Article 25fa pilot End User Agreement

This publication is distributed under the terms of Article 25fa of the Dutch Copyright Act (Auteurswet) with explicit consent by the author. Dutch law entitles the maker of a short scientific work funded either wholly or partially by Dutch public funds to make that work publicly available for no consideration following a reasonable period of time after the work was first published, provided that clear reference is made to the source of the first publication of the work.

This publication is distributed under The Association of Universities in the Netherlands (VSNU) ‘Article 25fa implementation’ pilot project. In this pilot research outputs of researchers employed by Dutch Universities that comply with the legal requirements of Article 25fa of the Dutch Copyright Act are distributed online and free of cost or other barriers in institutional repositories. Research outputs are distributed six months after their first online publication in the original published version and with proper attribution to the source of the original publication.

You are permitted to download and use the publication for personal purposes. All rights remain with the author(s) and/or copyrights owner(s) of this work. Any use of the publication other than authorised under this licence or copyright law is prohibited.

If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please contact the Library through email: copyright@ubn.ru.nl, or send a letter to:

University Library
Radboud University
Copyright Information Point
PO Box 9100
6500 HA Nijmegen

You will be contacted as soon as possible.
The security of access to accounts under the PSD2

P.T.J. Wolters\textsuperscript{a,}\textsuperscript{*}, B.P.F. Jacobs\textsuperscript{b}

\textsuperscript{a} Business and Law Research Centre, Radboud University, Nijmegen, The Netherlands
\textsuperscript{b} Institute for Computing and Information Science, Radboud University, Nijmegen, Netherlands

\textbf{A R T I C L E  I N F O}

Article history:
Available online xxx

Keywords:
PSD2
GDPR
Access to account

\textbf{A B S T R A C T}

The revised Payment Services Directive (‘PSD2’) has been adopted to stimulate the development of an integrated internal market for payment services. In particular, it facilitates payment initiation services and account information services by granting the providers of these services access to the accounts of the payment service users. At the same time, the recitals state that the PSD2 guarantees a high level of consumer protection, security of payment transactions and protection against fraud.

This paper answers the following question: To what extent does the access to accounts of the payment initiation service providers and account information service providers balance the development of the market for payment services with the security of the payment account and the privacy of the user? An analysis of the PSD2 shows that the development of the market for payment services has a higher priority. Security and privacy are ultimately subordinate.

First, the PSD2 does not adequately protect the personal data of the users. The definition of ‘account information service’ is broad and covers a wide range of services. This allows the payment service providers to circumvent the limitations of the access to accounts.

Next, the payment service providers have a ‘fall back option’ that allows ‘screen scraping’ if the dedicated interface is not functioning properly. Although this access is constrained by several safeguards, the fall back option gives the payment services provider unlimited access to the account of the user.

Finally, the payment service providers have considerable freedom to arrange their authentication process as they see fit. The banks seem to be required to trust this process. The PSD2 and regulatory technical standards do not demand that a bank is able to verify the authentication or the integrity of the payment order.

© 2018 P.T.J. Wolters and B.P.F. Jacobs. Published by Elsevier B.V. All rights reserved.

\textsuperscript{*} Corresponding author at: Business and Law Research Centre, Radboud University, Nijmegen, The Netherlands.
\textit{E-mail address:} p.wolters@jur.ru.nl (P.T.J. Wolters).
1. Introduction

The European revised Payment Services Directive (‘PSD2’)\(^1\) has several objectives. Since the adoption of the first Payment Services Directive,\(^2\) the retail payments market has experienced significant growth and innovation. The PSD2 has been adopted to adapt the legal framework to these developments.\(^3\) It aims to contribute to legal certainty, harmonisation, competition and to the development of an integrated internal market. At the same time, the recitals state that the PSD2 guarantees a high level of consumer protection, security of payment transactions and protection against fraud.\(^4\)

The PSD2 creates a legal framework for two new types of payment services: ‘payment initiation services’ and ‘account information services’. In particular, it facilitates these services by obligating ‘account servicing payment service providers’ (banks) to give the ‘payment initiation service providers’ and ‘account information service providers’ access to the online ‘payment accounts’ of the ‘payment service user’ free of charge.\(^5\) The introduction of this ‘access to accounts’ has important consequences for the payment services providers, banks and users (Section 2). The exact design of this access depends on the regulatory technical standards for strong customer authentication and common and secure open standards of communication (‘RTS’, Section 3).\(^6\) It is important for the security of the payment account and personal data of the user (Section 4). This article analyses the risks that are created by access to accounts. It answers the following question: To what extent does the access to accounts of the payment initiation service providers and account information service providers balance the development of the market for payment services with the security of the payment account and the privacy of the user? An analysis of the PSD2 shows that the development of the market for payment services has a higher priority. Security and privacy are ultimately subordinate (Section 5).

2. Access to accounts in the legal framework of the PSD2

The legal framework of the PSD2 and access to accounts is based on a consideration of various interests. Fintech companies develop new financial products, including new ways to pay or view account information. These payment service providers cannot offer their services if the traditional banks do not cooperate. After all, the banks control access to the payment accounts. This allows them to limit competition on the market for payment services.

The PSD2 restricts this possibility by facilitating payment services, in particular by giving the payment initiation service providers and account information service providers access to the accounts of the users. The exact content of this access to accounts depends on the offered payment service. We will expand on this in the next subsections.

The (potential) users of these services benefit from the access to accounts because it allows them to use the services. However, the access also creates security and privacy risks. For example, it could be misused to steal the available funds. The privacy of the users is threatened because new service providers gain access to their financial information. This information could be abused for identity theft, blackmail, illegal pricing discrimination or by selling it to data brokers. These risks are not entirely new. They exist under any form of (online) access to the payment accounts. However, the access of the payment service leads to a multiplication of the attack vectors (Section 4.4).

