The Second European Payment Services Directive (PSD2) and the Risks of Fraud and Money Laundering

Version 1.1
October, 2017

Authors:
I. Lammerts MSc CFE (ABN AMRO)
D. Ma MSc (ABN AMRO)
N. Ploeger MSc (ANTI MONEY LAUNDERING CENTRE)
Mr B.A. Deutekom (DUTCH PAYMENTS ASSOCIATION)
S.J. van Eerten MSc EMoC (DELOITTE)
N. Vink MSc (DE VOLKSBANK)
T.N. Wagemakers (FINANCIAL INTELLIGENCE UNIT)
K.I.M. Sanders MSc MA (KPMG)
C.L.S. Visser MSc (NATIONALE POLITIE / KNOOPPUNT FINEC)
R.B. Schaap MSc (NATIONALE POLITIE / TEAM HIGH TECH CRIME)

Disclaimer

This document is to introduce the revised European Payment Services Directive (PSD2) and related fraud and money laundering risks. It is based on input by the individual authors, written in a personal capacity and does not in any way represent the points of view and/or policies of the organisations they are connected with. Although the authors drew up this document with due care and made use of sources they considered to be reliable, they cannot guarantee it is fully correct, complete and up to date.

Contents

1. Introduction

1.1 Reason

In 2017, the Anti-Money Laundering Centre (AMLC) formed the topic group "money laundering via the Internet / new payments". The topic group is a group of cooperating parties originating from public, private and science domains. The topic group discusses expected and already identified money laundering risks. The objective is to identify common subjects which working groups and interested parties can further set out into concrete cooperation products. The first subject the topic group selected, is the second European Payment Services Directive (PSD2) that will come into effect in January 2018.

As a consequence of PSD2, banking institutions are to open their infrastructures to external service providers (TPP), a process that is called "access to the account" (XS2A). Although payment innovations are welcomed, the growing concern is that this provides criminals with possibilities to commit fraud and to launder money. In addition, PSD2 can also have certain implications for investigations. The topic group therefore formed a PSD2 working group in order to draw up a joint expert document. Members of this working group are ABN AMRO, AMLC, Dutch Payments Association, Deloitte, Financial Intelligence Unit (FIU), ING Bank, KPMG, National Police (Amsterdam Police Department, National FinEC hub and Team High Tech Crime) and de Volksbank.

1.2 Objective and scope

The key question the PSD2 working group considered was two-fold; in outline, what are *from Dutch perspective* the possible changes in the payment landscape as a consequence of PSD2 and what possible fraud and money laundering risks does the implementation of PSD2 entail?

This joint expert document was drawn up in order to internally inform the organisations participating in the PSD2 working group about the coming changes and the (possible) corresponding risks. Furthermore, the expert document and its conclusions and recommendations will be presented to the relevant supervisory institutions and parties that play a role in its implementation. It should be noted that terrorism financing is deliberately not mentioned in this document, as the focus of the topic group is not on this subject.

The contents of this report are based on developments until 1 September 2017.

1.3 Research questions

To be able to answer the key question, the PSD2 working group formulated the following research questions:

1. What is the objective of PSD2?
2. When and how should PSD2 be implemented?
3. Which new (payment) services are introduced in PSD2?
4. What new type of (payment) service providers are introduced in PSD2?
5. Which obligations do these new (payment) service providers have?
6. Which obligations do existing payment service providers have as soon as the new (payment) service providers become active?
7. What (risk) aspects of PSD2 have not (yet) been fully worked out and are subject to (national) interpretation?

8. What are the fraud and money laundering risks for banks and users of payment services as soon as PSD2 comes into force?
9. What are the consequences of PSD2 for investigations against fraud and money laundering?
10. What are the consequences of PSD2 for supervision when preventing fraud and money laundering?
11. What opportunities does PSD2 offer to banks, consumers, investigations and supervision in the fight against fraud and money laundering?

1.4 Research methods

To get the various research questions answered, the members of the PSD2 working group carried out literature study and approached several parties and found them willing to discuss the subject. For example, they had discussions with the Dutch Authority for Consumers & Markets (ACM), the Dutch Authority for Financial Markets, De Nederlandsche Bank (DNB) and the Dutch Bankers' Association (NVB). Also information on the subject was obtained from International Card Services (ICS) and the Ministry of Finance (MinFin). On 4 April 2017, a few members of the working group participated in a PSD2 event organised by the Dutch Payments Association and Holland FinTech. In order to discuss the progress, to spread the tasks and to discuss the contents of the expert document, the working group held several meetings.

Nb. If the report refers to "the investigation practice", it relates to the knowledge and experiences of members of the PSD2 working group that are actively involved in investigations.

1.5 Structure

After this introduction, chapter 2 discusses PSD2 and the (envisaged) changes. Subsequently, the PSD2 parts follow which play a role when fraud and money laundering risks are discussed. You will find these risks in chapter three. Chapter 4 concludes the expert document with conclusions and recommendations.

2. PSD2

2.1 Introduction

This chapter firstly pays attention to the objectives, extent and implementation of PSD2. Subsequently, the new payment services introduced in PSD2 are discussed and the extent to which the providers of these services come under supervision and anti-money laundering legislation. Finally, parts of PSD2 which still remain unclear and are subject to interpretation are discussed which, however, are relevant when discussing fraud and money laundering risks in chapter 3.

2.2. PSD2 Objectives

The objectives of PSD2 are: *"Firstly, strengthening internal markets for card payments, Internet payments and mobile payments. Secondly, innovation stimulation and facilitation, for example by regulating various payment services that came into being after publishing PSD I, such as the mentioned payment initiation services and account information services. The final objective of PSD II is to remedy indicated PSD I problems such as outdated or vague terms. In general, a balance is sought between innovation stimulation on the one hand and safety and consumer protection on the other hand"*[1].

