Some key topics under PSD2: open banking, strong customer authentication, and the platform/commercial agent exemption

mr. S. McInnes and mr. K. Berg[1]

The second Payment Services Directive (PSD2) updates the original Payment Services Directive (PSD1) which dates back from 2007. In this article, we will discuss the most important changes introduced by PSD2 and the new types of payment services which it permits, such as open banking and strong customer authentication.

1. Introduction

On 25 November 2015, the second Payment Services Directive (Directive 2015/2366[2] – 'PSD2') was adopted. PSD2 replaces the (first) Payment Services Directive (Directive 2007/64[3] – 'PSD1'), regulating payments, including the licensing of payment service providers.

EU Member States were required to implement PSD2 into their national law by 13 January 2018. However not all EU Member States were able to meet that deadline, with The Netherlands being one of the latest: the legislation transposing PSD2 into Dutch law only became effective on 19 February 2019.[4] Most of PSD2 has been transposed in the Dutch Financial Supervision Act (*Wet op het financieel toezicht*) and underlying regulations, and title 7B of book 7 of the Dutch Civil Code (*Burgerlijk Wetboek*) which covers payment transactions.

As its name suggests, PSD2 (and PSD1 before that) regulates the offering of payment services and generally requires anyone that provides payment services within the meaning of PSD2 to obtain a license from a national competent authority. The two most prominent changes introduced by PSD2 are (1) access to payment accounts by so-called Third Party Providers ('TPPs'), more widely referred to as 'open banking', and (2) strong customer authentication ('SCA'). We will focus on those in sections 2 and 3 of this article.

There are number of topics in PSD2 that raise interesting questions for the payments sector. It is outside the scope of this article to discuss all of those questions, but one issue that may be of particular interest to the reader is the question of whether a platform that handles the payment process (or parts of it) related to products sold via that platform are regulated under PSD2. We will discuss it in section 4 of this article.

2. Open Banking

PSD2 introduces the requirement for financial institutions that maintain payment accounts (so-called Account Servicing Payment Service Providers ('ASPSPs')) to open up their infrastructure to TPPs and give them access to payment accounts, provided that the relevant account holder has given its explicit consent to the TPP.[5]

[1] Scott McInnes is partner at Bird & Bird LLP in Brussels. Karen Berg is counsel at Bird & Bird LLP in The Hague.

[2] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market (OJ L 337, 23.12.2015)

[3] Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market (OJ L319, 5.12.2007)

[4] Royal Decree of 8 February 2019 (*Stb.* 2019, 60, 18 February 2019). As the Dutch legislator made a mistake in this Royal Decree determining the date on which the law and the decree transposing PSD2 into Dutch law became effective, an additional Royal Decree dated 5 March 2019 was published (*Stb.* 2019, 114, 15 March 2019).

[5] Pursuant to articles 65, 66 and 67 PSD2, implemented into Dutch law in articles 7:522a, 7:522b and 7:522c of the Dutch Civil Code and in the Decree prudential rules FSA (*Besluit prudentiële regels Wft*) pursuant to article 3:17 (2) of the Financial Supervision Act.

2.1. TPPs

There are three types of TPPs:

- Account Information Service Providers ('AISPs') - an Account Information Service ('AIS') is an online service to provide consolidated information on one or more payment accounts held by a customer with one or more ASPSP. An AISP will generally aggregate data from various payment accounts of a customer with different ASPSPs (e.g. different banks) and make that consolidated data available via one dashboard (e.g. an app or an online dashboard). PSD2 introduced this service to advance innovation in the payment sector and to stimulate the introduction of new services for customers.
- Payment Initiation Service Providers ('PISPs') - a Payment Initiation Service ('PIS') is a service to initiate a payment order at the request of the customer with respect to a payment account held at another Payment Service Provider ('PSP'). Typically those payments are credit transfers from the account of the payer to the account of the payee, and are therefore meant to compete with card-based payments such as Visa or Mastercard transactions, in particular for online payments.
- Card Based Payment Instrument Issuers ('CBPIIs') - Facilitates the issuance of card-based payment instruments by PSPs/card issuers that do not possess the cardholder's funds, and therefore have no view on the funds that the cardholder has available. CBPIIs issue cards to customers, typically debit cards, but have no visibility on the customers' funds and therefore cannot determine when to authorise or decline (debit) card transactions. With PSD2, when the card issued by the CBPII is used, the CBPII will have a right to obtain a 'yes' or 'no' confirmation from the ASPSPs that maintain the customers' funds on whether or not sufficient funds are available.[6] The CBPII will use that information to decide whether or not to authorise the (debit) card transaction.