The PSD2 reduces these risks by only allowing the provision of payment services by ‘payment service providers’.\(^7\) Article 1(1) of the PSD2 gives an exhaustive list of the categories of payment service providers. This list includes member states and other public authorities (under f), national central banks (under e) and institutions that are governed by another legal framework such as credit institutions (under a) or electronic money institutions (under b). Furthermore, an undertaking that wants to provide payment services can become a ‘payment institution’ by obtaining an authorisation from a competent national authority.\(^8\) Such an authorisation allows the payment institution to provide the services throughout the European Union pursuant to article 11(9) of the PSD2. Article

---

5 About these concepts, see PSD2, art 4(10)–(12), (15)–(19), Annex I (7)–(8), recitals 27–29. In this article, we will primarily use the terms banks (for account servicing payment service providers), payment service providers (if a rule applies to both payment initiation service providers and account information service providers) and users (for payment service users).
7 PSD2, art 4(1), 37(1).
8 PSD2, art 1(1)(d), 4(4), 5, 11, recital 34.
33 exempts institutions that only provide account information services from most of the requirements for an authorisation. They are only obligated to apply for a registration.9

The PSD2 is mostly disadvantageous for banks. As account servicing payment service providers, they are obligated to give the payment service providers access to the accounts of the user free of charge. The performance of this obligation can be costly. After all, the banks have to set up, maintain and secure a system that facilitates this access.10 Moreover, they are confronted with new liabilities. The banks are obligated to refund unauthorised or defective payment transactions, even if the transaction is initiated through a payment initiation service provider.11

Furthermore, the banks face new competition. Before the PSD2, they controlled the access to accounts.12 Other payment services providers had no legal right of access. The PSD2 removes this competitive advantage. This has consequences that reach beyond the market for payment initiation and account information services. The use of the services of competitors reduces the direct interaction between the bank and its customers. This weakens their ability to sell other products and services or detect fraud.14

The banks can also benefit from this development. As providers of payment initiation and account information services, the PSD2 allows them to gain access to the accounts of the customers of other banks.15 However, it is not likely that these possibilities outweigh the disadvantages of increased competition. It is expected that they will not only face increased competition from other banks, but also from large technology companies such as Facebook, Apple, Amazon, Microsoft and Google.16 The banks have a head start because of their expertise, infrastructure and reputation in connection with payment services. However, it is not clear to what extent, and for how long, these advantages offset the technological possibilities, size, market position and access to consumers of these technology companies.17

2.1 Payment initiation service

Article 4(15) of the PSD2 defines a payment initiation service as “a service to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider”. Examples of these services are iDEAL in the Netherlands, Sofort in Germany and Trustly in Sweden.

This service can be used to pay for products and services that are ordered online. It creates a software bridge between the customer and the online merchant. It gives the merchant the security that the payment has been initiated successfully, allowing him to deliver the goods or services without undue delay.18 Furthermore, the payment initiation service can streamline and simplify the payment by the customer. For example, the service can pre-set the amount and the beneficiary and eliminate the need to use the (separate) app or website of the bank.19 Finally, the payment initiation service can simplify the authentication. For example, an authentication process that uses a card, card reader and personal identification number could be replaced by a mobile phone and a fingerprint or facial recognition (Section 4.4).

The payment initiation service provider can only provide its service if the bank executes the transmitted payment orders. Next, it is necessary that the bank ‘understands’ the order and is able to establish its origin. For example, a payment initiation service cannot be used if the bank treats the account number as the amount of the payment. For this reason, the payment initiation service provider must have access to an interface that allows it to transfer the payment orders (Section 4.1).

Article 66 of the PSD2 regulates the access to accounts of the payment initiation service provider. Paragraph 1 formulates the freedom to use a payment initiation service provider as right of a payer with online access to the payment account. Paragraph 2 obligates the bank to honour this right. Pursuant to paragraph 4, the bank is obligated to provide information about the initiation and execution of the payment transaction to the payment initiation service provider. Furthermore, it must treat payment orders that are transmitted through the payment initiation service the same way as orders that are transmitted directly by the payer. Pursuant to paragraph 5, these obligations do not depend on the existence of a contractual relationship between the bank and the payment initiation service provider. For this reason, the bank is not allowed to charge a fee for the access to the account.20

Paragraph 3 limits the access in several ways. A payment initiation service provider can only supply the obtained information to the payee. Furthermore, it can only request data that are necessary to provide the service. The payment initiation service provider is not allowed to store sensitive payment data of the user. Pursuant to article 4(31) and (32), this includes

9 PSD2, art 5(3), recital 48.
11 PSD2, art 73(2), 90; Steennot (n 3) 958.
12 See also Hafstad and others (n 10) 45.
13 They were technically able to gain access. Section 4.2.
14 See also Temenos (n 10) 5, Finextra (n 10) 10, 21.
15 See also Hafstad and others (n 10) 11; Temenos (n 10) 11; Finextra (n 10) 21.
17 See also Hafstad and others (n 10) 27, 31, 34-37; Temenos (n 10) 11, 15; Caron (n 10) 57; Max Geerling, E-commerce: A merchant’s perspective on innovative solutions in payments’ (2018) 12 Journal of Payments Strategy & Systems 58, 60.
18 PSD2, recital 29; See also Donnelly (n 3) 830; Steennot (n 3) 955.
19 See also Geerling (n 17) 61.
'personalised security credentials' and other data that can be used to carry out fraud. Finally, the provider cannot use, access or store any data for other purposes than for the provision of the payment initiation service as explicitly requested by the payer.\footnote{21}

2.2. Account information service

Article 4(16) of the PSD2 defines an account information service as "an online service to provide consolidated information on one or more payment accounts held by the payment service user with either another payment service provider or with more than one payment service provider". This broad definition covers a wide range of services.

The PSD2 primarily envisions a service that allows a user to obtain information about several payment accounts held with one or more banks through a single online interface.\footnote{22} However, other services are not excluded. For example, an account information service could consist of an analysis of the user's spending habits and the use of this data to provide personalised advertisements.\footnote{23} It could also include the supply of the payment data to third parties such as financial advisors or credit reference agencies.\footnote{24}

The account information service provider can only provide its services when it has access to the account information. This access is regulated by article 67 of the PSD2. For the most part, it is shaped in the same way as the access of the payment initiation service provider. For example, it is also formulated as a right of the payment service user with online access to his payment account (Section 2.1). The limitations of the access are also similar. However, the broad definition of 'account information service' weakens these limitations.

