and transmit it to CESOP. They remain however an explanatory document with no legal value.

---

[1] Council Directive (EU) 2020/284 of 18 February 2020 amending Directive 2006/112/EC as regards introducing certain requirements for payment service providers (OJ L 62, 2.3.2020, p. 7)

[2] Council Regulation (EU) 2020/283 of 18 February 2020 amending Regulation (EU) No 904/2010 as regards measures to strengthen administrative cooperation in order to combat VAT fraud (OJ L 62, 2.3.2020, p. 1)

[3] Council Directive 2006/112/EC of 28 November 2006 on the common system of value added tax (OJ L 347, 11.12.2006, p. 1).

2 SCOPE OF THE REPORTING OBLIGATION

This section focuses on defining the scope of the reporting obligation laid down in article 243b of Directive 2006/112/EC as introduced by Council Directive (EU) 2020/284 ("CESOP reporting").

Article 243b (1) lays down the rules of the reporting obligation:

> *Member States shall require payment service providers to keep sufficiently detailed records of payees and of payments in relation to the payment services they provide for each calendar quarter to enable the competent authorities of the Member States to carry out controls of the supplies of goods and services which, in accordance with the provisions of Title V, are deemed to take place in a Member State, in order to achieve the objective of combating VAT fraud.*
>
> *The requirement referred to in the first subparagraph shall apply only to payment services provided as regards cross-border payments. A payment shall be considered a cross-border payment when the payer is located in a Member State and the payee is located in another Member State, in a third territory or in a third country.*

According to this article, there are three requirements that must apply to trigger the reporting obligation of a payment service provider (reporting entity):

1. The reporting entity must be a payment service provider as defined in article 243a (1) of Directive 2006/112/EC;
2. The reporting entity must provide payment services as defined in article 243a (2) of Directive 2006/112/EC;
3. The reporting entity must be involved in processing a payment as defined in Article 243a (3) of Directive 2006/112/EC, between a payer and a payee, where the payer is located in a Member State and the payee is located in another Member State, in a third territory or in a third country.

These three conditions form the essence of the scope of the reporting obligation and will be detailed in this section, each one answering one of the following questions:

2.1. What are the entities in scope?
2.2. What are the payments in scope?
2.3. What are the payment services in scope?

In addition to these three elements, two additional conditions are required to trigger the reporting obligation, the first of which is laid down in Article 243b (1), 2nd subparagraph and requires that the payments reported are cross-border, while the second is laid down in Article 243b (2) and requires that the payment service provider executes more than 25 cross-border payments per quarter to a given payee before transmitting any information. These two conditions to be monitored are detailed in section 3.

2.1 The entities in scope

The reporting obligation is only applicable to the payment service providers defined in Article 243a and which provide payment services in the European Union. Payment service providers which do not provide payment services in the European Union do not have to fulfil any reporting obligation.

As regards the definition of what a payment service provider is, article 243a refers to the definitions laid down in Directive (EU) 2015/2366[4] ("PSD2"). However, not all payment service providers covered by the PSD2 are automatically subject to the CESOP reporting obligation. Indeed, article 243a limits the scope of the reporting obligation to the following four categories of payment service providers:

a) Credit institutions, which covers e.g. fully licensed banks established in Europe as well as European branches of credit institutions that have their head office outside the EU and which provide payment services;

b) E-money institutions, which covers all payment service providers providing payment services via electronic money ("e-money") e.g. electronic wallet providers and electronic voucher/card providers;

c) Payment institutions, which is a residual category that can cover all companies providing payment services that do not qualify for any of the other categories listed in the PSD2. It can include companies that provide payment services such as issuing of credit/debit cards, acquiring of payment transaction, processing of payments, initiation of payments, etc.;

d) Post-office giro institutions which provide payment services.

The PSD2 adds to this list central banks and public bodies, however those entities are not in scope of the reporting obligation for CESOP as they typically do not provide the payment services in scope (see section 2.3.).

N.B.: The exemption for small payment service providers laid down in article 32 of the PSD2 is not applicable to the CESOP reporting obligation. As such, even small payment services providers will have to report data on payments and payees if all other conditions are fulfilled.

Although the definition of payment service providers is quite broad and covers most of the payment market, it must be read in conjunction with the rules applicable to the payment services in scope. Indeed, not all payment services are in scope of the reporting obligation. As such, it is possible that an entity qualifies as a payment service provider under the definition of article 243a (1) of Directive 2006/112/EC but does not provide any of the payment services referred to in article 243a (2). If that is the case, this payment service provider will not be subject to the reporting obligation. A good example of that is the situation of payment initiators which are payment institutions but do not provide any of the payment services in scope (see point 2.3.).

Article 3 (b) of the PSD2 also establishes a special rule which excludes from its scope payments done either via a commercial agent or via commercial agents who acts only on behalf of the payer or the payee. This implies that payments done either via a commercial agent or via commercial agents who acts on behalf of both the payer and the payee would be in scope of the PSD2. This is confirmed in recital 11 to the PSD2 which states that commercial agents who act on behalf of both the payer and the payee must be registered as payment service providers if they hold funds on behalf of both their clients. This rule is especially important in e-commerce since it implies that online platforms and marketplaces who hold funds on behalf of their clients must register as payment service provider (either as payment institution or other categories based on the service they provide) and will be in scope of the reporting obligation. As such, marketplaces which collect funds from the payer, hold them and then distribute them to the payee will have to report information on the payee to CESOP.

---

[4] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance) *(*OJ L 337, 23.12.2015, p. 35)

2.1.1 Territorial scope – the situation of European Economic Area countries and Northern Ireland

The rules of the PSD2 are applicable to all European Economic Area ("EEA") countries, which includes all Member States of the European Union as well as Iceland, Liechtenstein and Norway. This means that payment service providers wishing to provide payment services in the EEA must obtain a payment license in their country and respect the other requirements of the Directive if they want to use this license in another country.

Once a payment service provider from an EEA country has obtained a payment license in its country of establishment, it will be able to provide payment service in any Member States using the PSD2 passporting rules. These rules allow payment services providers that have received a payment license under the PSD2 to supply payment services to any other country of the EEA without the need to request a new payment license in this country. Instead, the payment service provider will only need to inform the other countries of its intention to supply payment services on their territory, which can be done either via a physical presence (for example a branch), the use of a commercial agent, or directly from its country of establishment via the freedom to provide services.

This means that payment service providers from EEA countries can also be in scope of the reporting obligation created for CESOP when they provide payment services in a Member State, even without a physical presence in the European Union.

For more details on how reporting will take place for EEA countries see section 4.4.2

N.B.: Although Northern Ireland is part of the EU VAT area as part of the Brexit agreement and its protocol, the scope of the reporting obligation created by Directive 284/2020 is not subject to any special arrangements with regard to Northern Ireland and Brexit. As such, payees and payment service providers established in Northern Ireland must be understood as being established in a third country (and should be reported as such) for the sake of the CESOP reporting obligation.

2.2 Payments in scope

The concept of payment is at the centre of the reporting obligation as it encompasses exactly the information that payment service providers will have to keep in their records. The concept of payment is closely linked to the definition of "payment transactions" laid down in article 4 (5) of the PSD2[5] but also covers money remittances as defined in article 4 (22) of the PSD2[6].

In simple term, a payment corresponds to a transfer of funds from a payer (the initiator) to a payee (the beneficiary). The definition of payer and payee are also laid down in article 243a which directly references the definition of the PSD2.

The payer is *"a natural or legal person who holds a payment account and allows a payment order from that payment account, or, where there is no payment account, a natural or legal person who gives a payment order"*. The payer is thus the one whose funds are being transferred in execution of the

[5] 'payment transaction' means an act, initiated by the payer or on his behalf or by the payee, of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee;

[6] 'money remittance' means a payment service where funds are received from a payer, without any payment accounts being created in the name of the payer or the payee, for the sole purpose of transferring a corresponding amount to a payee or to another payment service provider acting on behalf of the payee, and/or where such funds are received on behalf of and made available to the payee

payment. Although most of the time the payer will also be the initiator of the payment, in the case of direct debit the payee will initiate the payment following the authorisation granted by the payer in the direct debit mandate.

The payee on the other hand is *"a natural or legal person who is the intended recipient of funds which have been the subject of a payment transaction"*. The payee is thus the beneficiary of the funds transferred in execution of the payment. One of the key elements when it comes to the payee is the idea of "intended recipient". Payment processing often involves a multitude of actors and business models, and it is not uncommon that when funds are being transferred they are first passed among various payment service providers who can retain these funds for a certain period of time before transferring them to the payee. These payment service providers must not be confused with the payee as they are not the intended recipient of the payment from the payer but mere intermediaries. As such, the information that needs to be reported must regard the payee and not the intermediaries. However, since payment service providers rely on the information provided in the payment request, there are situations where an intermediary will appear as the beneficiary of the payment. These situations are detailed further in point 2.2.6.

As such, the payments to be reported to CESOP correspond to the transfer of funds from a natural or legal person whose funds are being transferred, to a natural or legal person who is the intended recipient of these funds.

N.B.: under article 243b, only payment that are initiated by a payer in the European Union are in scope of the reporting obligation. The payee on the other hand can be located in another Member States, a third territory or a third country.

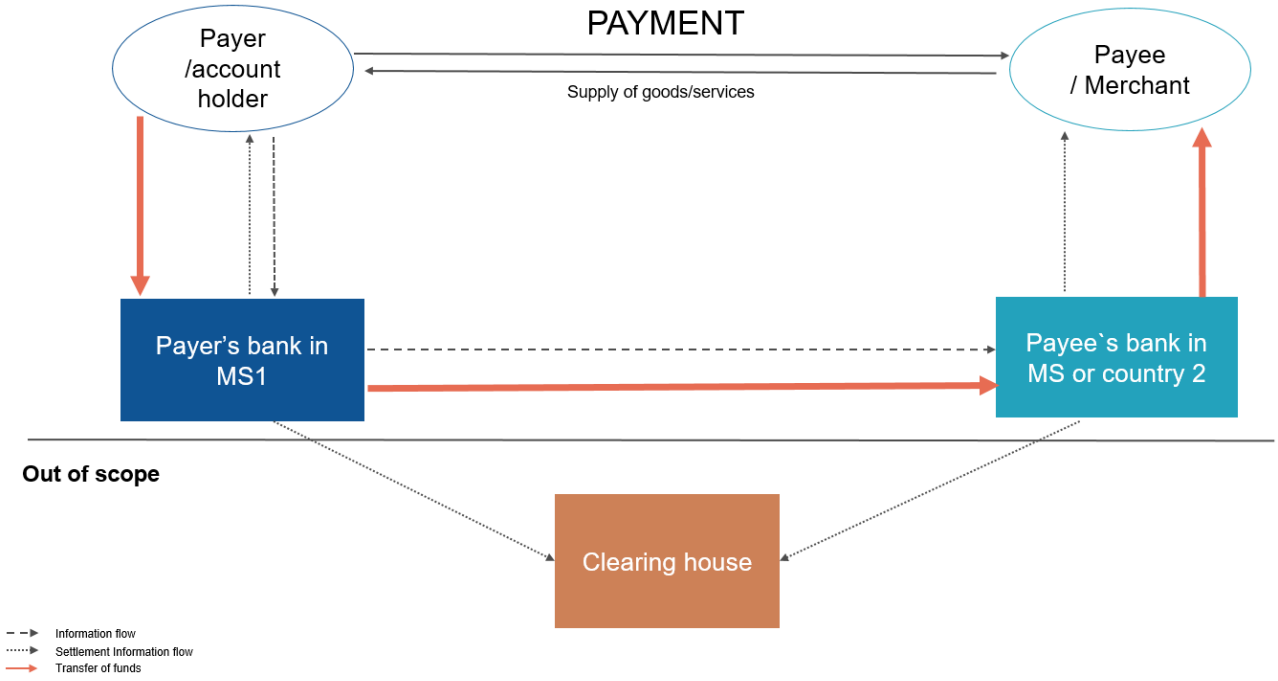
In practice, this means that the payment in scope includes:

- *payments from a payer in a Member State to a payee in another Member States (to be reported by the payee's payment service provider see section 4.3);*
- *payments from a payer in a Member State to a payee in a third territory or third country (to be reported by the payer's payment service provider see section 4.3).*

On the other hand, payments from a payer which is not in a Member States to a payee in a Member State are out of scope of the reporting obligation.

Although this definition can seem easy to comprehend, it must be pointed out that a payment between a buyer (payer) and a seller (payee) of goods or services often involves a multitude of payment services providers on both sides of the payment chain which all exchange information and transfer funds between each other in order to execute the payment between the buyer and the seller. The figure below illustrates this complexity using the example of a credit transfer.

Figure 1 – Overview of a credit transfer payment



The figure highlights four different types of flows in order to execute a single payment between the buyer (payer) and the seller (payee):

- The service flow corresponds to the various services that are provided by the different actors. The payer's and payee's banks provide payment services to their client while the clearing house provides clearing services to both payment service providers;
- The money flow corresponds to the movement of funds between the various actors. Indeed, the transfer of funds between the payer and the payee does not take the form of a single movement from one to the other, but instead correspond to a series of exchanges where the payer's bank will first take the funds from the payer's account before transferring them to the payee's bank which will credit the payee's account.
- The information flow corresponds to the exchange of information between the various actors in order to authorise, process and execute a payment. The payer will provide its payment service provider with information on the payee and the amount it wishes to transfer. Its bank will then use this information to identify the payee's bank and determine where it must send the funds. With the use of modern technology, these processes are almost immediate nowadays.
- The settlement information flow corresponds to the exchange of information between payment service providers and/or clearing house in order to proceed to the clearing and settlement between the actors. This flow is completely distinct from the payment between the payer and the payee and focuses on allowing the payment service providers involved in the payment to exchange the information and/or settle the debt created between themselves in execution of the payment.

All these various flows can cover one or several payment(s), however only the information flow will provide the relevant information on the payment between the payer and the payee. In that regard, one of the key stages of the information flow is the so-called "authorisation process" where a payment service provider will send information on the payment to the other payment service provider in order for the second to validate the details of the payment and confirm that the payment can take place. In modern days, this authorisation process takes place in a matter of seconds after the initiation of the payment and contains most of the data required under the CESOP reporting.

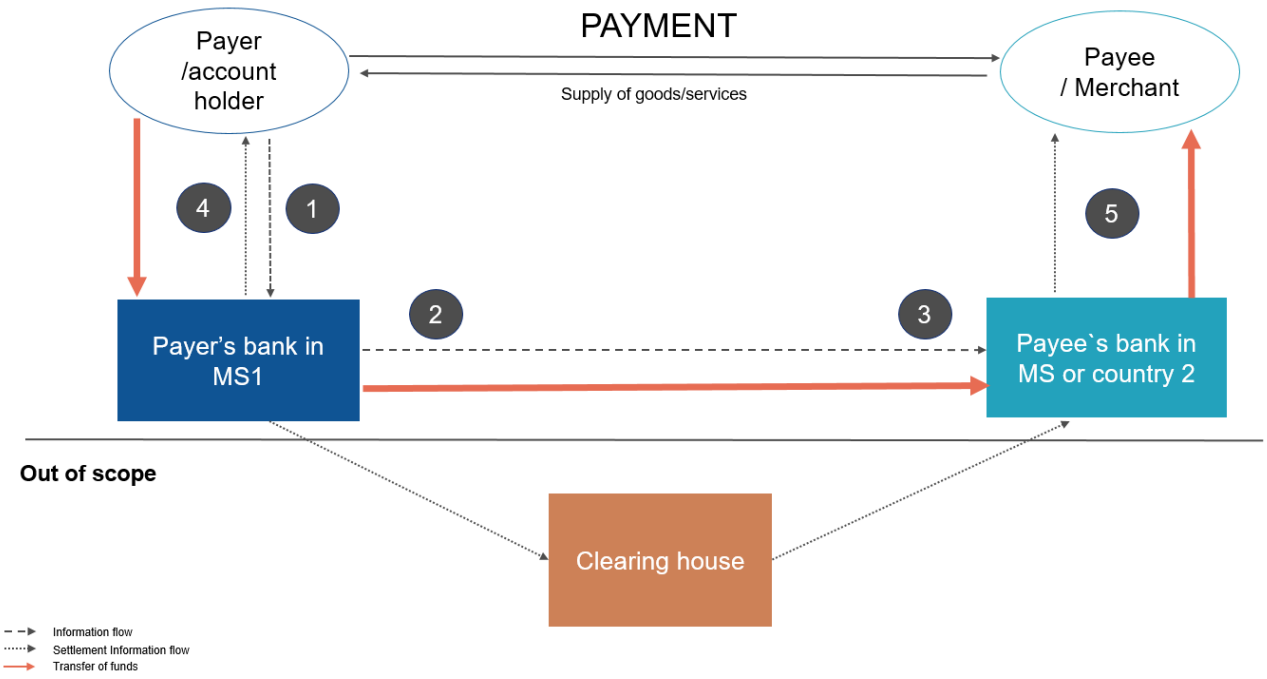
Even though the information has been recorded already, payment service providers do not transfer funds between each other at each payment transaction request, as this would imply enormous computing process between themselves for each of the millions payment transactions that are processed every day. To facilitate their activities, most payment service providers consolidate payment transactions over a period of time that can be more or less extensive and only transfer the funds between themselves at the end of this period, taking into consideration the amount they owe to another payment service provider and the amount this payment service provider owes them. This periodic transfer of funds between payment service providers is generally referred to as "settlement".

This is why the reporting obligation for CESOP is based on the information flow and the exchange of data between payment service providers (which is nearly instantaneous and includes information on the payer and the payee at transaction level) and not on the actual flow of money between themselves (which is done periodically using aggregated amounts of all payments authorised for a certain period).

The following sections will detail, for each of the main payment methods currently in scope of the reporting obligation, how they function, who the actors involved are, and how the information flow takes place. The examples provided here are not exhaustive as existing payment methods can evolve and vary and new payment methods could be developed in the future.

2.2.1 Credit transfer

Figure 2 – Functioning of a credit transfer payment



Credit transfer forms one of the oldest and most common form of transferring funds. All cross-border credit transfers in the European Union follow the rules established by the SEPA regulation and the schemes developed by the European Payment Council.

Credit transfer generally involve 3 different actors to process the payment:

- The payer's bank which holds the payer's payment account where the funds will be taken from;
- The payee's bank which holds the payee's payment account which will receive the funds;

- The payment system which provides clearing and/or settlement services to the banks in order to help them clear and/or settle the debt created by the various transfer of funds they execute. Alternatively, payment service providers might exchange payments and settle the debt directly or through other intermediaries.

In the figure, the information flow is highlighted by the blue numbers and takes place as follows:

1. The payer will initiate the payment order by providing the payee's details to its bank and requesting it to transfer a certain amount of funds to the payee's bank account;
2. The payer's bank will use the information provided by the payer to carry out a credit transfer. The payer's bank will then provide the information provided by the payer to the payee's payment service provider to credit the funds to the bank accounts of the payee.
3. The Payee's bank will verify the information provided by the payer's bank in the credit transfer request (e.g. that the bank account exist).

Once these steps are concluded, both the payer's and payee's banks have exchanged all the information necessary to execute the payment and hold almost all the mandatory information required under article 243d (for details on the information to provide, see section 4.5).

It is important to note that while the payment transaction can already be considered completed and recorded in the payment service providers records at the end of step 3, no actual transfer of funds has occurred between any of the payment services providers involved. The transfer of funds only occurs at a later stage which corresponds to the settlement and flow of money between the actors.

This settlement will take place as follows:

4. The payer's bank will debit the payer's bank account by the amount that has to be transferred to the payee.
5. The payee's bank on the other side will credit the amount of the payment transaction in the payee's account immediately after that amount is credited to the payee's payment service provider, so that the payee receives the funds in the required timeline (typically 1 business day for EU credit transfers).

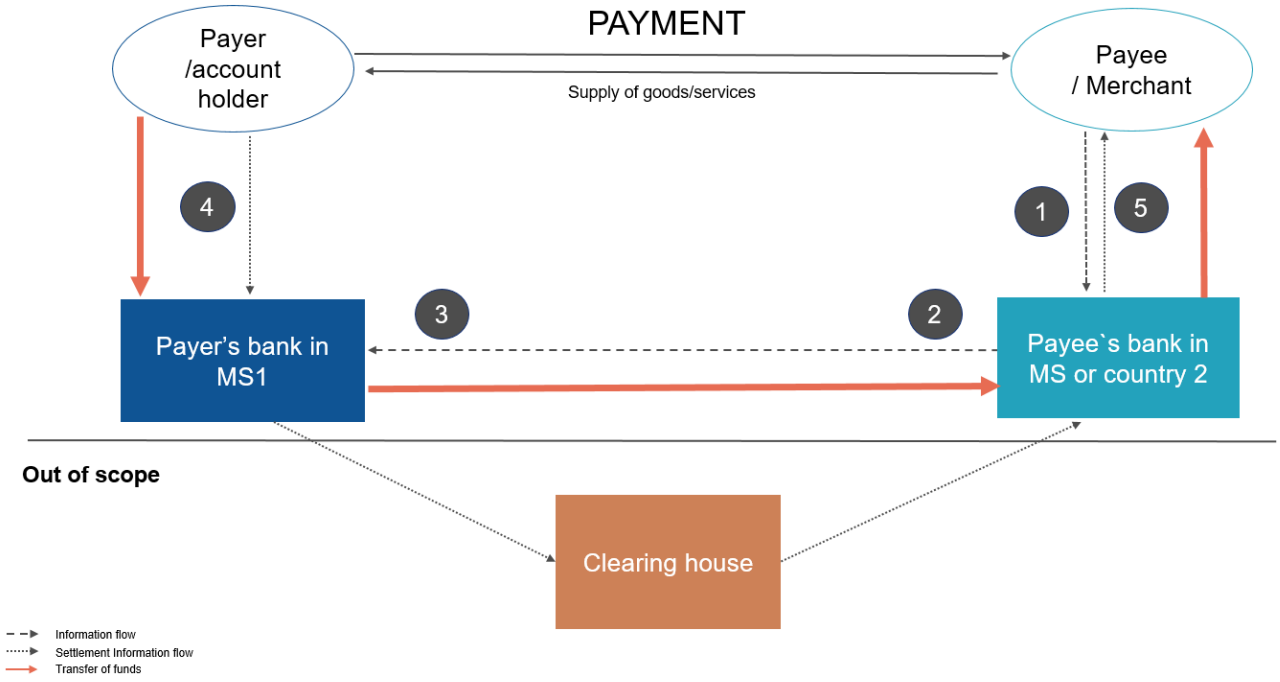
While the payment transaction between the payer and the payee requires that the payer transfers funds to the payee, it is actually possible that when both entities settle their debt at a later stage, the payee's bank is the one with a negative balance which will need to be paid to the payer's bank, if it has executed more transactions in favour of the payer's bank than it has received from it. This shows the importance of differentiating the exchange of data between the payer's bank and the payee's bank which relates directly to the payment transaction between the payer and the payee, from the exchange of funds between the two payment services providers which relates to their own activities and is not in scope of the reporting (as it is excluded from the definition of payments following article 3 (m) of the PSD2).

2.2.2 Direct Debit

Direct debits are mainly subject to the SEPA regulation. However, there are no international schemes currently in place for non-SEPA direct debit. As such, these situations remain rare in the practice and payment service providers will generally adopt specific rules between themselves for such transactions, which are often based on national practices or the SEPA rules themselves.

The presentation of direct debit that is done here is based on the SEPA rules.

Figure 3 – Functioning of a direct debit payment



The actors in direct debits are the exact same as for credit transfers (see point 2.2.1.).

The main difference between direct debits and credit transfers lies in the fact that direct debits will be initiated by the payee, on the basis of a mandate granted by the payer. They will not be initiated by the payer.

In the figure, the information flow takes place as follows:

1. Based on the mandate previously granted by the payer, the payee will initiate a series of direct debit requests to transfer funds from the payer's account to its account.
2. The payee's payment service provider will create the request and send it to the payer's payment service provider for execution.
3. The payer's payment service provider will check that funds are available and that the details of the request are correct. If so, the payer's payment service provider will debit the direct debit transaction at the due date.

These steps already include almost all the mandatory data to be reported to CESOP. They are then followed by the settlement phase where funds are effectively moved between the payment service providers (similar to credit transfers):

4. On the due date, the payer' payment service provider will debit the payer's account of the funds to be transferred.
5. The payee's payment service provider will credit the payee's account with the amount of the payment transaction in the payee's account immediately after that amount is credited to the payee's payment service provider, so that the payee receives the funds in the required timeline.

As for credit transfers, the exchanges of funds between payment service providers in execution of the settlement constitutes a separate operation for their own activities which is out of scope of reporting obligation.

2.2.3 Money remittance

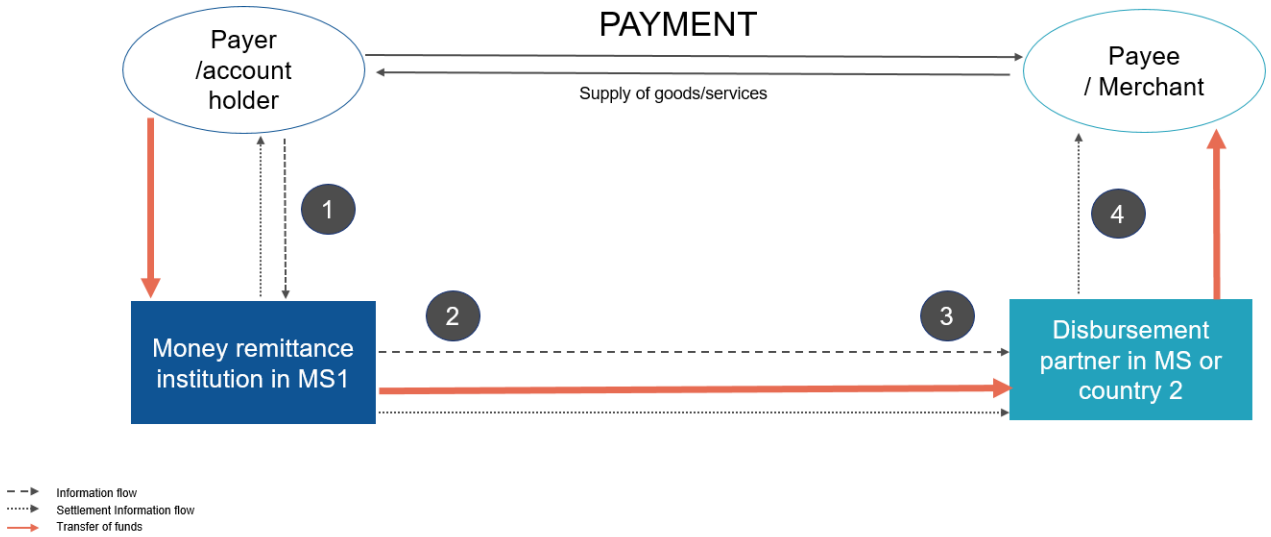
Money remittance is one of the oldest forms of transferring funds between people. Nowadays, this payment method has been supplanted by other methods such as credit transfer which offers similar functionalities at a reduced cost and faster execution. In the EU, this payment method is mainly used for so called "friend & family" payments between citizens sending funds abroad. However, it is still used commercially in other countries and is as such within the scope of the reporting obligation.

One particularity of money remittances compared to other forms of payments is the possibility to transfer funds without an existing payment account for the payee. Although modern remittances sometimes offer the possibilities to send funds directly to a bank account, it is still possible to send funds abroad via money remittance without the need to introduce the payee's payment account details. This particularity justifies the introduction of article 243d (1)(e) in Directive 2006/112/EC, which requires that the BIC or other unique identifier of the payment service provider acting on behalf of the payee (the "disbursement partner") be transmitted when there is no payment account of the payee. This information allows the system to identify who is the entity receiving the funds on behalf of the payee.

