The potential risks of the introduction of the second Payment Service Directive (PSD II)

With regards to 3rd party access to accounts and strong customer authentication

Vrije Universiteit, Amsterdam
IT audit, Compliance & Advisory

Name: Sanne Fransen
Email: sanne.fransen@nl.ey.com
Student number: 1854321
Thesis number: 8019
Supervisor VU: Paul Harmzen
Supervisor: Rudrani Djwalapersad
1 Preface

With this research I conclude 2.5 years of study at the Vrije Universiteit as part of the Executive Master IT Audit, Compliance & Advisory. Time flew by and I am grateful that I’ve been given the opportunity to study next to my daily job. I would like to express my gratitude to Paul Harmzen, who supervised and supported me during this process in a very professional and dedicated manner. I enjoyed our conversations and his growing interest in the topic. Also, I would like to thank Rudrani Djwalapersad for involving me in PSD II related activities within our team. I hope this research is just the starting point of my knowledge about the topic which I can develop further and put into practice. Next, I would like to thank my study colleagues for the support and many nice conversations we’ve had. Finally, special thanks go to Thomas Kal, who motivated me, provided me with unconditional support and enlightened me with his eternal optimism.

Sanne Fransen

Amsterdam, April 2019
2 Abstract

The key drivers for the introduction of PSD II were the growth in the number of internet- and mobile payments as well as the rapidly evolving European Fintech sector. Since the 19th of February 2019, the last European country officially transposed PSD II in their national legislation. PSD II is supported by six guidelines and five Regulatory Technical Standards (RTS). These include the RTS on Strong Customer Authentication and Common and Secure Communication. With the arrival of PSD II, the traditional payment landscape is facing disruptions. Banks are no longer responsible for the entire payments value chain resulting in reduced control. Also, new players entering the market implies new entries for attack. This research examined the risks for banks related to Strong Customer Authentication (SCA) and Third-Party Access to Accounts (XS2A).

The modus operandi for fraudsters are changing due to PSD II and the specific requirements of the RTS. Fraudsters can aim for the Application Programming Interfaces (APIs), by hacking the systems and processes of the third-party providers (TPPs). Also, the entrance of new players (and their solutions) can possibly result in a loss of customer ownership and insight for the banks. Banks should keep up with the innovations of TPPs since providing new services could possibly increase customer insight. Another potential risk lies in the radical changes that are needed to comply with the principle-based requirements of the RTS. Also, banks might face an increase in cyber-attacks due to the introduction of PSD II and there is a risk of misalignment between XS2A and the GDPR, which could result in high fines.

Banks do acknowledge the risk of a threatened customer experience due to enforcing SCA. However, there seems to be a certain risk acceptance since there are arguments which outweigh the risk. Also, transaction monitoring complexities exist due to the fact that first a system should be developed, where after rules are described, implemented and connected to the entire infrastructure. These complexities could lead to misunderstandings, excessive costs and time-consuming activities to implement proper mechanisms. The final risk is related to the new phishing possibilities that could be on the rise when players in the field choose for the embedded approach when implementing APIs. When using the embedded approach, the data of customers is entered in the TPP environment, which is sent to the bank via an API. Since banks do not know whether TPPs set up proper processes and protocols and the customer does not know whether its credentials are shared with a valid TPP, phishing possibilities are increased. This research resulted in a validated risk framework which can be used by banks as a starting point to mitigate the risks associated to XS2A and SCA.
3 Table of Contents

1 Preface .................................................................................................................................... 2
2 Abstract ................................................................................................................................... 3
3 Table of Contents ..................................................................................................................... 4
4 Abbreviations .......................................................................................................................... 6
5 Introduction ............................................................................................................................. 7
   5.1 Background & Trigger ....................................................................................................... 7
   5.2 Research Question & Sub-questions .................................................................................. 8
   5.3 Scope ............................................................................................................................... 9
   5.4 Research Methodology ..................................................................................................... 9
6 Theoretical Framework ........................................................................................................... 11
   6.1 The need to replace the PSD I Directive by the PSD II Directive ....................................... 11
       6.1.1 PSD I as the first step to a single European payment market .................................... 11
       6.1.2 The necessary introduction of PSD II ....................................................................... 12
   6.2 The main requirements of the PSD II Directive ................................................................ 13
       6.2.1 Existing & new payment services ............................................................................. 14
       6.2.2 Third party access to bank accounts ........................................................................ 17
       6.2.3 Strong customer authentication .............................................................................. 18
       6.2.4 Other requirements of the Revised Payment Services Directive ............................... 22
   6.3 The possible IT implications of the PSD II requirement regarding third party access to accounts ................................................................................................................................... 23
       6.3.1 New & changing fraud risks ..................................................................................... 23
       6.3.2 Decrease in revenue & market position ..................................................................... 24
       6.3.3 Loss of customer ownership & insight ...................................................................... 25
       6.3.4 Radical changes required to comply with principle-based requirements of RTS ........ 25
       6.3.5 Increase in cyber-attacks due to open interfaces (API) ............................................. 26
       6.3.6 Alignment of XS2A with the GDPR ........................................................................... 26
   6.4 The possible IT implications of the PSD II requirement regarding strong customer authentication ................................................................................................................................... 27
       6.4.1 Threatened customer experience ............................................................................. 28
       6.4.2 Transaction monitoring complexities ....................................................................... 28
   6.5 The PSD II Risk Framework ............................................................................................. 29
7 Empirical Research ................................................................................................................. 31
   7.1 Validating the Risk Framework ....................................................................................... 31
       7.1.1 Third Party Access to Accounts .............................................................................. 31