2.3 RTS on SCA

The *Regulatory Technical Standards on strong customer authentication and secure communication under PSD2* (RTS on SCA) include provisions regarding the authentication process of transactions and security of the communication channel[2]. The RTS on SCA can be considered the technical PSD2 framework and were drawn up by the *European Banking Authority* (EBA)[3]. When writing this expert report, the RTS on SCA is a concept and the European Commission still needs to present a final version to the European Parliament and the Council for approval. At political level there is no consensus yet whether access as a result of the RTS on SCA is only allowed via an *Application Programming Interface* (API), as the draft now provides for, or that *direct access* should also be allowed to account service providers, in particular banking institutions, to fall back on in case API is out of operation. With *direct access* the user of payment services logs in himself via the on-line portal of his payment account, a working method that is also called *screen scraping*. However, in respect of PSD2 these are not synonyms. PSD2 requires that for each transaction the TPP identifies itself to ASPSP, this is mentioned among others in Article 66, paragraph 3d. PSD2 does not allow that TPPs log-in under the names of users of payment services, which is the case with *screen scraping*. The contents of the RTS on SCA regarding certain subjects can still change the coming period. After approval by the European Parliament and Council it will take 18 more months, before the RTS on SCA come into force.

[1] Ministerie van Financiën & Ministerie van Veiligheid en Justitie (2016). *Memorie van toelichting op de implementatiewet herziene richtlijn betaaldiensten*. Den Haag.
[2] These subjects will be further dealt with in paragraphs 2.8 and 2.9 of this expert report.
[3] In respect of PSD2, EBA will draw up five RTSs and five guidelines.

2.4 Scope

Compared to its predecessor, the scope of PSD2 is extended regarding two items. The first European Payment Services Directive (PSD1) introduced supervision on payment service providers as far as the payment service providers involved in the payment transaction are both established in an EU Member State, and as far as the payment service providers carry out transactions using a Member State's currency. Payment service providers that come under PSD2 need licences for being payment institutions if they carry out payment services as their profession or business. The following situations fall within the scope of PSD2:

- Transactions at which only one of the two payment service providers is established in an EU Member State; and
- Payment services in any currency as far as they are performed within the EU[4].

There are also exceptions to the scope of the Directive which are mentioned in Article 3 of the Directive (2015/2366). The explanatory memorandum regarding the PSD2 implementation into Dutch law mentions the three main exceptions[5]:

1. Small, limited networks do not fall within the scope of PSD2. A limited network is held to mean that a payment service can only be used in the specific circumstances mentioned in the Directive's preamble. Limited networks that are making use of the exemption are required to report this to DNB[6].
2. The limitation regarding payment services performed via telecom equipment or networks, is defined more strictly[7]. Payment transactions connected with raising money for charitable institutions and payment transactions below a certain statutory threshold, are excluded from the PSD2 scope[8]. If any of the mentioned exceptions is made use of, it is required to report this to DNB.
3. The restriction regarding business agents is adjusted. Agents who act only on behalf of the payer or the recipient are excepted from the scope of PSD2, regardless of whether they have the money of their clients. Agents who act on behalf of both the payer and the recipient are only excepted if they do not have, or do not have control of their clients' money at any moment[9] [10].

2.5 Implementation

The Directive is based on full harmonization, which means that Member States are not allowed to swerve away from what is required in the Directive. So, the Member States cannot set higher requirements either. Countries in the European Economic Area (EEA) are required to have implemented the Directive in national legislation not later than 13 January 2018. In the Netherlands implementation will take place through the Financial Supervision Act (Wft) and book 7 of the Civil Code (Bw).

---

[4] Article 2 of PSD2.
[5] Ministerie van Financiën & Ministerie van Veiligheid en Justitie (2016). *Memorie van toelichting op de implementatiewet herziene richtlijn betaaldiensten*. Den Haag.
[6] Recital 13 of PSD2.
[7] Recital 16 of PSD2.
[8] Recital 16 of PSD2.
[9] Recital 11 of PSD2.
[10] Ministerie van Financiën & Ministerie van Veiligheid en Justitie (2016). *Memorie van toelichting op de implementatiewet herziene richtlijn betaaldiensten*. Den Haag.

As a consequence of PSD1 part 7B of Book 7 includes sections of law on the execution, assent and liability of a payment transaction[11]. The official consultation round has been closed by now, but the legislative proposal must still be submitted to the Parliament in the Netherlands. As mentioned earlier, the entry into force of the RTS on SCA by the European Parliament and the European Council – will take at least 18 months after approval. PSD2 includes a number of new licence requirements for payment institutions, which in the Netherlands are regulated by order in council. In practice, as from 18 January 2018 banks must provide third parties - as much as possible according to the RTS on SCA - with access to the payment accounts of their clients, if the clients have given their expressive consent. In this period, DNB will monitor whether the authentication and security proceedings of TPPs which want to have access, are up to standard. It is, however, unknown how DNB will publish the results.

2.6 New payment services

2.6.1 AISP & PISP

PSD2 introduces two new types of payment services and payment service providers (PSP); namely the payment initiation service provider (PISP) and the account information service provider (AISP)[12].

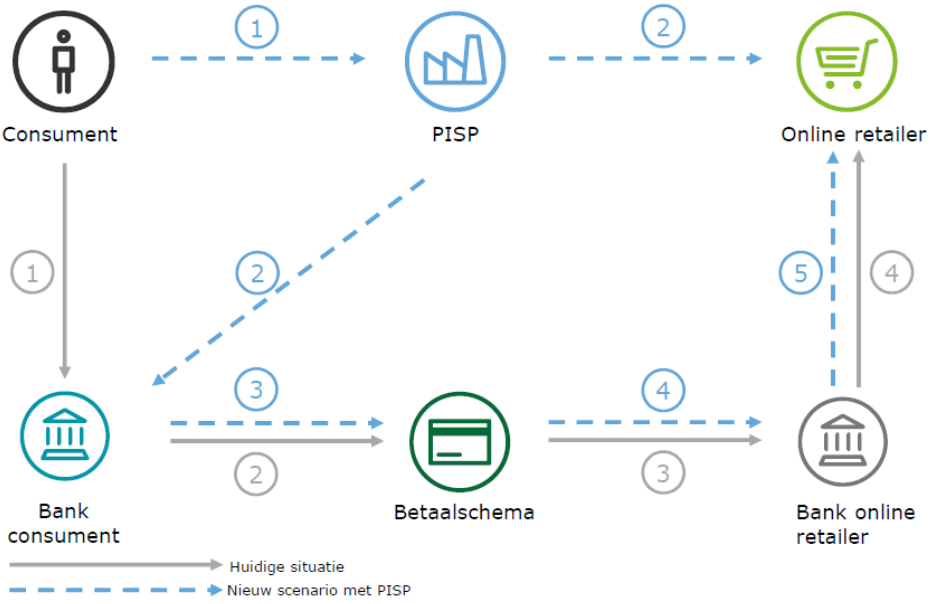

Figure 1. Diagram of payment service PISP.