Money Remittances generally involve two entities:

- The money remittance institution which will be used by the payer to transfer funds to the payee;
- The disbursement partner, which is a second money remittance institution who will receive the funds and make them available to the payee.

Figure 4 – Functioning of a money remittance payment



In the figure, the information flow is highlighted by the blue numbers and takes place as follows:

1. The payer will initiate a money remittance request by providing its payment service provider with the details of the payee and the transaction.
2. The payment service provider of the payer (money remittance institution) will create the transaction and forward it to the disbursement partner in another MS or third country or territory.

3. The disbursement partner (payment service provider of the payee) will check the data in the request and validate it if correct.
4. The disbursement partner will put the money at the disposal of the payee.

2.2.4 Card Payment

Card payments are probably the most used form of payment for e-commerce transactions in Europe. Although they are also subject to legislative oversight, the details of the rules applicable to the exchanges of data for processing card payments are laid down in the various rulebooks established by the card scheme providers. Although each scheme provider is free to establish its own rules, the market is still highly standardised via the use of different standards, such as the "Volume"[7], a document drafted by the European Cards Stakeholder Association, which lays down the rules applicable for the exchange of information between the payment service providers involved in card payments within the SEPA area, or the EMVco standards[8].

The processing of card payments generally involves three main actors:

- The card scheme provider establishes the rulebook applicable to the card. The card scheme provider can be a payment service provider if it distributes the cards itself or provides other payment services linked to the card (such as acquiring payment transactions). This is typically the case in a 3-party card scheme where the card scheme provider will act as both the card issuer and the commercial acquirer. On the other hand, 4-party card schemes typically imply that the card scheme will not provide any payment services and as such will not be a payment service provider.
- The card issuer is the payment service provider responsible for providing the payment card (debit or credit card) to the payer and executing payment transactions on his behalf.
- The commercial acquirer is the payment service provider responsible for acquiring the various payment transactions on behalf of the payee. A commercial acquirer will aggregate all the payment transactions executed over a period of time and send the consolidated amount to the payee on a regular basis.

Technical service providers are entities contracted by card acquirers or merchants to provide services necessary for the processing of card payments. One of the most important services is the provision of a terminal or dedicated webpage which can capture the card details and initiate the payment process (payment initiator). It is important to note that such technical service providers are out of scope of the PSD2 based on article 3 (j) as long as they do not enter into possession of the funds to be transferred. As such, these providers are not considered payment service providers and do not fall within the scope of the reporting.

N.B.: the number of actors in card transactions can increase based on the number of intermediaries. It is common for acquirers to use additional intermediaries to process parts of the payment transaction or to offer multiple payment methods to the merchant. Although the scheme can vary in practice, the fundamental principles that are highlighted are always applicable and the same data elements must always be exchanged between the acquirer and the issuer.

Card payments can be sub-divided in two categories: 3-party card schemes and 4-party card schemes. In the case of 3-party card payments, the card scheme providers act as both the issuer and acquirer and are

[7] https://www.e-csg.eu/scs-volume-v9
[8] https://www.emvco.com/document-search/

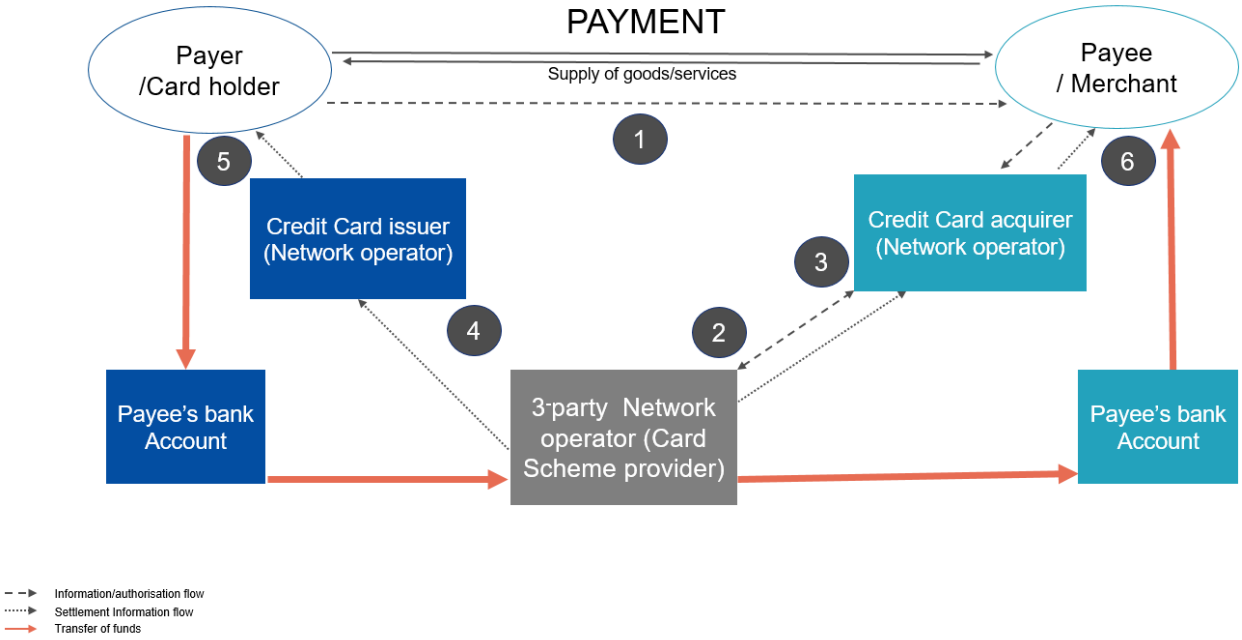
directly connected to the payer and the payee. On the other hand, 4-party card payments require that the functions of card issuer and of card acquirer are separate, with one linked to the payer and the other to the payee.

The following sub-section will detail each of these two types of card payments.

2.2.4.1 3-party card scheme

In a 3-party card scheme, the roles of scheme provider, card issuer and commercial acquirer are all performed by the scheme provider. As such, the scheme provider is central in this configuration as it will have direct relationship with both the payer and the payee. Henceforth, the scheme provider, as he is the card issuer and acquirer, will always be the key reporting entity and report both payments within the EU and payments outside the EU.

Figure 5 – Functioning of a 3-party card payment



In the figure, the information flow takes place as follows:

1. The payer will initiate the payment by providing its card details on an online interface which is linked to the payee's website.
2. Once the payer has successfully submitted its card information, the payment initiator will transfer this data to the card scheme provider acting as both acquirer and issuer. Using this information, the card scheme provider will check the data received and confirm that it is correct and that the payer has sufficient funds to execute the payment transaction.
3. The card scheme provider will authorise the transaction and send the confirmation to the payee.

After these steps which correspond to the authorisation process, the settlement phase will begin:

4. As the card scheme provider has covered the payer's expense via a credit line, it will now request the payer to pay-back the amounts that have been paid in advance via a statement of all the transactions executed (generally over a month period).

5. The payer will refund its credit by sending funds to the card scheme provider. This transfer of funds will generally take the form of a credit transfer from the payer to the card scheme provider, who acts as the payee for this payment.
6. The card scheme provider will at regular times credit the payee's payment account with the aggregated amount of all the transactions it has executed over a period of time. This payment also corresponds to a credit transfer from the card scheme provider to the payee.

N.B.: As highlighted in the graph, 3-party card payments generally involve other payment services providers (such as banks) to fund the card's credit line or to receive the funds from the commercial acquirer. For these payment service providers the transactions will look as a payment to the card issuer (for the payer's payment service provider) or a transaction from the commercial acquirer to the payee (for the payee's payment service provider). These transactions, although different from the one between the payer and the payee, are in scope of the reporting obligation and should be reported with either the card issuer as the payee, or the commercial acquirer as the payer. Indeed, they do not fall within the exclusion of article 3 (m) PSD2 for transaction between payment service providers for their own activities, since they do not serve the activities of the payment service providers involved but are part of the agreement between the payer/payee and the card issuer/commercial acquirer.

2.2.4.2 4-party card scheme

Although they follow the same basic principles, 4-party card schemes differ from 3-party card schemes as the card scheme provider, card issuer and commercial acquirer are all different entities. Because of this, the card scheme provider generally plays a less active role in the payment transaction and limits itself to establishing the rules and providing the infrastructure for the acquirer and the issuer to exchange information. Since it does not issue the card itself nor acquire transactions, the card scheme does not provide any payment services and is not a payment service provider under the PSD2. It is thus not subject to the reporting obligation.

The role of card issuer can vary greatly between the different situations, at times it will be the credit institution of the payer who will also take the role of card issuer and provide the payer with the card. At other times, it is a dedicated institution whose sole purpose is to provide credit/debit cards.

The same is also applicable to the role of acquirer which can at times be done directly by the credit institution of the payee. In most cases, this role is carried out by specialised entities called commercial acquirers.

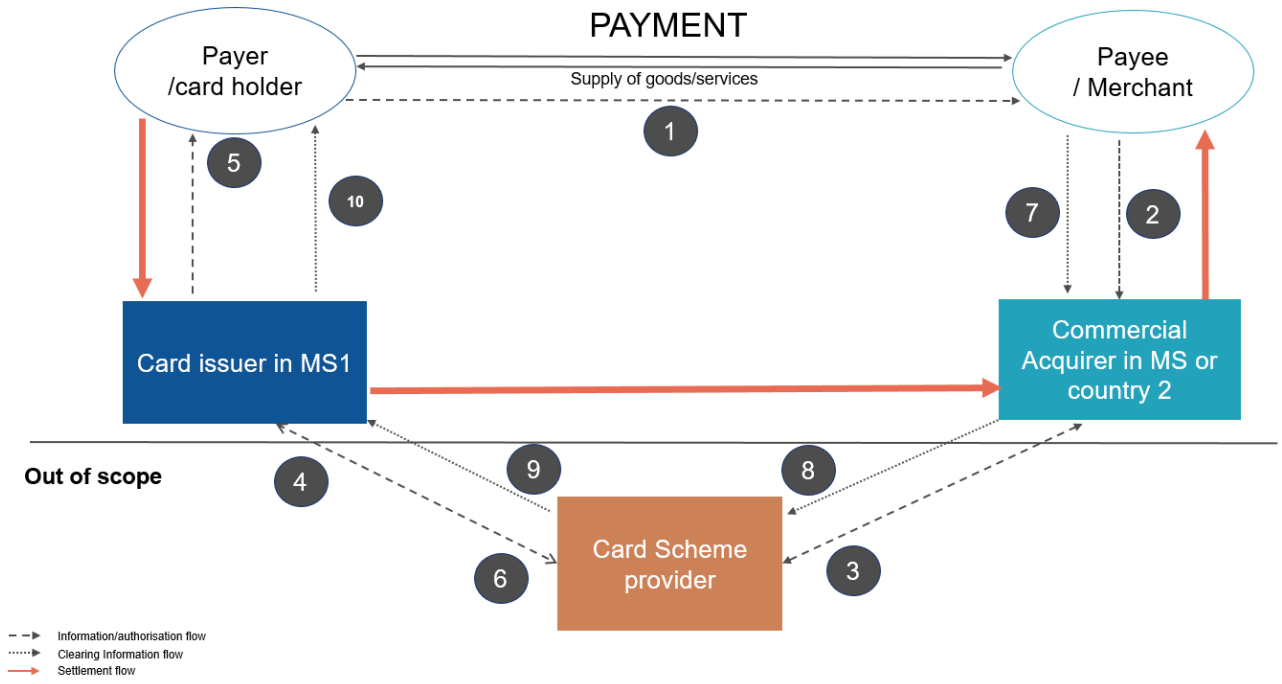
The processing of a card payment generally involves three main stages:

1. **Authorisation:** The authorisation process is there to enhance security, facilitate authentication, and for the issuer to confirm to the merchant that the card and proposed transaction is valid. The authorisation process is important for establishing liabilities between the issuer and the acquirer in accordance with card scheme rules. But not all card transactions need to be preceded by an online authorisation to the issuer. The authorisation can also take place between the card chip and the terminal (offline authorisation), common in e.g. contactless environments, mass-transit etc. And in some cases, a transaction is not authorised at all but sent for clearing anyway by the merchant or acquirer, at the merchant's own risk/liability.
2. **Clearing:** At the end of the business day the payee sends a batch file with the final transactions received in the payee's terminal/online webpage. The acquirer "re-packs" the information by card network and sends it together with received transactions from other merchant customers of the acquirer as large batch files to the respective card networks. The card network "re-packs" the

information and sends it to the different issuers of the cards, which receive daily batch files with all transactions received through a card network. The clearing is a serial flow, on which the three settlements are based.

3. **Settlement:** there are three settlements resulting from card-based transactions, which are all based on the clearing information but are separate and independent from each other, and can happen in any order of time:
    a. Settlement from the acquirer to the merchant
    b. Settlement from the issuer to the acquirer
    c. Settlement from the cardholder to the issuer (charging by the issuer of the cardholder's payment account)

Figure 6 – Functioning of a 4-party card payment



In the figure, the first steps represent the authorisation flow and the response from the card issuer:

1. The payer provides the details of its payment card in an online interface linked to the payee's website. This initiate the payment process.
2. Using the card information provided by the payer, the payee's terminal will transmit the information to the acquirer.
3. Using the information available on the card, the commercial acquirer will forward this information to the card scheme provider.
4. Always using the data transmitted, the card scheme provider will identify the card issuer and forward the authorisation message to it.
5. The card issuer will receive the authorisation request containing the card and transaction details. It will check that all elements are correct and that the payer has enough funds available.
6. The card issuer will send back a response message, positive or negative, to validate or negate the transaction. This response message will follow the same steps as the original request in reverse.

Once the transaction has been authorised (or send for clearing if there is no authorisation), the next steps will cover the clearing process:

7. The terminal of the payee will send, at the end of the business day a batch file with all payment transactions received by the payee during the day to the commercial acquirer.
8. This information is combined by the commercial acquirer for all payments done via a given card scheme. The commercial acquirer will then send these new batch files to the card scheme provider.
9. Using the information available in the batch file, the card scheme provider will split the file per card issuer and send the payment information relating to each card issuer.
10. Receiving this information, the issuer will split it for each card owner and inform them of their liability.

Finally, once the clearing is over the settlement phase will begin and happen at any order of time.

N.B.: Similarly to 3-party card payments, 4-party card payments often involve other payment services providers (such as banks) to fund the card's credit line or to receive the funds from the commercial acquirer. For these payment service providers the transactions will look as a payment to the card issuer (for the payer's payment service provider) or a transaction from the commercial acquirer to the payee (for the payee's payment service provider). These transactions, although different from the one between the payer and the payee, are in scope of the reporting obligation and should be reported with either the card issuer as the payee, or the commercial acquirer as the payer. Indeed, they do not fall within the exclusion of article 3 (m) PSD2 for transaction between payment service providers for their own activities, since they do not serve the activities of the payment service providers involved but are part of the agreement between the payer/payee and the card issuer/commercial acquirer.

2.2.5 Electronic money

Electronic money probably constitutes the most recent way of transferring funds between payment accounts. E-money offers many advantages compared to traditional payment methods such as speed of transaction, low fees and protection of financial data. The e-money sector is regulated under the Electronic money Directive ("EMD")[9] as well as the PSD2 since e-money institution are payment service providers.

Although the EMD establishes the basic rules applicable to the sector, each e-money provider has discretion to create its own system and its own way of processing payments. Because of that, there is little interaction between the different e-money providers and it is necessary for the payer and the payee to both subscribe to the same e-money provider services, in order to execute or receive payments via this e-money provider.

This lack of standardisation in the sector's functioning makes it impossible to cover all existing and future business models. However, despite this great variety of services provided, the e-money sector can be divided into two main business models: the e-wallet and the electronic voucher.

[9] Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC (Text with EEA relevance), (OJ L 267, 10.10.2009, p. 7)

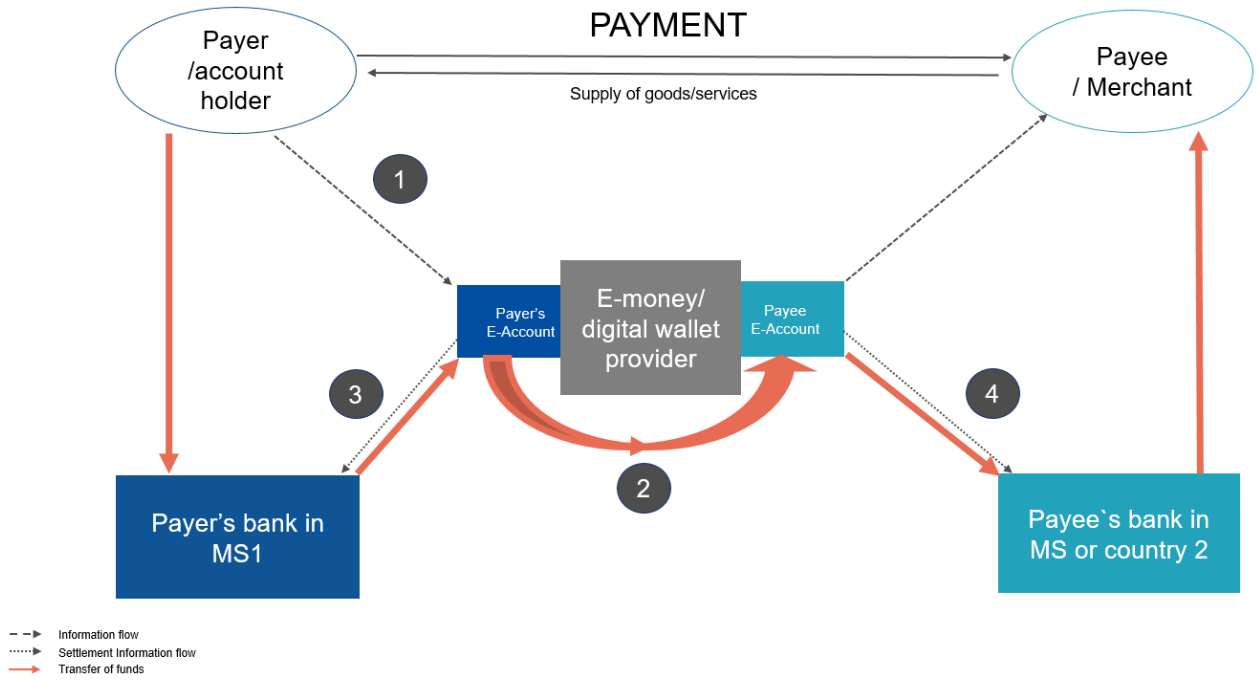
N.B.: Similarly to card payments and marketplaces, e-money payments generally involve other payment services providers (such as banks) to fund the e-money account or to withdraw funds from it. For these payment service providers the transactions will look as a payment to or from the e-money provider. These transactions, although different from the one between the payer and the payee, are in scope of the reporting obligation and should be reported with the e-money provider as either the payer or the payee. Indeed, they do not fall within the exclusion of article 3 (m) PSD2 for transaction between payment service providers for their own activities, since they do not serve the activities of the payment service providers involved but are part of the agreement between the payer/payee and the e-money provider.

2.2.5.1 E-wallet

In an E-wallet, the payment service providers offer a form of virtual wallet or e-wallet to the payer, which can be used to pay for goods or services. It is funded using a variety of payment methods such as card payments, credit transfers, exactly like a physical wallet would do with physical cards. Funds that are transferred to the e-wallet can be used to execute payments within the e-money provider's infrastructure. Funding the e-wallet can occur either in advance or simultaneously with the e-money transaction.

In addition to providing payment services to the payer, the e-wallet provider also offers payment services to the payee who also needs to be registered in the e-wallet provider's systems in order to receive payments via e-money. Because of that, the E-wallet provider has a direct relationship with both the payer and the payee and is thus the key actor in the reporting obligation. As already explained, although other payment service providers are also involved in e-money payment, they only act as funding sources for the e-wallet or as destination for the withdrawal of funds. They have no implication in the e-money payment between the payer and the payee which is managed solely by the e-money provider.

Figure 7 – Functioning of an e-wallet payment



In the figure, the information flow takes place as follows:

1. The payer will initiate the e-money transaction by providing its e-account details on the payee's webpage.
2. The e-wallet provider will receive the details of the transaction and confirm it is valid. If this is the case, the e-wallet provider will transfer the funds from the payer's e-account to the payee's e-account.

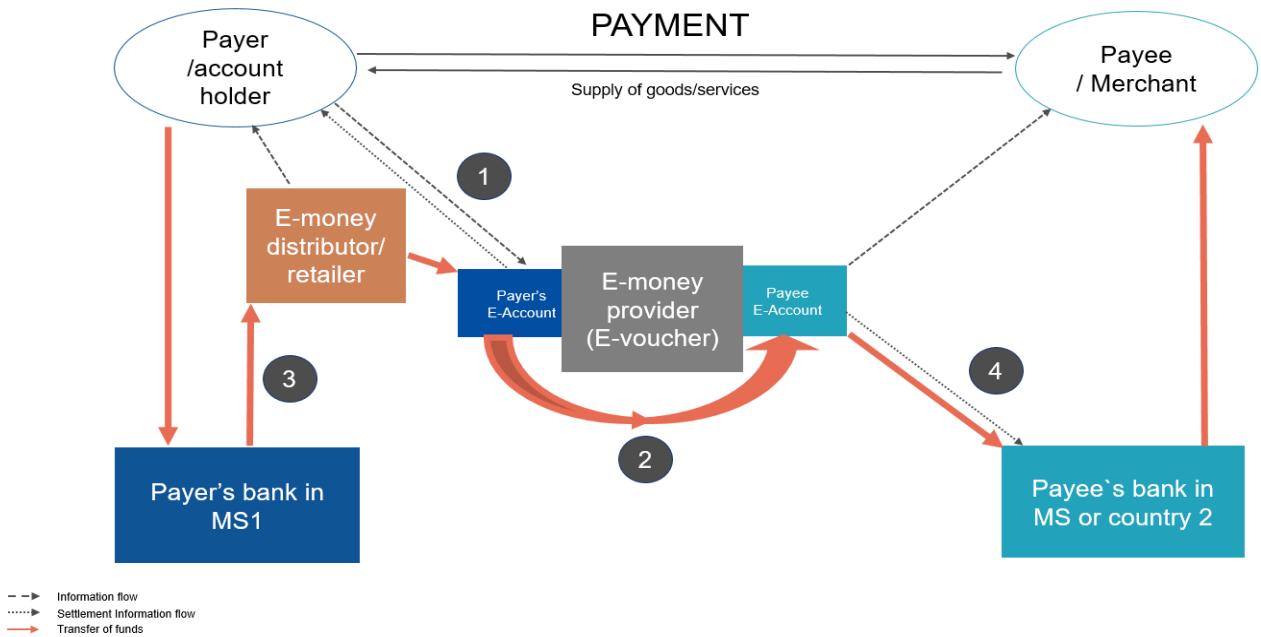
Once this is done, the transfer of funds within the e-money provider's systems is completed and no settlement is needed since the e-money provider is the only actor involved in the payment transaction. However, if the payer's e-money account was not funded, it is necessary for the e-money provider to request and settle these funds from the funding sources registered by the payer before executing the e-money payment:

3. The e-money provider will use the data provided by the payer when registering to request a transfer of funds from the payment service provider responsible for the payer's funding source (for example a credit transfer or a card payment). This will create a separate transaction between the payer and the e-wallet provider as the payee
4. Similarly, the payee can decide to withdraw the funds from its e-money account to its bank account or other payment account. As such, this will create another transaction where the e-wallet provider will be the payer and the merchant the payee. This separate transaction should be reported by the payment service provider of the payee (i.e. its bank).

2.2.5.2 E-voucher

Electronic vouchers differ from e-wallet as they do not create an e-wallet but focus on creating a single electronic form of payment, which often takes the form of pre-paid cards. These cards can be bought by the payer in selected distributors/retailers and allow the payer to execute payments via the e-money provider infrastructure without the need to include any financial information. As such in contrast to the E-wallet, E-vouchers providers do not have a direct relationship with the payer and do not require him to be registered in their systems to use the services. It is generally enough that the payer uses the e-voucher that he bought from the e-money provider's retailer. In the cases of e-vouchers, the e-money provider only has a direct relationship with the payee who still needs an e-account to receive payments.

Figure 8 – Functioning of an e-voucher payment



In the figure, the information flow takes place as follows:

1. The payer will initiate the e-money transaction by introducing the details of its e-voucher on the merchant's website.
2. The e-money provider will validate the information introduced by the payer and confirm the transaction. The e-money provider will then credit the payee's e-account with the amount of the transaction.

Once this is done, the transfer of funds within the e-money provider is completed and no settlement is needed since the e-money provider is the only actor involved in the payment transaction. However, a series of other operations generally occur outside the systems of the e-money provider:

3. The payer will buy an e-voucher from a selected distributor which has been authorised by the e-money provider to distribute its payment methods. The e-money provider is aware that a voucher has been sold at a given location. When purchasing the e-voucher, the payer will generally perform a payment transaction to pay the retailer for the e-voucher. Depending on the business model used, these funds will be transferred to the retailer or directly to the e-voucher provider. In both situations, there is a different transaction (occurring before the payer uses the e-voucher to pay for goods or services) where the retailer or the e-voucher provider will be the payee.
4. Similarly, as with e-wallets, the payee can decide to withdraw the funds from its e-money account. As such, this will create another transaction where the e-money provider will be the payer and the merchant the payee. This separate transaction should be reported by the payment service provider of the payee.

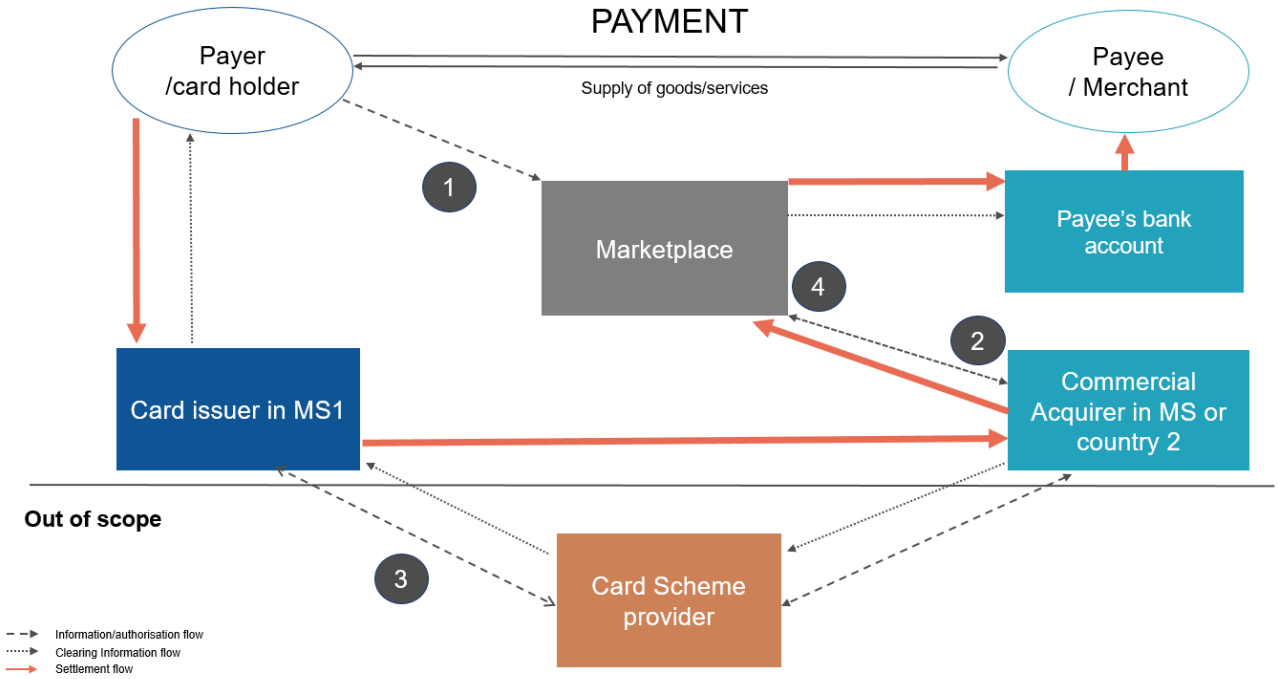
2.2.6 The case of marketplaces and intermediaries collecting funds in their own name

Although not a payment method in itself, the situation of marketplaces and intermediaries can change the way data is exchanged within a given payment. This is due to the fact that when they collect and keep funds in their own name before distributing them to the payee, these entities act as a payment service provider and must be registered as such. However, this also means that for the other party to the payment chain, they look like the payee as they hold the funds transferred in their name and will be reported as such.