4
7.1.2 Strong Customer Authentication ................................................................. 35
7.2 Extending the Risk Framework ................................................................. 37
7.3 Redefining the extended Risk Framework ............................................... 38
8 Conclusion .................................................................................................... 41
8.1 Answering sub-questions ........................................................................ 41
8.2 Answering central question ...................................................................... 43
8.3 Directions for further research ............................................................... 45
8.4 Personal reflection .................................................................................... 45
9 Literature List ............................................................................................... 46
4 Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AISP</td>
<td>Account Information Service Provider</td>
</tr>
<tr>
<td>API</td>
<td>Application Programming Interface</td>
</tr>
<tr>
<td>ASPSP</td>
<td>Account Servicing Payment Service Provider</td>
</tr>
<tr>
<td>B2B</td>
<td>Business to Business</td>
</tr>
<tr>
<td>EEA</td>
<td>European Economic Area</td>
</tr>
<tr>
<td>EBA</td>
<td>European Banking Authority</td>
</tr>
<tr>
<td>ECB</td>
<td>European Central Bank</td>
</tr>
<tr>
<td>GDPR</td>
<td>General Data Protection Regulation</td>
</tr>
<tr>
<td>PISP</td>
<td>Payment Initiation Service Provider</td>
</tr>
<tr>
<td>PSP</td>
<td>Payment Service Provider</td>
</tr>
<tr>
<td>PSD I</td>
<td>Payment Service Directive</td>
</tr>
<tr>
<td>PSD II</td>
<td>Second Payment Service Directive</td>
</tr>
<tr>
<td>PSU</td>
<td>Payment Service User</td>
</tr>
<tr>
<td>QTSP</td>
<td>Qualified Trust Service Provider</td>
</tr>
<tr>
<td>ROPA</td>
<td>Record of Processing Activities</td>
</tr>
<tr>
<td>RTS on SCA &amp; CSC</td>
<td>Regulatory Technical Standards on Strong Customer Authentication &amp; Common and Secure Communication</td>
</tr>
<tr>
<td>SEPA</td>
<td>Single Euro Payments Area</td>
</tr>
<tr>
<td>SCA</td>
<td>Strong Customer Authentication</td>
</tr>
<tr>
<td>TPP</td>
<td>Third Party Provider</td>
</tr>
<tr>
<td>XS2A</td>
<td>(third party) Access to Accounts</td>
</tr>
</tbody>
</table>
5 Introduction

5.1 Background & Trigger

On November 1st 2009, the EU Directive 2007/64 came into effect, known in the market as the 'Payment Service Directive' (PSD I). By creating a single legal framework for payments within the EU, the European Parliament aimed to create a uniform payment market. The goal of PSD I was to make cross-border payment transactions as simple, efficient and as secure as the domestic payment transactions of individual EU countries (European Commission, 2007). The growth in the number of internet- and mobile payments as well as the rapidly evolving European Fintech sector has led to the fact that the PSD I is no longer covering all payment services. The Directive had to be revised. Therefore, on January 13, 2018 the EU Directive 2015/2366, known in the market as the second 'Payment Service Directive' (PSD II), came into effect (European Commission, 2015a).

PSD II has three objectives. Firstly, the Directive strengthens the internal market for card-, internet- and mobile payments. Secondly, innovations are encouraged and facilitated, among other things by regulating newly introduced payment services that have entered the payment market after the publication of PSD I. Finally, PSD II aims to remedy the shortcomings identified of its predecessor (Ministry of Finance & Ministry of Security and Justice, 2016). Some of the most fundamental changes of PSD II include: third party access to accounts (XS2A), strong customer authentication (SCA), the introduction of two new payment services and stricter conditions for licensing (European Commission, 2015a).

With the arrival of PSD II, two new types of payment services are being introduced: the payment initiation service provider or PISP and the account information service provider or AISP. Lammerts et al. (2017) describe that a PISP can make a payment on behalf of a user, for example when purchasing an item in a web store. In that case, the customer can give the PISP permission to access his / her payment account with another payment service provider, such as a bank. On the other hand, an AISP can provide consolidated information from one or more payment accounts on the instructions of a user. In this light, third party access to accounts and the importance of strong customer authentication in connection with the consent that must be granted is a major factor due to the arrival of these new payment services. The introduction of these new payment services, under the PSD II known as Third Party Providers (TPPs), plays a central role in this research.