TPPs need the explicit consent from the customer before they can access its payment account(s) and only that customer is entitled to withdraw the consent provided by it. For CBPIIs, there is also a separate explicit consent that the customer must give to its ASPSP to allow the ASPSP to provide the yes/no response (on availability of funds) to the CBPII.

2.2. Interplay PSD2 and GDPR

Issues have arisen as to the interplay between PSD2 and GDPR.[7] This is not surprising since the objectives of the Directive and the Regulation are to some extent contradictory: while PSD2 is targeted at ASPSPs opening up their infrastructure and giving access to data (including personal data) to TPPs, GDPR is intended to establish a framework ensuring that entities keep personal data that they hold safe, secure and protected against undue sharing with other parties (at least without a lawful basis as provided for under the GDPR). Some of the most pressing issues that we have encountered over the last year or so have been summarized in an article.[8] These issues include the difference between the concept of 'explicit consent' under PSD2 as compared with the GDPR, and the processing of 'silent party' data under PSD2 and GDPR. Additionally, the majority of the discussions in Dutch Parliament about the implementation of PSD2 into Dutch law were about the requirement of explicit consent for a PISP or AISP to get access to the customer's payment account data and the processing of personal data, as some members of parliament were concerned that customers would give their consent too easily and that PSD2 would insufficiently protect the customers' rights and their payment account data.

2.3. Access to payment accounts

To date, TPPs – AISPs and PISPs in particular – have accessed accounts, and not only payment accounts, using 'screen scraping' and/or 'reverse engineering' methods.[9] Looking at these two methods in more detail:

- When accessing an account via screen scraping, a TPP accesses the account through the customer interface with the use of the customer's security credentials that were issued by the ASPSP.
- Reverse engineering is a method to 'dissect' the ASPSP's mobile banking app that allows a customer to access its account and 're-engineer' it so that a TPP can access the account as if it were the customer by using the customer's security credentials.

The Regulatory Technical Standards on strong customer authentication and secure communication ('RTS')[10] adopted by EC provide for two different

[6] Pursuant to article 65 PSD2, implemented into Dutch law in article 7:522a of the Dutch Civil Code.

[7] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (OJ L119, 4.5.2016).

[8] EU: The interplay of PSD2 and GDPR – some selected issues by Scott McInnes and Lupe Sampedro, published on the DataGuidance platform (only accessible for members) and also made available via: https://www.twobirds.com/en/news/articles/2019/global/eu-the-interplay-of-psd2-and-gdpr-some-select-issues.

[9] For the avoidance of doubt: we are in this respect referring to screen scraping or reverse engineering with the consent of the relevant account holder and not to fraudulent use of these methods.

[10] Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and com-

methods as to how ASPSPs can provide a TPP access to the payment accounts of customers.[11] An ASPSP can either give the TPP access to the interface that the ASPSP makes available to its customer, but adapted in order to allow the TPP to identify itself vis-à-vis the ASPSP (also referred to as 'screen scraping plus') or alternatively make available a dedicated interface available to TPPs (typically referred to as an 'API': application programming interface).