For example, most marketplaces use a business model where the payments are first directed to the marketplace itself, who will keep these funds for a given period of time, before distributing them to the payee in a consolidated amount and after application of the marketplace fees. This way of proceeding is also used by some payment service providers who will have a single contract with the payee where they offer a variety of payment methods. The advantage for the payee is that it will not need to contract and register directly with all the providers of these various payment methods, but will be able to offer them to its clients via the services of the intermediary who has all the contracts. The consequence is that the intermediary will first consolidate all the transactions received from the various payment methods in dedicated accounts before distributing the aggregated sums to the merchants.

In both these cases, the presence of an intermediary in the payment chain that will shield the payee's or payer's information from all the other actors creates a discrepancy in the data exchanged, since the intermediary will appear as the payee for all the actors before it, and as the payer for all those after it.

Figure 9 – Functioning of a credit card via marketplace payment



To detail the functioning of a payment going through an intermediary, we will use the example of a card payment to a marketplace. In the figure, the information flow is highlighted by the blue numbers and takes place as follows:

1. The payer will provide its card details on the marketplace's website in order to initiate the payment.
2. The marketplace will transfer this information to the commercial acquirer which will use it to identify the issuer using the card scheme network.
3. The issuer will validate the transaction details and send the confirmation to the acquirer via the card scheme network.
4. The acquirer will validate the transaction for the marketplace.

The key difference from a standard card payment is that neither the acquirer nor the issuer receive any information on the merchant (the payee). Instead, they will both see a payment transaction going to the marketplace itself. This implies that the acquirer and issuer will not be able to report the final payee (the merchant) of the transaction.

Considering that the details of the payee are not available to them, the card issuer and the acquirer should thus report the marketplace as the payee. On the other hand, since the marketplace acts for both the payer and the payee and is in possession of all the data necessary to have a full view of the payment and its intended beneficiary (the merchant), it must identify the real payee (i.e. the merchant) when reporting the data.

2.3 The payment services in scope

In addition to specifying the four categories of payment service providers in scope presented in section 2.1., article 243a of Directive 2006/112/EC also limits the reporting obligation to the payment services laid down in points 3 to 6 of Annex I of the PSD2. This means that only payment service providers which provide the following payment services will be in scope of the reporting obligation:

- Executing payment transactions and transfers of funds on payment accounts
- Executing payment transactions covered by a credit line
- Issuing of payment instruments and acquiring of payment transactions
- Money remittance.

This means that payment service providers who provide services linked to operating a payment account, cash deposit and withdrawal, payment initiation services and account information service provision, are not in scope of the reporting obligation. The reason behind this exclusion is that these types of services either do not refer to the execution of payment transactions, or they would provide information that is already provided by the other payment service providers involved in payment transactions.

In addition, Article 3 of PSD2 sets out specific payment service exclusions which further restrict the scope of reporting. As such, the following payment methods do not fall within the scope of reporting:

- Paper based vouchers and payments in cash (article 3 (g));
- Cheques (article 3 (a));
- Payment methods with limited use (article 3 (k)).

2.3.1 Payment methods with limited use – vouchers

Payment methods with limited use must be understood as being valid to pay only a strictly limited (and often pre-established) number of merchants or pay for a limited range of goods and services. Article 3 (k) of the PSD2 defines such payment method as:

> *(k) services based on specific payment instruments that can be used only in a limited way, that meet one of the following conditions:*
>
> *(i) instruments allowing the holder to acquire goods or services only in the premises of the issuer or within a limited network of service providers under direct commercial agreement with a professional issuer;*
>
> *(ii) instruments which can be used only to acquire a very limited range of goods or services;*
>
> *(iii) instruments valid only in a single Member State provided at the request of an undertaking or a public sector entity and regulated by a national or regional public authority for specific social or tax purposes to acquire specific goods or services from suppliers having a commercial agreement with the issuer;*

Payment methods with limited use must not be confused with the use of an e-voucher. An e-voucher (see point 2.2.5.2.) is in scope of the reporting obligation as it is a valid (pre-paid) payment method that can be used to purchase goods potentially everywhere (as long as the merchant has contracted with the e-money provider to provide this type of payment). The key aspect to differentiate the two is the limited usage of the former, either regarding the places where it can be used (only at the premises of its issuer or in a single Member State), or what it can buy (limited range of goods or services). As such, it is

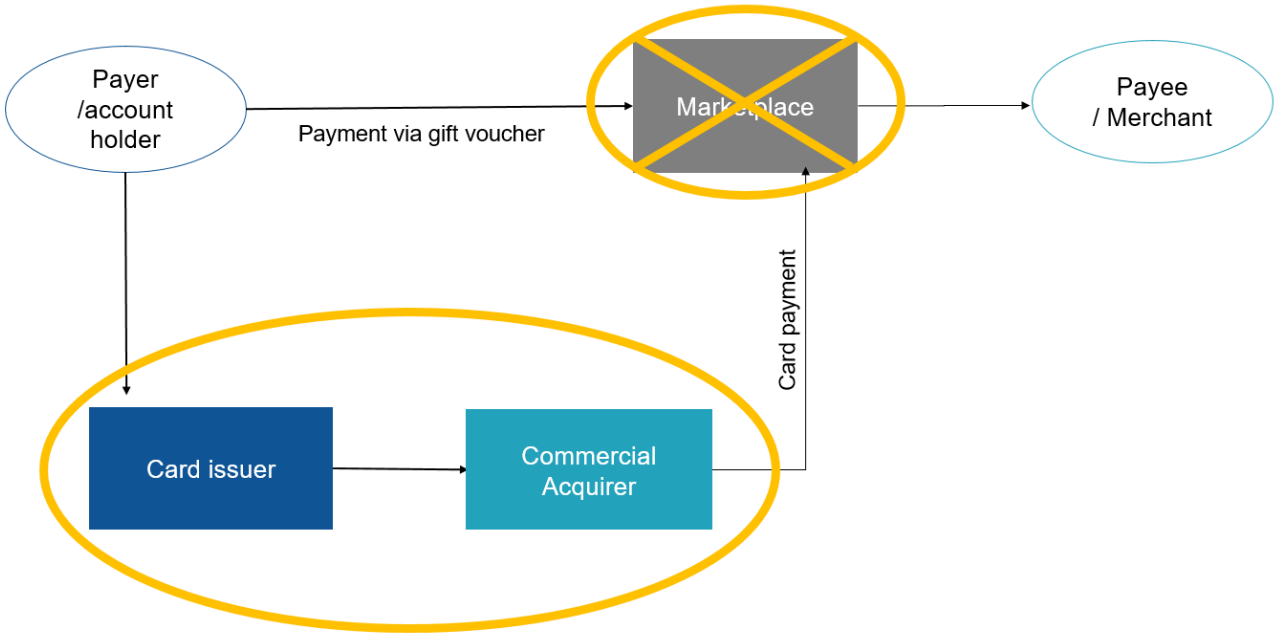
necessary to identify whether the payment method can potentially be used by any merchant to buy anything or is only limited to the different sellers or goods and services offered by a given brand, network, etc.

The fact that a payment method is only accepted by few merchants does not mean that it automatically falls within the category of payment methods with limited use. Indeed, the limited acceptance could be due to various reasons and increase over time leading to a more widespread adoption. For example, the same would apply with card payments where merchants will not necessarily accept all the card schemes in existence but only a number of them. A payment method with limited use however, will not generally see a huge increase of its acceptance since it will only be accepted at the premises of its issuer.

Among payment methods with limited use, the most common ones would be "gift vouchers" or "gift cards", which are bought for a given amount and then allow the holder of the card or voucher to buy the goods and services offered by the issuer of the card/voucher or its partners.

The figure below highlights how reporting will take place in a payment done via gift vouchers

Figure 10 – Reporting of payments via gift vouchers



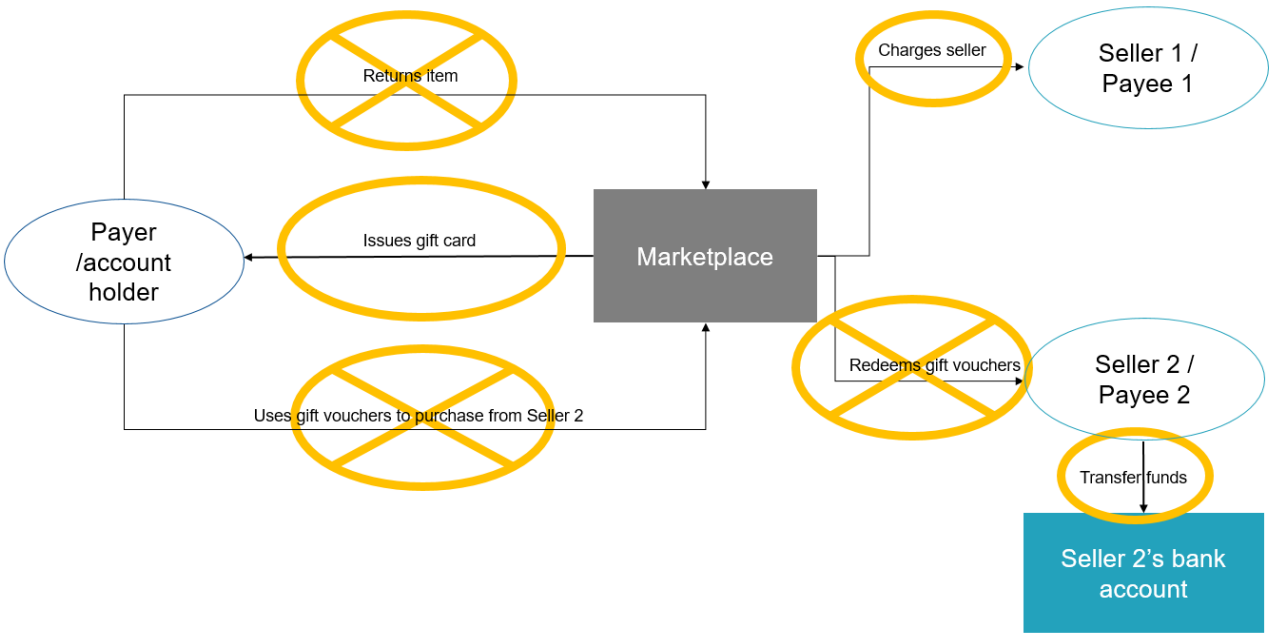
The figure clearly highlights that the marketplace will not report the payment from the payer to the payee made using the voucher. However, the payment made by the payer (or someone else) to buy the voucher together with the disbursement of funds from the marketplace to the payee bank account would be reported, as they are payments executed by payment services providers providing the payment services in scope of the reporting obligation.

2.3.2 Vouchers and refund

If the payer is not satisfied with the goods ordered and wishes to return them, it is not uncommon that marketplaces and businesses provide the payer with the option to receive a voucher rather than a refund. This practice offers advantages to the business who does not need to transfer funds back and also to the payer who is provided with an equally valid payment method to buy similar goods. These vouchers can also be offered as compensation if the goods are damaged, delayed or if any issue occurred during the delivery.

The figure below illustrates what happens in such situation for the reporting.

Figure 11 – Reporting of refunds and payments via gift vouchers



The first payment from the payer to the marketplace (using an in-scope payment method) is in scope of the reporting obligation and will be reported. In the case where a refund is requested by the payer, the marketplace will also report this refund.

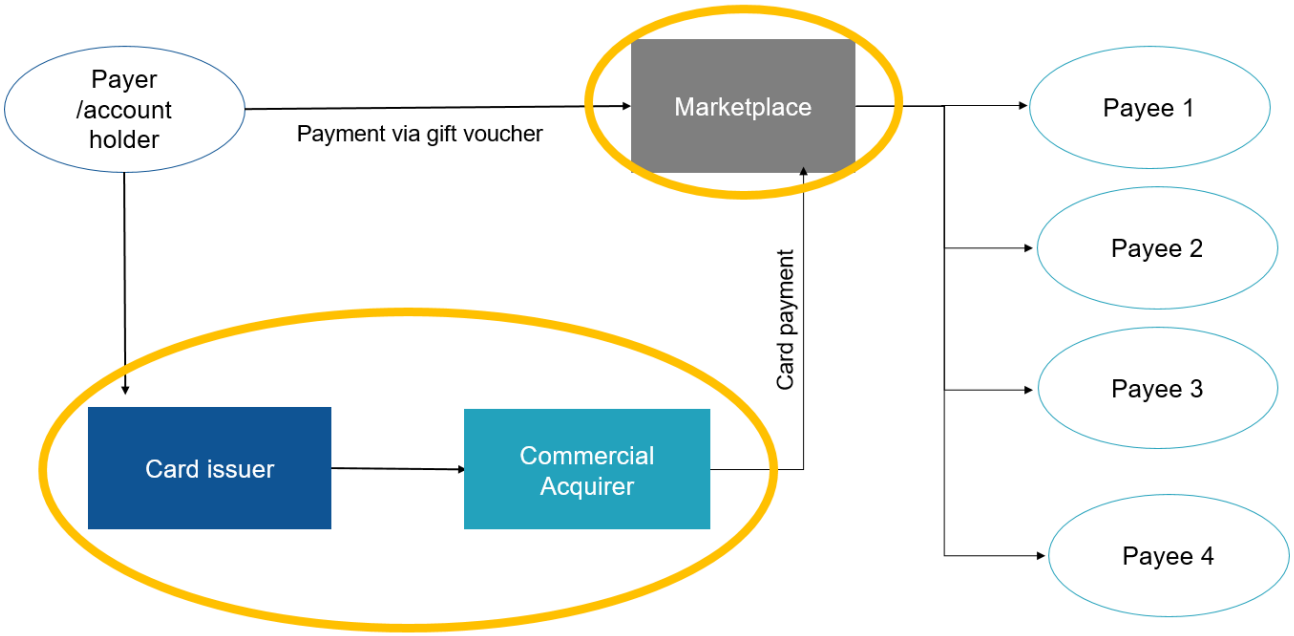
However, all the following payments performed via the gift voucher will not be subject to the reporting obligation. As highlighted in the figure, this can lead to situations where the payer buys goods from a first seller, which is reported to CESOP, but then ask for a refund via a gift card. Although the marketplace will report the refund, it will not report the issuance of the gift card to the payer and will not report the following transaction done by the payer who, using the gift card, now buys goods from another seller. However, once the marketplace proceeds to the disbursement of the funds it owes the second seller, this disbursement will be subject to a reporting from the second seller's bank which will report the consolidated amount.

As such, even though part of the transaction chain will not be visible due to the use of the gift card, CESOP will still receive information on how much funds were received by the first seller, how much was refunded on the first transaction, and will have information on the total amount received by the second seller due to the reporting by its payment service provider.

2.3.3 The use of vouchers together with in-scope payment methods

This final situation focuses on cases where the payer uses a gift card or voucher to buy goods or services, but the value of the voucher is insufficient to pay for the purchase in full and the balance must be paid by a regular transfer of funds done via in-scope payment methods.

Figure 12 – Reporting of payments via gift vouchers together with in-scope payment methods



In such a situation and if the rules were applied without considering the monitoring and the limitation of article 243b (2), the reporting should happen as follows:

- The payment service provider executing the in-scope payment (card payment, credit transfer, e-money, etc…) would report that payment with the marketplace as the payee;
- The marketplace would not report the part of the payment made via the voucher as it is out of scope, but would report the payment made using the in-scope payment method with the seller of the goods as the payee;
- The payment service provider of the payee (seller) would report the disbursement from the marketplace to the payee which would include an aggregation of all payments received over a given period of time.

Although this scheme could be applicable when the seller is a single entity, buying goods on a marketplace generally implies that a multitude of sellers may be involved in a single transaction, each one of them providing part of the items that constitute the payer's total purchase. As a consequence, marketplaces do not divide the various payments between vouchers and other payments, but rather group them all in one payment that mix vouchers and in-scope payment methods. Because of that, marketplaces are often unaware of which part of the amount they attribute to each seller is coming from the voucher and should be excluded.

As such, given the impossibility for marketplaces to split the value of a voucher between the different sellers when it is coupled with in-scope payment methods, and considering that exceptions should be interpreted restrictively, which would go contrary with the exclusion of the whole payment transaction, it is accepted that the marketplaces report the full payment transaction(s), including the amounts covered by a voucher, when they are not able to identify which exact part of the payment is coming from an out of scope payment transaction.

In practice, this implies that if the marketplace is not able, for each payment transaction to each payee, to determine which part of that payment is covered by a voucher, then the marketplace will report all payment transactions to each payee in full as if there was no voucher used.

2.4 Practical application per payment method

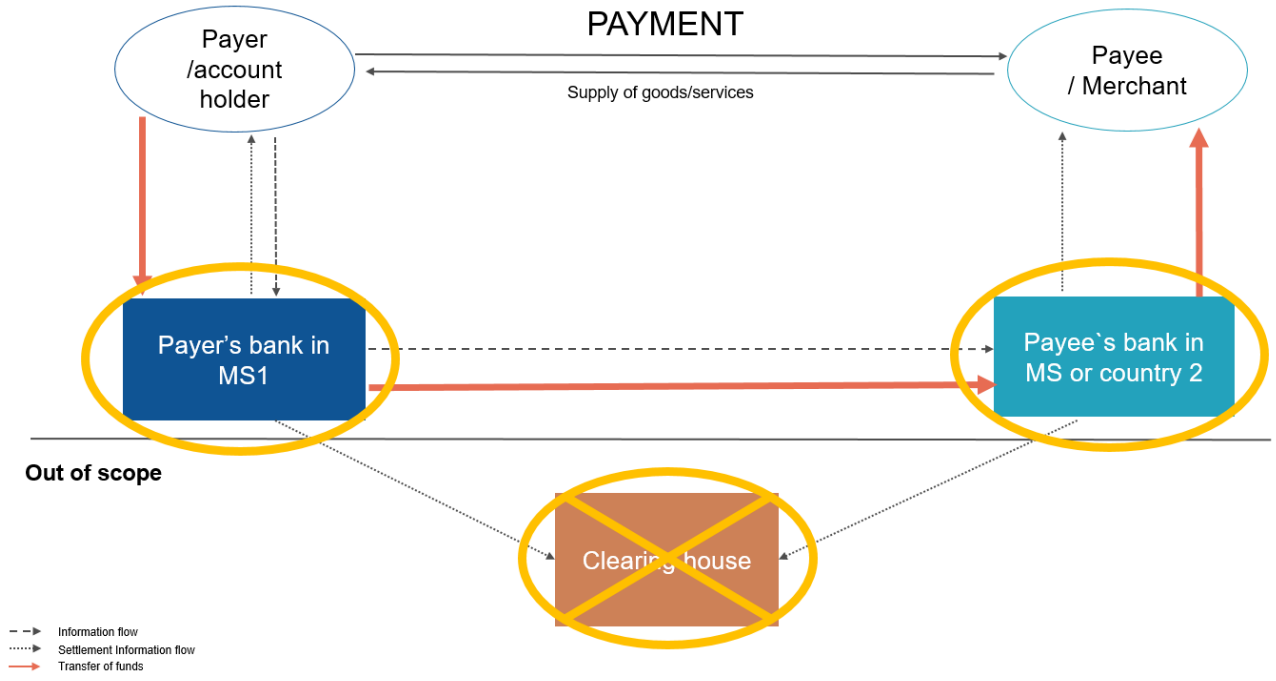
The following section will illustrate, for each of the main payment methods mentioned in section 2.2, who are the entities that must report data. The entity circled in red represents the one that will report the payment between the payer (buyer) and the payee (seller), while those circled in yellow represent payment service providers who will also report a payment as part of the overall payment chain, but which does not strictly refer to the payment between the buyer and the seller.

Each example only highlights the entities in scope but does not establish which one will effectively report the payment data in accordance with the rule of article 243b(3). For details on this, see section 4.3.

2.4.1 Credit transfer

For credit transfers, the payment service providers in scope of the reporting obligation are the bank of the payer and the bank of the payee. The clearing house or any other intermediary agent or payment service provider should not report any data as it is not a payment service provider providing payment services to the payer or payee.

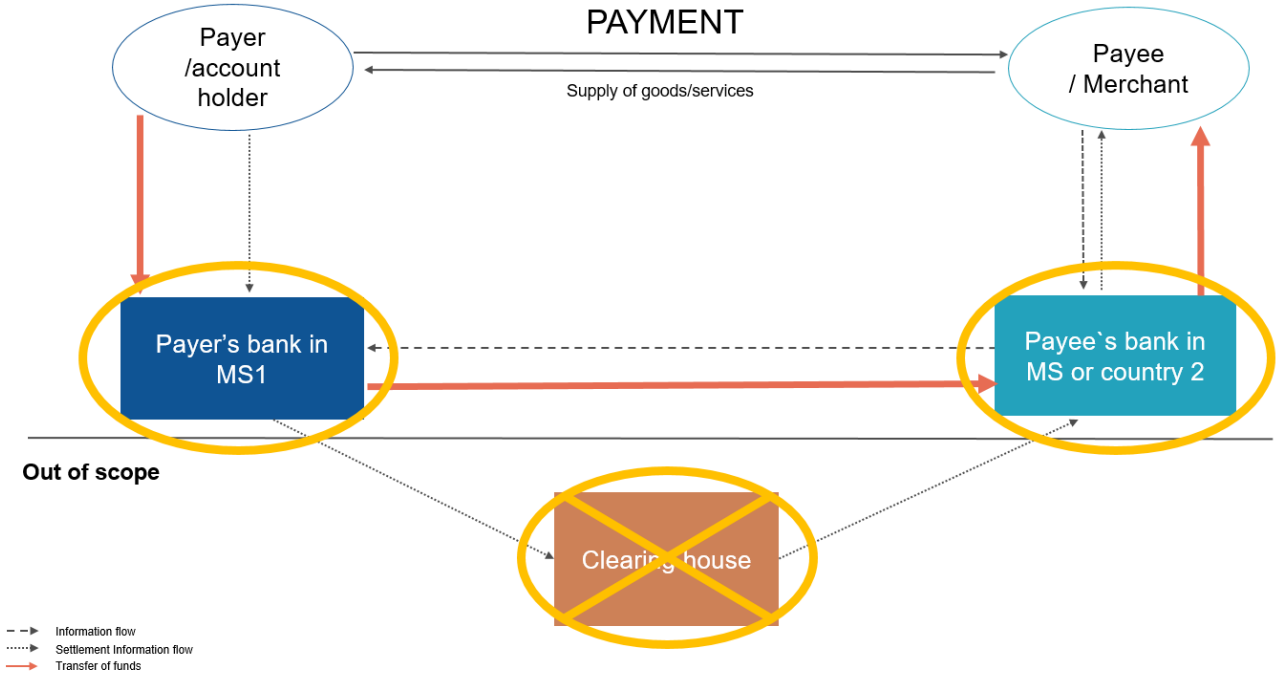
Figure 13 – In scope entities for credit transfers



2.4.2 Direct Debit

As they work in a similar way to credit transfer, the exact same rules apply to direct debits. The payer and the payee bank are thus in scope of the reporting obligation while the clearing house is not.

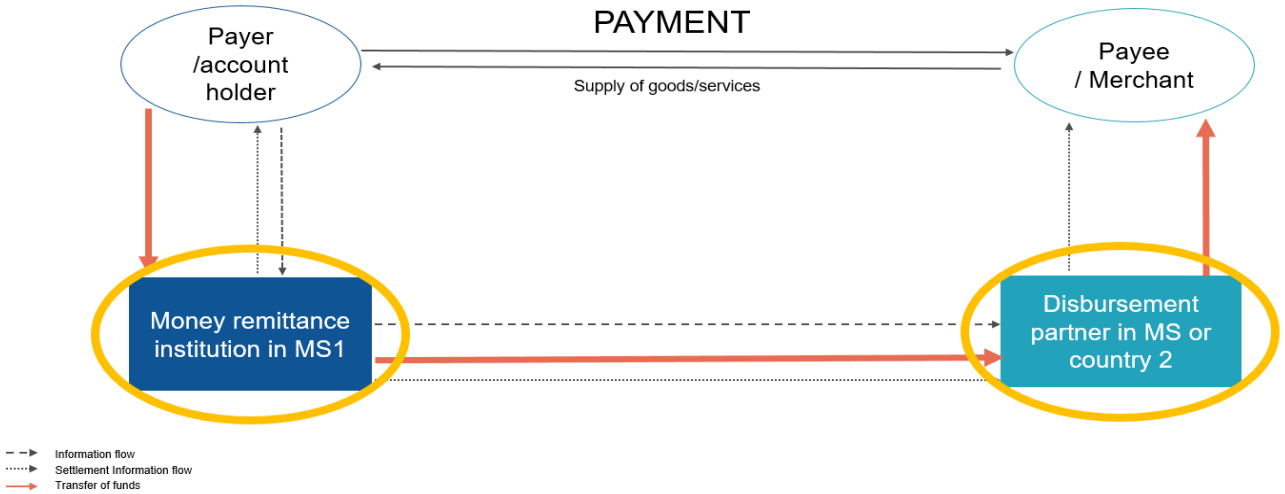
Figure 14 – In scope entities for direct debits



2.4.3 Money remittance

In money remittance payments, both the money remittance institution and the disbursement partner are payment service providers in scope of the reporting obligation.

Figure 15 – In scope entities for money remittances



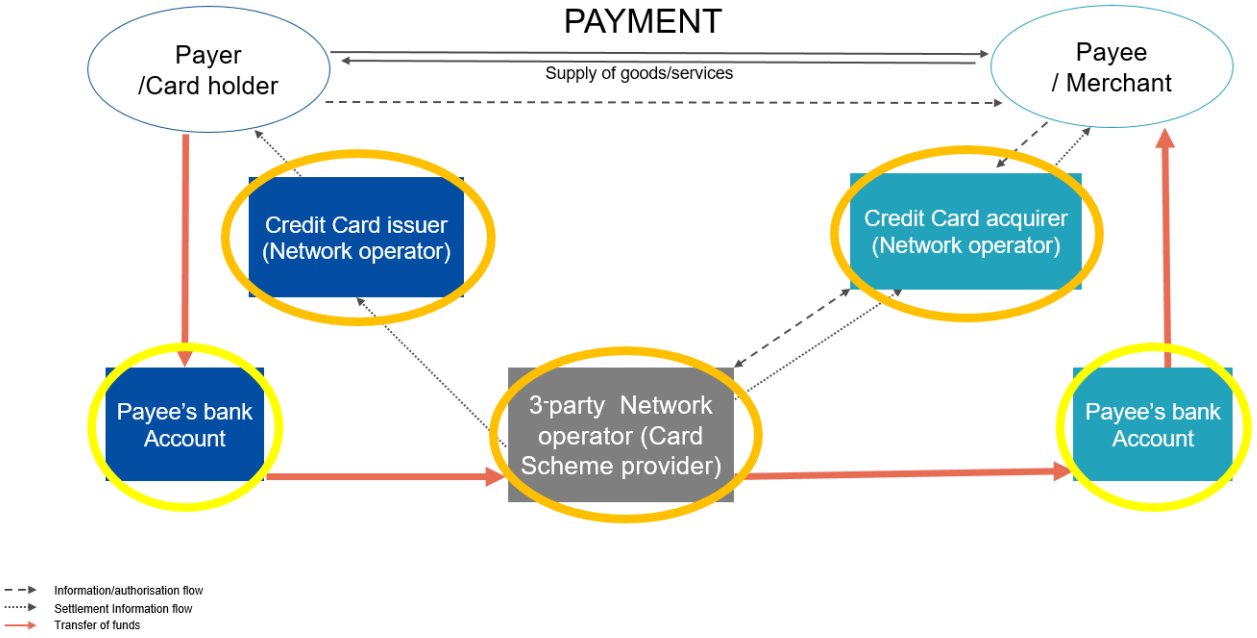
2.4.4 Card payments

2.4.4.1 3-party card scheme

As for all card payments, the credit card issuer and acquirer are the key entities for the reporting obligation and are in scope. For 3-party card schemes, since these functions are performed by the card scheme itself, the card scheme will also be a payment service provider and will be in scope of the reporting obligation.