What possible (IT) risks does third party access to accounts and strong customer authentication entail? Banks have enormous amounts of data such as transaction data, customer data, creditworthiness data, etc. With the arrival of PSD II, the ECB facilitates the concept of 'Open Banking', the exploitation of
customer data. Open Banking foresees in the possibility for third parties to use data from the banking domain and offer new services based on this data (Voerman, 2017). In such a situation, banks will have reduced control over the data. Banks have invested greatly over the years in securing their ecosystem, but with the arrival of new payment services, banks are no longer responsible for the entire payments value chain. If banks do bear the responsibility for the entire chain of payments, it is possible to recognize all the risks within this chain. However, due to the arrival of Open Banking the ecosystem grows but the level of control is reduced. This involves possible (new) risks for the banks. For example, an important question that can be posed is: how can banks ensure that users have given their permission to execute payments or payment related actions?

This research examines the possible risks related to third party access to accounts and strong customer authentication, mainly from the perspective of the banks. What risks arise from the introduction of PSD II and how can these risks be controlled?

5.2 Research Question & Sub-questions

Based on the in chapter 5.1 described background and trigger for this research, the following central question has been formulated:

Research question:
What are the possible risks of the introduction of the second Payment Service Directive in terms of third party access to accounts and strong customer authentication?

To answer the research question as formulated above, the following sub-questions are drafted:

Sub-questions:
I. What is the need to replace the PSD I Directive by the PSD II Directive?
II. What are the main requirements of the PSD II Directive?
III. What are the possible IT implications of the PSD II requirement regarding third party access to accounts?
IV. What are the possible IT implications of the PSD II requirement regarding strong customer authentication?
5.3 Scope

Within the PSD II Directive, primarily five players play a role; three existing and two new players. PSD II introduces two new players in the market: the Payment Initiation Service Provider (PISP) and the Account Information Service Provider (AISP). Next to this, Payment Service Users (PSU) are operating as the clients that hold a bank account. This can be both a company and a consumer, but also the government. The Payment Service Providers (PSP) are the banks and other service providers of electronic payment services to customers. Finally, PSD II distinguishes traditional payment services providers, also known as Account Servicing Payment Service Providers (ASPSP). These are the banks. Customers hold accounts here and initiate payments via an ASPSP.

This research focuses on the risks that arise for the traditional banks, often functioning in the role as ASPSPs. Over the years, ASPSPs spent a lot of time and money securing and protecting their entire ecosystem. However, responsibilities become more scattered with the introduction of PSD II, since the (opportunities within the) ecosystem are enlarged, but the amount of control traditional banks had is reduced. ASPSPs are not the only player responsible for the payment value chain any more. This potentially changes the amount and the type of risks for banks. This research focuses on these potential new risks for the banks.

5.4 Research Methodology

The chosen research strategy is based on the objective of this research and is in line with the research questions drafted. This research starts with outlining the theoretical framework in which the following concepts around PSD II are highlighted:

- The need and background of the introduction of PSD II;
- An elaboration of the most important requirements of the PSD II Directive;
- The possible implications of PSD II within the field of third party access to accounts (XS2A) and strong customer authentication (SCA);

Subsequently, an empirical analysis is conducted by means of a case study. The risks as derived from the literature review are tested and expanded if deemed necessary based on in-depth investigations conducted at two Dutch banks. This research follows the approach of Robert Yin (2014) as described in his book “Case Study Research: Design and Methods”. The chosen typology of the case study is a holistic multiple case design (single unit of analysis at multiple cases). The research results are evaluated and linked to the theoretical framework. Finally, an attempt is made to formulate an answer to the research question.
In order to understand and identify aspects that are intrinsic to the risks related to XS2A and SCA, a qualitative research method is chosen. Qualitative research is useful for understanding why underlying relationships occur as they do and the rationale behind it. Also, qualitative research provides rich data which is useful to explain phenomena. Since little is known about the risks related to XS2A and SCA, this study is exploratory in nature because “an exploratory study is a valuable means of finding out what is happening; to seek new insights, to ask questions and to assess phenomena in a new light” (Saunders, Lewis & Thornhill, 2009:139).

As part of this qualitative research, the risk framework deriving from the theoretical research is tested in practice at the banks. This is done by conducting interviews and inspecting supporting documentation. In order to test the risk framework on completeness, semi-structured interviews are conducted. Semi-structured interviews exist of a pre-determined set of open questions, but there is also space to ask unstructured follow-up questions resulting from the time and scope a respondent gets to express their opinions on a particular subject. The interviews allow flexibility to stimulate unstructured discussions (Saunders et al., 2009).
6 Theoretical Framework

PSD II addresses all the concepts that businesses, customers and fraudsters have in common: online payments, 24x7 service, speed and seamless experiences across channels. PSD II was adopted by the European Union in 2015 to improve the existing rules of PSD I and take new digital payment services into account. The main goal of PSD II is to make it easier, faster, and less expensive for consumers to pay for goods and services, by “promoting innovation enhancing payment security, and standardizing payment systems across Europe.” (Sandrock and Firnges, 2016). More specifically, the primary goals of PSD II are to: a) make it easier and safer to use internet payment services; b) better protect consumers against fraud, abuse, and payment problems; c) promote innovative mobile and internet payment services; d) strengthen consumer rights and e) strengthen the role of the European Banking Authority (EBA) to coordinate supervisory authorities and draft technical standards (European Commission, 2015a).