If an ASPSP decides to make a dedicated interface (or API) available to TPPs, the RTS provide for certain requirements that the API must comply with:[12]

- First, the API must guarantee the same level of availability and performance as the interface which the ASPSP makes available to its customers who are directly connecting to the ASPSP.
- Second, similar to the scenario where the ASPSP gives the TPP access via the interface it makes available to the customers, the ASPSP must ensure that the TPP can be identified and can rely on the authentication procedures provided by the ASPSP to its customers.
- Finally, the ASPSP must have a contingency mechanism (i.e. a fall-back) available in case the API fails to perform in compliance with the requirements described in the two bullets above. The ASPSP can be exempted from the obligation to have a fall-back available if it meets certain conditions. These conditions include having the API available for testing for at least six months (i.e. as of 14 March 2019, 6 months before the RTS come into force, if it wants to be exempted from the fallback altogether and therefore not have to build one) and the API being widely used for at least three months by TPPs. Following calls from the payment sector for additional clarity on the exemption conditions and to ensure consistent application across the 28 EU Member States, the European Banking Authority ('EBA') published guidelines on this topic,[13] covering – inter alia - service levels, stress testing, design and testing to the satisfaction of PSPs and problem resolution.

In addition to an EBA Opinion on the implementation of the RTS,[14] the EBA has set up a working group on APIs under PSD2 which regularly publishes clarifications on issues related to APIs under PSD2.[15] Finally, more guidance can be found via the EBA's Q&A portal, where the EBA regularly publishes its responses to questions about various provisions of PSD2 and the RTS.[16]

The RTS come into force on 14 September 2019. This means that until that date, TPPs are allowed to accept payment accounts, but the technical requirements contained in the RTS do not have to be complied with. In practice, this means that until 14 September 2019, TPPs can continue to access payment accounts on the basis of screen scraping or reverse engineering.

2.4. Access to non-payment accounts

PSD2 and the RTS only concern TPP access to 'payment accounts'. On 4 October 2018, the EU Court of Justice[17] ruled that an account which does not allow the account holder to make payments to third parties, or to receive payments from third parties, does not qualify as a 'payment account'. This will mean that in most EU countries savings accounts do not qualify as payment accounts.

While PISPs may be content with just having a PSD2 regulated access to current accounts (but not savings accounts), AISPs do need access to savings accounts and other accounts in order to offer an attractive service to their users. Therefore AISPs need to continue to have access to non-payment accounts. Since that access is not regulated by PSD2 and the RTS, it begs the question as to whether AISPs are legally allowed to access non-payment accounts. In short, the emerging view is that a combination of arguments under competition law and GDPR mean that AISPs are entitled to access non-payment accounts. For example, as accessing those accounts under PSD1 was considered to be legal, there is no reason to consider this would have become illegal under PSD2. And by restricting access to non-payment accounts, ASPSPs may potentially face legal issues under competition law. Furthermore, one may argue that a PSU giving his 'explicit consent' to an AISP to access his non-payment accounts would be nothing else than the PSU exercising his right to data portability which is regulated by article 20 GDPR. [18]

mon and secure open standards of communication (OJ L69, 13.3.2018).

[11] Pursuant to article 31 RTS.

[12] See articles 32 and 33 RTS.

[13] Guidelines on the conditions to benefit from an exemption from the contingency mechanism under article 33 (6) of Regulation (EU) 2018/389 (RTS on SCA & CSC), dated 4 December 2018 (https://eba.europa.eu/documents/10180/2250578/Final+Report+on+Guidelines+on+the+exemption+to+the+fall+back.pdf/4e3b9449-ecf9-4756-8006-cbbe74db6d03).

[14] Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC, dated 13 June 2018 ('EBA Opinion') (https://eba.europa.eu/documents/10180/2137845/Opinion+on+the+implementation+of+the+RTS+on+SCA+and+CSC+%28EBA-2018-Op-04%29.pdf).

[15] See https://eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/eba-working-group-on-apis-under-psd2 under 'Publications & News'.

[16] See https://eba.europa.eu/single-rule-book-qa/-/qna/search/legalAct/6.

[17] Judgement of the fifth chamber, C-191/17

[18] In this sense, following the Article 29 WP guidelines on the right to data portability (WP242 v01 - Guidelines available here: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233), one may argue that a request to access non-payments accounts should not be treated as a data portability right under the GDPR, unless the PSU clearly requests this formally (article 29 WP includes the following exam-

The technicalities of that access are not regulated so:

- some ASPSPs may offer access to non-payment accounts on the basis of dedicated interfaces/APIs (perhaps the same API made available for access to payment accounts), for free or a fee ('premium API'). A recent assessment of the APIs that are currently being market tested by the largest Dutch banks, shows that indeed some allow access to non-payment accounts and some do not; or
- AISPs will screen scrape or reverse engineer in order to collect the data related to non-payment accounts.