When it comes to the payers' and payees' banks, they will be subject to a reporting obligation as highlighted by the graph. However, they will not report data on the payment from the payer to the payee but will report a different transaction, either from the payer to the card scheme provider to settle its card credit, or from the scheme provider to the payee to transfer the aggregated payments.

Figure 16 – In scope entities for 3-party card schemes

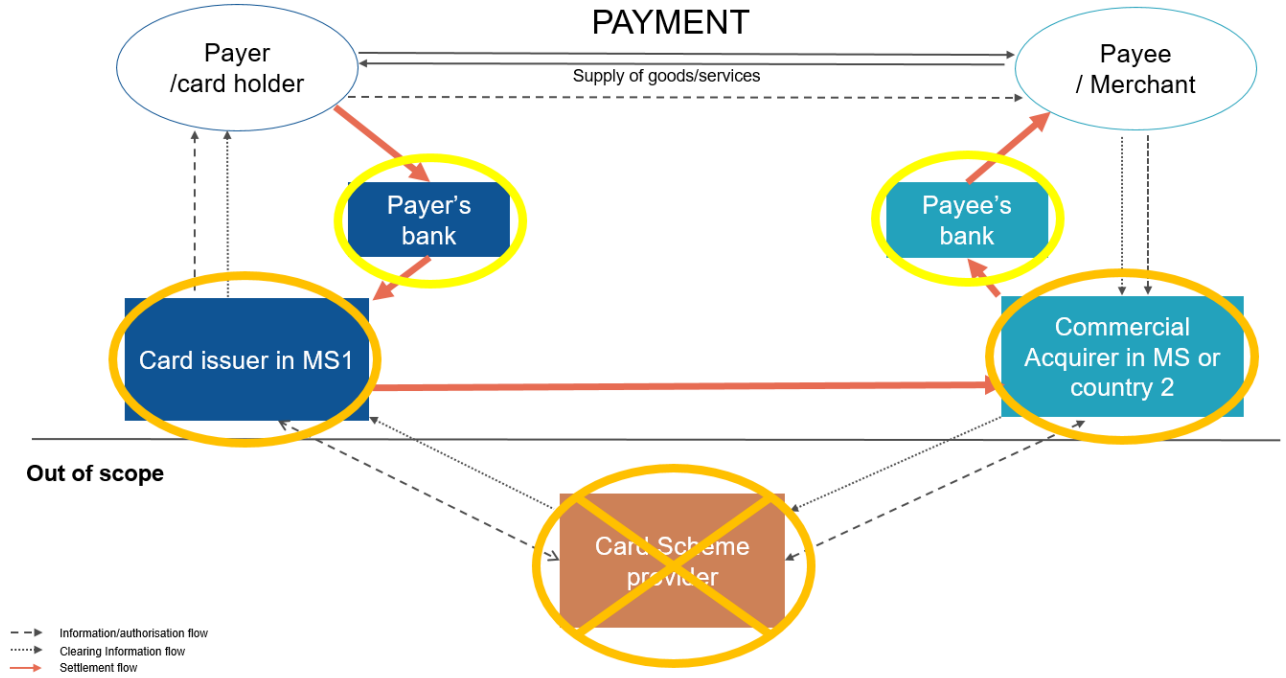


2.4.4.2 4-party card scheme

The example below uses the situation where both the credit card issuer and the commercial acquirer would differ from the payer's and payee's banks. In such case, the key reporting entities for the payment between the payer and the payee will be the card issuer and the acquirer who will have to report the data. The card network however is not a payment service provider and will not be subject to any reporting obligation.

Similarly, as with 3-party card schemes, the payer's and payee's banks will be subject to a reporting obligation as they are payment service providers. However, they will not report data on the payment between the payer and the payee but will report a different transaction, either from the payer to the card issuer to settle its card credit, or from the acquirer to the payee to transfer the aggregated amounts (settlement).

Figure 17 – In scope entities for 4-party card schemes



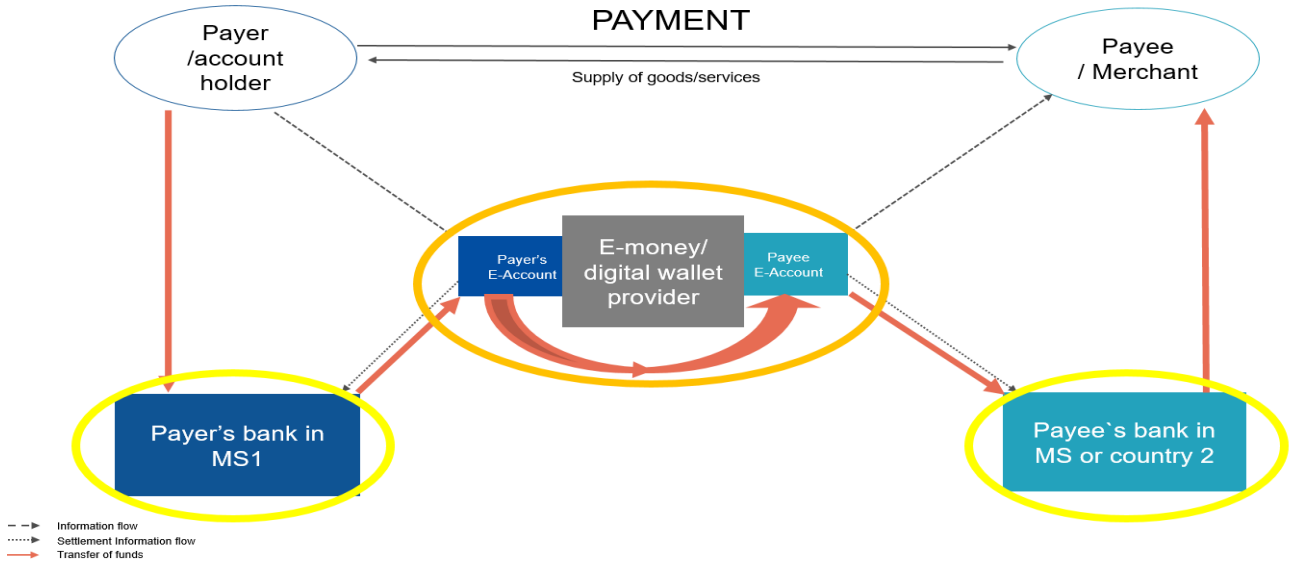
2.4.5 E-money

2.4.5.1 E-wallet

In the case of e-wallet, the e-money provider is the central reporting entity and the only one that has full visibility on the transaction between the payer and the payee. The e-money provider will thus be in scope of the reporting obligation and always report the data on the payment between the payer and the payee.

The situation of the payer's and payee's banks are similar to card payments. They are payment service providers in scope of the reporting obligation, however, they are not involved in the transaction between the payer and the payee. Instead, they will report a payment from the payer to the e-money provider for the payer's bank, and from the e-money provider to the payee for the payee's bank.

Figure 18 – In scope entities for e-wallet

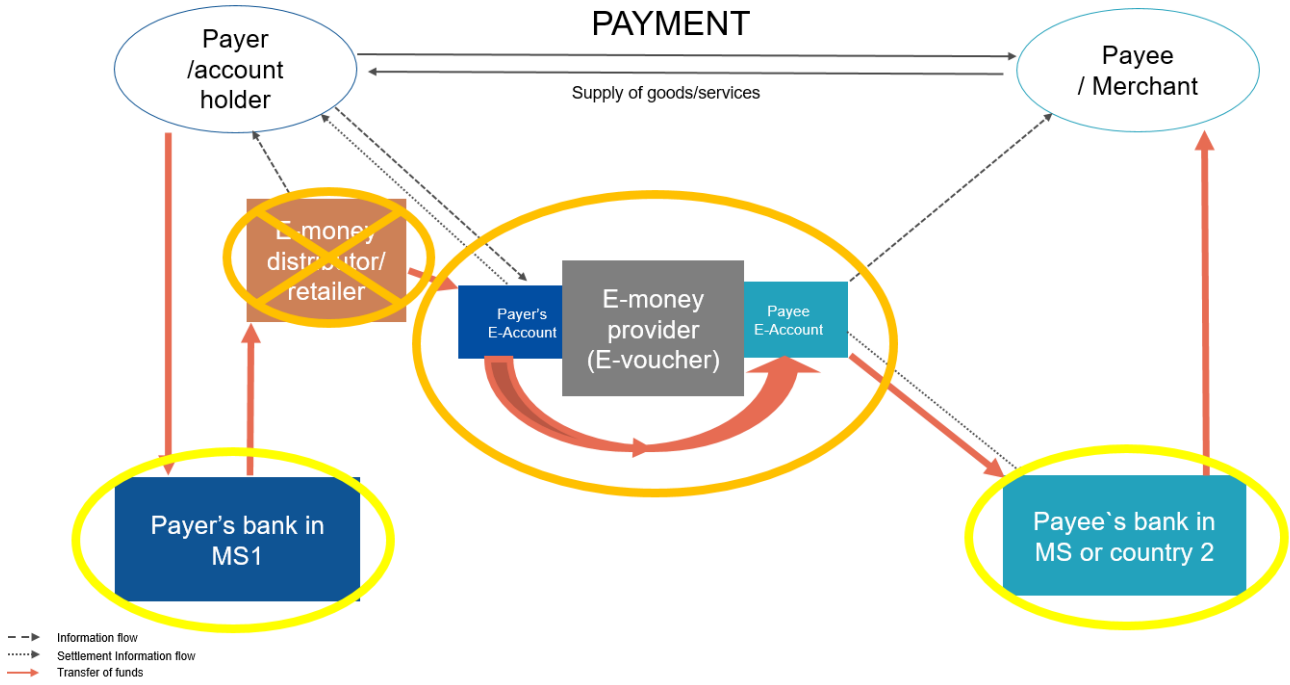


2.4.5.2 E-voucher

The situation of e-vouchers is similar to the e-wallet when it comes to the central role of the e-money provider for the reporting, therefore the e-money provider will be in scope of the reporting obligation. The difference lies in the presence of the distributor/retailer of the e-voucher, which is not a payment service provider and as such will not have any reporting obligation.

The situation of the payer's and payee's banks is identical to the one described for the e-wallet.

Figure 19 – In scope entities for e-vouchers



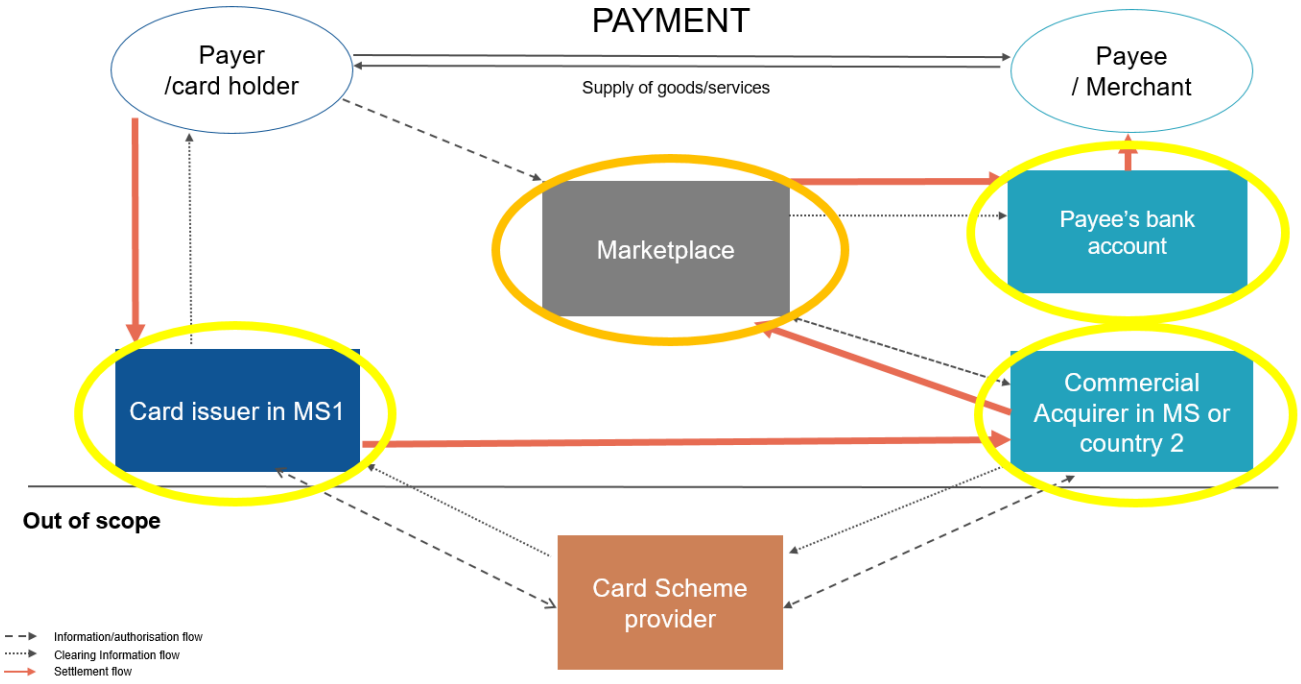
2.4.6 Marketplace

The example below takes the situation of a payment made on a marketplace using a 4-party card payment. The conclusions are however perfectly applicable to credit transfers or other means of payment.

In the situation of the marketplace, the marketplace itself is a payment service provider according to the rules of the PSD2 if it holds funds on behalf of both the payer and the payee. As such, in the case of a card payment to a marketplace, the regular actors of card payments will be in scope (and the card network will not), but the marketplace will also be in scope of the reporting obligation. This involvement of the marketplace is key to the reporting since the marketplace is the only entity with the full visibility on the payment between the payer and the payee. Both the issuer and acquirer can only report a payment going through the marketplace as it collects the funds in its own name. Only the marketplace can report the information about the real beneficiary of these funds.

The situation of the payee's bank on the graph is the same as for regular card payments. The payee's bank is not involved in the transaction between the payer and the payee and will only report the disbursement amount from the marketplace to the payee.

Figure 20 – In scope entities for marketplaces



3 MONITORING AND TRIGGERING OF THE REPORTING OBLIGATION

Once the conditions of article 243b, as detailed under point 2, are fulfilled, a payment will be in scope of the reporting obligation. However, it will not be reported unless two additional conditions are met. This will be determined by a monitoring test performed by the payment service providers.

These two additional conditions are that:

- The payment reported must be a cross-border payment (point 3.1) and
- The payment service provider providing payment services in a Member State must execute at least 25 cross-border payments in that Member State per quarter to a single payee in order to trigger the reporting obligation (point 3.2).

It is important to clearly detach monitoring rules from the data to be reported under article 243d. The monitoring rules ensure the proportionality of the reporting obligation for subsidiarity and data protection purposes. Their objective differs from the reporting obligation which purpose is to help the fight against VAT fraud. As such, the monitoring rules rely on proxies so that they can be easily applied by all payment service providers. They should however not influence the data to be transmitted which needs to be as precise as possible in order to be effective.

In particular, location rules must not impact the location transmitted as the address of the payee. It is perfectly acceptable that the address transmitted does not correspond to the location of the payee determined via the rules of article 243c (see point 3.1 for more details).

Similarly, the threshold aggregation must be distinguished from the actual reporting of data which must be done using transactional data and not payee identification data. This means that payment service providers must not merge the data relating to two payment accounts when reporting a payment even if they have identified that the accounts are owned by a single payee (see point 3.2 for more details).

Information relating to monitoring rules is to be used exclusively by the payment service providers in order to help them identify when a payment should be reported. This information is not part of the data elements required under article 243d and must not be automatically reported to Member States.

3.1 Cross-border payments - Location rules of article 243c

The first condition that payment service providers must monitor in order to determine whether a payment should be reported is whether this payment is a cross-border payment pursuant to the rules of article 243c of Directive 2006/112/EC.

1. For the application of the second subparagraph of Article 243b(1) and without prejudice to the provisions of Title V, the location of the payer shall be considered to be in the Member State corresponding to:

(a) the IBAN of the payer's payment account or any other identifier which unambiguously identifies, and gives the location of, the payer, or in the absence of such identifiers,

(b) the BIC or any other business identifier code that unambiguously identifies, and gives the location of, the payment service provider acting on behalf of the payer.

2. For the application of the second subparagraph of Article 243b(1), the location of the payee shall be considered to be in the Member State, third territory or third country corresponding to:

(a)the IBAN of the payee's payment account or any other identifier which unambiguously identifies, and gives the location of, the payee, or in the absence of such identifiers,

(b)the BIC or any other business identifier code that unambiguously identifies, and gives the location of, the payment service provider acting on behalf of the payee.

Only data on cross-border payments should be transmitted to Member States and to CESOP. No data on national payments should be collected in accordance with the rules of the Directive.

3.1.1 Table of identifiers to determine the location of the payer and payee

Article 243c lays down the rules applicable to determine when a payment shall be considered as cross-border. These rules rely on proxies in order to assign a country easily and quickly to the payer and the payee. The fact that the location of the payer and the payee based on these proxies could differ from their real location does not matter for the purpose of article 243c.

The table below lists the identifiers or data elements from which the location of the payer and the payee should be retrieved by payment service providers for the main payment methods in use. The table is however indicative and other elements could be used if deemed more relevant.

Table I – Location identifiers per payment methods and reporting entity

Payment Method	Payer's PSP reporting (Extra-EU)		Payee's PSP reporting (Intra-EU)	
	Payer Location	**Payee Location**	**Payer Location**	**Payee Location**
Credit transfer	- IBAN - (BIC of the PSP)	- IBAN - BIC of the PSP[10] - Payment account number[11]	- IBAN - (BIC of the PSP)	- IBAN - (BIC of the PSP)
Direct Debit[12]	- IBAN - (BIC of the PSP)	- IBAN - BIC of the PSP - Payment account number	- IBAN - (BIC of the PSP)	- IBAN - (BIC of the PSP)
Card payments	- BIN	- Merchant address - Card Acceptor location	- BIN	- Merchant address
E-money	- Payer e-account (location captured at onboarding) - IBAN - E-vouchers: seller country code	- Payee e-account (location captured at onboarding) - IBAN	- Payer e-account (location captured at onboarding) - IBAN - E-vouchers: seller country code	- Payee e-account (location captured at onboarding) - IBAN
Money remittance	- Payer Location (own records) - IBAN	- BIC of the disbursement partner	- BIC of the disbursement partner	- Payee location (own records)

[10] To be used when no IBAN is available

[11] This identifier does not necessiraly contain a country code, and will often be linked to the BIC of the payment service provider.

[12] There is currently no international scheme applicable to direct debit. As such, the identifiers listed here for the payer's payment service provider reporting are mainly theorethical.

It is important to note that although article 243c requires payment service providers to primarily use identifiers linked to the location of the payer and payee, some of these identifiers will ultimately be linked to the location of the payment service providers (e.g. IBAN). This can impact the reporting obligation (see point 3.1.2.).

Contrary to the rule laid down in article 243d (1) (d), there is no order of preference when it comes to the identifier to use (apart from the obligation to use the identifier of the payer/payee first). This implies that if a payment service provider has different identifiers available that provide a different location, it must chose the identifier that best reflects the location of the payee.

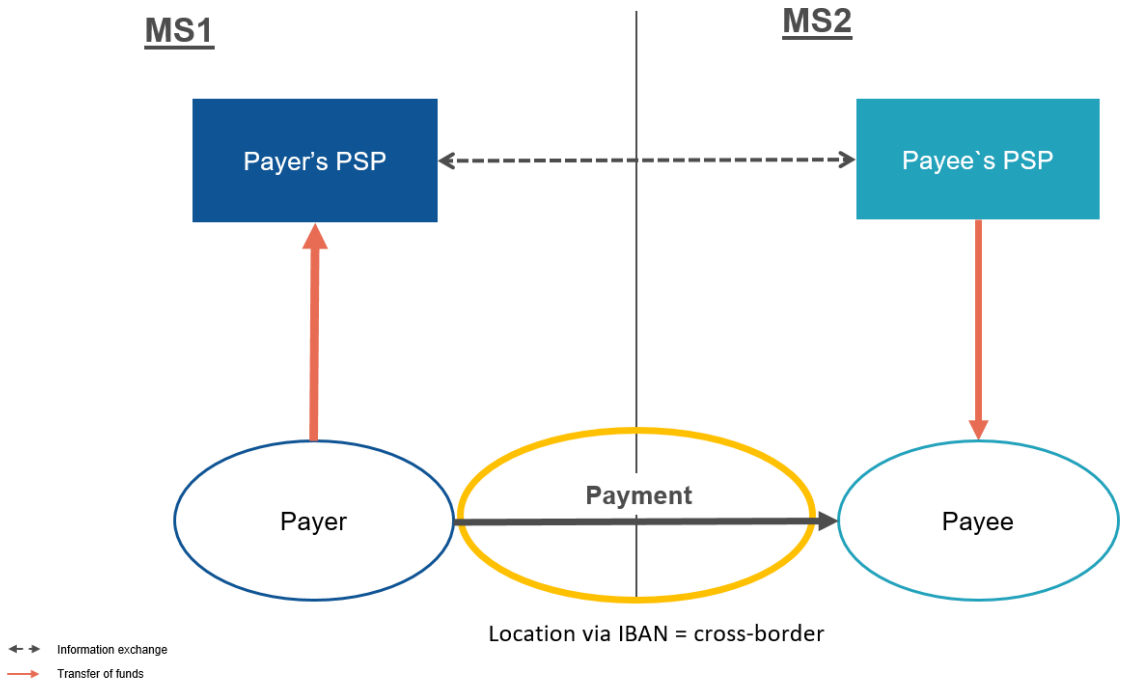
Example: if an e-money provider has an IBAN with a country code that differs from the one of the address provided by its client during onboarding and which has been confirmed by official documents (ID cards, passport, driving license, etc.), it must chose the location provided by the client as it better reflect the location of its client.

Example 2: the BIN range of a credit card can be used to identify where the issuer of the card is located or where the card has been issued. In application of the above rules, payment service provider must use the BIN range that indicates where the card has been issued as it is the one that best reflect the location of the payer.

3.1.2 Practical application

3.1.2.1 Credit Transfer/Direct Debit – Payer, payee and payment service providers in different Member States

Figure 21 – identification of cross-border credit transfers with payer and payee and their payment service providers in different Member States

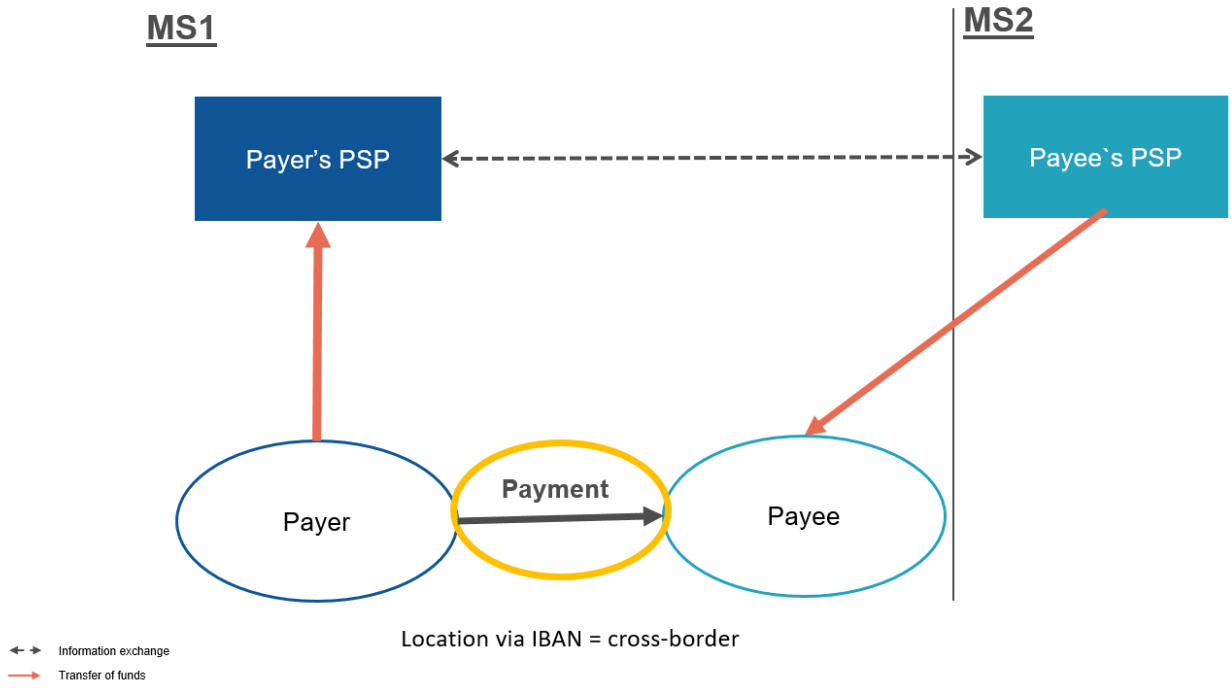


In the situation above, the payer and payee are in two different Member States and use payment service providers established in their Member States to execute a credit transfer/direct debit.

Following the rules of article 243c, the most relevant identifier for these payment methods will be the IBAN of the payer's and payee's payment accounts. Since both IBAN will refer to two different Member States, the payment will be considered as cross-border.

3.1.2.2 Credit Transfer/Direct Debit – Payer and payee in the same Member States

Figure 22 – identification of cross-border credit transfers with payer and payee in the same Member States but their payment service providers in different Member States



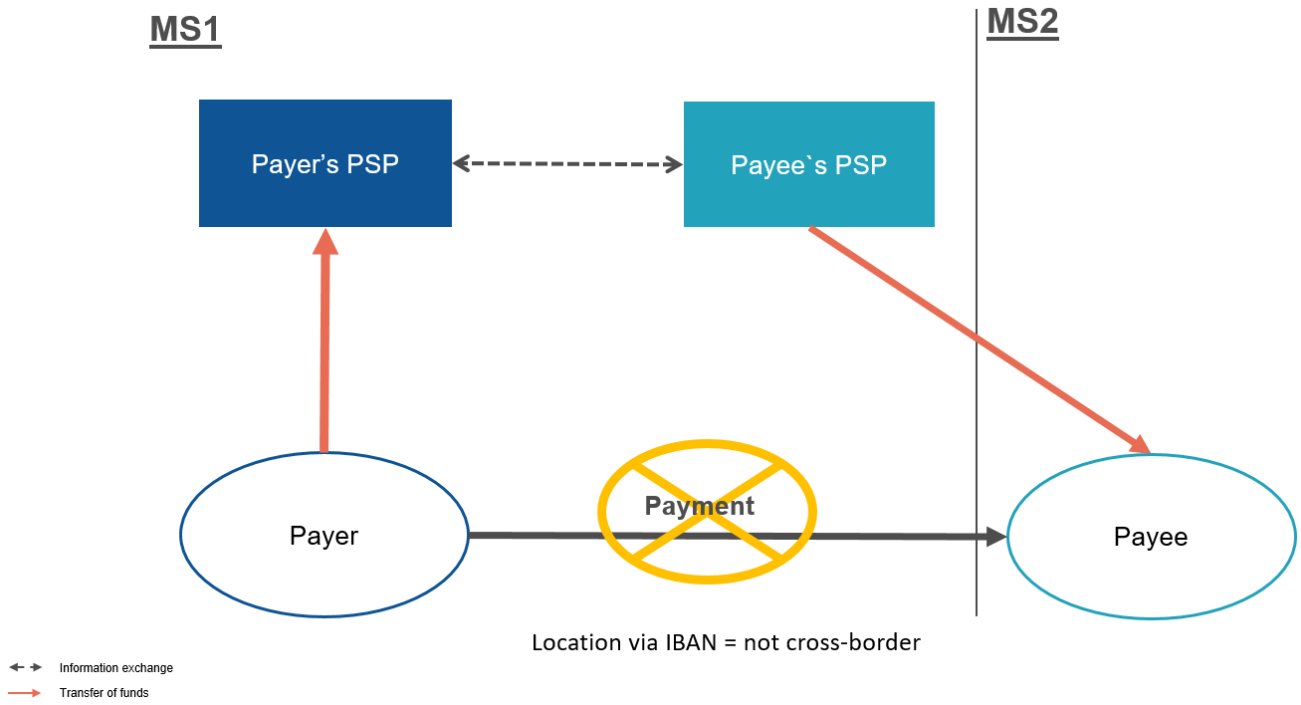
In this situation the payer and the payee are located in the same Member State but the payee uses the services of a payment service provider from another Member State.