Due to the new legislation, third party providers (TPPs) can now be used by bank customers to manage their finances. PSD II introduces the concept of Access to Accounts (XS2A), a requirement which obliges banks to provide TPPs with access to their customer’s account data through application programming interfaces (API). In this way, third parties are enabled to build financial services on top of the bank’s data and infrastructure (Helstrom, n.d.). Note that TPPs refer to a diverse group of potential players such as Fintechs, merchants, banks, and payment institutions, as long as they adhere to the regulatory requirements of PSD II (Cortet, Jung, Matzner & Schaefer, 2017). The traditional way to think about banking and financial services, is to think about banks as the main providers. However, as Bill Gates stated in 1990: “Banking is necessary, banks are not”. PSD II might act as a facilitator in the changing financial market, but could also introduce a new range of risks that banks are not yet prepared for.

6.1 The need to replace the PSD I Directive by the PSD II Directive

6.1.1 PSD I as the first step to a single European payment market

After the start of the European Union and the introduction of the Euro as a currency, free traffic of individuals, services, capital and goods was allowed. As a result, there was an increase in economic activity across the different EU member states. As of 2002, euro notes and coins circulated freely throughout the euro area. However, electronic euro payments were still organized at a national level. The European payment systems did not undergo the necessary transformations to strengthen this new form of economic growth (long execution times, high transaction fees).
Seeking further harmonization within its borders, the EU aimed at standardizing payments methods and enabling more competition. In 2007, Directive 2007/64/EC, known as the first Payment Service Directive (PSD I) was developed, adopted and implemented by all 30 member states (European Commission, 2007). PSD I established a modern and harmonized legal framework necessary for the creation of an integrated payments market to facilitate quick, efficient and secure payments throughout the EU. The main objectives of PSD I were: making cross-border payments as easy, efficient and secure as domestic payments, increasing competition by opening the payment market to new entrants and establishing the legal foundations for the key achievement of PSD I: the Single Euro Payments Area (SEPA) initiative. With the introduction of SEPA, costs for cross-border payments were reduced to the same level as domestic payments. Also, efficiency of cross-border payments was improved and the fragmented national market for euro payments turned into a single ‘domestic’ market (European Commission, 2012).

Since the adoption of PSD I, new digital payment services were invented, such as the account information service. This service provides the payment service user aggregated valuable online information on payment accounts hereby enabling a continuous overall view of its financial situation. The growth in the number of internet- and mobile payments as well as the rapidly evolving European Fintech sector has led to the fact that the PSD I was no longer covering all payment services. The Directive had to be revised.

6.1.2 The necessary introduction of PSD II

The European Commission proposed a review on PSD I to modernise it and consider new types of payment services. The revision of the Directive was inevitable since these new service providers were previously unregulated although they brought a lot of innovation and competition by providing more and cheaper alternatives for internet payments. Bringing them within the scope of the PSD significantly increased transparency, innovation and security (European Commission, 2018).

Furthermore, PSD I provided the possibility for Member States to individually transpose or apply certain rules as set out in the Directive. However, this led to both regulatory arbitrage and legal uncertainty. Moreover, in several areas it also created weakened consumer protection and competitive distortions. Since consumer protection in the context of payments is highly important, updated definitions would ensure a level playing field between different providers (European Commission, 2018).

As PSD I stimulated payment institutions to introduce new online and mobile commerce payment services, the introduction of PSD II led us to another transformational change in the EU payment landscape. PSD II builds on the initial goals as set out in PSD I, such as further achieving harmonization of the EU payments landscape. However, PSD II goes beyond the objectives of its predecessor, by strengthening consumer protection, to drive competition and facilitate innovation by further opening the payments market (Cortet
et al., 2017). The revised payment services Directive is providing a legal framework for these new types of payment services and parties.

PSD II introduces some important changes to the regulatory framework for payment services, including expanding the scope of coverage, clarifying the extent of consumer rights and provider obligations and introducing security and authentication requirements. PSD II also provides a more integrated approach to financial services regulation. The EBA, working in close co-operation with the European Central Bank (ECB), plays a crucial role in the delivery of PSD II (Donnelly, 2016).

Since PSD I was adopted in 2007, new services have emerged in the area of internet payments. Until then, the banks themselves managed their customer account information which they did not (or rarely) share with other banks or players in the market. PSD II sets out the requirements so that Third Party Payment Service Providers can access bank customer account information as it has become mandatory for banks to provide this information. As more providers will be allowed to retrieve valuable customer account information, innovation and competition will increase (Hatfield, 2017). As a result, banks fear for the persistence of their conservative business models and realize there is an urgent need to redefine them. PSD II makes it possible for many service providers to initiate payments and access bank information from a customer’s account if the right authorizations are in place (European Commission, 2015a).

As the European Commission stated in their factsheet of January 2018, the main differences between PSD I and PSD II are that: “PSD II widens the scope of PSD I by covering new services and players as well as by extending the scope of existing services (payment instruments issued by payment service providers that do not manage the account of the payment service user), enabling their access to payment accounts.” Furthermore, with regards to authorisation and supervision of payment institutions, PSD II enhances cooperation and information exchange between authorities. The European Banking Authority (EBA) will maintain a central register of, under the PSD II authorised and registered, payment institutions. Furthermore, to increase the safety of electronic payments, PSD II introduced enhanced mandatory security measures for all payment service providers. More specifically, PSD II requires payment service providers to use strong customer authentication (SCA) for its transactions (European Commission, 2018). The main requirements, among which SCA, will be further explained in the next chapter.