First, article 67(2)(f) states that the service provider cannot use the obtained information for other purposes than for performing the account information service. For example, it is not allowed to use the data to offer other products and services. However, this limitation can be circumvented by offering a service that explicitly includes making personalised offers that are based on the account information. Moreover, the account information service can consist of providing data to a third party. It can be a part of a more comprehensive relationship such as a credit application. In this example, the account information service provider would provide the data to a lender that would use them to offer a personalised loan.

Furthermore, the PSD2 does not clarify whether the account information service provider can use the data for other purposes if the processing is lawful pursuant to another ground such as the additional consent of the user. Article 67(2)(f) states that the account information service provider cannot process the data for other purposes, "in accordance with data protection rules". This addition suggests that the data can be processed for other purposes as long as this is done in accordance with the General Data Protection Regulation (‘GDPR’).\footnote{25} It is a relevant deviation from the similar article 66(3)(g) of the PSD2. The prohibition to process the data for other purposes than the provision of the payment initiation service is not qualified in this manner. This suggests that a payment initiation service provider cannot circumvent the prohibition by obtaining additional consent from the user.

Next, the PSD2 does not clarify which data fall under the scope of the access to accounts.\footnote{26} Sensitive payment data is excluded pursuant to article 67(2)(f). Furthermore, article 67(2)(d) determines that the account information service provider can only access information from 'designated payment accounts and associated payment transactions'. In any event, the access must be limited to the information that is necessary for the provision of the account information service. This follows from the principle of 'data minimisation' from article 5(1)(c) of the GDPR.\footnote{27} However, the necessity of information depends on the offered service. An account information service provider can circumvent this limitation by offering a broadly defined service.

A further limitation of the access violates the principles and goals of the PSD2. Access to accounts is meant to facilitate the provision of account information services by others than the banks. It will not fulfil this goal if the user can only access a limited amount of data through an account information service. The account information service provider would remain in a disadvantaged position compared to the bank. For this reason, it should have access to the same data as the user of the online banking environment that is offered by the bank.\footnote{28}

The account information service provider, and not the bank, is ultimately responsible for the selection of the necessary data. It must implement suitable and effective mechanisms that prevent access to other information.\footnote{29}

The account information of the user can also relate to other natural persons. The information that user Alice transferred money to (or received money from) Bob, also means that Bob received money from (or transferred money to) user Alice. By providing an account information service to user Alice, the service provider also processes the personal data of Bob. Similarly, the bank processes this data by granting access to the.

\footnote{21} About these limitations, see PSD2, art 66(3)(c), (e)–(g).
\footnote{22} PSD2, recital 28; Donnelly (n 3) 631.
\footnote{23} Cf Cortet, Bijks and Nijland (n 3) 26; Hafstad and others (n 10) 45–47; Financial Conduct Authority (n 20) 16, 214; Caron (n 10) 58.
\footnote{24} Financial Conduct Authority (n 20) 16.
\footnote{25} European Parliament and Council Regulation 2016/679/EU of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L119/1. About this issue, see European Data Protection Board, Letter to Sophie in ‘t Veld, 5 July 2018, stating that processing for other purposes is possible with additional consent.
\footnote{26} See also European Banking Federation, Guidance for implementation of the revised Payment Services Directive. PSD2 guidance (EBF, 020819, 2016) 25.
\footnote{27} See also EBA, ‘Opinion of the European Banking Authority on the European Commission’s intention to partially endorse and amend the EBA’s final draft regulatory technical standards on strong customer authentication and common and secure communication under PSD2’ EBA/OP/2017/09, 8; Sections 2.3, 4.2.
\footnote{28} RTS, art 36(1)(a); Financial Conduct Authority (n 20) 209.
\footnote{29} RTS, art 36(3). About the division of responsibility between the bank and payment service provider, see also Sections 2.3, 4.4 and 4.5.
account information service provider. However, in contrast to Alice, Bob has not given consent for this processing. For this reason, the processing of this ‘silent party data’ must be based on one of the other grounds of article 6(4) of the GDPR. This problem is not exclusive to the PSD2. It also exists when the silent party data is shared on another ground, such as the right of access or the right to data portability under the GDPR.

Article 6(1)(c) of the GDPR provides a ground for the processing by the bank: as soon as the PSD2 is implemented, the bank has a legal obligation to grant access to the account information service provider. The lawfulness of the processing by the account information service provider can only be based on article 6(1)(f) of the GDPR. The processing is necessary for the purposes of the legitimate interests pursued by the service provider and its user. These legitimate interests must be weighed against the interests or fundamental rights and freedoms of the data subject. The result of this deliberation depends on the nature of the account information service.

If the service consists of providing information about several payment accounts through a single online interface, this deliberation is no different from the situation in which the user accesses the data in the online banking environment that is offered by the bank. After all, Bob has not given consent to the processing of his data by the bank. Alice’s interest in getting an online overview of her transactions, and the interest of the bank in offering this service, outweigh the violation of the privacy of Bob. One could argue that account information service providers are less reliable than banks. Although this is a relevant risk, it is not in line with the principles of the PSD2. The PSD2 works from the assumption that payment service providers in the sense of article 1 can be trusted. For this reason, Alice should also be able to view Bob’s personal data through the account information service.

The result of this deliberation can be different if the data are meant for different purposes. For example, an account information service can consist of the analysis of the financial state of the user. Even before the PSD2, lenders frequently ask for financial information, such as a transaction overview, that contains data about silent parties. In theory, this data could be relevant. For example, frequent payments from Bob to Alice can indicate that Alice financially depends on him. However, the frequent use of account information services allows third parties to access the silent party data on a much larger scale than is done currently. This will lead to a greater violation of the privacy of a larger group of silent parties. For this reason, account information service providers should only process this data to the extent that this is truly necessary for the provision of the service to Alice. They are not allowed to keep or use the data for other purposes. For example, they cannot use it to build a profile about Bob or when Bob applies for a loan.

2.3 Access to accounts and the protection of the payment service user

The PSD2 aspires to balance the development of the market for payment services with security and privacy (Section 1). In this light, the extensive access to accounts is accompanied by several safeguards.