On the instructions of an user, a PISP can make payments, for example when purchasing a product in a web shop. The user can authorise a PISP for obtaining access to his payment account with *another* payment service provider, such as a bank.

The subject "access to payment accounts" is dealt with in paragraph 2.7. Not at any moment is a PISP allowed to come into possession of the funds of the payment services user[13]. Businesses that offer products and services to consumers, will have the possibility, through PSD2, to integrate the payments

[11] Act of 15 October 2009 for the amendment of the Financial Supervision Act, the Civil Code and Money Service Businesses Act, and repeal of the Cross-Border Payments Act for the implementation of Directive no. 2007/64/EC of the European Parliament and the Council concerning payment services on the internal market and the amendment of the Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC, and repeal of Directive 97/5/EC (PbEUL319).

[12] Article 4 of PSD2.

[13] Article 66, paragraph 3a of PSD2.

into the overall user experience. For example, a client card or a shop's mobile App, in which payment details, discounts and loyalty points are combined and the client can automatically pay wireless when leaving the shop.

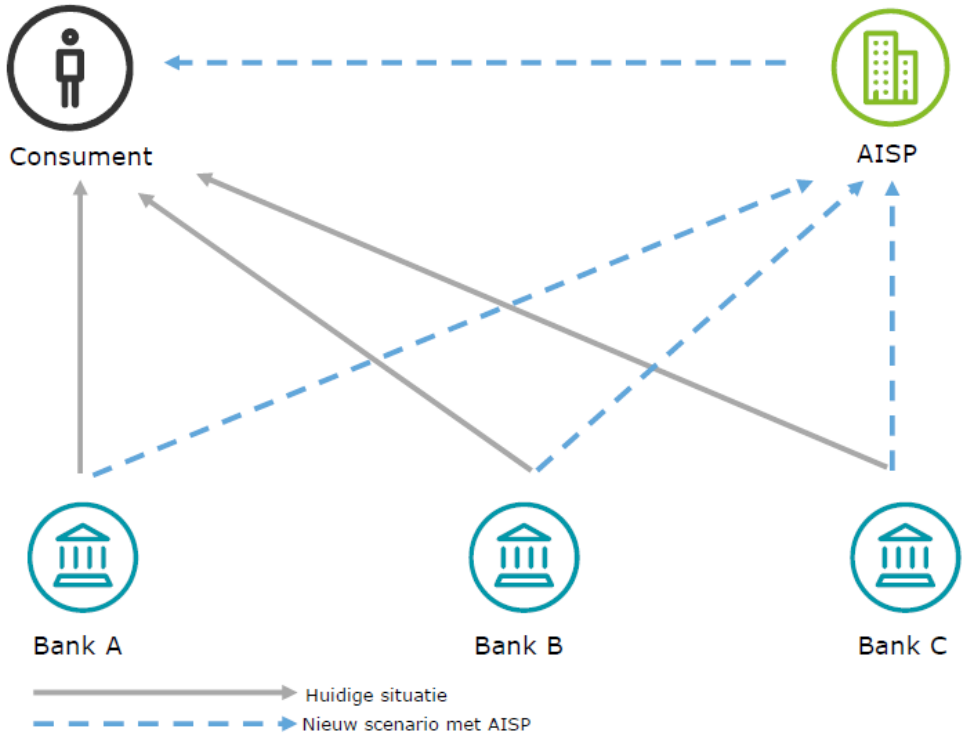

Figure 2. Diagram of payment service AISP.

A precursor of account information services is AFAS Personal, an on-line housekeeping book by which one can (graphically) obtain insight into expenditures, and budgets and estimates can be prepared. On the instructions of an user, an AISP can provide consolidated information, originating from one or more payment accounts with one or more ASPSPs. However, AISPs may not request sensitive payment information[14]; this information is susceptible to fraud, for example through personal security details[15]. By the way, providing financial advice does not come under the licence of an account information service.

2.6.2 Market access and supervision

Being payment institutions, PISPs are obliged to have licences, and fall under the DNB's risk based integrity supervision. In addition, PISPs can also make use of the so-called EU Passport, with which it is possible, if a Member State has granted a licence, to also provide services in other Member States. Although AISPs also fall under the scope of the category payment institutions and can make use of EU Passports, they only have to comply with part of the obligations[16]. Also, DNB will conduct only a mild form of integrity supervision.

[14] Article 67, paragraph 2e of PSD2.
[15] Article 4, paragraph 1, under 32 of PSD2.
[16] Article 33, paragraph 2 of PSD2.

When payment institutions apply for licences, a number of requirements have to be fulfilled, including descriptions of:

- a business plan with budget prognostications for the next three financial years;
- proof of the initial capital;
- a guarantee or insurance as security for the funds of its users;
- complaints and security incident procedures;
- a security policy, among other things for protecting its users against fraud and illegal use of (personal) data;
- (if applicable) internal control mechanisms to comply with the obligations following from the European Anti-Money Laundering legislation;
- the identity of managers and directors, as well as proof that they are reliable and competent[17].

Contrary to PSD1, PSD2 includes as extra licence demand that payment institutions can only be established in a Member State if at least a substantial part of the activities are actually performed in this Member State[18]. This so-called substance demand is not set out in more detail in PSD2. When applying for licences, directors are screened by DNB for their liability[19] and eligibility[20]. Directors are not obliged to have the nationality of the country of establishment. Compared to PSD1, PSD2 widens the scope of cancelling licences; namely in the case that confidence in funds transfers is at stake or if the supervisor is not informed of important developments relating to licence conditions[21].

In the Netherlands, apart from the DNB[22] also other supervisory authorities play a role in the supervision of payment institutions, namely the ACM[23], AFM[24] and the Dutch Data Protection Authority[25]. In addition to competition regulation, ACM also is the supervisory authority for access to payment systems and the access of TPPs to account services of credit institutions[26]. The market conduct supervision of AFM is aimed at fair and transparent financial market procedures, clean relations among market parties, and the due care of both payment service providers and users of payment services. It appears that the supervisory tasks of ACM, AFM and DNB overlap regarding the subjects market access, the conduct of payment service providers towards the payment service users and fraud incidents. For money laundering incidents, DNB will be the designated supervisory authority. The Dutch Data Protection Authority supervises the usage and processing of personal details. In addition, DNB supervises the rules mentioned in PSD2 regarding data protection in respect of the issue of licences and ongoing supervision[27]. At an European level, EBA is the supervisory authority for PSD2 compliance.