### 6.2 The main requirements of the PSD II Directive

To focus on the possible risks that arise due to the introduction of new requirements under the PSD II, these main requirements should be explained first. This chapter starts with introducing all possible players in the payment field, following the concept of third party access to accounts (XS2A) and the requirements around strong customer authentication (SCA). The chapter ends with a short description of other essential
requirements of the Directive which will not be the main focus of this research, but contribute to an overall understanding of the topic.

6.2.1 Existing & new payment services

As stated earlier, on top of the already existing players within the payments playfield, the PSD II introduces two new types of TPPs (the AISP and the PISP). All stakeholders will be introduced below.

Payment Service Provider (PSP)
A PSP offers electronic payments services to customers (PSU’s). The group of PSP’s will start growing under PSD II. PSPs act as the gateway that offer e.g. retailers services for accepting payments since they are responsible for the security and authorization of payment transactions.

Payment Service User (PSU)
A PSU is the customer, which holds a bank account. This can be both a consumer and a business entity.

Account Servicing Payment Service Provider (ASPSP)
ASPSPs are the traditional financial institutions that provide payments services. The PSU holds one or more accounts at these institutions and issues payments from this platform. These players are the banks (e.g. European Bank) that hold customer accounts. Other financial institutions that are recognized and authorized as payment institutions, can also act as an ASPSP, such as credit card companies. Boden, Hipperson, Sawyer, Williams-Gardener & McParlane (2015) define in their Whitepaper of the Starling Bank ASPSPs as: 'any financial institution that offer payment accounts (e.g. current accounts, credit cards) with online access (internet banking) ...'.

Account Information Service Provider (AISP) - new
PSD II introduces two new types of TPPs. One of them is the Account Information Service Provider (AISP). An AISP aggregates data from customers (PSU) accounts from one or more ASPSPs. AISPs act as aggregators of a consenting customer’s financial information across all accounts and financial services institutions (e.g. money dashboard). Moreover, an AISP can provide a consolidated overview of all payments accounts of a customer on an online platform, even if those accounts are held on multiple PSPs. For example, if a customer has an account at Bank A and an account at Bank B, they will be able to view the balances and transactions from both banks from within the user interface provided by the AISP. In the light of the recently enforced General Data Protection Regulation (GDPR) it is useful to mention that the AISP cannot use customer data for any other purpose other than those provided by the service. An AISP will not be able to transfer funds out of a payment account, they only provide an aggregated view of past
transactions (Lammerts et al., 2017). Refer to figure 1 for a schematic overview of the role of AISPs before and after the introduction of PSD II.

**Payment Initiation Service Provider (PISP) - new**

Another TPP under PSD II is the PISP. This is a service provided by those that stand between the payer and his/her online payment account by starting a payment to a third-party beneficiary. In other words, PISPs act as a link between a payer’s bank account and a merchant’s banking platform. PSUs must give permission to PISPs to initiate payments on behalf of them. This is done by building a software bridge, known as an Application programming Interface (API) between the merchant and the banking platform (e.g. IDEAL, Sofort, Trustly). The payer can then make an online payment by direct debit on its account, using the PISP to initiate the transaction. The Directive does not require the PISP to be linked to the ASPSP from a contractual relationship to allow operations on the account of the payer. Besides this, the PSP (where the PSUs/ASPSPs account is held) shall ensure that the PISP has access to the online account of the payer. Also, the PISP should not come into possession of the funds from the payer (Lammerts et al., 2017).
To complete an online purchase under the PSD I, you had to fill in all personal details and account information, before completing an additional authentication measure as required by your card issuer. When buying multiple products from different merchants, a similar exercise had to be repeated. Under the PSD II, the customer gives permission to a PISP to access his/her bank account and there is no need to provide the merchant with any card data or details. The next time when doing online purchases, customers access their bank account with their PISP through the website of the merchant, use their bank login and the PISP will direct debit it from the customer’s account (24Solutions, 2016). The change to a real-time transaction process means there is no longer a need for an acquirer or payment network and therefore also no interchange fee to account for anymore. Refer to figure 2 for a schematic overview of the role of PISPs under PSD II.

Figure 2: PISPs under PSD II

<table>
<thead>
<tr>
<th>Legend</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consumer</td>
<td>Buys a service or goods from a merchant, uses PISP to initiate payment</td>
</tr>
<tr>
<td>Merchant</td>
<td>Company that sells the service or goods</td>
</tr>
<tr>
<td>PISP</td>
<td>Initiates payment for consumer by accessing its account</td>
</tr>
<tr>
<td>Acquiring bank</td>
<td>Maintains merchant’s bank account; receives payment via card network</td>
</tr>
<tr>
<td>Issuing bank</td>
<td>Maintains consumer’s bank account; exchanges payment as instructed by the PISP via card network to Acquirer</td>
</tr>
</tbody>
</table>
6.2.2 Third party access to bank accounts