3. Strong Customer Authentication

PSD2 requires a PSP to 'apply' SCA when (a) a payer accesses his payment account online; (b) a payer initiates an electronic payment transaction; or (c) a payer carries out any action through a remote channel which may imply a risk of payment fraud or other abuses.[19] As with the open banking provisions discussed above, the requirement to apply SCA shall become effective on 14 September 2019.

The SCA requirement under (a) applies whether the user accesses his account online directly at his bank (e.g. via a banking mobile app) or indirectly via an AISP. Same under (b) above, the SCA requirement applies whether the user initiates a payment directly from its banking mobile app or via a PISP.[20]

PSD2 defines SCA as authentication based on the use of two or more elements categorised as knowledge (something that only the user knows, e.g. a password), possession (something that only the user possesses, e.g. a smartphone or card reader) and inherence (something the user is, e.g. a fingerprint or other biometrics) that are independent (where independent means that the breach of one element does not compromise the reliability of the others), and is designed to protect the confidentiality of the authentication data. Although this does not follow from this definition or from other provisions in PSD2, the EBA has indicated that the two elements must belong to different categories.[21]

In practical terms, when using a payment card in a brick-and-mortar store, SCA consists in performing chip & PIN (i.e. inserting the card in the terminal and keying a PIN) or contactless & PIN. In a remote context, SCA generally takes the form of 'Verified by Visa' in relation to a Visa card or 'Mastercard SecureCode' in relation to a Mastercard card, but it can also be a simple fingerprint applied on a phone fingerprint sensor or facial recognition.

It is important to highlight that (b) only applies when the payer initiates the electronic payment. This means that where the payee (e.g. the merchant) initiates a payment, SCA will not be required. For example, a direct debit is considered as initiated by the payee and is therefore not subject to SCA (except a one-off SCA to setup a recurring direct debit), whereas credit transfers are considered as initiated by the payer and therefore are subject to the SCA requirement. Card payments come in two 'flavours':

- some card payments are considered as initiated by the payer (e.g. a consumer using his card to buy goods or services on a merchant website) and are therefore in principle subject to SCA;
- some card transactions are considered as initiated by the payee, for example subscriptions – whether for a fixed amount (e.g. for interactive television service) or a variable amount (e.g. utilities such as electricity or gas). Those payee-initiated card payments are referred to a Merchant Initiated Transactions ('MIT'). As MITs are not initiated by the payer, the recurring transactions are not subject to SCA. However, when the payee grants the mandate remotely, the setting up of the mandate will require a one-off application of SCA.[22]

3.1. Exemptions to SCA

The RTS further elaborate on the SCA requirements, but also contain exemptions from the requirement to apply SCA that PSPs can invoke in order to avoid having to require the payer to do an SCA.

As regards (a) above (i.e. when a customer accesses his payment account online), SCA will not be required when the customer is only accessing the balance of his payment accounts and/or payment transactions executed in the last 90 days via such payment account. [23] However, this exemption shall not apply when a customer is accessing this information online for the first time or more than 90 days have elapsed since the last time the customer accessed his payment transactions online and SCA was applied.

As regards (b) above (i.e. when the payer initiates a payment), the RTS provides for multiple exemptions for category (b).

- In relation to face-to-face transactions, these

ple in its guidelines to data portability: '*if the data subject's request aims specifically at providing access to his banking account history to an account information service provider, for the purposes stated in the Payment Services Directive 2 (PSD2) such access should be granted according to the provisions of this directive*'). Secondly, it is important to note that the right to data portability is not an 'absolute' right that can be requested in all circumstances and over any kind of data. In this sense, data portability is limited to data concerning the PSU that he has provided to the data controller, and the processing operations must be based either on consent or contractual necessity.

[19] Pursuant to article 97(1) PSD2, implemented into Dutch law in article 26h (4) Decree prudential rules FSA (*Besluit prudentiële regels Wft*).