[17] Article 5, paragraph 1 of PSD2.
[18] Article 11, paragraph 3 of PSD2.
[19] Article 5, paragraph 1, under n of PSD2.
[20] Article 5, paragraph 1, under m of PSD2.
[21] Article13, paragraph 1 under c and d of PSD2.
[22] Section 1:24, paragraph 2 of the Financial Supervision Act.
[23] Section 1:25a of the Financial Supervision Act.
[24] Section 1:25, paragraph 2 of the Financial Supervision Act.
[25] This is now on the basis of the Personal Data Protection Act, on 25 May 2018 on the basis of the General Data Protection Regulation (AVG) and Section 6, paragraph 2 of the Implementation Act General Data Protection Regulation.
[26] Article 36 of PSD2.
[27] Ministry of Finance & Ministry of Security and Justice (2016). Explanatory memorandum of the Amended Payment Services Directive Implementation Act. The Hague, page 8

2.7 Definition of payment account

PSD2 does not strictly define the term payment account. Payment accounts have to be available online so that AISPs and PISPs can consult them[28]. For the time being it concerns accounts in legally recognised currencies, of which the balance is really disposable: *"an account held in the name of one or more payment service users that is used for making payment transactions"*[29]. The scope of the term payment account applied in PSD2 seems similar to the definition mentioned in the European Payment Account Directive published in 2014 (2014/92/EU):

> *"payment accounts with which consumers can at least:*
> *a) transfer funds into a payment account;*
> *b) can make cash withdrawals from a payment account;*
> *c) can receive or make payment transactions, including transfers from and to third parties.*
> *The Member States may decide to apply all provisions of this Directive or part of it to other payment accounts than referred to in the first paragraph."*

Although initially one thinks of payment and (some) savings accounts with banks, the definition provides space to payment accounts operated by other institutions, such as providers of (prepaid)credit cards and e-money accounts that can be used for making payments to third parties. The European Commission's opinion on this is unclear.

2.8 Access to payment accounts

As mentioned, PSD2 introduces access to payment accounts for AISPs and PISPs. AISPs provide services that users of payment services explicit consent to[30] and have merely access to the information regarding the designated payment accounts and the concerned payment transactions[31]. PSD2 does not give any rules for which information must be shared and whether historical data also come under this. Clarity on this will determine the future provision of services. PSD2 provides possibilities for PISPs to initiate payments at the request of the account holders[32]. PISPs may not come into possession of the funds of the users of the payment services[33]. Neither may they store any sensitive payment details[34]. Full access to client accounts with ASPSPs is not allowed.

ASPSPs may deny access to the payment account if there are objective suspicions of fraudulent access to the payment account[35]. According to the draft RTS on SCA, access to the payment account must come into being through API. The concerned payment service providers are required to facilitate this. No rules exist about the uniformity of APIs, for example how it should be developed or implemented. Each ASPSP has to work this out itself. There is the requirement that APIs must offer the same level of availability and performance as the surroundings the holder of the payment account is using[36]. However, ASPSPs are subject to the obligation to investigate before granting TPPs access to API. XS2A is a right of the payment account holder and concerns an agreement between the payment account holder and the TPP. The provision of payment initiation services and account information services may

[28] Article 66, paragraph 1, and article 67, paragraph 1 of PSD2.
[29] Article 4, under 12 of PSD2.
[30] Article 67, paragraph 2, under a of PSD2.
[31] Article 67, paragraph 2, under d of PSD2.
[32] Article 66, paragraph 1 of PSD2.
[33] Article 66, paragraph 3, under a of PSD2.
[34] Article 66, paragraph 3, under e of PSD2.
[35] Article 68, paragraph 5 of PSD2.
[36] Article 32, paragraph 1 of the draft RTS on SCA (EBA/RTS/2017/02).

not depend on agreements between ASPSPs and TPPs[37]. For disputes on these matters, AFM is the supervisory authority. As mentioned in paragraph 2.3 about the RTS on SCA, at an European level discussions are held now whether and under what circumstances *direct access* is granted as alternative option if API is out of operation.

2.9 Strong client authentication

Although the RTS on SCA will not yet be in force on 13 January 2018, as from this date payment service providers are required to apply SCA in conformity with Article 97 of PSD2. The authentication of a payment order should also contain elements that, in the case of a transaction, dynamically link the transaction with a specific amount and specific beneficiary. Until the moment that the RTS on SCA has come into force, 18 months after approval by the European Parliament and the European Council, SCA has to be applied as much as possible in accordance with the spirit of the RTS on SCA. Authentication is described as a procedure by which payment service providers can verify the identity of a payment service user or the validity of the use of a specific payment instrument. This includes the use of the personal security details of the payment service user[38]. This verification will be done through the so-called SCA. For strong authentication at least two of the following factors are used:

1. Knowledge (something only the user knows)
2. Possession (something only the user has in possession)
3. Inherent characteristic (something the user is)[39].

These characteristics should each be independent, so that compromise of one of these factors cannot harm the liability of the other factors and the confidentiality of the authentication details are protected[40]. Examples of knowledge are passwords, PIN codes or drawing patterns (like when unlocking a mobile phone). By possession is referred to something with which a code can be generated. For example, this could be a telephone on which an authentication code is received via text message or a mobile application. It could also be a device which shows a code when pushing a button. A code can also be based on time; a device generates a new code every thirty or sixty seconds, because the previous code is no longer valid. To conclude, a device can also have an integrated keyboard on which the user first has to type a code before the device will generate a new code; this concerns the combination of possession and knowledge in one code. Examples of inherent characteristics are fingerprints, iris scan, voice recording and facial recognition. For this extra hardware might be required.