Since the IBAN of the payee's payment account will be linked to the location of its payment service provider and not to the location of the payee itself, the payment between the payer and the payee will still be considered as a cross-border payment and will have to be reported to CESOP.

N.B.: In the theoretical case where the payee uses a non-EU payment service provider, this payment would appear as an extra-EU cross-border payment. In this situation, the payer's payment service provider would be liable to do the reporting. This case is however unlikely in practice due to the PSD2 requirements for payment service providers to have a payment license in the EU, and would only occur for EEA countries (see section 4.3.2.).

3.1.2.3 Credit Transfer/ Direct Debit – Payer and payee's payment service providers in same Member State

Figure 23 – identification of cross-border credit transfers with payer and payee in different Member States but their payment service providers in the same

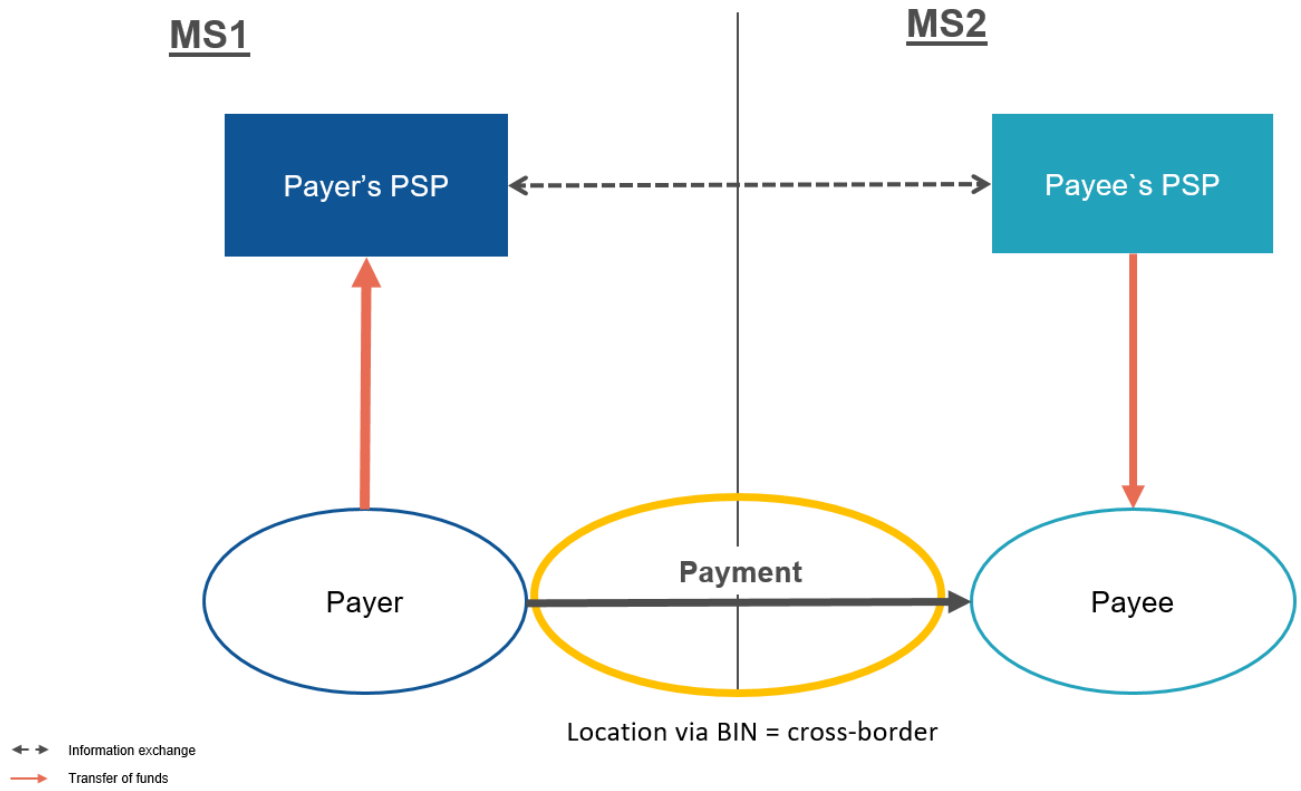


In this situation, the payer and the payee are located in different Member States but the payee uses the services of a payment service provider located in the same Member State as the payer.

Since the IBAN of the payee's payment account will be located where its payment service provider is, the payment between the payer and the payee will appear as a national payment since both payment service providers are located in the same Member State. As such, it will not be reported to CESOP. The fact that the payer and payee are located in two Member States is irrelevant according to the rules of article 243c.

3.1.2.4 Card payment – Payer, payee and payment service providers in different Member States

Figure 24 – identification of cross-border card payments with payer and payee and their payment service providers in different Member States

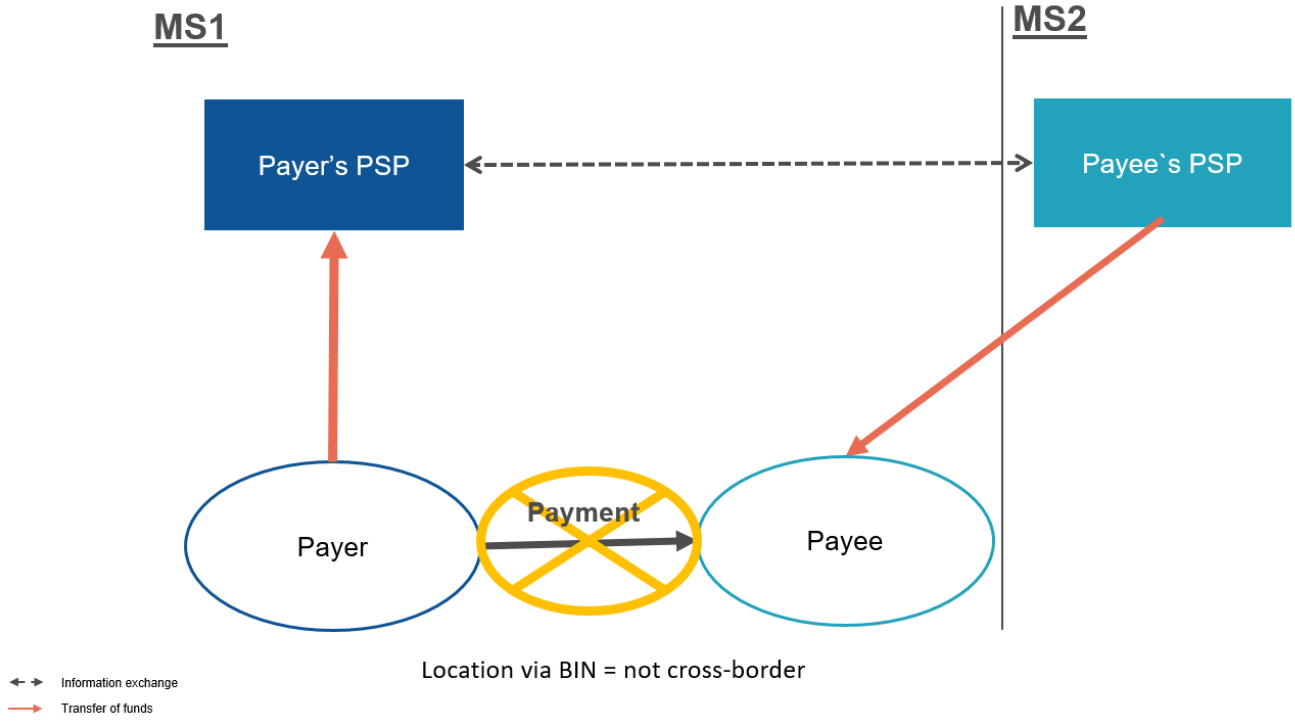


In this situation the payer and the payee are both located in different Member States and use the services of payment service providers from their respective Member States to execute a card payment.

For card payments, the most relevant identifiers to use would be the BIN range of the payer's card for the payer's location, and the address or identifier of the merchant for the payee's location. Both these identifiers will locate the payer and the payee in different Member States. The payment is thus cross-border and subject to reporting.

3.1.2.5 Card payment – Payer, payee in same Member State

Figure 25 – identification of cross-border card payments with payer and payee in same Member State and their payment service providers in different Member States

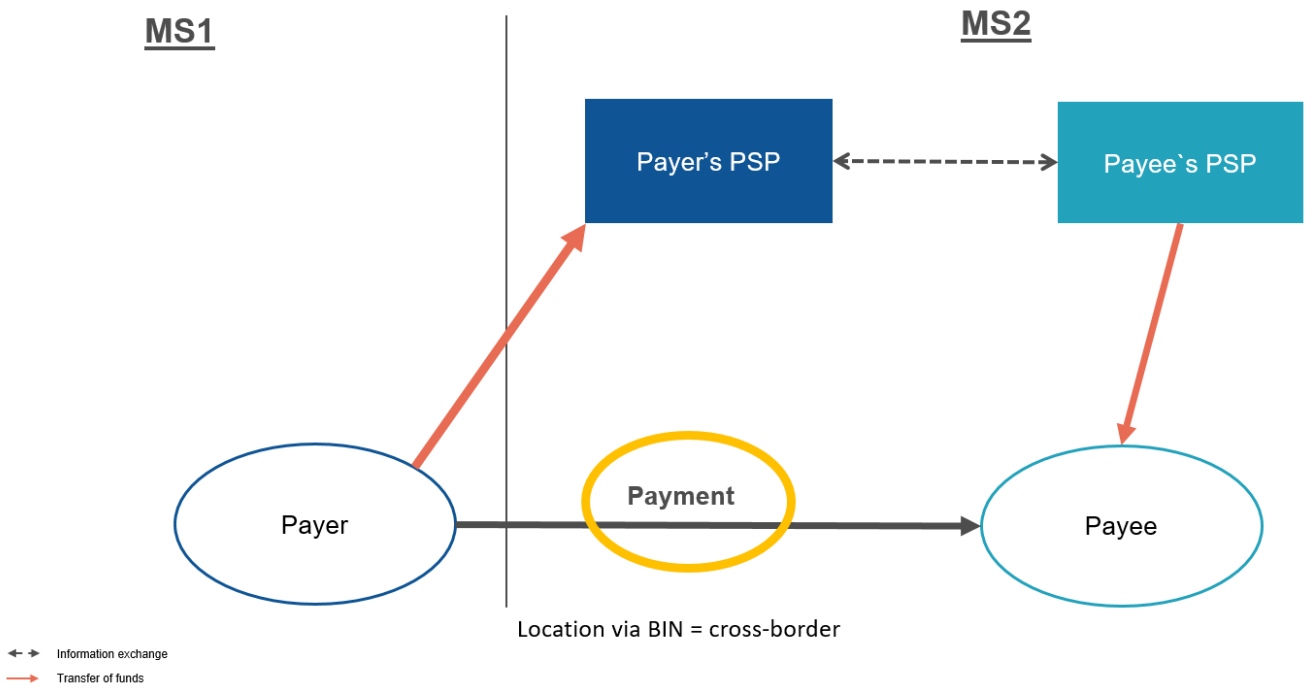


In this situation the payer and the payee are both located in the same Member State but the payee uses the services of a payment service provider in another Member State to execute a card payment.

Given that both the BIN range and the merchant identifier or address will refer to the actual position of respectively the payer and the payee, the payment will be considered as a national payment and will not be reported.

3.1.2.6 Card payment - Issuer and Payer in different Member States

Figure 26 – identification of cross-border card payments with payer and payee in different Member States but their payment service providers in the same



In this situation the payer and the payee are located in different Member States while both the payer and the payee's payment service providers are located in the same Member State. The payer uses the services of a card issuer in the Member State of the payee to execute a card payment.

For such cases, the BIN range must use the data on where the card has been issued and not the data on where the card issuer is located. As such, the BIN range should indicate that the payer is located in a different Member State to the payee and the payment should be considered as cross-border and be reported.

3.1.2.7 E-Money/marketplace – Payer and Payee in different Member States

In this case, the payer and the payee are using the service of an e-money institution or marketplace to execute the payment. In both cases, the payment service provider will have a relationship with both the payee and payer.

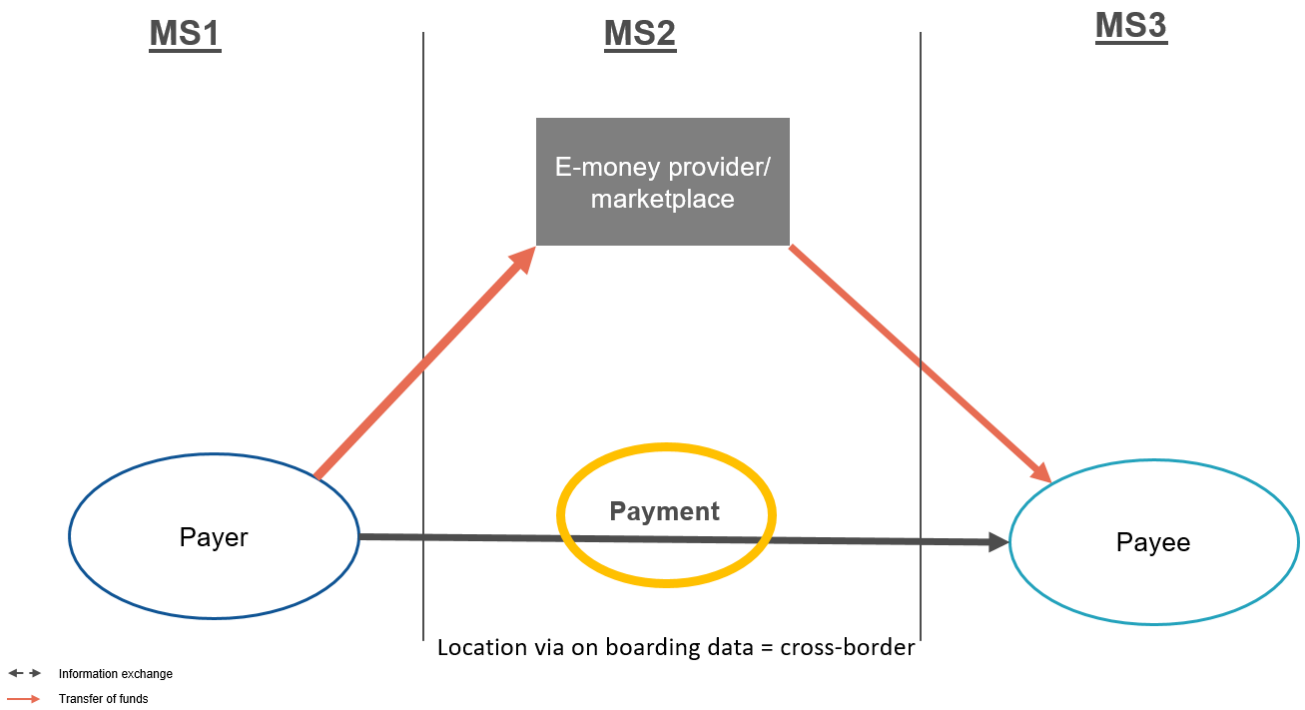
E-money institutions and marketplaces can have a multitude of identifiers and data to locate the payer and payee (IBAN, card BIN, own identifier and address taken during registration). They are free to choose the identifier that can best locate the payer and payee. In many cases, this identifier might well be their own identifier which can use a variety of information collected during the account creation to effectively locate the payer and the payee.

Using this identifier, the e-money provider/marketplace will be able to locate the payer and payee in two different Member States and determine that the payment is cross-border and should be reported.

N.B.: Even though from an external perspective, all payments made through e-money providers or marketplaces will appear to be located at the e-money provider's/marketplace's establishment, both

entities have the information available to determine the actual location of the payer and payee and must use this information to differentiate cross-border payments from national payments.

Figure 27 – identification of cross-border e-money/marketplaces payments with payer and payee in different Member States

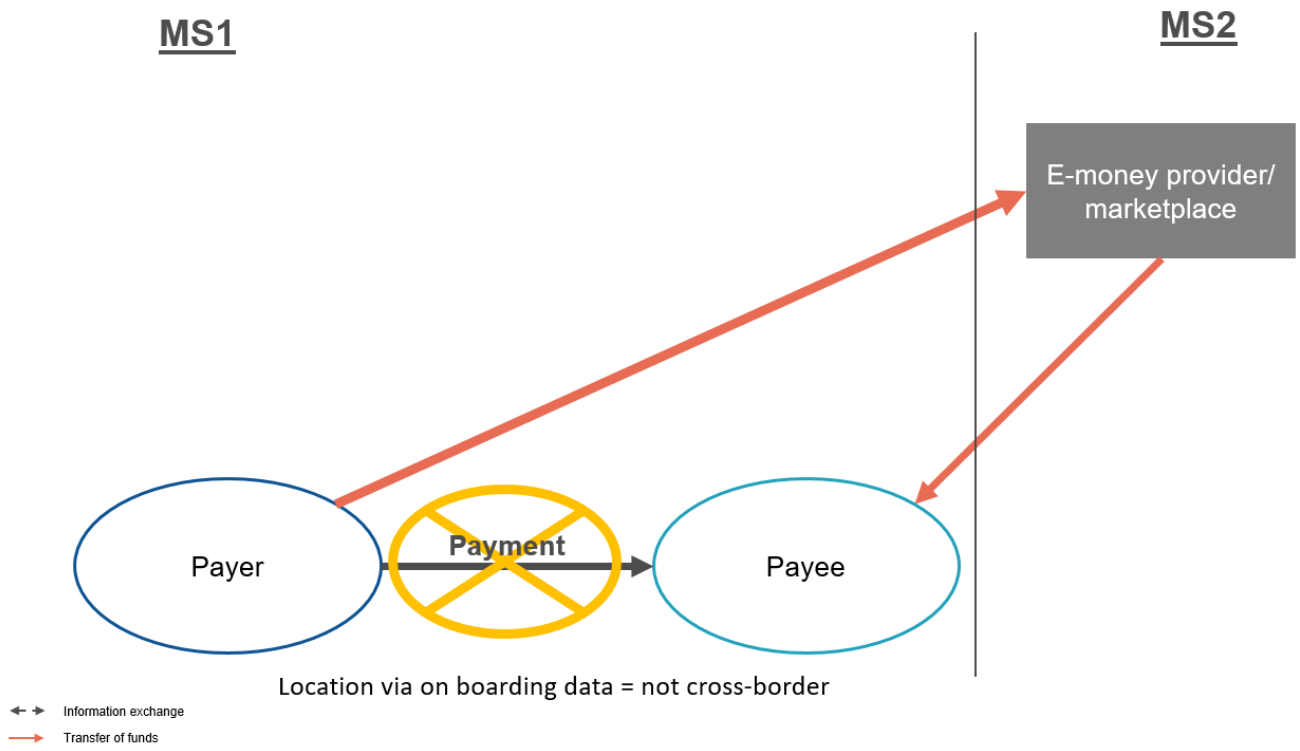


3.1.2.8 E-Money/marketplace – payer and payee in same Member State

In this case, the payer and the payee are located in the same Member State and are using the service of an e-money institution or a marketplace to execute their payment. In both cases, the payment service provider will have a relationship with both the payee and payer.

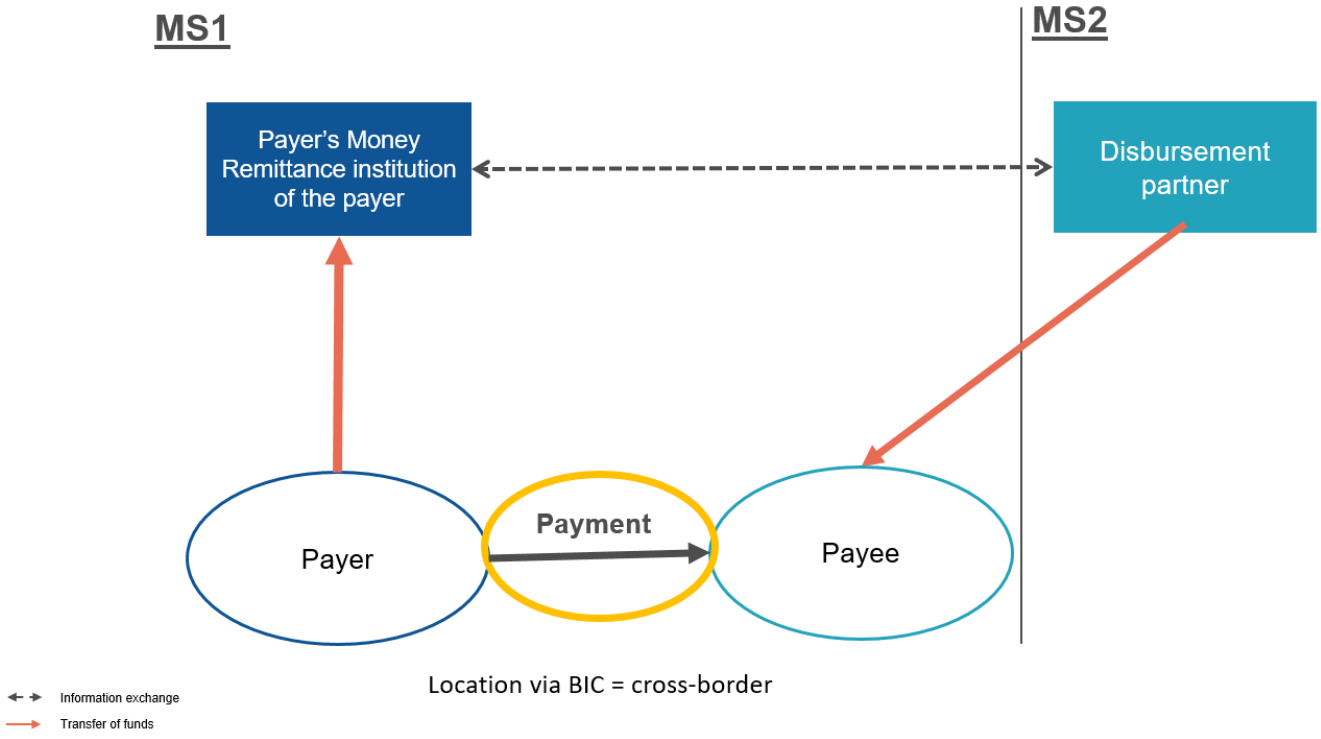
The payment service provider will locate the payer and the payee using the identifiers at his disposal which should indicate the real location of the payer and the payee. As such, the payment should be considered as national and not be reported.

Figure 28 – identification of cross-border e-money/marketplaces payments with payer and payee in same Member State



3.1.2.9 Money Remittance – Payer and Payee in same Member State

Figure 29 – identification of cross-border money remittances payments with payer and payee in same Member State



In this case, the payer and the payee are located in the same Member State but are using money remittance institutions in different Member States to perform a money remittance.

As money remittances are performed without the need for payment accounts, the identifiers to use to locate the payer and the payee will be the BIC of their respective money remittance institutions. Since both institutions are located in different Member States, this payment should be considered as cross-border even though the payer and the payee are located in the same Member State.

3.2 Threshold of 25 cross-border payments under article 243b (2)

The second monitoring to be performed by payment service providers regards the threshold of 25 cross-border payments laid down in article 243b (2) of Directive 2006/112/EC.

> *The requirement to which payment service providers are subject under paragraph 1 shall apply where, in the course of a calendar quarter, a payment service provider provides payment services corresponding to more than 25 cross-border payments to the same payee.*
>
> *The number of cross-border payments referred to in the first subparagraph of this paragraph shall be calculated by reference to the payment services provided by the payment service provider per Member State and per identifier as referred to in Article 243c(2). Where the payment service provider has information that the payee has several identifiers the calculation shall be made per payee*

In order to trigger its inclusion in a payment service provider's quarterly report, this article requires that the payee receives more than 25 cross-border payments per quarter. In the case where a payment service provider did not execute more than 25 cross-border payments to the same payee, it will not have to report any data on that payee. On the other hand, if the threshold is exceeded, the payment service provider will have to report all transactions to the payee (and not only the transactions exceeding the threshold.

The second sub-paragraph lays down the details of the threshold calculation. The threshold rule has been established to ensure that only data on taxable persons is collected and that data on private citizens receiving occasional cross-border payments will not be collected or transmitted to CESOP. It also acts as a simplification measures and a presumption of economic activities, meaning that payment service providers must report payees that exceed the threshold no matter whether they have information that they are taxable persons or not.

3.2.1 The basic rule – Calculation of cross-border payments per identifier

The basic rule under article 243b (2) is that the number of cross-border payments for a payee should be calculated using the identifier of the payee referred to in article 243c (2). In that regard, we refer to section 3.1.1 for the overview of relevant identifiers per payment method. In addition, only cross-border payments should be used in the calculation (see section 3.1. for the definition of cross-border payments).

In application of this rule, payment service providers will, for example, have to take into consideration all cross-border payments made to a single IBAN to calculate the total. If that amount exceeds 25 cross-border payments, then all the payments executed to that IBAN over the quarter will have to be reported to CESOP along with the details of the account holder (see section 4 for the full list of data to transmit).

In addition, the calculation has to be done regarding the payment services provided per Member State. This means that if a payment service provider has establishments in several Member States, each of these establishments should perform the calculation separately and not consolidate all their transactions at group level. The same is applicable if the payment service provider provides payment services in different Member States via commercial agents or directly.

3.2.2 The additional rule – Aggregation of cross-border payments per payee

It is not uncommon that a given payee will have a number of payment methods available for the payer, which can be linked to different identifiers (for example an IBAN for credit transfer, a merchant ID for card payment and an e-money account). In order to ensure payments to businesses are not reported because they are split into several payment methods, article 243b (2) lays down an additional rule which requires payment service providers to aggregate payments executed to multiple identifiers when they have the knowledge that these identifiers actually refer to the same payee.

According to this rule, if a payment service provider executes a series of payments using two different IBAN, or for example using an IBAN and a merchant ID, and it knows that the same payee owns both payment accounts, the payment service provider must consider the two payment accounts as one for the purpose of comparison to the threshold and include all payments to both the accounts in their calculation.

N.B.: the aggregation of payment accounts for the calculation of the threshold must not impact the reporting of the data itself. The later must be done using transactional data and thus considering both accounts as different payment accounts. Payment service providers must thus not aggregate the data transmitted in application of this rule.