First, the payment services need to be adequately secured. Pursuant to article 68(5) and (6) of the PSD2, a bank can deny the access to an account for objectively justified and duly evidenced reasons relating to unauthorised or fraudulent access to the payment account. It must report the incident to the competent authority. The bank should again grant access once the objectively justified and duly evidenced reasons no longer exist.

Pursuant to article 95 of the PSD2, payment service providers must establish a framework with appropriate mitigation measures and control mechanisms to manage the operational and security risks in relation to the payment services that they provide. Article 96 obliges them to notify the competent authorities and the users in the case of a major operational or security incident. These obligations apply to payment initiation service providers and account information service providers, but also to banks. As ‘account servicing payment service providers’, banks are also payment service providers in the sense of the PSD2.

When the user wishes to use a payment initiation service or account information service, the providers are obligated to apply ‘strong customer authentication’ pursuant to article 97. This is defined by article 4(30) of the PSD2 as authentication that is based on the use of two or more independent elements categorised as knowledge, possession and inherence. Finally, the payment service providers and banks must communicate securely with each other.

The safeguards are also aimed at the protection of the personal data of the user. Recital 89 states that directive 95/46/EC (Data protection) and its national implementations apply to the processing of personal data for the provision of

---

30 The “disclosure by transmission, dissemination or otherwise making available” is a ‘processing’ of ‘personal data’. GDPR, art 4(1), (2).
32 Cf GDPR, arts 15(4), 20(4), recital 63 (the right to obtain a copy of the personal data and the right to data portability should not adversely affect the rights and freedoms of others).
33 European Data Protection Board (n 25). In the context of the right to data portability, see Article 29 Data Protection Working Party, Guidelines on the right to data portability (16/EN WP 242 rev:01, 2017) 11–12.
34 See also European Data Protection Board (n 25). They must also be able to demonstrate this necessity. GDPR, arts 5(1)(a)–(c), (2), 24(1).
35 The GDPR also imposes these obligations in relation to personal data. GDPR, arts 32-34. See also PSD2, recital 89.
36 PSD2, art 4(17), Annex I(1), (2).
37 See also RTS, arts 4-9; Donnelly (n 3) 837. For exceptions, see RTS, arts 10–21.
38 PSD2, arts 66(3)(b), (d), (4)(a), 67(2)(b)–(c), (3)(a). See also Section 4.3.
39 See also PSD2, arts 66(3)(g), 67(2)(f); Section 2.2.
to the processing of personal data and on the free movement of such data [1995] OJ L281/31.

41 European Data Protection Board (n 25).
42 About the scope of the GDPR, see GDPR, arts 1–3.

3. The regulatory technical standards for strong customer authentication and common and secure open standards of communication

The European Banking Authority (‘EBA’) plays an important role in the elaboration of the safeguards of articles 95, 96 and 97 of the PSD2. Pursuant to articles 95 and 96, they have the obligation to issue ‘guidelines’ about these measures in accordance with article 16 of the ‘EBA Regulation’.44 This must be done in close cooperation with the European Central Bank and after consulting all relevant stakeholders.

Next, article 98(1) obligates the EBA to develop draft regulatory technical standards on strong customer authentication and secure communication in accordance with article 10 of the EBA Regulation. These ‘RTS’ must work towards a balance between the goals of the PSD2.45 As shown in Section 4, they significantly affect the design and security of the access to accounts.

Again, the draft must be developed in close cooperation with the European Central Bank and after consulting all relevant stakeholders. After the consultation on the basis of a ‘Discussion Paper’ and a ‘Consultation Paper’, the EBA published its draft on 23 February 2017.46 However, unlike the guidelines of article 16 of the EBA regulation, the RTS are ultimately adopted by the European Commission pursuant to article 10(1). The content of the RTS were a point of contention between the EBA and the European Commission. Specifically, they debated the legitimacy of ‘screen scraping’ (Section 4.2). After some back and forth, the European Commission adopted the RTS on 27 November 2017.47

46 EBA, ‘Discussion Paper’ (n 45); EBA, ‘Consultation Paper. On the draft Regulatory Technical Standards specifying the requirements on strong customer authentication and common and secure communication under PSD2’ EBA-CP-2016-11; EBA, ‘Final Report’ (n 45). Access to accounts was a matter of significant concern during this consultation. EBA, ‘Final Report’ (n 45) 3–4, 44, 46. Cf PSD2, art 98(4) (the deadline for the draft is 13 January 2017).
47 Commission, ‘Communication to the Commission on the intention to endorse, with amendments, the draft Regulatory Technical Standards submitted by the European Banking Authority for strong customer authentication and common and secure open standards of communication in accordance with Article 98(4) of Directive (EU) 2015/2366’ (Communication) C(2017) 3459 final; O. Guerent, ‘Commission intention to amend the draft regulatory technical standards on strong customer authentication and common and secure open standards of communication submitted by the EBA in accordance with Article 98(4) PSD2’ (Letter to A. Enria) Ref. Ares(2017)2639906;
intention to publish a draft technical specification on March 2018 and will apply from 14 September 2019.

The delay in the adoption of the RTS affects the balance between the goals of the PSD2 during the transitional period. Pursuant to article 115, the PSD2 should have been implemented on 13 January 2018. Payment service providers can benefit from the access to accounts from the moment of its implementation. Furthermore, payment service providers that were active in a member state before 12 January 2016 can continue to perform their activities pursuant to article 115(5). However, the payment service providers are not bound by the corresponding security measures until the application of the RTS. Pursuant to article 115(4) of the PSD2, the security measures referred to in articles 65, 66, 67 and 97 do not have to be applied during the transitional period between 13 January 2018 and 14 September 2019. Instead, they are only bound by the more general obligations to manage the operational and security risks and to secure the processed personal data.

4. Access to accounts under the RTS

This section analyses the influence of the RTS on the design and security of access to accounts under the PSD2. It subsequently discusses the difference between a dedicated and a user interface (Section 4.1), the admissibility of ‘screen scraping’ (Section 4.2), the role of the authentication procedure provided by the bank (Section 4.3), the option of the payment service provider to use its own authentication procedure (Sections 4.4 and 4.5) and the requirements of identification, authentication and dynamic links (Section 4.6). For each of these topics, the subsection discusses the relevant security risks.