Regarding the question who will apply the SCA, there are two possible scenarios. The first scenario is that the PISP leaves the SCA up to the ASPSP and that for this the *credentials* issued by the ASPSP are used. The PISP can also choose to issue *credentials* itself and to apply SCA. When a payment service user denies that he or she approved a payment transaction or states this was not executed correctly, the payment service provider must present proof that the payment transaction was authenticated, properly registered and booked, and that no technical or other failure of the service provided by the payment service provider took place[41]. In principle, in case of an incident the payment service user will first contact the ASPSP of his payment account. Next, the payment service user can claim financial

[37] Article 66, paragraph 5 and article 66, paragraph 5 of PSD2.
[38] Article 4, par. 29 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market (PbEU 2015, L337/58)
[39] Article 4, paragraph 1 of the concept RTS on SCA (EBA/RTS/2017/02).
[40] Article 4, paragraph 30 of PSD2.
[41] Article 72, paragraph 1 of PSD2.

compensation if the payment service provider of this payment service user does not require SCA (unless it concerns a fraudulent act)[42]. If an ASPSP's liability can be attributed to another payment service provider or an intermediary, then the TPP or intermediary will compensate the ASPSP for all losses suffered, including compensation when one of the payment service providers does not apply SCA[43]. After all, the national supervisory authorities must make sure that payment service providers apply strong client authentication when a payment service user logs into his on line payment account, initiates an electronic payment transaction or carries out a transaction via a communication means which can entail the risk of payment fraud or other forms of abuse[44].

Only under strict conditions may PSPs leave out SCA. A concept playing a role here is transaction risk analysis (TRA). If PSPs want to rely on applying more flexible authentication methods for low-risk transactions, they should comply with a few conditions:

- For transactions amounting over 500 Euro SCA is always required, irrespective of the fraud ratio;
- in most cases the maximum amount is less, depending on the specific instrument used. The EBA has defined fraud ratios for each instrument, and only in case that the fraud ratios for a certain instrument are lower than the benchmark fraud ratios set by the EBA, can a transaction be carried out without SCA;
- this means that all PSPs must register fraud ratios and also make TRA transparent, which must be audited periodically.

2.10 Processing (personal) data

Article 94, par. 1 of the PSD2 indicates that payment service providers may process personal data when necessary to safeguard the prevention, investigation and detection of payment fraud. Individuals must be informed about the processing in accordance with the Data Protection Directive (Directive 95/46/EC), which has been converted into the Personal Data Protection Act (Wbp) in the Netherlands. This guideline, however, will be repealed on 25 May 2018. It is replaced by the General Data Protection Regulation (GDPR) – called the *Algemene Verordening Gegevensbescherming (AVG)* in the Netherlands – which has a direct European effect and, therefore, does not have to be implemented separately in Dutch legislation.

Article 94, par. 2 of the PSD2 also states that payment service providers shall only access, process and retain personal data necessary for the provision of their payment services, with the explicit consent of the payment service. Although explicit consent is required, both the PSD2 itself and the so-called explanatory notes do not provide any further explanation about how this explicit consent should be given or recorded[45].

[42] Article 74, paragraph 2 of PSD2.

[43] Article 92, paragraph 1 and article 74, paragraph 2 of PSD2.

[44] Article 97, paragraph 1 and article 74, paragraph 2 of PSD2.

[45] Voerman, A. (2017). *The implementation of PSD2 in the Netherlands*. Payments & Fintech Lawyer, p.11.

3. Fraud and money laundering risks

3.1 Introduction

The starting point of the PSD2 in which a third party is given access to the payment account, has implications for the protection of customer data, secure payment and the integrity of payments. This is why some risks are associated with the introduction of the PSD2, that are discussed in this chapter. Although there is some overlapping, the risks are divided in:

- fraud risks;
- money laundering risks;
- supervision and investigation risks.

Some comments are to be made here in advance. First of all, the interpretation of the PSD2 and its implementation in national regulations is not entirely clear yet. In addition, it is not yet known what (new) mitigating measures will be introduced by payment institutions and what positive effect supervision will have on limiting the risks. This means that the risks described below are initially of a *theoretical* nature and that nothing can be said in advance about the extent to which these risks will actually take place.

3.2 PDS2 and fraud risks

3.2.1 Unreliable and criminal TPPs

The entry into force of the PSD2 may lead to an increase in (foreign) TPPs, that are active on the Dutch payment market. It is assumed that the majority of them will be in good faith and will act in accordance with the regulations. A scenario that should be taken into account is that the payment industry can also be confronted with unreliable and criminal TPPs.

ASPSPs are obliged to allow TPPs access to the payment account, with the explicit consent of the payment service user. The question is, however, whether ASPSPs and consumers can sufficiently assess the reliability of TPPs and the offered payment infrastructure. If *direct access* is allowed, the ASPSP is also unable to verify if the TPP actually executes the transaction in accordance with the wishes of the payment service user.

Furthermore, two other risks should be mentioned. Malicious persons who aim to commit large-scale (identity) fraud, can set up a TPP themselves to facilitate fraudulent payments and/or to get access to a large amount of confidential information. As mentioned in chapter 2, AISPs are also faced with a milder form of integrity supervision. The set-up of a 'criminal TPP' seems to be a less likely scenario for small-scale fraud, as there are simpler ways to commit fraud. (Cyber) criminals using an existing TPP, e.g. by infecting it with malware, presents a bigger risk.

Consumers may get into contact with these fraudulent TPPs e.g. by entering their details on fake websites or mobile payment apps; a method of working that is not (very) different from *phishing*. The criminal can then use this information to access information about the consumer and/or to make payments in the name of this consumer (see also paragraph 3.2.2). It is unclear which detection systems are currently able and/or designed to recognise this type of fraud patterns and tackle them (see also paragraph 3.2.3). It is attractive for criminals to operate in countries with a mild 'supervision climate'.

Innovative payment apps are increasingly used in online payment transactions. There is a risk that criminals may design payment apps that are aimed at facilitating fraudulent transactions and/or stealing confidential information.

3.2.2 Misuse and phishing of data

The risks described in this subparagraph are risks that also apply to the current payment industry. The PSD2 working group states that the PSD2 affects the current risks to such an extent, that these risks are therefore discussed in this expert report.

In the case that direct access is allowed as fallback option, it is possible that consumers are invited to provide personal data and login details to TPPs under certain circumstances. ASPSPs, however, have advised their customers for many years now not to provide confidential (login) details to third parties, to prevent them becoming victims of fraud. It is becoming confusing for consumers in which cases, to whom and on which websites or payment apps they can or cannot provide confidential (login) details; after all, (vulnerable groups of) consumers are not able to verify if the API of their ASPSP is actually not sufficiently reachable and/or if the offered payment infrastructure and the TPP are reliable.