[20] Pursuant to article 97(4) PSD2, implemented into Dutch law in article 26h (4) Decree prudential rules FSA (*Besluit prudentiële regels Wft*).

[21] See the EBA Opinion.

[22] EBA Q&A 2018_4404.

[23] Pursuant to article 10 RTS.

exemptions include:
- contactless payments (provided that the individual transaction does not exceed €50, and the cumulative amount of previous contactless transactions since the last SCA does not exceed € 150 or the number of consecutive contactless transactions since the last SCA does not exceed five); and
- unattended terminals where one pays for a transport fare or a parking fee (e.g. tollways on motorways) irrespective of the amount.[24]

– In relation to remote transactions, the exemptions include:
- recurring transactions for the same amount and with the same payee (apart from the creation, amendment or initiation for the first time);
- low-value transactions (provided that the individual transaction amounts to less than €30, and the cumulative amount of previous contactless transactions since the last SCA does not exceed € 100 or the number of consecutive contactless transactions since the last SCA does not exceed five); and
- where the PSP has identified the relevant payment as low-risk (to be determined on the basis of conditions provided for in the RTS).[25]

Additionally, SCA is not required for payments – remotely or face-to-face – to trusted beneficiaries. However, creating or amending this white-list of trusted beneficiaries will require SCA.[26]

As mentioned above, the EBA published an Opinion on the implementation of the RTS on SCA which contains helpful information on the various exemptions to SCA, and it also regularly publishes responses to questions on its online portal.

4. Platforms / commercial agent exemption

When operating an internet-based platform bringing buyers and sellers of goods or services together, the platform may decide to step into the payment chain by taking payments from customers for the products or services sold via the platform, with the proceeds of those transactions being paid into its account and then subsequently forwarding such proceeds to the sellers on a periodic basis. When doing so, the platform will, *prima facie*, be providing a payment service within the meaning of PSD2 and require a regulatory authorisation. PSD2 provides for various exemptions from the requirement to seek authorisation by the relevant national competent authority and one of these exemptions, known as the ‘commercial agent’ exemption, is particularly helpful for internet-based platforms.

The commercial agent exemption is available to a person who is in a payment chain only as a ‘*commercial agent authorised via an agreement to negotiate or conclude the sale or purchase of goods or services on behalf of only the payer or only the payee*’.[27] The commercial agent can thus not be an agent for both the customers and the sellers, and he must be authorised to negotiate or conclude transactions on behalf of the principal(s) for whom he is acting. In the context of selling via internet, there is generally little scope for negotiating, so when seeking to rely on this exemption one should definitely be concluding transactions on behalf of the principal. Furthermore, when the commercial agent receives payment from a customer, the receipt of that payment should fully discharge the obligation of that customer to pay the seller.

Unfortunately, this exemption seems to be subject to different interpretations by the various national competent authorities in different countries (i.e. some being more generous than others in terms of the scope of the exemption). A careful case-by-case assessment is therefore crucial.

5. Closing

In this article, we discussed the two most prominent changes introduced by PSD2: open banking (i.e. the access to payment accounts by TPPs) and strong customer authentication (SCA). When discussing open banking, we touched upon access to payment accounts and non-payment accounts and the interplay between PSD2 and GDPR. We summarised the concept of SCA, when it will be required and what exemptions apply.

Additionally, we explained under what circumstances a platform that handles the payment process (or parts of it) related to products sold via that platform may stay outside the scope of PSD2 by relying on the commercial agent exemption.

The impact of PSD2 thus goes well beyond the 'traditional' financial sector by advancing innovation and stimulating the introduction of new services for customers and attracting new players, such as start-ups, but also large BigTechs, to access the payment sector. This creates many opportunities and new propositions, which sometimes trigger legal challenges, some of which we have touched upon in this article.

[24] Pursuant to article 11 and 12 RTS, respectively.

[25] Pursuant to article 14, 16 and 18 RTS, respectively.

[26] Pursuant to article 13 RTS.

[27] Article 3(b) PSD2, implemented into Dutch law in article 1:5a of the Financial Supervision Act.