4.1. A dedicated interface or an adapted user interface

A bank that offers its users online access to their payment accounts, is obliged to have an interface in place that allows payment service providers to access the accounts pursuant to article 30(1) of the RTS. Pursuant to article 31, the bank can choose between a separate ‘dedicated’ interface for payment service providers or by allowing them to utilise the user interface.

Even if the bank chooses the latter option, it cannot simply open the user interface to payment service providers. It needs to modify the interface. Pursuant to article 30(1) of the RTS, the interface must enable the providers to identify themselves, to request and receive information one or more designated accounts and associated transactions and to initiate a payment order. Furthermore, it should not provide unlimited access to the accounts. Instead, the access should be limited to the information that is necessary for the provision of the payment services.

4.2. The admissibility of ‘screen scraping’ and the demands on a dedicated interface

The payment service providers depend on the bank for the provision of their service. They cannot provide their service in compliance with the PSD2 if the bank does not offer an adequately functioning interface. This allows a bank to frustrate the desired development of the market for payment services. The RTS contains several rules to prevent this. Pursuant to article 30(3), (4) and (5), a bank is, among other things, obligated to follow international or European standards, document and provide the technical specifications of its interface, communicate changes and make a testing facility available. A dedicated interface creates additional possibilities to frustrate the competition on the market for payment services. For example, a bank could limit the data that is accessible through this interface or reduce its speed or availability.

Fear of use of these possibilities has influenced the content of the RTS. In particular, it has influenced the discussion about the admissibility of ‘screen scraping’. With this form of access, the payment service provider gains access to the payment account without identifying itself. Instead, it receives personalised security credentials, such as a PIN, from the payment service user to gain access ‘as the user’. Several existing service providers, such as Sofort in Germany, were using this form of access before the adoption of the PSD2. Fig. 1 gives an overview of access to accounts through screen scraping.

A payment service provider that uses this form of access violates its obligation to identify itself. A bank can take measures to discover screen scraping. However, as a starting point, it does not know that it is dealing with a payment service provider instead of the user. The payment service provider gains unlimited access to the online banking environment. It gains access to all available information, including sensitive payment data and information that is not necessary for the

---


50 PSD2, art 95; GDPR, art 32.


52 E.g. EBA, ‘Final Report’ (n 45) 11, 46, 113; EBA, ‘Opinion on the European Commission’s intention’ (n 27) 7.


55 PSD2, arts 66(3)(d), 67(2)(c).
provision of the service. For these reasons, the draft of the EBA prohibited screen scraping.\(^56\)

Payment service providers lobbied against this prohibition.\(^57\) They argued that they should keep the option to gain access through the user interface, especially if the dedicated interface does not function adequately. The draft by the EBA did not contain such a ‘fall back option’. However, it did demand that the dedicated interface offered the same level of availability and performance as the user interface. Furthermore, the bank was obligated to take measures to prevent and repair malfunctions.\(^58\)

The European Commission has been more receptive to the lobby of the payment service providers. Its draft of May 2017 allowed the payment service providers to utilise the user interface if the dedicated interface malfunctioned and certain other conditions were met.\(^59\) Among other things, the payment service provider had to identify itself. The bank was obligated to ensure that the user interface facilitated this identification.

The EBA was opposed to this fall back option. Among other objections, it stated that this solution can force banks to maintain both a dedicated interface and an adapted user interface that allows identification. To avoid these costs, they may decide to abandon the development of a standardised dedicated interface altogether. This increases the costs for new payment service providers and hinders the development of a single European market for payment services.\(^60\) Instead, the EBA proposed more stringent requirements for dedicated interfaces.\(^61\)

The European Commission was partly convinced by these objections.\(^62\) Article 33(4) of the adopted RTS still contains the fall back option. However, the competent authorities can exempt a bank pursuant to article 33(6) if the dedicated interface complies with all of the obligations as set out in article 32, has been tested by the payment service providers, has been widely used for at least three months and any problems have been resolved without undue delay. The EBA has published a consultation paper for the draft guidelines on these conditions. It allows a bank to obtain an exemption before the RTS apply.\(^63\)

Article 33(6) of the RTS allows a bank to avoid the costs of maintaining the adapted user interface. Furthermore, it strengthens the protection of the personal data of the users. If the bank is exempted and the transitional period has ended (Section 3), payment service providers will under no circumstances be allowed to use screen scraping.

### 4.3. The authentication procedure of the bank

The interface that is offered by the bank should allow the payment service providers to rely on all the authentication procedures that are provided by the bank to the user.\(^64\) This option facilitates the provision of payment services. It allows a payment service provider to offer its services without developing and using its own strong customer authentication. The payment service providers can instruct the bank to start their authentication procedure along with the payment order or the request for information. The RTS do not clarify how this authentication should be resolved. Figs. 2 and 3 display the most important variations.

The interface should establish and maintain communication sessions between the bank, payment service provider and user pursuant to article 30(2)(b) of the RTS. The existence of a communication session between the bank and the user suggests that the authentication can be resolved without the involvement of the payment service provider. Instead, the

---

\(^{56}\) EBA, ‘Final Report’ (n 45) 4, 11, 46, 113, 117–118; EBA, ‘Opinion on the European Commission’s intention’ (n 27) 8. See also Sections 2.1, 2.2.


\(^{58}\) EBA, ‘Final Report’ (n 45), art 28.

\(^{59}\) Guersen (n 47), art 33(3).

\(^{60}\) In more detail, see EBA, ‘Opinion on the European Commission’s intention’ (n 27) 8–11.

\(^{61}\) Amended draft by the EBA (n 47), arts 31, 32.


\(^{64}\) PSD2, recital 30, 69, 96; RTS, art 30(2).
payment service provider redirects the user to the bank or the authentication is done through a decoupled approach.⁶⁵

Under this system, the payment service provider does not process personalised security credentials in any way. This is in accordance with the goals of the PSD2. An account information service provider is not allowed to request sensitive payment data, including personalised security credentials (Section 2.2). A payment initiation service provider cannot store them (Section 2.1). Furthermore, article 5(1)(g) of the PSD2 obligates a payment institution to submit a description of the process that is used to restrict access to sensitive payment data at the time of the application for authorisation.