It is also questionable if consumers are aware of what exactly they give their consent to and what the consequences could be. In addition, there is a risk that TPPs processing data of payment service users become victim of cyber-attacks, resulting in data leaks. The data can then be used by criminals (for personal gain) or can be sold to third parties. Although this problem initially concerns the data protection of TPPs, ASPSPs can suffer reputational damage as a result of this.

As mentioned above, AISPs are faced with a milder form of integrity supervision than other payment service providers, which also means risks in relation to the misuse of data. In addition it is questionable whether payment service users are aware of what data TPPs are allowed to process for them. There is a risk that sensitive data is shared with malicious parties.

It is expected that criminals also build websites or payment apps to present themselves as a PISP and/or introduce false screens that appear to be identical to those of the login interface of the ASPSP or TPP, depending on who carries out the SCA, in order to gain access to confidential data of the payment service user. In the absence of a real TPP, the ASPSP (or the customer) will be held liable for the damage.

ASPSPs must inform their customers about the new conditions two months before the PSD2 comes into force. There is a risk that criminals will send phishing mails in this period to cheat payment service users out of confidential data. If a fraudulent TPP also cheats consumers out of Citizen service numbers, the risk of (identity) fraud is substantial.

3.2.3 Reduced fraud detection

The PSD2 opens the payment market for new entrants, who may not have gained any experience with compliance and fraud detection yet. The payment chain will also change and the PSD2 working group expects an increase in international transactions. This may affect the quality and effectiveness of fraud detection. ASPSPs must adapt their current detection systems to the changes in the payment chain. It may take some time to write new detection rules that (can) sufficiently anticipate possible unusual transactions via PISPs.

At the moment there is a growing trend to accelerate payment transactions via *instant payments*, which also makes an accelerated cash-out possible. The importance of adequate fraud detection in relation to ASPSPs, therefore, increases. The risk that fraud transactions are conducted successfully gets bigger. Moreover, it is still unclear how detection systems in relation to PISPs will be organised; this still seems to be insufficiently described in the PSD2. Are PISPs able in the future to detect fraudulent transactions, for instance as a result of phishing or malware?

A point of concern is to what extent the information position of the ASPSPs may be limited by the arrival of PISPs. If SCA takes place via the PISP, the ASPSP may no longer have the disposal of information about the location and/or the device that is used to login. This would mean that it not only takes longer before the detection systems are adapted to the new payment chain, but also that these systems will be less effective. The ASPSP, however, will have the disposal of additional information that relates to the TPPs authorised by the customer.

Under certain circumstances PSPs do not have to apply SCA. If SCA is not applied, the risk of fraud will be higher. In that case PSPs are obliged to keep fraud ratios as well as a transparent TRA. Crucial in this respect is to what extent PSPs are able to do this and to what extent auditing or supervision will be sufficient to identify possible shortcomings. The PSPs themselves are responsible for setting up a robust SCA process. PSD2 includes clauses that hold PSPs liable for unlawful transactions that take place as a result of inadequate authentication. In that sense there is a positive incentive for PSPs to set up an adequate authentication. Articles 73 and 74 of the PSD2 are about liability of the payment service provider and the consumer's own risk in relation to unauthorised transactions. The ASPSP will have to immediately compensate the customer in case of unauthorised transactions, unless it appears that fraud was committed. This payment service provider, for instance the bank, can seek recovery from the PISP if it can be held responsible. This is the case if it cannot account for the SCA (not executed or not executed demonstrably) or if there seems to be a technical failure. Although the burden of proof falls on the PISP, in practice the risk and possible reputational damage mainly hits the ASPSP. The PSD2 reduces the payment service user's own risk in case of damages as a result of misuse from €150 to €50.

The PSD2, however, also offers an opportunity; in future, transactions involving a TPP will have an extra possibility for fraud detection. The possibilities to combat fraud could be given a boost, provided that TPPs set up sufficient fraud detection.

3.3 PDS2 and money laundering risks

3.3.1 Introduction

Payment institutions must fulfil the obligations resulting from the Money Laundering and Terrorist Financing (Prevention) Act (Wwft). This also means that AISPs and PISPs must also provide for procedures on behalf of customer screening and reporting unusual transactions. Based on the Wwft, FIU Netherlands is the organisation where several institutions with a legal duty to report should report (intended) unusual transactions. The FIU investigates whether transactions and flows of money are (perhaps) related to money laundering, terrorist financing or underlying criminal offences. After transactions have been declared suspicious by the head of FIU Netherlands, they are put at the disposal of various enforcement and investigation services. In addition, investigation services can ask information from FIU Netherlands if there is a suspicion of a criminal offence.

At the moment, the fourth European anti-money laundering directive is being implemented in the Netherlands, that came into force on 26 June 2017[46]. The most important changes for payment service providers and payment institutions are:

- an extension of the risk-based approach of the obligations of the Wwft, that is expressed -for instance- in the obligation for institutions to set up a risk analysis;
- changes in the obligations of customer screening;
- an extension of the supervising authority's enforcement instruments;
- the introduction of publication rights for the supervising authority with regard to imposed administrative measures and sanctions;
- as a result of the directive FIUs are given more powers to promote the international exchange of information and cooperation between the FIUs.

In addition, negotiations are taking place about the directive proposal to change the fourth anti-money laundering directive, that was published by the European Commission in the summer of 2016[47]. For payment service providers and payment institutions that come within the scope of the PSD2, a number of elements of the directive proposal is especially relevant. It is proposed, for instance, to:

- extend the scope of the fourth anti-money laundering directive to platforms for exchanging virtual currencies and wallet providers;
- extend the obligations regarding customer screening in case of electronic money;
- harmonise the customer screening measures regarding 'risky third countries';
- oblige member states to set up a central register with information from bank account holders.

The changes provided for in this directive proposal will be implemented in Dutch legislation and regulations by means of a separate legislative procedure once the directive has been determined.