The banking industry has been tightly controlled and heavily regulated. Technology changes have tended to be evolutionary rather than disruptive (Mansfield - Devine, 2016). Until now. Following the discussion in chapter 5.2.1, new TPPs can enter the payments playfield when PSD II came into force. Up till then, it was almost impossible for TPPs to enter the financial services market as their solutions required access to consumer bank accounts. Banks are often not eager to share their data due to the fear for direct competition. PSD II enables access to customer's bank accounts not only to financial but also to non-financial institutions. This requirement is known as third party access to accounts (XS2A) and the impact will be huge. ASPSPs have to offer valuable data and processes without commercial contracts. Under PSD II, banks are forced by law to give TPPs access to customer accounts if the customer has given its consent. Article 35 of the Directive states: “Member States shall ensure that the rules on access of authorised or registered payment service providers that are legal persons to payment systems are objective, non-discriminatory and proportionate and that they do not inhibit access more than is necessary to safeguard against specific risks such as settlement risk, operational risk and business risk and to protect the financial and operational stability of the payment system” (European Commission, 2015a).

Access to customer's accounts will be gained by means of APIs, which will be discussed more in detail below. With this requirement, customers and potentially TPPs on behalf of its customers, will be able to carry out banking operations via APIs. Banks need new revenue streams to offset this change and they most likely have to invest in APIs to comply with the revised Directive (Mansfield - Devine, 2016). XS2A allows new players to come into the field. This is done by cutting out the middle man such as card payment providers that charge fees and whose fee structures and processes vary widely across Europe. In this way, the new open banking requirement could cut costs. However, other issues might arise, such as authentication and creating, managing and securing APIs. The question that raises is: will costs really be cut or will they just be replaced, for example because an entirely new infrastructure is required (Mansfield - Devine, 2016)?

Application Programming Interfaces

In addition to the PSD II directive, the EBA has developed five Regulatory Technical Standards (RTS) and six supporting guidelines. The RTS on Strong Customer Authentication & Common and Secure Communication (RTS on SCA & CSC, hereafter: RTS) is the main focus of this research. PSD II and its RTS are promoting access by TPPs to foster competition within the payment services market. APIs will allow all PISPs and AISPs to connect to ASPSPs in a secure an effective manner. APIs are a means for accelerating digital transformation and can be considered as a mechanism that allows the capabilities of a computer program to be used by other computers. An API is a software-to-software interface that allows web-based applications to communicate with each other and share data. Organizations with large data
platforms such as Google or Facebook offer APIs to third parties already for several years to stimulate third party innovation and share data (Woods, 2015). The use of APIs is not mandated by the Directive, however, the industry considers APIs as the best technical solution for PSD II compliance (Deutsche Bank, 2017).

XS2A for AISPs and PISPs
PSD II drives business and creates digital opportunities mainly for two new players in the payments field: AISPs and PISPs. Why do these parties require access to a customer’s bank account? AISPs can provide a consolidated overview of all payment accounts of a customer on an online platform. By means of XS2A, the Open Banking principle of PSD II, AISPs are allowed to aggregate customers’ data from one or more ASPSPs (but only if they have consent and use the data for the purpose that it was gathered for).

On the other hand, PISPs act as a link between a payer’s bank account and a merchant’s banking platform. By means of XS2A, PISPs can access a customer’s bank account to direct debit online purchases, if the customer gave permission to do so. Article 66 and 67 of the Directive prescribe rules on access to (and use of) payment accounts when using PISPs and AISPs. For example, article 66 states that PISPs shall not hold at any time the payer’s funds in connection with the provision of the payment initiation service or store sensitive payment data of the PSU. Article 67 states amongst others that the AISP, after receiving the PSUs specific consent, can access only the information from designated payment accounts and associated payment transactions (European Commission, 2015a).

6.2.3 Strong customer authentication
As explained above, PSD II facilitates the exploitation of customer data by means of open Banking. This will increase customer experience, but might also facilitate fraud. Customers who use open banking to make payments will not be protected by the card schemes such as MasterCard and Visa, but by their card issuer, which might open (other) possibilities for fraud. Banks are being tasked with building a new channel (API) and protecting it from fraud, however, by doing so they need to step out of their comfort zone since it is outside the data-context that banks are used to operate in (Feedzai, n.d.).

To stop these possible fraud gaps, PSD II introduces a new legal requirement regarding strong customer authentication (SCA) in payer-not-present context. The Directive identifies strong customer authentication as an ‘authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data’
(European Commission, 2015a). Examples of knowledge factors can be a password or an answer to a secret question, examples of possession factors can be a card reader or a token and inherence factors are often biometrical, such as a fingerprint reader. As of September 2019, unauthenticated payments that require SCA must be declined by the customer’s bank. As a result, the payment will have to be re-submitted to the customer with a request for SCA. Under PSD II the SCA-procedure is the responsibility of the ASPSP. PISPs must use the credentials issued by the ASPSP, unless there is a prior contractual agreement in place between the PISP and the ASPSP that the former’s credentials may be used (Mennes, 2017).