The system of Fig. 2 limits the security risks to a minimum.⁶⁶ The payment service provider has no access to personalised security credentials and cannot abuse them. Furthermore, criminals cannot steal or intercept security credentials from the payment service provider. These advantages do not exist if the authentication, including the personalised security credentials issued by the bank, are resolved in whole or in part through the payment service provider via an embedded approach.⁶⁷ This system also facilitates fraud. Before the PSD2, banks have warned customers to never share their PIN or other security credentials with others. These warnings cannot be given if the PSD2 allows the system of Fig. 3. This enables a criminal to pose as a legitimate payment service provider in order to induce a user to share his personalised security credentials.

Several norms suggest that this system is allowed. The articles 66(3)(b) and 67(2)(b) of the PSD2 state that the payment service providers should ensure that personalised security credentials are not accessible to other parties with the exception of the user and the issuer of the credentials. Furthermore, the articles obligate them to transmit personalised security credentials through safe and efficient channels. Next, article 30(2) of the RTS states that the interface should ensure the integrity and confidentiality of the credentials that are transmitted by or through the payment service providers. Finally, the payment service providers should ensure that transmitted personalised security credentials and authentication codes are not readable by any staff at any time pursuant to article 35(5) of the RTS. They are obligated to inform the user and the issuer in case of a loss of confidentiality of the credentials under their sphere of competence. These norms illustrate that the payment service providers can be an intermediate in the authentication procedure that is provided by another party such as the bank.⁶⁸

---

⁶⁵ See also EBA, ‘Opinion on the implementation’ (n 51) 11.
⁶⁶ See also Cortet, Rijks and Nijland (n 3) 24.
⁶⁷ See also EBA, ‘Opinion on the implementation’ (n 51) 11.
⁶⁸ See also EBA, ‘Final Report’ (n 45) 118, 123, 145–147.
4.4. An authentication procedure of the payment service provider

The payment initiation service provider and account information service provider are obligated to apply strong customer authentication (Section 2.3). They have the right to use the procedure that is provided by the bank (Section 4.3). However, the PSD2 and RTS do not obligate them to use this procedure. They can also utilise another form of two-factor authentication. The development of user-friendly means of payment is one of the objectives of the PSD2. Fast and convenient authentication procedures contribute to this goal.

An authentication procedure that is offered by the payment service provider is required to comply with the PSD2 and the RTS. It is governed by the same legal security standards as the authentication procedure of the bank. Nonetheless, the use of alternative authentication procedures creates additional risks. Fig. 4 gives an overview of these risks.

If only the authentication procedure of the bank can be used, criminals can only gain illegal access if they manage to circumvent or break this procedure. The authentication procedures of the payment service providers lead to a multiplication of the attack vectors, even if they are secured just as well as the procedures of the bank. The mere fact that more procedures can be used, increases the chance that one of them contains a vulnerability that is discovered and exploited by a criminal.

This is amplified by the fact that, without the use of its own authentication procedure or a digital signature (Section 4.6), a bank is not able to judge if the user of the payment service is the same person as the account holder. It cannot verify whether the holder truly consents to the access to his account. Instead, it must rely on the payment service provider. In theory, every authorised payment initiation service provider or registered account information service provider can gain access to every payment account, even if it does not have consent from or a contractual relationship with the alleged user. Similarly, (foreign) intelligence services and criminals can gain access to an account by hacking into the computer system of any payment service provider. Alternatively, they can gain access if they obtain their own authorisation or registration to become a payment institution.

---

69 E.g. PSD2, art 98(2)(e), recital 30; EBA, ‘Discussion Paper’ (n 45) 9, 18–19, 27; Gerd Cimiotti and Christina Nadine Dahl, ‘Paying in 2025: Scenarios for payment systems in Germany in 2025’ (2016) 10 Journal of Payment Strategy & Systems 253, 255–256; EBA, ‘Final Report’ (n 45) 38, 41, 117; Section 2.1. Cf PSD2, arts 64(2) (“Consent to execute a payment transaction or a series of payment transactions shall be given in the form agreed between the payer and the payment service provider. Consent to execute a payment transaction may also be given via the payee or the payment initiation service provider”), 66(4)(c), 67(3)(b) (an account servicing payment provider shall treat the payment orders and data requests transmitted through the services of a payment initiation service provider or account information service provider without any discrimination); RTS, art 36(4) (“Payment initiation service providers shall provide account servicing payment service providers with the same information requested from the payment service user when initiating the payment transaction directly”). It could be argued that ‘the form agreed’, ‘the same information’ and ‘without any discrimination’ also refers to the authentication. However, this interpretation does not correspond to the goals of the PSD2. Furthermore, if a payment service provider decides to rely on the strong customer authentication of the bank, the decision to apply an exemption also remains with the bank. EBA, ‘Opinion on the implementation’ (n 51) 8.

4.5. One-time authorisation with the authentication procedure of the bank

The additional risks can be limited by demanding the one-time, or yearly, authorisation of the payment service provider with the authentication procedure of the bank. Although this safeguard does not remove all of the additional attack vectors, it reduces the risks to payment service providers that have been authorised by the user.

Article 95(1) of the PSD2 obligates the payment service providers to limit the risks in relation to their payment

70 See also Financial Conduct Authority (n 20) 137; EBA, ‘Consultation Paper. Draft Guidelines’ (n 63) guideline 5.2(c); EBA, ‘Opinion on the implementation’ (n 51) 4; Implementatiebesluit herziening richtlijn betaaldiensten (clarification of the proposed Dutch Implementation) www.internetconsultatie.nl/implementatiebesluitherzieningbetaaldiensten accessed 25 June 2018, 16–17.
services.\textsuperscript{71} The prevention of unauthorised access is one of the goals of this obligation.\textsuperscript{72} One-time authorisation contributes to its performance. Furthermore, the use of the authentication procedure of the payment service provider does not prove that the user is also the account holder.\textsuperscript{73} For example, a payment service provider that uses a fingerprint for the authentication, does not know whether the fingerprint is also associated with the account holder. Similarly, this cannot be verified by a bank that does base its authentication on a fingerprint. For this reason, the payment service provider should associate the identities of the user and the account holder with each other. Although the PSD2 does not prescribe the authentication procedure of the bank, the one-time authorisation is a secure and user-friendly way to establish this association.\textsuperscript{74}

This does not automatically mean that a bank can also refuse the access until the payment service provider has been authorised. Such a right or obligation is not explicitly incorporated in the PSD2 or the RTS.\textsuperscript{75} However, several norms provide a potential legal basis. First, article 68(5) of the PSD2 states that a bank can deny the access for objectively justified and duly evidenced reasons relating to unauthorised or fraudulent access to the payment account (Section 2.3). Next, article 95 also applies to the bank. Although the risks are primarily related to the payment initiation and account information services, the abuse is only possible if the access is actually granted. For this reason, the risks are also related to the provision of a payment account. Finally, article 2 of the RTS obligates payment service providers, including banks, to have transaction monitoring mechanisms in place that enable them to detect unauthorised or fraudulent payment transactions.