3.3.2 Unreliable and criminal TPPs

As mentioned in the previous paragraph, the introduction of the PSD2 is expected to lead to an increase of (foreign) TPPs on the Dutch payment market. As far as AISPs are concerned there do not seem to be any direct money laundering risks beforehand; after all, it is not possible to conduct transactions via these service providers. PISPs, however, may present a risk. For instance, a criminal PISP can conduct *automated* transactions via APIs, using various payment accounts with various ASPSPs (see figure 3, situation A). As the trail becomes longer it becomes more difficult to trace the actual provenance of the money and more time-consuming for (e.g.) the investigation services to follow the flows of money (see also paragraph 3.4).

[46] See also: https://www.internetconsultatie.nl/implementatiewetvierdeantiwitwasrichtlijn , consulted on 16 August 2017.
[47] See also: http://ec.europa.eu/justice/newsroom/criminal/news/160705_en.htm , consulted on 16 August 2017.

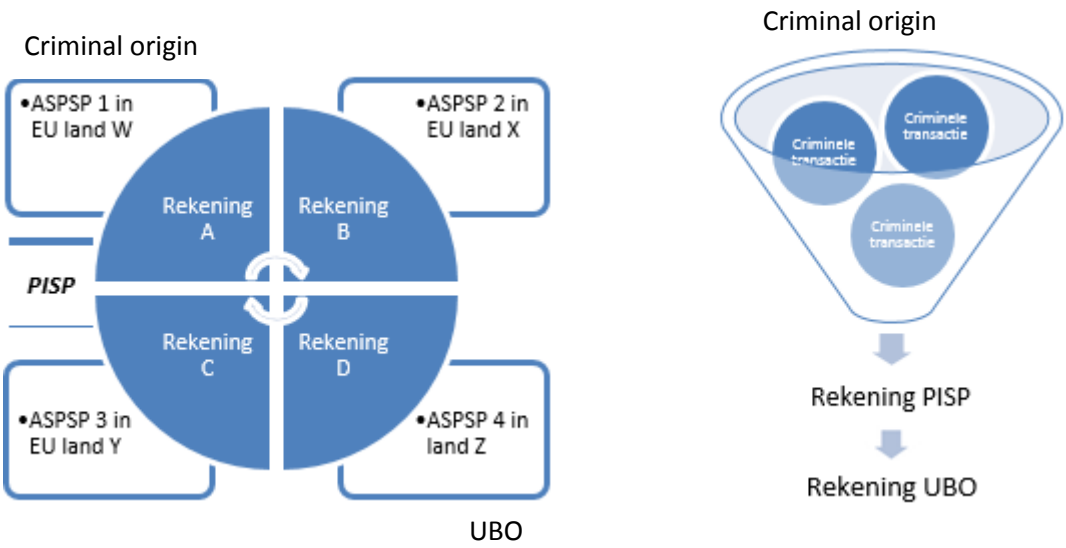

Figure 3. Automated payments via payment accounts (situation A) & concealment of UBO by PISP (situation B).

Often an additional document such as a contract, invoice or other agreement is required to legitimise the flow of money, depending on the source and the destination of the money. Criminals who own criminal assets on open loop prepaid cards[48], can pay for fictitious goods or services via (e.g.) their own company, after which the money is moved to one or more payment accounts abroad via the PISP. In principle, the beneficiary of these payments cannot be concealed by the PISP, because a PISP, contrary to a collecting PSP, may not gain possession of the payment service user's funds. Moreover, the ASPSP must know what the contra account is, otherwise the funds cannot be transferred. The exception to this is the case in which if a criminal PISP provides an 'own' account number, receives the money and then transfers it to the ultimate beneficiary (see figure 3, situation B). The ASPSP probably cannot establish that it concerns an own payment account of the PISP and will, therefore, conduct the transaction.
Investigation procedures show that supervision up to transaction level is not an automatic process; in the past few years the FIOD and the National Police have conducted various money laundering investigations in which a financial institution in the Netherlands was involved (as a suspect) in money laundering transactions over a longer period of time.

3.3.3 Increase in international (money laundering) transactions and inefficient reporting chain
The entry into force of the PSD2 will probably (in due course) lead to an increase in the number of international transactions in on-line payments and the number of international payment options. This makes it easier to use concealed assets[49] abroad for payments in the Netherlands. In addition, PISPs with complex international flows of money may facilitate money laundering, either intentionally (in the case of a criminal PISP) or unintentionally. The reporting chain, therefore, is not only fragmented across various parties but also across various countries. Experience teaches us that institutions and companies that are under an obligation to report, sometimes find it difficult to recognise possible

[48] These are cards connected to the MasterCard or VISA network. A prepaid card is linked to an account into which money has to be paid first. Depending on the provider this can be done with cash or bank money, but also with all kinds of other payment methods that can be used on the Internet.
[49] Assets that are not declared to the tax administration and/or have a criminal provenance and that are concealed from the authorities.

money laundering transactions; criminal investigations show that transactions that should have been reported, remained unreported.
As customer contact becomes more and more digital and direct customer contact (face to face) decreases, the know your customer (KYC) processes for banks also change and the parties involved must adjust their money laundering detection systems accordingly.

Classifying TPPs on behalf of the determination of risk indicators can be a challenge for ASPSPs. Large well-known (on-line) stores that have a licence, e.g. as a PISP, are unlikely to present an increased risk, but a (foreign) company dealing in virtual currencies perhaps does. If it is not entirely clear to an ASPSP what kind of service a PISP offers, this may cause problems.

Payment service providers report unusual or suspicious transactions in the country where they are established. Unusual transactions, however, are not automatically shared with FIUs in other countries. Suspicious transactions are not shared with an FIU in another country until there is a *hit* with a subject from a criminal investigation. Subsequently a request for legal assistance is required to be able to use the information in a criminal investigation. The fourth European anti-money laundering directive offers more opportunities for international cooperation and exchange of information between FIUs. In practice it will turn out whether this is sufficient to gain insight into dubious international transactions of Dutch citizens via foreign TPPs.

It should be noted that the introduction of TPPs, especially AISPs, may also offer advantages in the fight against money laundering. For instance, AISPs may have valuable information about insight into (unexplainable) assets and the reporting of unusual transactions.