More specifically, SCA is required when customers are accessing their payment account online, initiate an electronic payment transaction or carry out any action through a remote channel which may imply a risk of payment fraud or other abuses (EBA, 2017). Organizations that can drive fraud levels down below well-defined levels will be able to bypass SCA for certain transaction amounts. Therefore, advanced fraud detection during the customer authentication process can play a critical role in minimizing the friction that customers experience during authentication. This is often referred to as transaction risk analysis and will be discussed below.

Exemptions on SCA

Often, enhanced security measures are not necessarily increasing the user-friendliness of certain actions, or in this case, payment related actions. To improve confidence in transactions over the internet, a proper balance between the interests in enhanced security in remote payments and needs of user-friendliness and accessibility should be established. To allow more user-friendly, accessible and innovative means of payment for low-risk payments, certain exemptions to the principle of SCA are drafted, considering the following elements (European Commission, 2015a):

a) The level of risk involved in the service provided;

b) The amount and/or the recurrence of the transaction;

c) The payment channel used for the execution of the transaction.

These exemptions as described in the RTS on SCA & CSC will be discussed in more detail below. Two of the exemptions are new in relation to PSD I, others are modified. The new exemptions are the ones with regards to (c) payment transactions at unattended payment terminals for transport and parking fares and (f) transaction risk analysis (Cortet et al., 2017).

PSPs are exempted from applying SCA where a PSU is consulting its (a) payment account information. More specifically, this applies when a PSU is limited to accessing the balance and/or the payment transactions executed in the last 90 days of one or more designated payment accounts without disclosure of sensitive data. These exemptions do not apply when the PSU is accessing the information for the first time or when SCA was applied more than 90 days ago. Another exemption is related to (b) contactless
payments at point of sale. If a PSU initiates a contactless electronic payment transaction where the amount is below EUR 50 and the cumulative amount, or the number of, previous contactless electronic payment transactions does not exceed respectively EUR 150 or 5 consecutive transactions, PSPs are exempted to apply SCA. Also, PSPs are exempted from applying SCA where the PSU initiates an electronic payment transaction at an unattended payment terminal for the purpose of paying a (c) transport or parking fee (e.g. to avoid queues, potential accidents at toll gates and the risk of shoulder surfing) (EBA, 2017).

PSPs are furthermore exempted from SCA in the case of (d) trusted beneficiaries and recurring transactions. This exemption applies when the payee is included in a list of trusted beneficiaries previously created/confirmed by the payer through its ASPSP or when the payer initiated a series of payment transactions with the same amount and the same payee. Another exemption is related to (e) payments to self. No SCA is required when the payer initiates a credit transfer where the payer and the payee are the same natural/legal person and both payment accounts are held by the same ASPSP. Furthermore, with regards to (f) low-value transactions; if a PSU initiates a remote electronic payment transaction where the amount is below EUR 30 and the cumulative amount, or the number of, previous remote electronic payment transactions does not exceed respectively EUR 100 or 5 consecutive transactions, PSPs are exempted to apply SCA (EBA, 2017).

Finally, the EBA drafted in its RTS an exemption on (g) transaction risk analysis. PSPs need to put in place transaction monitoring mechanisms in order to enable them for detecting unauthorized or fraudulent payment transactions. A PSP will be required to perform a real-time risk analysis to determine if SCA should be applied or not. When performing this risk analysis, PSPs will have to assess factors such as:

- Abnormal behaviour or spending;
- Previous purchase patterns;
- Unusual information about the payer’s device or software;
- Possibility that payee is in a high-risk location;
- Malware within the authentication procedure;
- Known fraud scenarios.

Based on the above elements, a risk score, or fraud rate, based on certain transaction monitoring parameters is calculated. The fraud rate should be assessed at the PSP-level, as it cannot be assessed on an individual basis for a specific merchant. The exemption on SCA will only be applicable if the PSP’s fraud rates do not exceed the thresholds as presented in table 1 (EBA, 2017):
Remote card-based payments | Credit transfers
---|---
EUR 500 | 0.01% | 0.005%
EUR 250 | 0.06% | 0.01%
EUR 100 | 0.13% | 0.015%

Table 1: Reference Fraud Rate (EBA, 2017)

Types of SCA
There are several types of SCA that can be applied by banks. These types can be divided into three main categories: **two-device authentication**, **two-app authentication** and **one-app authentication**.

1. **Two-device authentication** means that a customer makes use of two independent devices: one device is the mobile app or website (banking device) and the other device is to authenticate him/herself (authentication device), such as hardware authentication token or a dedicated app on a mobile device. The authentication device generates a one-time password (OTP).

2. **Two-app authentication** does not rely on two different devices, but on two different apps (running on the same device). When doing transactions, the banking app automatically opens the authentication app. After verification and confirmation, the authentication app generates an OTP which is send to the banking app for verification.

3. **One-app authentication** implies that a single app is used to initiate and authenticate transactions. The above categories can be combined with an out-of-band approach, whereby the OTP is generated by a separated communication channel (e.g. SMS, email) and sent to the user’s device (Mennes, 2017).

Security measures for the application of strong customer authentication
The Directive prescribes two important elements with regards to SCA. First, PSPs must ensure that when applying SCA, it includes elements that dynamically link the transaction to a specific amount and payee. Also, PSPs must have adequate security measures in place to protect the confidentiality and integrity of PSUs personalized security credentials. These two elements are explained more in detail below (European Commission, 2015a).