The requirement of a one-time authorisation will surely be justified if other circumstances also suggest that a risk of fraud exists.\textsuperscript{76} For example, such additional circumstances could exist if the spending pattern is abnormal.\textsuperscript{77} Furthermore, a bank could demand the one-time authorisation if it knows or objectively suspects that the payment service provider does not use another authentication procedure that fulfils the requirements of the PSD2 and establishes the association of the identities of the user and the account holder.

Furthermore, article 68(1) of the PSD2 allows the payment service provider and payer to agree on spending limits when a specific ‘payment instrument’,\textsuperscript{78} such as a payment initiation service, is used to give consent. Although this is not explicitly stated in the article, a textual reading suggests that a bank, as an account servicing payment service provider, can also impose these spending limits in the contract with its user. Furthermore, if a general spending limit is allowed, it should also be possible to stipulate that the limit only applies if the payment service provider is not authorised with the authentication procedure of the bank. Next, article 68(2) states that the ‘framework contract’\textsuperscript{79} can create a right for the payment service provider to block the payment instrument for objectively justified reasons relating to the security of the payment instrument or the suspicion of unauthorised or fraudulent use of the payment instrument.

If, and under what circumstances, a bank can demand the one-time authorisation of the payment service provider, is not clarified by the PSD2 or the RTS. This demand strengthens the security of the payment account and personal data of the user. However, it also limits the competition on the market for payment services because it creates an additional obstacle for the use of the services. Nonetheless, this limitation is marginal, especially in the light of the security obligations of the payment service providers.

Larger limitations of the access to accounts could violate the PSD2. The justified goal of the prevention of fraud cannot be abused as an instrument to restrict the competition. For this reason, a bank cannot too easily deny the access for objectively justified and duly evidenced reasons relating to unauthorised or fraudulent access to the payment account. Similarly, the contractual limitations should not go further than necessary to prevent fraud and protect the user.

### 4.6. Identification, authentication and dynamic linking

The payment service providers are obligated to identify themselves towards the bank (Sections 4.1 and 4.2). For this purpose, article 34 of the RTS requires them to use qualified certificates for electronic seals or for website authentication as referred to in article 3(30) and (39) of the ‘eIDAS regulation’.\textsuperscript{80} The annexes III and IV of the eIDAS regulation stipulate the requirements for these certificates. Among other things, they should contain an ‘advanced electronic signature’ of a ‘qualified trust service provider’.\textsuperscript{81} The certificates do not only allow ‘identification’. They also enable ‘authentication’. They allow a payment service provider to prove its identity to the bank.

The payment service providers are obligated to apply strong customer authentication or rely on the procedure of the bank (Sections 2.3, 4.3 and 4.4). The articles 4 and 5 of the RTS further develop this obligation. Pursuant to article 4, the

---

\textsuperscript{71} Section 2.3. See also PSD2, arts 5(1)(e), (i), (j), 11(4). Account information service providers are exempted from PSD2, arts 5(1)(i), 11(4). PSD2, art 33(1).

\textsuperscript{72} EBA, ‘Consultation Paper. On the draft Regulatory Technical Standards’ (n 8) 6, 21.

\textsuperscript{73} Cf RTS, art 24 about the association of the identity of the user and his personalised security credentials.

\textsuperscript{74} In a more general sense, banks can benefit from the PSD2 and open banking by offering digital identity services. Fineextra (n 10) 22-23. E.g. ‘iDIN’, online identification based on the authentication of Dutch banks. www.idin.nl accessed 25 June 2018. The association can also be established through other digital identity services that can ascertain that the user is also the account holder. E.g. ‘IRMA’. https://privacybydesign.foundation/en/ accessed 25 June 2018.

\textsuperscript{75} N 69. Cf Temenos (n 10) 14.

\textsuperscript{76} See also Financial Conduct Authority (n 20) 211 (the mere fact that a customer uses a payment initiation or account information service is insufficient).

\textsuperscript{77} See a contrario the criteria for an exception from the obligation to apply strong customer authentication based on a transaction risk analysis. RTS, art 18(c); Steennot (n 3) 960.

\textsuperscript{78} PSD2, art 4(14).

\textsuperscript{79} PSD2, art 4(21).


\textsuperscript{81} About these concepts, see eIDAS regulation, arts 3(11), (20) and 26.
authentication of the payer must be based on two or more elements which are categorised as knowledge, possession and inherence and should result in the generation of an 'authentication code'. The payer must use this code to access the payment account, initiate an electronic payment transaction or to carry out any action through a remote channel which may imply a risk of payment fraud or other abuses. The code must meet several requirements. It should be unforgeable, only be accepted once, not contain information on any of the elements and be impossible to generate based on the knowledge of previously generated codes.

The articles 97(2) of the PSD2 and 5(1) of the RTS demand a 'dynamic link' for electronic remote payment transactions.\(^2\) This means that the generated authentication code should be linked to a specific amount and a specific payee. Any change should invalidate it. This establishes the 'integrity' of the payment order. However, the RTS do not seem to require that third parties, such as banks, are able to verify this. It does not demand that the authentication code is secured by a digital signature or another technique that establishes 'non-repudiation'. Furthermore, the payment service provider is obligated to make the payer aware of the amount and the payee. Pursuant to article 5(2) of the RTS, the payment service provider should take security measures to ensure the confidentiality, authenticity and integrity of the amount, the payee and the displayed information throughout all of the phases of the authentication.