***For example**: this implies that if a payment service provider has identified that a payee has two payment account, it must not include both these accounts as the payee's account for each transaction.*

3.2.2.1 <u>When should payment accounts be aggregated for the calculation</u>

Payment service providers must always try to identify whether two payment accounts are actually linked to the same payee using the information available to them. However, payment accounts should only be aggregated when they refer to the same payee. Following the definition of the PSD2, this implies that the holder of both payment accounts must be a single natural or legal person.

In application of this rule, aggregation is to be performed when the payment accounts are owned by the same person, company, or a branch of the same company. On the opposite, no aggregation should take place when the owners of the payment accounts are different entities, even if linked between themselves. This is for example the case for franchises or subsidiaries which should not be subject to aggregation.

N.B.: in the specific case where an account is held by two or more holders, the payee shall be considered as being all the holders put together. This implies that if one of the holder also has another payment account, the aggregation should not take place unless all the holders of both accounts are the same.

Example: Mr. X and Mr. Y hold a bank account to receive payments for their business activity. Mr. X also has a bank account with Ms. Z his wife, while Mr. Y has another account alone. In this situation, none of the account should be aggregated as the owners of the three accounts are not all the same.

3.2.2.2 <u>Data elements to use for aggregation</u>

In order to determine whether a payee behind multiple payment accounts is actually a single entity, payment service providers are free to use any information at their disposal, including information collected during the creation of the payment account. Indicators with a high degree of fuzziness, such as names, should only be used when they offer a reasonable degree of uniqueness in the individual case in order to avoid distorting the reporting (e.g. avoid aggregation of common names).

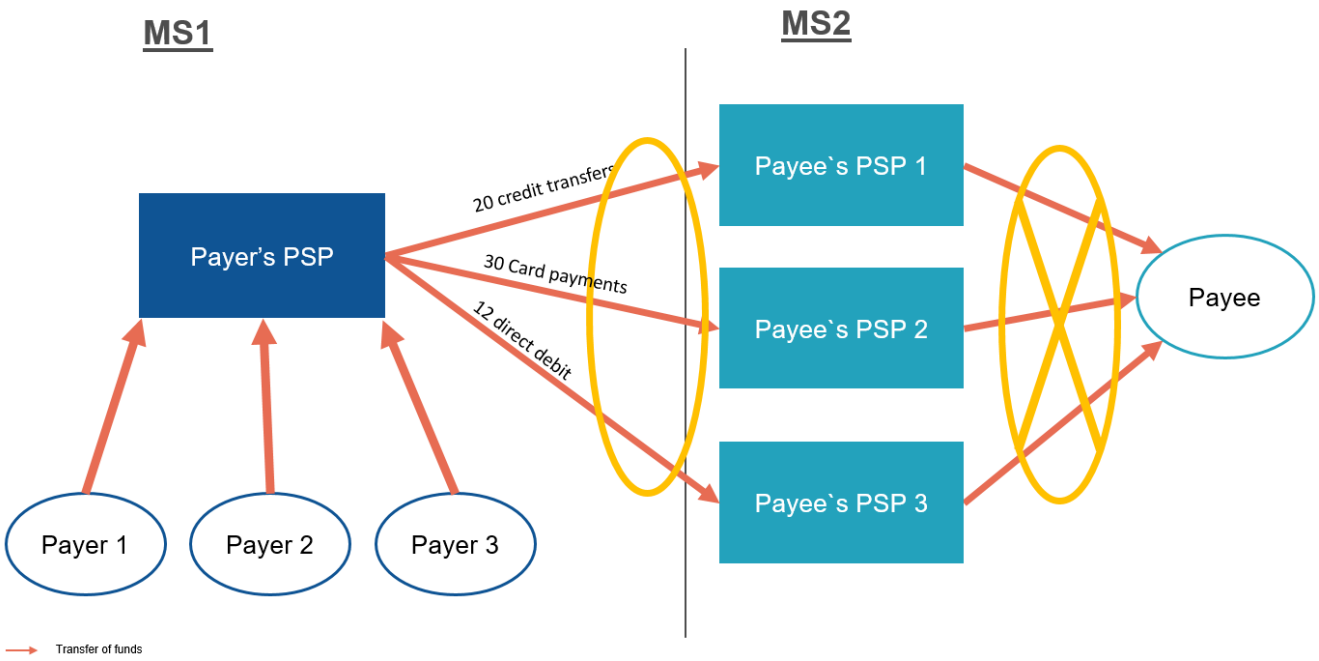
However, among the data elements to be transmitted to CESOP, there are a number which can also serve as indicator that the payee is a single entity:

1. **VAT/Tax Number:** although this data element might not always be available to the payment service provider, when it is it can be a strong hint that the payees between two payment accounts are actually a single entity. Indeed, only a single company will be allowed to share the same VAT or Tax number. As such, when payment service providers can determine that the payees of two payment accounts share the same VAT/Tax number, it is very likely that these payees are a single entity.
2. **Name:** the name of the payee can also help identify that it is the same entity. Although it can be subject to mistake, and companies could switch between their legal and business name, it remains a strong indicator that two payees might be a single entity. Especially if coupled with the address or other information available to the payment service provider.
3. **Address:** Even if their names differ, the fact that two payees share the same address is also an indicator that they might be the same entity. This should of course be cross-checked with other information available but can still prove useful in aggregating payment accounts.
4. **Other:** as said above, payment service providers are free to use any information at their disposal to aggregate payment accounts. This could include for example business identification number, IP address, E-mail address, contracts, etc…

3.2.3 Practical application

3.2.3.1 Aggregation of multiple payment methods

Figure 30 – Aggregation of multiple payment methods to a single payee



In this situation, a multitude of payers, having payment accounts with a single payment service provider are initiating payments toward a single payee. The payee offers different payment methods, such as credit transfer, direct debit, and card payments which are all used by the payers and are all managed by different payment service providers for the payee.

In application of the basic rules, the payment service provider of the payers should normally calculate the threshold using each identifier separately. As such, only the 30 card payments should be reported to CESOP.

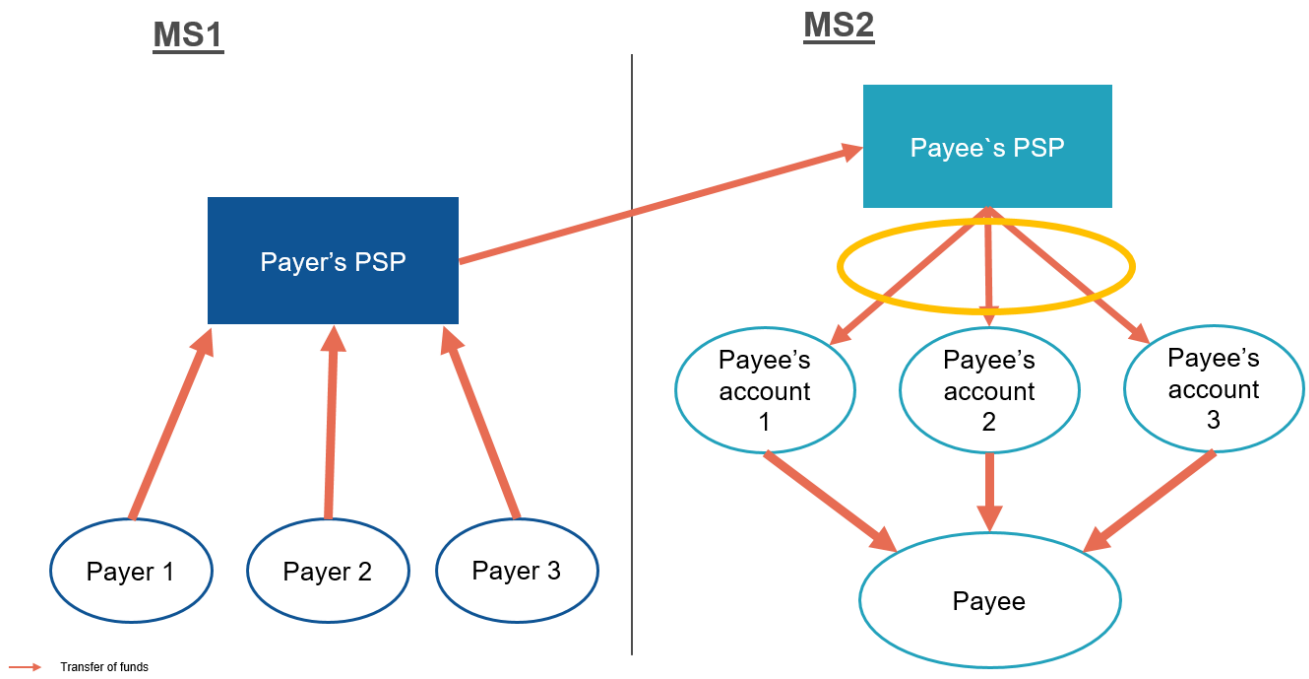
However, since the payee at the end is a single entity, the payers' payment service provider must identify whether all these payment accounts are actually linked to a single entity. If for example, the name and address of the payee as available for all payment methods is the same, the payers' payment service provider could safely consider that the payee behind these payments account is a single entity and as such aggregate all payments. The result is that the credit transfers and direct debits would also be reported to CESOP instead of only the card payments.

On the opposite, the aggregation should only be performed on the payments executed by a single payment service provider per Member States. As such, the payment service providers of the payee must not aggregate the payments between each other since they cannot know what is done by the others.

N.B.: even though the payer's payment service provider will not report the transaction as it is intra-EU, it should still perform the aggregation in application of article 243b (3), see section 4.3.

3.2.3.2 Aggregation of multiple payee's account within a single payment service provider

Figure 31 – Aggregation of multiple payee's accounts within a single payment service provider



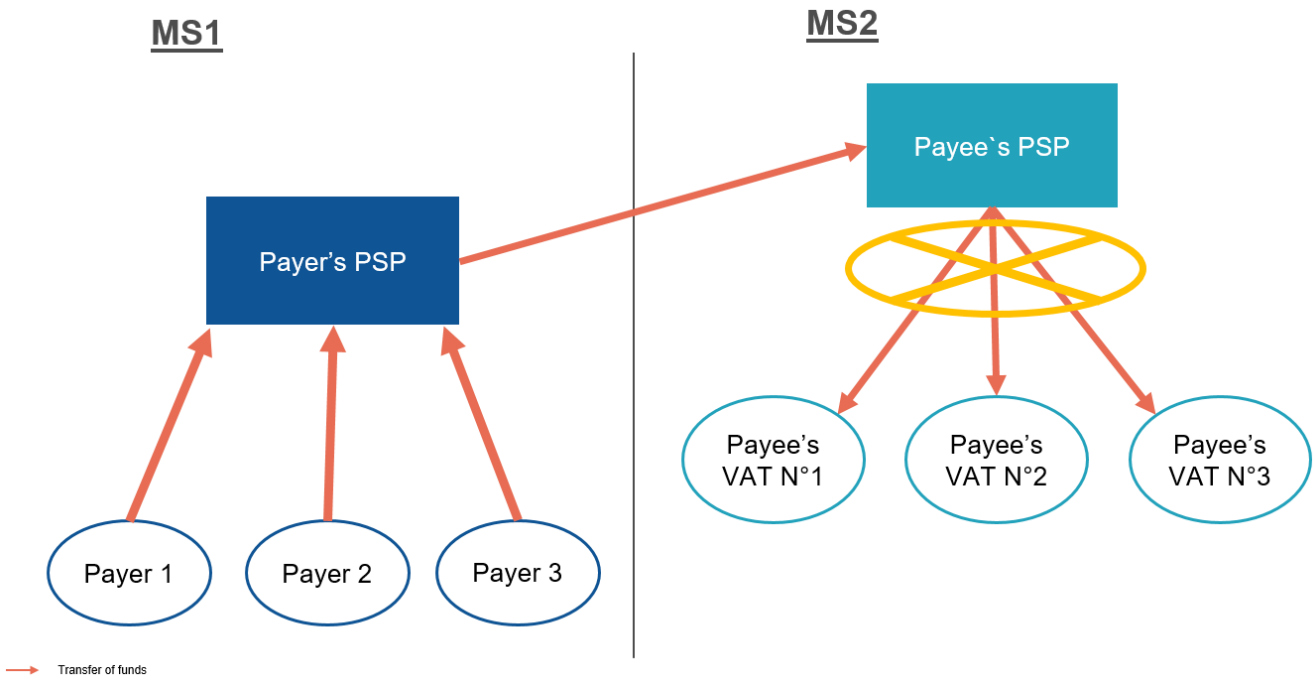
In this situation, the payment service provider of the payee receives multiple payment to different payment accounts which are all owned by a single payee. In order to identify whether the payments to these accounts should be reported the payment service provider will have to use the information it has available to determine that the accounts refer to the same payee and aggregate all the payments it executes to these payment accounts.

The payment service provider of the payer on the other hand will not be subject to the reporting obligation in accordance with article 243b (3) as there is a payment service provider of the payee in the European Union. It will however have to take these payment into consideration for the calculation of the

threshold in case it should also report payments to a non-EU payment account of the same payee (see section 4.3).

3.2.3.3 Payee is a franchise

Figure 32 – Non-aggregation of franchise



In this case, the payees adopt a franchise model where they all share a similar trade name or brand and distribute the same products, however they are all independent and different legal entities.

As explained previously, aggregation should only take place when the payment accounts are all owned by the same legal entities. In the case of a franchise, all entities will be different and have different VAT/Tax numbers. With this information available, the payment service provider of the payee can easily determine that they are not the same payee despite their close name and will not have to aggregate payments to the various accounts.

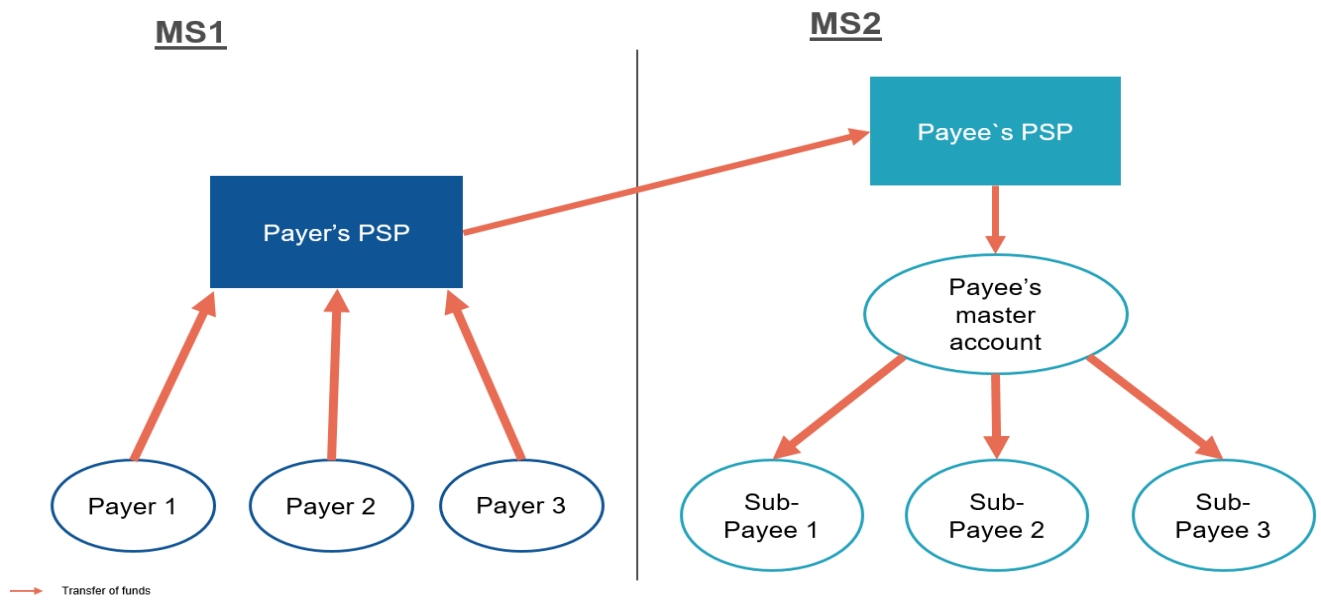
3.2.3.4 Aggregation of "Master" account

In this situation, the payee uses a main account within a single payment service provider to receive funds and later redistributes the payments to various "sub-accounts" and various payees. This process is especially common for marketplaces which will tend to centralise payments before redistributing them.

In such case, it is important to keep in mind that article 243b (2) does not include any form of disaggregation even if the data suggests that these accounts are used by multiple payees. This means that multiple payment accounts could be aggregated, but a single payment account should never be divided even if in practice this payment account will serve multiple payees.

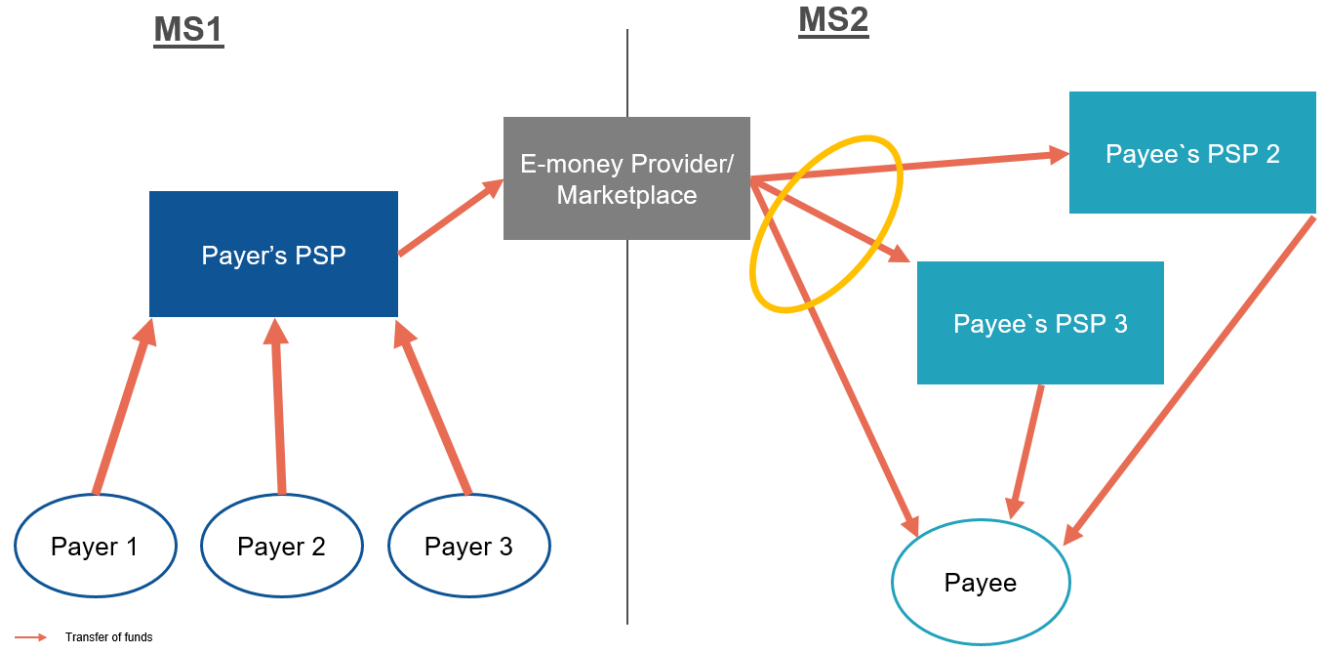
As such, when faced with this situation, the payment service providers will have to calculate the payments executed to the "master" account and report them, without looking at the sub-accounts.

Figure 33 – Calculation of threshold for master accounts



3.2.3.5 Aggregation by e-money providers and marketplaces

Figure 34 – Aggregation by e-money providers and marketplaces



In this case, the payments are centralised by an intermediary (e-money institution or marketplace) which holds the funds before redistributing them to various payment accounts of the payee. Contrary to the case of the master account, the payee here does not hold a single account but several where it receives the funds transmitted by the intermediary (e.g. e-money account, bank account, etc.).

For the payment service provider of the payers, all these payments will be sent to the intermediary account, meaning there is no need to aggregate (nor disaggregate). The intermediary however will have to use the information it has available to aggregate all the payments executed to the payee's various payment accounts.

4 REPORTING

4.1 What triggers the reporting obligation?

Article 243b (1) of Directive 2006/112/EC, added by Directive 284/2020, establishes all the rules applicable to the reporting obligation. According to this article, and as explained in section 2 and 3 of these guidelines, there are two elements that must be taken into consideration to trigger the reporting obligation:

- Whether the conditions to be in scope are fulfilled (see section 2);
- Whether the monitoring conditions are fulfilled (see section 3).

In practice, this implies that only payment service providers who are providing the payment services in scope of the reporting obligation (as laid down in article 243a of Directive 2006/112/EC), and which execute more than 25 cross-border payments per quarter to a given payee should report the data.

These two conditions must be checked and fulfilled during each calendar quarter for the reporting obligation to take place.

For example, if during a calendar quarter a payee fulfils these conditions with a payment service provider, the payment service provider must include this payee in its reporting. However, if it happens that during the following calendar quarter, the same payment service provider does not execute more than 25 cross-border payments to this payee, then it must not include it in its reporting.

If again the payee was to exceed the threshold in the following quarter, then the payment service provider must include the payments it has received during that quarter in its quarterly reporting.

The payments from the period in which all conditions were not fulfilled must never be reported.

4.2 How often shall the data be reported?

Article 243b(1) of Directive 2006/112/EC, added by Directive 284/2020 lays down the rules regarding the period of reporting.

Member States shall require payment service providers to keep sufficiently detailed records of payees and of payments in relation to the payment services they provide ***for each calendar quarter*** *to enable the competent authorities of the Member States to carry out controls of the supplies of goods and services which, in accordance with the provisions of Title V, are deemed to take place in a Member State, in order to achieve the objective of combating VAT fraud.*

According to this paragraph, payment service providers are required to keep detailed records of the payees and the payments they receive each calendar quarter. This constitutes the period over which information shall be collected and referred to. Following this, article 24b (1)(a) of Regulation 904/2010, as added by Regulation 283/2020, indicates the period over which Member States shall collect the data.

Each Member State shall collect the information on the payees and the payments referred to in Article 243b of Directive 2006/112/EC.

Each Member State shall collect the information referred to in the first subparagraph from payment service providers:

(a) no later than by the end of the month following the calendar quarter to which the information relates;

These two articles combined provide the timeline for the reporting of payment data from payment service providers. This reporting will take place every quarter starting from January 2024 and will require payment service providers to send the data to the Member States at the latest by the end of the month following the calendar quarter to which the data relates.

The table below lists the four reporting periods for payment service providers and the respective dates by which the data must be submitted to the Member States.

Reporting periods for payment service providers:

- 1st Period (January- March): **30 April**
- 2nd Period (April-June): **31 July**
- 3rd Period (July-September): **31 October**
- 4th Period (October- December): **31 January**

Once the data has been collected by Member States, they shall transmit it to CESOP by the 10th day of the second month following the end of the reporting period, according to article 24b (3).

The table below sets out the deadlines for the transmission of the data to CESOP by Member States.

Deadlines for the transmission of data to CESOP:

- 1st Period (January- March): **10 May**
- 2nd Period (April-June): **10 August**
- 3rd Period (July-September): **10 November**
- 4th Period (October- December): **10 February**

4.3 Who shall report the data under article 243b(3)?

Notwithstanding that a payment service provider may be in scope of the reporting obligation, article 243b (3) limits the obligations of the payment service provider of the payer.

The requirement laid down in paragraph 1 ***shall not apply to payment services provided by the payment service providers of the payer*** *as regards any payment* ***where at least one of the payment service providers of the payee is located in a Member State****, as shown by that payment service provider's BIC or any other business identifier code that unambiguously identifies the payment service provider and its location. The payment service providers of the payer shall nevertheless include those payment services in the calculation referred to in paragraph 2.*

In practice, the payment service provider of the payer will not have to keep records on the payees where at least one of the payment service providers of the payee is located in a Member State, as shown by this payment service provider's BIC or other business identifier. It is only when there are no payment service providers of the payee in a Member State that the payment service provider of the payer will have to keep and report data.

N.B.: the requirement to be located in a Member State shall be understood as a Member States in the territorial meaning of article 5 (2) of the VAT Directive and should not as such include third territories as defined in article 6 of the VAT Directive. As such, if the payment service provider of the payee is established in a third territory, the reporting shall be done by the payment service provider of the payer.

This means that when the payment service providers of the payee are in a Member State, the reporting obligation shall fall exclusively on them. The article does not create a limit regarding the number of payment service providers that should report the transaction, meaning that if, based on their business model, more than one payment service provider is involved in the payment from the payer's side (for example because of subcontracting), then all payment service providers of the payer shall be responsible to report data.

In the specific case of payment refunds, the reporting is to be performed by the payment service provider that reported the original transaction as it is the best placed to link both reporting.

Finally, the last sentence of article 243b (3) establishes a special rule regarding the threshold calculation: even if a payment shall not be reported by a payment service provider in application of this rule, it shall still be included in the calculation and aggregation of the 25 cross-border transactions threshold.

Example: A payment service provider from Member State 1 (payer's payment service provider) executes payment transactions to a payee that has a payment account in Member State 2 and another in a third country. Over a given quarter, the payment service provider of the payer executes:

- 200 payments to the payment account in Member State 2,
- 20 payments to the payment account in the third country.

In application of the rules of article 243b, all the conditions to trigger the reporting obligation are fulfilled, however the payment service provider of the payer will not report the payments to the payment account in Member State 2, as those will be reported by the payment service provider of the payee in Member State 2.

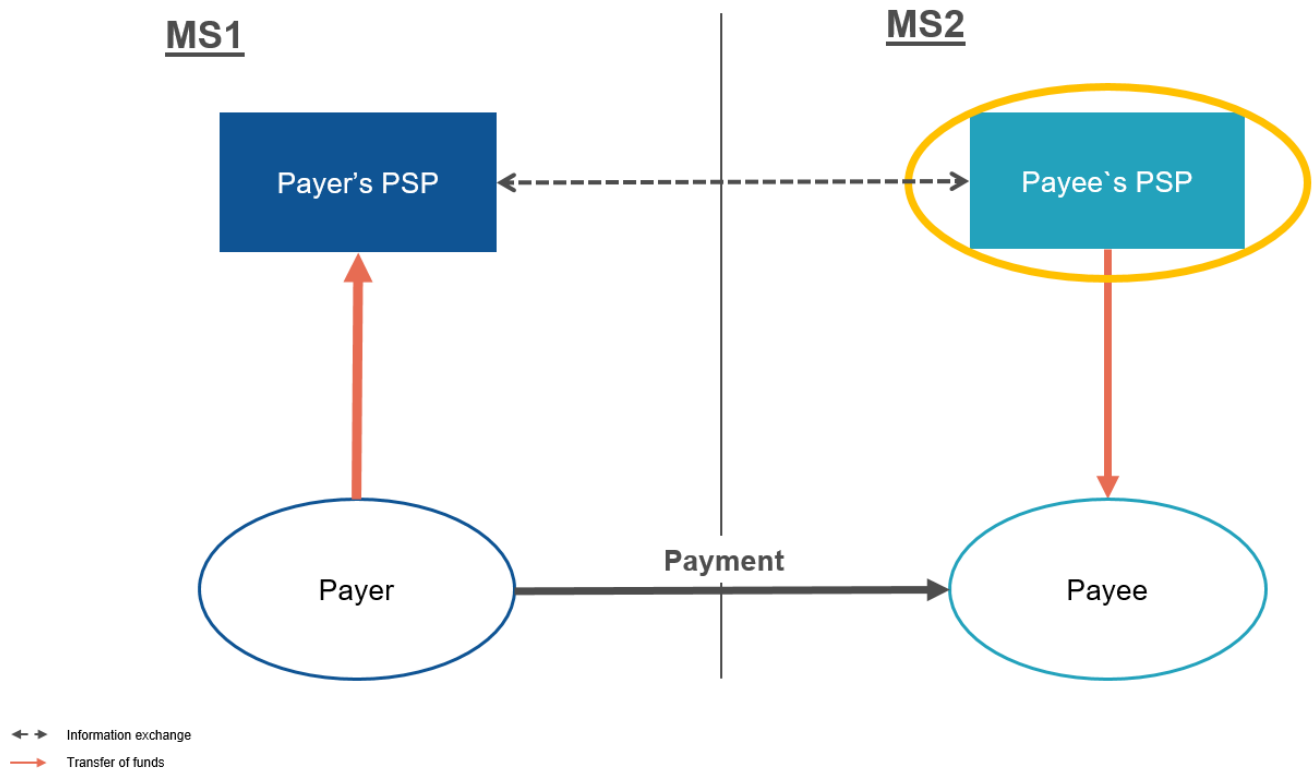
It will however have to report the payments to the payment account in the third country, as the threshold must be calculated inclusive of the payments to the payment account in Member State 2 and is therefore exceeding 25 cross-border payments.