3.4 Supervision and investigation risks

The supervision of payment service providers involves several supervising authorities; in the Netherlands they are the AP, the ACM, the AFM and DNB. The supervising authorities should work together on a national basis in order to control the implementation of the PSD2. There are also challenges from an international perspective. For instance, non-residents can start a TPP in the Netherlands. In that case the DNB will have to screen the directors for reliability and suitability. For this purpose the Dutch supervising authority is dependent on information supplied by foreign supervising authorities. Another question is to what extent European supervision is converged and whether EU countries regulate and enforce in a uniform manner. As already mentioned, the PSD2 working group expects an increase in international transactions via PSPs. A consequence could be that foreign PSPs will be playing a more important role on the Dutch payment market. The extent to which supervision presents a risk, partly relates to the level of stringency and susceptibility to fraud of the process through which a PSP can be set up and the extent to which the business operations are audited.

For entities who wish to conceal assets abroad it will become easier to use these assets for regular payments in the Netherlands. If PSPs are used the tax authorities will not be able to recognise these transactions quickly. Having a Dutch bank account appears to become less important in order to be able to participate in regular payment transactions. This makes the PSD2 a challenge also from a fiscal perspective.

The PSD2 will also represent a challenge for the investigation services. It is already labour-intensive, complex and time-consuming to follow international payment transactions; this will only increase due to the PSD2. Investigations show that criminals use foreign payment accounts, foreign PSPs and complex money laundering structures. Without additional possibilities for investigation services to order (quick) disclosure of information by foreign parties, the PSD2 may lead to major problems. Consideration should also be given to automated transactions via APIs. Investigation practice shows that handling an international request for legal assistance sometimes can take months. In addition, the penalisation of money laundering varies in the European countries, which may act as a barrier in international criminal investigations. In some cases the introduction of TPPs can also be an added value for criminal investigations; after all, these parties can be an important source of information concerning the subject of an investigation. It is also possible to find out quickly at which ASPSP there may be assets available that can be attached.

Soon the PSD2 will apply to all payments to and from the EU. This means that payments to countries outside the EU will be monitored more closely as the transactions must comply with European regulations. The PSD2 also leads to a further harmonisation of the fight against fraud and data security. In due course this may also provide opportunities for criminal investigations.

4. Conclusions and recommendations

4.1 Conclusions

The European payment landscape will develop further as a result of the PSD2. In due course the new payment services will undoubtedly lead to a larger variety of (new) providers of payment products. At the moment discussions are taking place on a European level about a number of elements of the RTS on SCA and certain articles of the PSD2 must still be implemented in national legislation. This makes it difficult to draw any meaningful conclusions in relation to the fraud and money laundering risks in advance.

For large (international) companies the PSD2 offers the opportunity to make paying for products or services part of the overall user experience by means of a PISP licence. By developing and offering innovative services AISPs can also play an interesting role on the payment market. It seems likely that the PSD2 will lead to a further increase in international transactions, and in the number of foreign parties offering their payment services to Dutch customers.

Criminals will also use the new payment services in some way. Unreliable and criminal TPPs whose objective is to facilitate fraudulent payments and/or misuse of information, present a risk. It is also possible that the payment infrastructure is also false or unreliable. Direct access presents an additional risk in this context. In addition, the PSD2 will bring about some challenges as far as fraud detection is concerned. Although it is not a part of the PDS2, the acceleration of transactions by means of *instant payments* will put further pressure on fraud detection. The current fraud detection systems of the ASPSPs must be adjusted and it is the question what the quality of fraud detection of the new, inexperienced newcomers on the payment market is.

PISPs can also play a role, intentionally or unintentionally, in the laundering of criminal assets. Logically, criminal PISPs who organise SCA themselves present a major risk, because they are able to perform concealing acts with automated APIs and/or own payment accounts.

Effective monitoring appears to be necessary to combat fraud and money laundering. The question is, however, whether the multitude of supervising authorities and the presumed increase in foreign parties on the Dutch market make effective monitoring possible.

However, the PSD2 also offers a number of chances. With the introduction of TPPs more financial information becomes available for investigation services. Especially AISPs can play an important role in this context in the future. In addition, both AISPs and PISPs come under the Wwft (Money Laundering and Terrorist Financing (Prevention) Act), as a result of which there should be an increase in the number of reportings of unusual transactions. Foreign TPPs that serve Dutch customers, however, will submit their reportings in the country of establishment. Although the exchange of information between FIUs is extended by the fourth anti-money laundering directive, practice will have to show to what extent the reporting chain and investigation services in the Netherlands can benefit from this.

On the other hand, payment transactions are becoming more international and more complex, which makes monitoring transactions and tracing assets labour-intensive and time-consuming. If this is not already the case, international cooperation is becoming crucial. Differences between countries regarding the penalisation of money laundering are an obstacle, just like the (slow) handling of requests for legal assistance. It is time for Europe to make uniform arrangements about this, creating possibilities for investigation services to obtain information from foreign parties in time.

4.2 Recommendations

The PSD2 working group makes the following recommendations to prevent and combat fraud and money-laundering:

- informing payment service users about the changes in payment options as a result of the PSD2 and the possible risks involved;
- informing payment service users about payment options that go hand in hand with a high fraud risk and (major) incidents;
- stimulating public-private (international) cooperation between providers of appstores, (new) payment service providers, investigation services and supervising authorities with the aim to share information on fraud patterns, fraud trends and modus operandi of criminals to combat fraud and money laundering;
- developing and organising work processes and new fraud and money laundering detection systems for payment service providers to detect and block unauthorised and/or fraudulent transactions[50];
- providing payment service users access to an on-line environment with an overview of the TPPs authorised by them, with the possibility to (temporarily) block authorisations;
- keeping the European register with registered, authorised payment service providers up-to-date and accessible on-line (automated) for all the parties involved;
- elaborating further on the substance demand on a European level and/or in national legislation;
- placing AISPs under the risk-based integrity supervision of the DNB;
- (international) cooperation between supervising authorities to increase the effectiveness of supervision;
- submitting payment service providers to supervision up to transaction level to be able to recognise possible money laundering transactions;
- making it possible for Dutch investigation services and supervising authorities to consult business accounts of foreign payment service providers relating to Dutch customers and/or payment accounts in such a way, that ordering the disclosure of information becomes simpler and/or international requests for legal assistance are unnecessary, for instance via a permanent representative in the Netherlands;
- making it possible for investigation services and supervising authorities to use the same technical access channels (such as APIs) that are available to payment service providers as a result of the PSD2, in order to improve efficiency and effectiveness of investigation and supervision activities.

[50] Considering the large number of data the parties involved exchange with the introduction of TPPs, there will be a strong focus on data analytics.