Although article 5 of the RTS only applies to electronic remote payment transactions, the underlying principles can also be used for account information services. In this scenario, a change in the privileged service provider or the scope of the access would invalidate the authentication code. Furthermore, the user would have to be made aware of the privileged provider and the exact scope of the access throughout all of the phases of the authentication.

The PSD2 and RTS use several related concepts.\(^3\) The concepts 'identification', 'authentication' and 'digital signature' are related but give fundamentally different guarantees. They achieve different security goals. The RTS impose more stringent security measures than the PSD2. The required identification of payment service providers is strengthened by demanding the use of certificates that also allow authentication. For electronic remote payment transactions, article 5 of the RTS enhances the required authentication by also imposing, among other things, a dynamic link that establishes integrity. However, this obligation only exists in the relationship between the user and the authenticating payment service provider. The RTS do not require that the authentication code is secured by a digital signature. The bank does not need to be able to verify the authentication or the integrity of the payment order.\(^4\) The RTS probably do not impose this requirement because digital signature technology is not in wide-spread use yet. However, it is right thing to use in this situation, not only because of additional security guarantees (non-repudiation), but also because signed statements can be passed on by the payment service provider and can be verified by the bank itself. Without this requirement, the RTS do not take away the additional risks that are created by allowing payment service providers to use their own authentication procedures (Section 4.4). Fig. 5 gives an overview of the differences between the PSD2 and the RTS.

5. Synthesis and conclusion

This article addresses the following research question: To what extent does the access to accounts of the payment initiation service providers and account information service providers balance the development of the market for payment services with the security of the payment account and the privacy of the user? An analysis of the PSD2 and the RTS shows that the development of the market for payment services has a higher priority. Security and privacy are ultimately subordinate.

First, the PSD2 does not adequately protect the personal data of the users. On the one hand, the access to accounts is limited in several ways and the GDPR applies to the provision of payment services (Section 2.3). However, the definition of 'account information service' is broad and covers a wide range of services. This facilitates innovation on the market for payment services but also allows the payment service providers to circumvent the limitations of the access to accounts (Section 2.2). Furthermore, the PSD2 does not address the privacy consequences that can result from the large scale processing of account information (Section 2.3).

The compromise about the admissibility of screen scraping leads to a similar conclusion (Section 4.2). Screen scraping gives a payment service provider unlimited access to the account of the user, even if this access is not necessary for the provision of the payment service. For this reason, the EBA has advocated for a prohibition. However, the European Commission has decided that the risk of a restriction of the competition is more important. The adopted RTS allow payment service providers to utilise the user interface if the dedicated interface is not functioning properly. This access to the user interface is constrained by several safeguards. However, these safeguards only enable ex-post review, after the payment service provider has already had unlimited access. Again, the protection of the innovation and competition on the market for payment services trumps the security of the payment accounts and the privacy of the users. The possibility of an exemption does not diminish the conclusion. After all, a bank can only obtain such an exemption if the dedicated interface complies with all of the requirements of the RTS has been tested by the payment service providers, has been widely used for at least three months and any problems have been resolved without undue delay. There is no real risk of a restriction of the innovation and competition if these conditions are met.

The norms on strong customer authentication also emphasise innovation and competition over the security of the payment account. The payment service providers have the right to rely on the authentication process of the bank. However, the RTS do not clarify how this process should be resolved (Section 4.3). Instead, the freedom of the payment

---

\(^2\) See also PSD2, recital 95; Steennot (n 3) 959.

\(^3\) About these concepts, see also Philip J. Windley, Digital Identity (O’Reilly Media 2005) chs 6–7.

\(^4\) See also RTS, recital 4. The recital only mentions a digital signature as one of the possibilities to create a dynamic link.
service providers to arrange the authentication as they see fit outweighs the interest of making this process as secure as possible. Even though redirection or a decoupled approach can be more secure, the PSD2 and the RTS suggest that the authentication, including the personalised security credentials issued by the bank, can also be resolved through the payment service provider via an embedded approach.

This ordering of interests also applies if the payment service providers use their own authentication process. Although the PSD2 does not state this explicitly, the bank seems to be required to rely on the payment service provider. The PSD2 and RTS do not demand that the bank is able to verify the authentication. For example, it cannot require a digital signature from the user (Sections 4.4–4.6). The bank only has limited options to restrict the access to accounts (Section 4.5). For this reason, it only has a limited power to restrict the provision of payment services. However, it also leads to a multiplication of the risks. In theory, a criminal can gain access to an account through every payment initiation or account information service provider.

The RTS increase the security. They impose more stringent security measures than the PSD2 (Section 4.6). At the same time, they do not alter the principal ordering of the PSD2: payment service providers have extensive opportunities to offer their services, even if this increases the risks.

The PSD2 prioritises the development of the market for payment services over the security of the payment account and the privacy of the user. This does not automatically mean that the users are not adequately protected. In the end, it depends on the reliability of the payment service providers. The PSD2 assumes that they can be trusted as long as they comply with the requirements for an authorisation or registration (Section 2). This assumption will be tested in the next few years. The security of the payment accounts and the privacy of the users could come under pressure if, in some member states or in the entire European Union, the authorisations are granted too easily or if the supervision by the competent authorities is lacking. Furthermore, they could be at risk if the payment service providers start using a large variety of alternative authentication processes without properly testing them.

This places the banks in a troublesome position. The removal of their legal monopoly to the access to accounts is the most important goal of the PSD2. A measure against the abuse of this access can easily be interpreted as an illegal restriction of the competition. At the same time, the banks are obligated to protect personal data and prevent fraud (Section 4.5). They can use these legal obligations to limit the access of unreliable third parties and stimulate the development of secure alternative authentication processes in cooperation with legitimate payment service providers and competent authorities. However, these options should never be used to restrict competition.

The PSD2 does not guarantee security and privacy when these goals conflict with the development of the market for payment services. In these situations, security and privacy depend on the application of the PSD2. They rely on the provision and use of payment services and the development of the legal norms by banks, payment service providers and competent authorities.