4.3.1 Practical application

4.3.1.1 Payee's payment service provider and payee are in another Member State

This example is a clear application of the rules laid down in article 243b. According to article 243b(3) – all other conditions being fulfilled – the payment service provider of the payee, when located in a Member State, will be solely responsible for the reporting obligation.

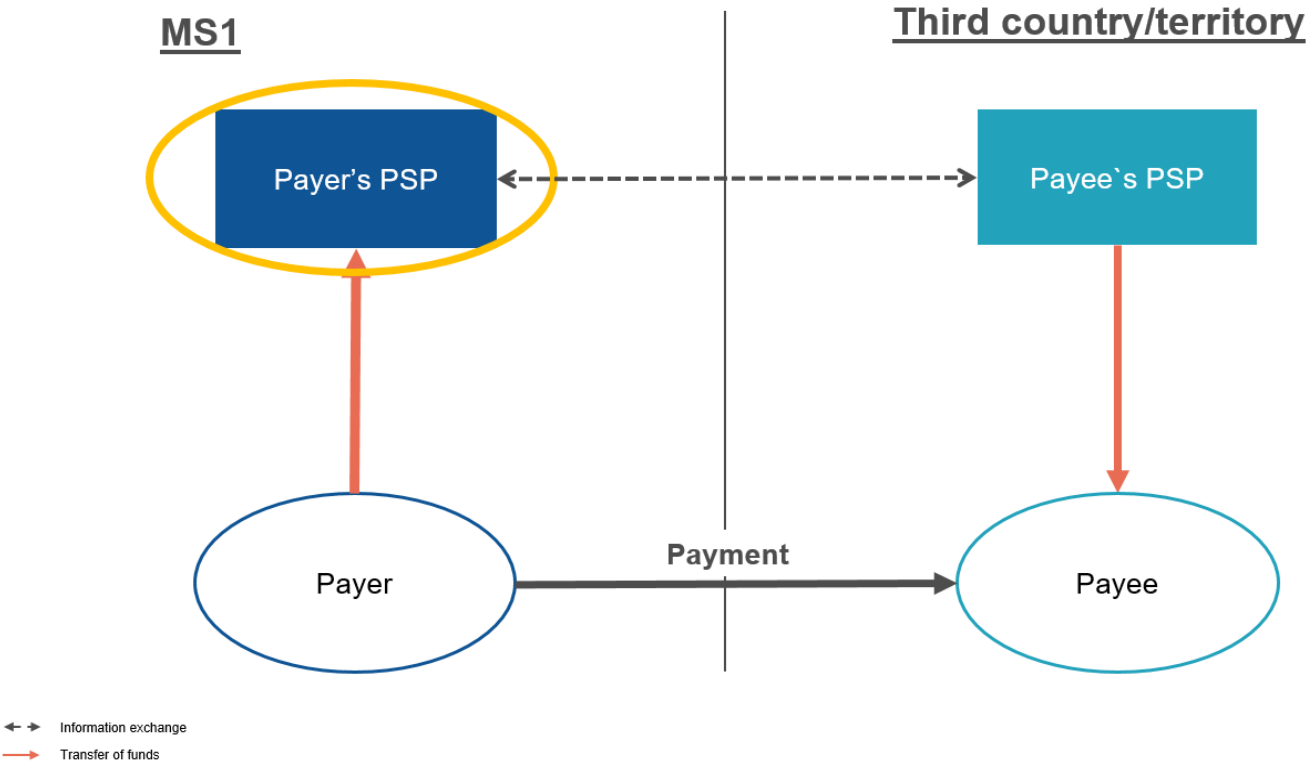
Figure 34 – Reporting when payment service provider of the payee is in another Member State



4.3.1.2 Payee's payment service provider and payee are in a third country

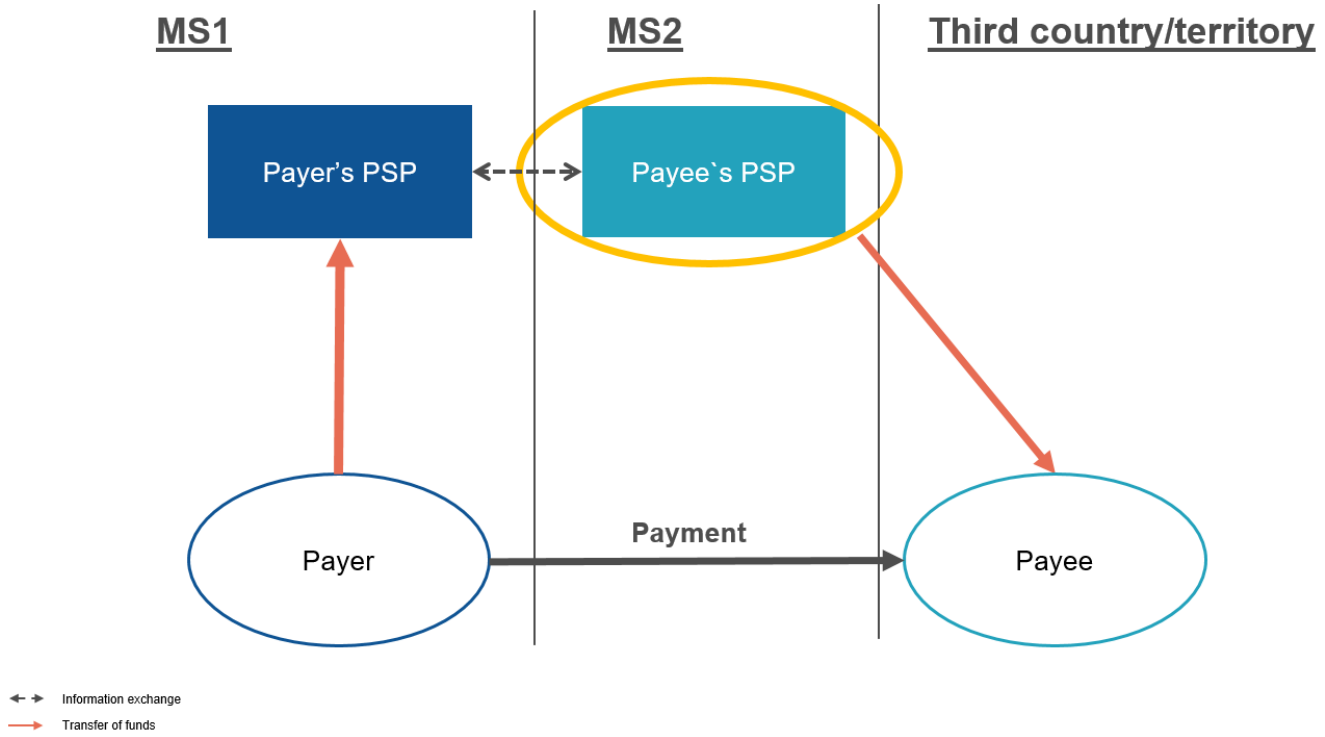
This is also a straightforward application of the rules laid down in article 243b. Since there is no payment service provider of the payee located in another Member State, the payment service provider of the payer will be responsible for the reporting obligation.

Figure 35 – Reporting when payment service provider of the payee is in a third country or territory



4.3.1.3 Payee's payment service provider is in a Member State and payee in a third country

Figure 36 – Reporting when payment service provider of the payee is in a Member State but payee is in a third country or territory



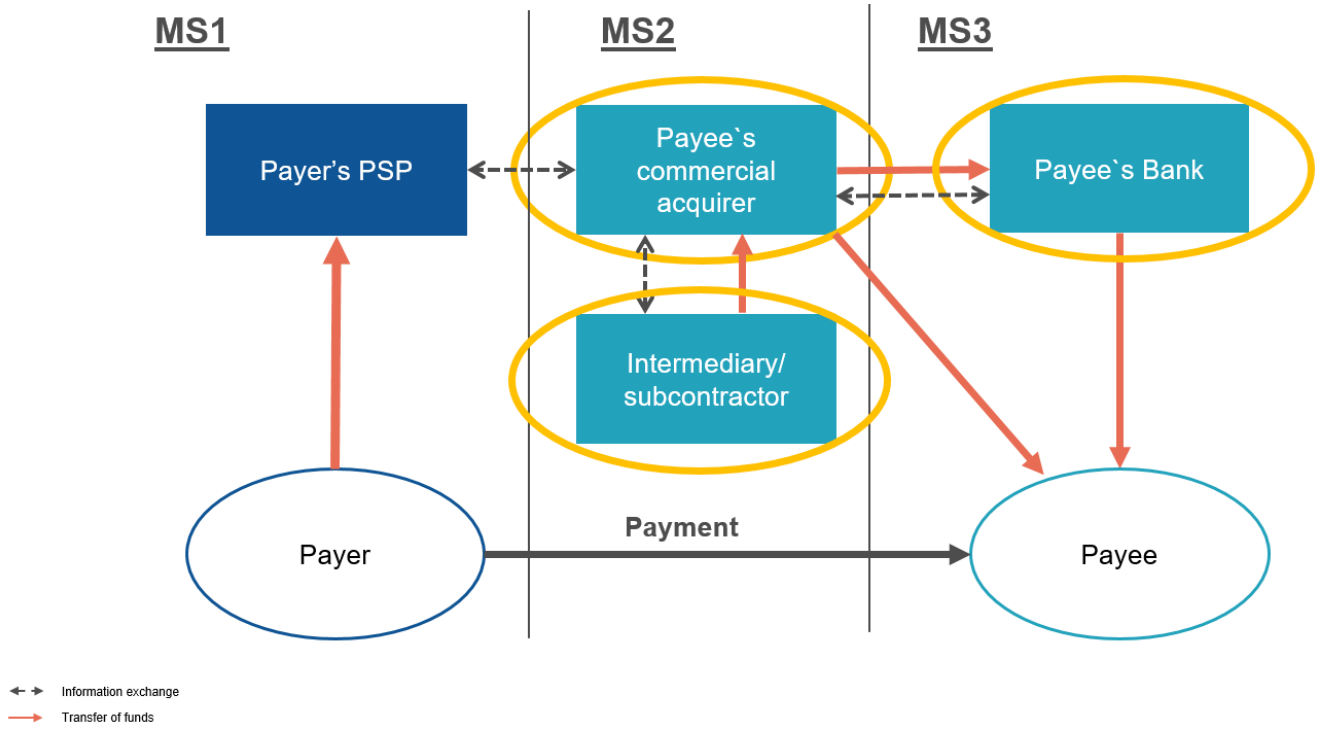
In this case the payee who is located in a third country, uses a payment service provider that is located in a Member State. Since article 243b(3) limits the reporting of the payment service provider of the payer when the payment service provider of the payee is in a Member State, the payment service provider of the payee shall be solely responsible for the reporting obligation.

4.3.1.4 Payee in a Member State with multiple payment service providers involved in the payment transaction

In this situation, the payee uses multiple payment services providers located in different Member States to process a payment transaction. Given that article 243b (3) does not include any limitation to the number of payment service providers of the payee responsible for the reporting, all of them that fulfil the conditions to be in scope of the reporting obligation shall be responsible to report the payment.

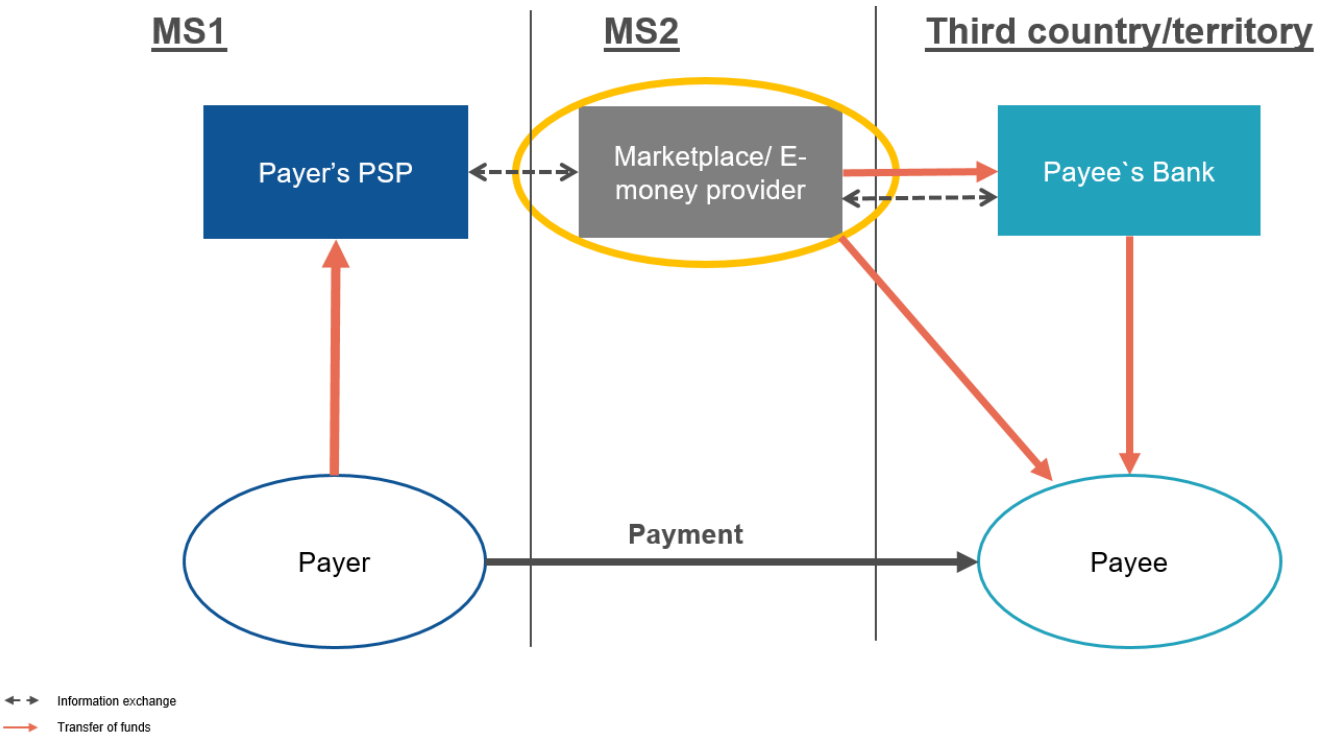
N.B.: an intermediary in the payment transaction shall not be responsible to report any payment if its activities only cover the provision of technical services which only support the provision of payment services without it entering into possession of the funds to be transferred at any time, since these entities do not qualify as payment service providers.

Figure 37 – Reporting when multiple payment service providers of the payee are in Member States



4.3.1.5 The payee is in a third country but uses a payment service provider in a Member State

Figure 38 – Reporting when at least one payment service provider of the payee is in a Member State



In this example, the payee is located in a third country and has a payment account with a non-EU payment service provider. However, since the payee also uses an intermediary in the European Union, such as a marketplace or an e-money provider, in order to supply the EU market, that intermediary will be responsible for the reporting obligation.

The payment service provider of the payer and the payee's bank located in the third country will not have to report data.

4.3.2 The situation of EEA countries

EEA countries are included in the territorial scope of the PSD2, and non-Union EEA States can have payment service providers providing payment services in the EU. The limitation rule of article 243b only applies when these payment service providers have a presence in another Member State that can be verified using the IBAN or other business identifier of the EEA payment service provider.

This means that if the payment service provider of the payee is located in an EEA country, according to its IBAN or other business identifier, it is the payment service provider of the payer that will have to report the data. In contrast, if a payment services provider from an EEA country operates branches in a Member State, these branches will be subject to the reporting obligation and could be considered as payment service providers of the payee.

4.4 Where should the data be reported?

The rules regarding where the data shall be reported are laid down in article 243b(4)(b) of the amended VAT directive.

> *Where the requirement for payment service providers laid down in paragraph 1 applies, the records shall:*
>
> *(b)be made available in accordance with Article 24b of Regulation (EU) No 904/2010 to the home Member State of the payment service provider, or to the host Member States when the payment service provider provides payment services in Member States other than the home Member State.*

According to this article, payment service providers shall report the payment data to their home Member State or, when they provide payment services in several Member States, to the host Member State(s).

The definition of home and host Member State are included in article 243a of the Directive, which refers directly to the relevant article of the PSD2.

According to the definition of the PSD2, the home Member State will be the Member State where a payment service provider has requested and obtained its payment license, which should correspond to the Member State in which it has its registered office or head office.

The host Member State on the other hand will be any Member State other than the home in which the payment service provider is providing payment services either via an agent, a branch or directly.

> **Example:** a payment service provider has a payment license from Member State 1 and also supplies payment services in Member State 2 via a branch, and Member State 3 via an agent.
>
> In application of the rules, this payment service provider will have to report the payments it executes in Member State 1 to Member State 1, the payments it executes in Member State 2 to Member State 2, and the payments it executes in Member State 3 to Member State 3.
>
> **Example 2:** an e-money provide has a payment license to provide payment services from Member State 1. It then uses passporting rules to provide payment services in all other Member States of the

Union. According to the rule of article 243b(4), it will report data in all Member States for the respective payments it executes in each one of them.

4.4.1 Direct provision of payment services in the host Member States

Determining the Member States where a payment service provider should report its payments is made easier when it has a physical presence in these Member States, such as when it does so via a branch or an agent. Where payment services are provided directly from one Member State to another is slightly more complex as there is no physical presence which allows a clear differentiation between the activities in the host Member State and the home Member State.

Payment service providers should follow their payment license to determine where they provide services. A payment service provider has to inform the authority of the host Member State before it can provide payment services in its territory, which is then documented in the register of payment service providers of that Member State[13]. Through that register, and using the information available from its client database, a payment service provider should be able to clearly identify which services are provided where.

Example: an e-money provider has its payment license in Member State 1 and also provides payment services in Member State 2 and 3. In order to determine what data should be reported in each Member State, it will look at its payment license and where its clients are located.

As such, if the e-money provider acts as the payment service provider of the payer for payments going from Member State 1 to a third country, it will report these payments in Member State 1. If it acts as payment service provider of the payee for payments going from Member State 3 to Member State 2, it will report these payments in Member State 2.

4.4.2 The situation of EEA countries (Iceland, Liechtenstein, Norway)

As we explained in session 2.1.1., the PSD2 also applies to countries that are members of the EEA. This means that these countries can legally obtain a payment license in their home country, and then use passporting rules to provide payment services all over the European Union, including the direct provision of payment services without a physical presence.

As we said in section 4.3.2., payments to EEA countries shall be considered as payments to third countries. In such cases, the payment service provider of the payer established in a Member State will report the payment in the Member State of the payer (whether it is its host or home Member State).

In contrast, payment service providers established in EEA countries who provide payment services in the European Union will have to report these payments in their host Member State. However, the rules of article 243b still apply, and only payments initiated by a payer (or through a payer's mandate in the case of direct debits) in the European Union (according to the location rules of article 243c) shall be reported to CESOP. As such, they should not report payments that are initiated from an EEA country.

[13] Information on the home and host Member States of a payment service provider can also be found on the European Bank Authority website (https://euclid.eba.europa.eu/register/)

Example: a payment service provider with a payment license from Norway provides payment services in Sweden and Iceland. According to the rules of article 243b, this payment service provider will:

- Report in Sweden all payment that are initiated by payers in Sweden to Norway, Iceland or any other third country;
- Report in Sweden all payments going to payees in Sweden where the payer is in a Member State other than Sweden;
- Not report any payments between Norway and Iceland or between either Norway or Iceland and any third country
- Not report any payments that are initiated by payers in Sweden to payees in another Member State.

4.5 What data should be reported by payment service providers?

The list of data that needs to be reported is laid down in article 243d of the amended Directive 2006/112 and can be divided into two sets of data: data related to the payee (article 243d (1)), and data related to each payment received by the payee (article 243d(2)).

1. The records to be kept by the payment service providers, pursuant to Article 243b, shall contain the following information:

(a)the BIC or any other business identifier code that unambiguously identifies the payment service provider;

(b)the name or business name of the payee, as it appears in the records of the payment services provider;

(c)if available, any VAT identification number or other national tax number of the payee;

(d)the IBAN or, if the IBAN is not available, any other identifier which unambiguously identifies, and gives the location of, the payee;

(e)the BIC or any other business identifier code that unambiguously identifies, and gives the location of, the payment service provider acting on behalf of the payee where the payee receives funds without having any payment account;

(f) if available, the address of the payee as it appears in the records of the payment services provider;

(g)the details of any cross-border payment as referred to in Article 243b(1);

(h)the details of any payment refunds identified as relating to the cross-border payments referred to in point (g).

2. The information referred to in points (g) and (h) of paragraph 1 shall contain the following details:

(a)the date and time of the payment or of the payment refund;

(b)the amount and the currency of the payment or of the payment refund;

(c)the Member State of origin of the payment received by or on behalf of the payee, the Member State of destination of the refund, as appropriate, and the information used to determine the origin or the destination of the payment or of the payment refund in accordance with Article 243c;

(d)any reference which unambiguously identifies the payment;

(e)where applicable, information that the payment is initiated at the physical premises of the merchant.

This data has to be transmitted via a standard XML form which is detailed in the Annex to Implementing Regulation[14]. The specification for the form (XML Schema Definition) together with the user guide are available on the dedicated CESOP page of the Europa website[15].

Given the multitude of data elements that can be collected for the different fields, the following section will focus on detailing what is expected for each data field and try to provide examples of data elements for each of the main payment methods that could be reported to CESOP. This list is not exhaustive and other elements could be valid as long as they correspond to the data listed in article 243d.

4.5.1 Overview of data elements

According to the annex to the Implementing Regulation, there are 15 main data elements to be included in the electronic form which represents the data requested under article 243d of the VAT Directive.

These data elements are listed in the table below which also includes a description of what they shall represent and whether the data is mandatory or not. For the purpose of the table, the following definitions shall apply:

- **Mandatory:** this data element shall always be provided and present in the form. Failure to provide the data element will result in a rejection of the form and a non-compliance with the reporting obligation.
- **Optional mandatory**: this data element shall always be provided when it is available to the payment service provider. Failure to provide the data element when it is available will result in non-compliance with the reporting obligation. However, if the data is not available to the payment service provider and the field is not completed, the form will not be rejected, and the reporting obligation will still be considered fulfilled.
- **Mandatory when applicable:** this data element shall be provided when the specific conditions for it to be requested are fulfilled. Failure to provide the data element when the conditions are fulfilled will result in a rejection of the form and non-compliance with the reporting obligation. If the conditions are not fulfilled, then the data will not have to be provided. Most of the data elements marked as such regard choices between two possibilities which are mutually exclusive.

[14] https://ec.europa.eu/taxation_customs/system/files/2022-04/C_2022_2043_F1_COMMISSION_IMPLEMENTING_REGULATION_EN_V3_P1_1727569-1.pdf

[15] https://ec.europa.eu/taxation_customs/taxation-1/central-electronic-system-payment-information-cesop_en

Table 2 – Overview of data elements to be transmitted

Box N°	Data Element Name	Art. 243d	Description	Mandatory
1	BIC/ID reporting PSP	(1), point (a)	This data element will be used to identify the payment service provider reporting the payment data to the tax authority. The data to be reported should be: • The Business Identifier Code (BIC) as defined in Article 2, point (16), of Regulation (EU) No 260/2012 of the European Parliament and of the Council[16] of the payment service provider reporting the data or; • any other business identifier code that unambiguously identifies the payment service provider transmitting the data. This can include national identifiers such as corporate numbers, national registration numbers, etc. This box should not be confused with the data element in box 5. Although the identifiers requested are the same, box 1 refers to the identifier of the payment service provider reporting the data, while the one in box 5 refers to the identifier of the payment service provider acting on behalf of the payee, which can be different from the one reporting the data if the payment goes outside the EU.	Mandatory
2	Payee name	(1), point (b)	Under this field, all available names of the payee, as available in the records of the payment service providers, shall be provided. If the payment service provider has no records for the payee, the name introduced by the payer shall be considered as the name in the records. Names can include the legal name, the "doing business as" (DBA) name, the name used for registration and contacts, etc. If the name in the records conflicts with the name introduced by the payer to initiate the payment transaction, the name in the records shall take precedence.	Mandatory
3	Payee VAT/TIN	(1), point (c)	Under this field, all available tax numbers of the payee shall be provided. These can include the European VAT identification number, the national VAT identification number, the tax identification number (TIN), or any national number which, although not strictly related to tax purposes or issued by a tax authority, is used for tax purposes and allows the unique identification of its holder (e.g. social security numbers, corporate registration number, etc.).	Optional Mandatory
4	Payee account ID	(1), point (d)	This field aims to precisely identify the payment account of the payee where the funds are being transferred. As such, it shall include either:	Mandatory when applicable, if funds are transferred to a

[16] Regulation (EU) No 260/2012 of the European Parliament and of the Council of 14 March 2012 establishing technical and business requirements for credit transfers and direct debits in euro and amending Regulation (EC) No 924/2009 (OJ L 94, 30.3.2012, p. 22).

			• the IBAN of the payee's payment account, as defined in Article 2, point (15), of Regulation (EU) No 260/2012 or; • any other identifier, which unambiguously identifies and gives the location of the payee involved in the transaction. This can include Merchant ID (MID), e-money accounts, SWIFT registration numbers, national account numbers, etc. Article 243d (1)(d) establishes a priority for the IBAN. It is only when it is not available that another identifier should be provided.	payment account of the payee.
5	BIC/ID Payee PSP	(1), point (e)	This field aims to identify the payment service provider acting on behalf of the payee when the payee receives funds without having a payment account (money remittance). As a payment account does not exist, an identifier for it under box 4 cannot be collected. As such, the reporting entity will have to provide the identifier of the payment service provider acting on behalf of the payee. Under this field, the data to be provided is either: • The Business Identifier Code (BIC) as defined in Article 2, point (16), of Regulation (EU) No 260/2012 of the European Parliament and of the Council of the payment service provider acting on behalf of the payee or; • any other business identifier code that unambiguously identifies the payment service provider acting on behalf of the payee. This can include national identifiers such as corporate numbers, national registration numbers, etc. This field should not be confused with the data requested under box 1 (see above). In addition, box 4 and 5 are mutually exclusive and only one of them should be completed.	Mandatory when applicable, if funds are transferred to a payee without a payment account.
6	Payee Address	(1), point (f)	Under this field, all available addresses of the payee that are in the records of the payment service provider, shall be provided. Addresses can include the legal address, business address, warehouse address, as well as e-mail addresses, webpages addresses or IP address. Based on the data available to the payment service provider, the address can be more or less detailed, ranging from the country to the street. In addition, the address reported does not need to be aligned with the one used under article 243c to determine the location of the payee. This means for example that the address reported can be in a different country than the one of the payee's payment account (IBAN). This field shall only be completed if the payment service provider has at least one address for the payee in its records. If the payment service provider has no address in its record but the address can be deduced from the payment account (e.g. country code of an IBAN), this field does not need to be completed.	Optional Mandatory

7	Refund	(1), point (h)	This field is intended to differentiate between payments **made by** a payer and refunds **made to** a payer. Refunds can include technical refunds as defined in the PSD2 but also commercial refunds, or any other type of refund as long as the payment service provider is aware of it. If a payment service provider is not aware that a transaction is a refund, it should then report it as a regular payment (given that all other conditions for the reporting are fulfilled). Under this field, payment service providers shall indicate that the payment is a refund. The refund transaction ID and reference to the original transaction shall be reported in box 14.	Mandatory when applicable
8	Date/time	(2), point (a)	Under this field, the date and time of the payment shall be reported. Given the multitude of dates available for a single payment transaction, it is possible for payment service providers to report multiple dates. However, in order to facilitate the detection of multiple reporting and the standardisation of the reporting, the following sections lists, for each payment method, at least one date that is common between all the payment service providers involved in a single payment transaction and which should always be reported (see infra).	Mandatory
9	Amount	(2), point (b)	Under this field, the total amount of the payment transaction or of the payment refund shall be reported.	Mandatory
10	Currency	(2), point (b)	Under this field, the currency of the payment transaction or of the refund transaction shall be reported. When there is a change of currency, the amount of the payment shall be reported in the original currency before booking and currency conversion by any of the payment service providers.	Mandatory
11	MS origin payment	(2), point (c)	Under this field, the country code for the Member State of origin of the payment received by the payee shall be provided. Payment service providers must indicate the Member State of origin resulting from the information indicated in box 13 and in accordance with article 243c. In cases where a payment service provider can identify several Member States for the origin of the payment, it must use the one that most accurately corresponds to the location of the payer (see section 3.1.1).	Mandatory when applicable, if transaction is a payment
12	MS Destination refund	(2), point (c)	Under this field, the country code for the Member State of destination of the refund received by the payer shall be provided. All the rules applicable to box 11 also apply here.	Mandatory when applicable, if transaction is a refund under box 7
13	Payer Location information	(2), point (c)	Under this field, the information used to determine the origin of the payment or the destination of the refund shall be provided in accordance with article 243c. The information can include any data element available to the payment service provider, as described in box 11 (IBAN, address, card number, etc.). It is important to note that this field	Mandatory

			shall only indicate what data was used, the data itself must not be transmitted. This implies that payment service provider will for example indicate that the location of the payer was established in a Member State using the IBAN of the payer's payment account. The IBAN of the payer itself, however, shall never be transmitted.	
14	Transaction ID	(2), point (d)	This field aims to allow easy identification of payment duplicates. As such, any reference which unambiguously identifies the payment transaction shall be reported under this field. When several transaction identifiers are available, priority should always be given to the one that is passed along the payment chain and is available to other payment service providers in the payment chain. In the case of refunds, as detailed in box 7, the transaction identifier reported for the refund shall be identical, or at least include the transaction identifier of the initial transaction.	Mandatory
15	Physical presence	(2), point (e)	This field aims to allow an easy identification of the physical payments made by the payer at the premises of the payee, in opposition to online payments. Under this field, any reference which indicates the presence of the payer in the physical premises of the merchant when initiating the payment shall be reported.	Mandatory when applicable

4.5.2 Data to be reported per payment method

4.5.2.1 Credit transfer

In a regular credit transfer, the payer will initiate an order for its bank to transfer funds to the bank account of the payee.

Table 3 – Overview of data elements to be transmitted for credit transfer

N°	Data Element	Available to payment service provider		Possible standard format accepted	Comments
		Payer	Payee		
1	BIC/ID reporting PSP	Yes	Yes	BIC (ISO 9362)	
2	Payee name	Yes	Yes		
3	Payee VAT/TIN	Not always	Not always	EU VAT number shall respect the EU standards. No standards required for other identifier.	VAT number/TIN are not mandatory elements to process the payments. They might be available, together with other identifiers, occasionally or following stricter requirements in national legislations. As such, payment service providers that do not collect the VAT number/TIN of their clients are not obliged to transmit this data. Payment service providers of the payee are more likely to have VAT number/TIN or other identifier based on "know your customer" ("KYC") requirements.
4	Payee account ID	Yes	Yes	IBAN (ISO 13616)	For payments to a country that does not use IBAN, national account numbers can be provided instead.
5	BIC/ID Payee PSP	Not applicable	Not applicable	/	An account number should always be available in credit transfers.
6	Payee Address	Not always	Yes	/	The address is not mandatory in order to process payments via credit transfers but shall be available to payment service providers of the payee through KYC obligations.
7	Refund	Yes	Yes	/	
8	Date/time	Yes	Yes	Settlement date	
9	Amount	Yes	Yes	Amount should be reported with two decimals	
10	Currency	Yes	Yes	ISO 4217	
11	MS origin payment	Yes	Yes	ISO 3166-1 Alpha 3	

12	MS Destination refund	Yes	Yes	ISO 3166-1 Alpha 3	
13	Payer Location information	Yes	Yes	Not applicable	
14	Transaction ID	Yes	Yes	No standard	Transaction IDs for credit transfers are proprietary to the payment service provider and are only unique within a payment service provider's system.
15	Physical presence	Not applicable	Not applicable		

4.5.2.2 Direct debit

As described in section 1, direct debits work mainly like credit transfers with the exception that the payment is initiated by the payee instead of the payer. It is important to highlight again that there are currently no existing standards for non-SEPA direct debit. As a consequence, international direct debits are performed using ad-hoc rules which are either copied from the SEPA rules or from national systems. Because of this, the figure below focuses on the standards applicable to the payee's reporting, as no standards exists for reporting done by the payer in non-EU payments.

Table 4 – Overview of data elements to be transmitted for direct debits

N°	Data Element	Available to payment service provider		Possible standard format accepted	Comments
		Payer	**Payee**		
1	BIC/ID reporting PSP	Not applicable	Yes	BIC (ISO 9362)	
2	Payee name	Not applicable	Yes		
3	Payee VAT/TIN	Not applicable	Not always	EU VAT number shall respect the EU standards. No standards required for other identifier.	VAT number/TIN are not mandatory elements to process payments. They might be available, together with other identifiers, occasionally or following stricter requirements in national legislations. As such, payment service providers that do not collect the VAT number/TIN of their clients are not obliged to transmit this data. Payment service providers of the payee are more likely to have a VAT number/TIN or other identifiers based on "know your customer" ("KYC") requirements.
4	Payee account ID	Not applicable	Yes	IBAN (ISO 13616)	

5	BIC/ID Payee PSP	Not applicable	Not applicable	/	An account number should always be available in direct debits.
6	Payee Address	Not applicable	Yes	/	The address is not mandatory to process payments via direct debits but shall be available to payment service providers of the payee through KYC obligations.
7	Refund	Not applicable	Yes	/	
8	Date/time	Not applicable	Yes	Settlement date	
9	Amount	Not applicable	Yes	Amount should be reported with two decimals	
10	Currency	Not applicable	Yes	ISO 4217	
11	MS origin payment	Not applicable	Yes	ISO 3166-1 Alpha 3	
12	MS Destination refund	Not applicable	Yes	ISO 3166-1 Alpha 3	
13	Payer Location information	Not applicable	Yes	Not applicable	
14	Transaction ID	Not applicable	Yes	/	Transaction IDs for direct debits are proprietary to the payment service provider and are only unique within a payment service provider's system.
15	Physical presence	Not applicable	Not applicable	/	

4.5.2.3 Money remittance

Money remittances differ from other payment methods by the fact that they do not necessarily require a payment account to execute the payments. Although it is nowadays possible to include payment accounts in money remittance orders, it is still possible to transfer funds without these. As such, the main difference for money remittance institutions will be to provide an identifier in box 5 to identify the disbursement partner in the absence of a payment account identifier.

Table 5 – Overview of data elements to be transmitted for money remittances

N°	Data Element	Available to payment service provider		Possible standard format accepted	Comments
		Payer	Payee		
1	BIC/ID reporting PSP	Yes	Yes	BIC (ISO 9362)	

2	Payee name	Yes	Yes		
3	Payee VAT/TIN	Not always	Not always	EU VAT number shall respect the EU standards. No standards required for other identifier.	VAT number/TIN are not mandatory elements to process the payments. They might be available, together with other identifiers, occasionally or following stricter requirements in national legislations. As such, payment service providers that do not collect the VAT number/TIN of their clients are not obliged to transmit this data. Payment service providers of the payee are more likely to have a VAT number/TIN or other identifiers based on KYC requirements.
4	Payee account ID	Not applicable	Not applicable	IBAN (ISO 13616)	Traditional money remittances do not require a payment account to be executed. It is however possible to provide the information. If this is the case, then it must be reported instead of the BIC in box 5.
5	BIC/ID Payee PSP	Yes	Yes	BIC (ISO 9362)	The BIC or other identifier shall allow the identification of the payment service provider where the funds are sent. If no BIC is available, then any national identification number can be provided as long as it allows unique identification of the payment service provider.
6	Payee Address	Not always	Yes	/	The address is not mandatory to process payments via money remittances but shall be available to payment service providers of the payee through KYC obligations.
7	Refund	Yes	Yes	/	
8	Date/time	Yes	Yes	Execution date	
9	Amount	Yes	Yes	Amount should be reported with two decimals	
10	Currency	Yes	Yes	ISO 4217	
11	MS origin payment	Yes	Yes	ISO 3166-1 Alpha 3	
12	MS Destination refund	Yes	Yes	ISO 3166-1 Alpha 3	
13	Payer Location information	Yes	Yes	Not applicable	
14	Transaction ID	Yes	Yes	No standard	Transaction IDs for money remittances are proprietary to the payment service provider and are only unique within a payment service provider's system.

15	Physical presence	Not applicable	Not applicable		

4.5.2.4 Card payments

Card payments are initiated by the payer using its credit or debit card details in order to trigger a payment order that will be processed by its card issuer and the payee's commercial acquirer. Although card payments can be divided into three party card payments and four party card payments based on the model used by the issuer and acquirer, the data to be reported will be nearly identical as both systems function similarly to process payments.

It is also important to note that card payments are heavily dependent on the scheme used to process the payments. In this regard, it is impossible to review the data exchanged in every existing card scheme. The below table focus on the rulebooks issued by the two most popular card schemes for international transactions, namely VISA and MasterCard.

Table 6 – Overview of data elements to be transmitted for credit card payments

N°	Data Element	Available to payment service provider		Possible standard format accepted	Comments
		Payer	**Payee**		
1	BIC/ID reporting PSP	Yes	Yes	BIC (ISO 9362)	
2	Payee name	Yes	Yes	Card acceptor name (MC DE043) Merchant name (VISA TCR0 pos. 92-116)	
3	Payee VAT/TIN	Not always	Not always	EU VAT number shall respect the EU standards. No standards required for other identifier.	VAT number/TIN are not mandatory elements to process the payments. They might be available, together with other identifiers, occasionally or following stricter requirements in national legislations. As such, payment service providers that do not collect the VAT number/TIN of their clients are not obliged to transmit this data. Payment service providers of the payee are more likely to have a VAT number/TIN or other identifiers based on KYC requirements.
4	Payee account ID	Yes	Yes	Merchant ID / Card Acceptor ID (MC DE042	Merchant ID and Card acceptor ID must be combined to identify the merchant selling the goods behind a given acquirer.
5	BIC/ID Payee PSP	Not applicable	Not applicable	/	
6	Payee Address	Yes	Yes	MC DE043 VISA TCR0	

7	Refund	Yes	Yes	/	If reference to the original payment is included, it should be reported as part of the transaction ID in box 14
8	Date/time	Yes	Yes	MC: DE 12 - Date and Time, local transaction Visa : TC05 Purchase date	Date should at least include month and year of the transaction.
9	Amount	Yes	Yes	Mastercard : DE04/ DE05/DE06 VISA : TC05 Source Amount & Source currency code Amount should be reported with two decimals.	
10	Currency	Yes	Yes	ISO 4217	
11	MS origin payment	Yes	Yes	ISO 3166-1 Alpha 3	For the location of the payer, the Bank Identification Number ("BIN") range of the card number shall be used to determine where the card has been issued rather than where the issuer is located.
12	MS Destination refund	Yes	Yes	ISO 3166-1 Alpha 3	For the location of the payer, the BIN range of the card number shall be used to determine where the card has been issued rather than where the issuer is located.
13	Payer Location information	Yes	Yes	Card number BIN	
14	Transaction ID	Yes	Yes	MC : DE 31—Acquirer Reference Data Visa : TC05 - Acquirer Reference Number	The transaction ID to be reported shall be the one provided by the acquirer which is unique within the card scheme used and common to all payment service providers involved in the payment.
15	Physical presence	Yes	Yes	MC : DE 22 Point of Service (POS) Entry Mode Visa : TC05 POS Entry Mode	

4.5.2.5 <u>E-money</u>

A typical e-money payment is initiated by the payer using the funds on its e-money account to order a transfer to the payee's e-money account. The funding of the e-money account can be done using different

payment methods (credit transfer, card payment, etc.) and either before the e-money payment or simultaneously with it (if the payer had no funds on its e-money account to execute the payment). These payments to fund or withdraw from the e-money account will appear, to the external payment service providers involved in the transaction, like a payment from the payer to the e-money institutions which will be identified as the payee (if the payer funds its e-money account) or as the payer (if the payee withdraws the funds from its e-money account). The e-money account can also take the form of a pre-paid card in the case of E-vouchers.

E-money payments have the peculiarities in that there are no existing standards for e-money transaction. E-money payments are performed in a close system where both the payer and the payee have contracted with the e-money provider and they are regulated by the rules established by the e-money provider itself, which as such is free to adopt the rules it wants. This close system on the other hand, allows the e-money provider to have full visibility on the payment transaction as well as the payer and payee.

Table 7 – Overview of data elements to be transmitted for e-money payments

N°	Data Element	Available to payment service provider		Possible standard format accepted	Comments
		Payer	Payee		
1	BIC/ID reporting PSP	Yes	Yes	BIC (ISO 9362)	
2	Payee name	Yes	Yes		
3	Payee VAT/TIN	Not always	Not always	EU VAT number shall respect the EU standards. No standards required for other identifier.	VAT number/TIN are not mandatory elements to process the payments. They might be available, together with other identifiers, occasionally or following stricter requirements in national legislations.
4	Payee account ID	Yes	Yes	IBAN (ISO 13616)	If IBAN is not available, the e-money provider can, for example, provide the e-money account number as an identifier or provide another identifier such as the merchant ID.
5	BIC/ID Payee PSP	Not applicable	Not applicable	/	
6	Payee Address	Yes	Yes		
7	Refund	Yes	Yes		If reference to the original payment is included, it should be reported as part of the transaction ID in box 14
8	Date/time	Yes	Yes	Execution date	
9	Amount	Yes	Yes	Amount should be reported with two decimals	
10	Currency	Yes	Yes	ISO 4217	
11	MS origin payment	Yes	Yes	ISO 3166-1 Alpha 3	

12	MS Destination refund	Yes	Yes	ISO 3166-1 Alpha 3	
13	Payer Location information	Yes	Yes	IBAN, e-account address, card number BIN, IP address.	E-money providers must establish the location of the payer using all information available in their records to determine the one that best represents the location of the payee.
14	Transaction ID	Yes	Yes		Transaction IDs for e-money transactions are proprietary to the e-money provider and are only unique within one e-money provider's system.
15	Physical presence	Not applicable	Not applicable		

4.5.2.6 Marketplaces

Marketplaces do not offer specific payment methods but rather allow their users to use other payment methods to buy goods or services on their centralised platform. Because of this specificity, the way marketplaces acting as payment service providers process payments is both similar to the way the related payment method works, and to the way e-money providers act at the centre of the infrastructure.

As such, the data marketplaces will be able to report can vary based on the payment method used and offer (e.g. whether payment will be done via credit transfer, card payment, e-money, etc.). However, being at the centre of the payment processing and holding funds on behalf of both the payer of the payee, the marketplace will always have full visibility on the payment transaction as well as the payer and payee.

Table 8 – Overview of data elements to be transmitted by marketplaces

N°	Data Element	Available to payment service provider		Possible standard format accepted	Comments
		Payer	**Payee**		
1	BIC/ID reporting PSP	Yes	Yes	BIC (ISO 9362)	
2	Payee name	Yes	Yes	(name on selling account)	
3	Payee VAT/TIN	Not always	Not always	EU VAT number shall respect the EU standards. No standards required for other identifier.	VAT number/TIN are not mandatory elements to process the payments. They might be available, together with other identifiers, occasionally or following stricter requirements in national legislations.
4	Payee account ID	Yes	Yes	IBAN (ISO 13616)	If IBAN is not available, the marketplace can provide other account identifier, including the marketplace account ID.

				Merchant ID (MC DE 042)	
5	BIC/ID Payee PSP	Not applicable	Not applicable	/	
6	Payee Address	Yes	Yes		
7	Refund	Yes	Yes		If reference to the original payment is included, it should be reported as part of the transaction ID in box 14
8	Date/time	Yes	Yes	Execution date	
9	Amount	Yes	Yes		
10	Currency	Yes	Yes	ISO 4217	
11	MS origin payment	Yes	Yes	ISO 3166-1 Alpha 3	
12	MS Destination refund	Yes	Yes	ISO 3166-1 Alpha 3	
13	Payer Location information	Yes	Yes	IBAN (ISO 13616) Card number BIN IP address	Marketplaces must establish the location of the payer using all information available in their records to determine the one that best represents the location of the payee.
14	Transaction ID	Yes	Yes		Transaction ID will be attributed by the marketplace and will not be available to other payment service providers in the payment chain.
15	Physical presence	Not applicable	Not applicable		

4.5.3 Data quality aspects

The data to be transmitted by payment service providers will vary based on the payment method used and whether the reporting entity is the payment service provider of the payer or the payee. Specifically, in the latter case, the data transmitted by the payment service provider of the payer may be of lower quality or impossible for the payment service provider to cross-check as it will lack the contact with the payee.

Under the reporting obligation, payment service providers are not requested to ask their partners for more data than the one already available to them or exchange during the payment processing. They are also not requested to verify the data they used other than what is required in order to process a payment and comply with KYC and AML obligations. This implies that if a data element cannot be verified by a payment service provider, for example where it refers to a national system of a third country, the payment service provider can report this data as it is and does not need to further check its validity.

The data quality might also vary based on the payment service provider's business models. E-money providers typically have full visibility on the transfer between the payer and the payee which should allow them to report higher quality data on the payee.

The main data quality issues will occur when the data is reported by the payment service provider of the payer as it cannot confirm that the data transmitted is correct. This problem is further exacerbated in payment methods where fields take the form of a free text box completed by the payer, mainly credit transfer

The table below provides an overview of the expected quality of the data transmitted by payment service providers for the main payment methods presented in these guidelines. Elements in yellow are expected to be either rarely available or of lower quality. Marketplaces are not represented as they use the data from other payment method which is completed by their own data on both the payer and the payee. As such, they are not expected to have any difficulties with data availability or quality.

Table 9 – Overview of data and expected data quality levels

Data requirements (Art. 243d)	**Card payments**		**Bank transfers**			**Direct Debits**		**E-money**		**Money Remittance**	
Linked to the payee	**PSP Payer (Issuer)**	**PSP Payee (Acquirer)**	**PSP payer (SEPA- IBAN)**	**PSP payer (Swift)**	**PSP payee (SEPA)**	**PSP Payer**	**PSP payee**	**PSP payer**	**PSP payee**	**PSP payer**	**PSP Payee**
1a) BIC PSP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
1b) Name of payee	Card acceptor name (MC DE043) Merchant name (VISA TCR0)	Card acceptor name (MC DE043) Merchant name (VISA TCR0)	Payee name (provided by payer)	Payee name (SWIFT 59a)	Creditor name (records)	Creditor name (records)	Creditor name (records)	Payee's name (own records)	Payee's name (own records)	Payee's name	Payee's name
1c) VAT/Tax ID	Optional	Mandatory in some MS	Optional	Optional	Mandatory in some MS	Optional	Mandatory in some MS	Optional	Optional	Optional	Optional
1d) IBAN, ID payee	Merchant/card acceptor ID (MC DE042)	IBAN + Merchant/card acceptor ID (MC DE042)	IBAN	SWIFT field 59/59a	IBAN	IBAN (EU)	IBAN (EU)	E-account identifier (+ IBAN)	E-account identifier (+ IBAN)	IBAN when available	IBAN when available
1e) BIC PSP payee	NA	NA	NA	BIC or Other ID	NA	NA	NA	NA	NA	BIC or Other ID	BIC or Other ID
1f) Address payee	Card Acceptor street (DE043 sub2)	Payee address (own records)	Payee address (provided by payer)	Payee address (SWIFT field 59)	Payee address (own records)	Payee address (transmitted by payee)	Payee address (own records)	Payee address (own records)	Payee address (own records)	Payee address (provided by payer)	Payee address (own records)

Data requirements (Art. 243d)	Card payments		Bank transfers			Direct Debits		E-money		Money Remittance	
Linked to the payment	**PSP Payer (Issuer)**	**PSP Payee (Acquirer)**	**PSP payer (SEPA-IBAN)**	**PSP payer (Swift)**	**PSP payee (SEPA)**	**PSP Payer**	**PSP payee**	**PSP payer**	**PSP payee**	**PSP payer**	**PSP Payee**
2a) Date and time	Local Transaction (MC DE12) Purchase Date (TC05)	Local Transaction (MC DE12) Purchase Date (TC05)	Interbank settlement date	Execution date (Field 32a)	Interbank settlement date	Interbank settlement date	Interbank settlement date	Execution date	Execution date	Execution date	Execution date
2b) Amount and currency	Origin currency	Origin currency	Origin currency	Origin currency	Origin currency	Origin currency	Origin currency	Origin currency	Origin currency	Origin currency	Origin currency
2c) MS of origin	BIN	BIN	IBAN	IBAN	IBAN	IBAN	IBAN	Account location	Card issuer code	Disbursement Partner country code	Disbursement partner country code
2d) Transaction ID	Acquirer reference (MC DE31 – VISA TC05)	Acquirer reference (MC DE31 – VISA TC05)	Own ID	Own ID	Own ID	Own ID	Own ID	Own ID	Own ID	Own ID	Own ID
2e) POS payments	MC DE 22 – VISA TC05	MC DE 22 – VISA TC05	NA	NA	NA	NA	NA	NA	NA	NA	NA

5 RULES FOR (RE)SUBMISSION

This section focuses on the rules applicable to the submission or resubmission of data from payment service providers to Member States, which could impact the transmission of data to CESOP. However, since the rules applicable to the collection of payment data at national level are not established in Directive 284/2020 or in Regulation 283/2020, apart for the Member States obligation to collect the payment data using the electronic standard form defined in the Annex to the Implementing Regulation and within the timeframe laid down in article 24b introduced by Regulation 283/2020, this section mainly lists best practices and recommendations to limit the impact that national resubmissions and errors during the national collection can have on the transmission to CESOP.

The sections below give an overview of what payment service providers can expect from the (re)submission process at the national level, i.e. guidelines that individual Member States are recommended to follow. These rules, however, should be read in conjunction with the relevant national legislation applicable in each Member State for the collection of payment data which can differ in some aspects.

5.1 Validation of the payment information at the national level

Payment service providers should validate the payment message prior to submitting it to the national tax administration in accordance with the Annex to the Implementing Regulation. This includes both a check of the XML Schema Definition ("XSD Schema") and a check of the business rules, to ensure that errors are caught as early as possible in the process.

When receiving the payment message, national tax administrations should validate the received payment data against the XSD schema. In case the XSD schema is not respected (negative validation result), the whole file will be rejected, and the payment service provider will have to resubmit the whole file. The validation message sent by the tax administration to the payment service provider will use the same XML schema as used by CESOP for the validation message.

In order to avoid impact of errors on the submission to CESOP, it is *recommended* that:

- The national tax administration immediately validates the received payment message against the XSD schema.
- The national tax administration immediately informs the payment service provider of the XSD schema validation result in case of a negative result.
- In case of a positive XSD schema validation, the national tax administration immediately forwards the payment information to CESOP.
- In case of a negative XSD schema validation, the validation result message lists all technical error codes, so that the payment service provider can correct them all at once.
- The national tax administration does not perform a validation of business rules. Business rules are checked at the CESOP level.

5.2 Validation of the payment information at the CESOP level

Once it receives the payment message from the national tax administration, CESOP will validate the payment data message against the XSD schema and the business rules described in the XSD User Guide. Normally, the XSD schema check should not show any errors at the CESOP level, since this check was already done at the national level. On the other hand, the check of the business rules might lead to a negative validation. It is thus possible that a payment data message passes validation by the Member State but is later negatively validated by CESOP. CESOP will send the validation result to the relevant

national tax administration, whether the validation result is positive or negative. Under no circumstances will the national Tax administration change the content of the payment data message.

In order to swiftly react to error in the transmission of data to CESOP, it is *recommended* that:

- The national tax administration forwards the validation result from CESOP to payment service providers in case of both positive and negative result.
- The national tax administration forwards the validation result from CESOP to payment service providers in case of both positive and negative result.

5.3 Resubmissions

In case of a negative validation result, the payment service provider must resubmit a payment data message with the correct data. If the negative validation is due to failing the XSD check at the national level, the payment service provider shall resubmit all the data for that quarter. This is due to the fact, CESOP will not have received any data yet from the payment service provider for that quarter, and therefore sending only corrections for certain specific payees will not be applicable.

Alternatively, when a payment service provider receives a negative validation result that came from CESOP, Member States should allow it to resubmit only data on the payees that are subject to corrections. Resubmitted payment data messages will go through the exact same process as the initial submissions.

In order to limit the impact resubmissions and corrections can have on the reporting to CESOP and availability of data in the system, it is *recommended* that:

- The national tax administration gives the payment service provider a time frame to resubmit the payment message.
- The time frame should not exceed 30 calendar days, starting from the date the validation message is sent by the Member State to the payment service provider.
- The national tax administration should send a notification about the resubmission to the payment service provider after half of the time frame provided by the national tax administration has passed.
- If the submission is not done before the end of the resubmission period, a notification should be sent to the payment service provider with a deadline to comply with the resubmission obligation.
- Each Member State should enact legislation that allows for the sanction of payment service providers who fail to submit or resubmit payment data within the given time frame.

These recommendations also apply in case a payment service provider does not submit any payment message before the submission deadline and in case a payment service provider submits data that is not in scope (e.g. a payment service provider sends data of payees that did not pass the threshold of 25 transactions). In the latter case, the notification should indicate what data should not have been transmitted and request its deletion from the resubmission. The submission of data under the threshold shall be considered as non-compliant with the rules established with article 243b and can be subject to sanctions.

In the case of late submission of payment data messages by payment service providers, they should be added to CESOP as soon as they are received and have successfully passed the validation check, since the data will be useful for the system. This however does not preclude Member States to apply sanctions for late-submission of the data.

5.4 Spontaneously correcting mistakes

Even though payment service providers must check the validity of the data they transmit with the XSD schema and the business rules, they might still send erroneous payment data to CESOP.

In this case, once payment service providers find out that they have sent erroneous data to CESOP, they can spontaneously send new files with the corrected data to the Member States in accordance with the rules laid down in the XSD User Guide.

There is no specific deadline for this in the EU legislation as it always important for CESOP to receive correct data. Nevertheless, spontaneous corrections should be sent before the expiry of the reporting period to which they refer, in order to avoid sanctions, and at the later before the end of the retention period for data in CESOP (5 years). After this period, correction will not be possible as the original data will be deleted.

6 FINAL REMARKS

These guidelines aim to provide practical information and explanations on the reporting of payment data by payment service providers and on their collection by Member States. They do not have legal value and only serve to explain the legal obligation without going against it.

The guidelines may be subject to changes and update in the future following the evolution of the payment market and the application of the reporting obligation.

Questions or comments about the guidelines can be sent to TAXUD-CESOP@ec.europa.eu.