PSD II introduces a requirement for dynamic codes when doing electronic payment transactions. PSPs must apply strong authentication methods that include elements which dynamically link the transaction to a specific amount and payee. In this way, the PSU is always aware of the amount and the payee being authorized. More specifically, PSPs must adopt security measures that ensure the following (EBA, 2017):

a) The PSU is made aware of the amount of the payment transaction as well as the payee;

b) An authentication code is generated which is specific to the amount of the transaction and the payee agreed to the payer (PSU) when initiating the transaction;
c) The authentication code accepted by the PSP corresponds to the original amount of the transaction and the payee. Any change to the amount or the payee must result in an invalid authentication code.

Other security measures that must be in place are closely related to (protection of) the authentication code of the PSU. More specifically, if SCA is applied, the authentication based on two or more elements (knowledge, possession, inherence) must result in an authentication code. PSPs must ensure that no information on any of the elements of SCA can be derived from the disclosure of the authentication code. Also, it should not be possible to generate a new authentication code based on the knowledge of any previously generated codes. Finally, the authentication code cannot be forged.

Next to the above, the number of consecutive failed authentication attempts is maximum five. Both a temporary and a permanent block can be carried out. In case of the latter, an alert to the payer is guaranteed. Whenever a block is permanent, a secure procedure is established allowing the payer to regain use of the blocked electronic instruments. Finally, communication sessions are protected against manipulation or the capture of authentication data and the maximum time for inactivity after being authenticated is set at five minutes (EBA, 2017).

6.2.4 Other requirements of the Revised Payment Services Directive

Besides the PSD II requirements regarding XS2A and SCA, it is worth mentioning a few other changes/requirements for the sake of completeness. First, in relation to PSD I, the revised Payment Services Directive widens its scope. In terms of information and transparency, the ruleset applies to transactions in all currencies, not just EU currencies. In addition, the regulation is also applicable to transactions from the EU to outside the EU and vice versa. However, the regulation for these so-called 'one-leg' transactions only applies to the European part of the transaction (at least one participant is based in the EU). Furthermore, the PSD II complies with the SEPA directives with regard to the right to a refund on direct debit. Finally, the PSD II prohibits the charging of costs of payment transactions to the customer. In addition, a European regulation has been launched in which the level of interbank fees for debit and credit card payments is curbed ("Multilateral Interchange Fees" or MIFs). As of now, providers may charge a fee of no more than 0.2% of the total amount for debit card transactions and 0.3% for credit card transactions (European Commission, 2015b).
6.3 The possible IT implications of the PSD II requirement regarding third party access to accounts

Traditionally, European lawmakers indicated the dominance of banks, with their limited speed in bringing innovation to the payments area, as a key risk. Most innovation in the financial services sector was primarily introduced by non-banks, such as Fintechs. PSD II has a transformative impact, both on the front-end due to new services and propositions as well as on the back-end payment processing infrastructure. As a result, new or changing risks for banks might arise, especially since they are required to open up their customer database to TPPs. What are these possible implications of the new PSD II directive regarding XS2A for banks (Cortet et al., 2017)? The risks as described below are derived from the literature, varying from related laws & regulations, opinion articles, whitepapers and journals. The goal is to present an overview of risks that is as complete as possible.

6.3.1 New & changing fraud risks

Customers were traditionally protected by well-known players like MasterCard or Visa when doing payments, supported by industry standards such as PCI DSS (Payment Card Industry Data Security Standard). PCI DSS is an information security standard for organizations that handle branded credit cards from the major card schemes (PCI Security Standards Counsel, n.d.). However, customers who use open Banking under PSD II will now be protected by their card issuer. Furthermore, since TPPs can now act as intermediaries between customers and banks, banks might lose the grip on customer data where they traditionally relied on to make fraud-related decisions. Also, the entrance of TPPs means new data streams coming in, which could also lead to new risks (Tengur, 2017; Feedzai, n.d.).

Another potential issue is whether banks can judge the reliability of TPPs and identify potential fraudulent/unreliable TPPs. If direct access is allowed, ASPSPs are not able to check whether the TPP executes transactions conform the requirements of the PSU. Attackers who aim to commit large-scale identity fraud can set up a TPP to facilitate fraudulent payments and gain access to large amounts of confidential data. However, the greater risk lies in criminals who, for example, inject an existing TPP with malware. In addition, if the security at TPPs does not suffice, fraudulent actions or data leaks at these TPPs can indirectly lead to reputational damage for banks. Not to mention the fact that AISPss face a milder form of integrity supervision under the PSD II than other payment service providers, thereby increasing the risk of data misuse (Lammerts et al., 2017).

In short, new complexities are on the rise. There will be a fast increase in entry-points for attack for fraudsters, since banks are required to provide APIs to TPPs. PSD II acknowledges these fraud challenges,
and tries to mandate SCA to mitigate these risks, but the amount of complexities is so high that it is unknown whether SCA suffices. By fighting existing fraud, new/evolving fraud will arise. It is expected that there will be an increase in card-not-present fraud, director- and invoice fraud, new attacks on users of new payments services and new social engineering schemes (Feedzai, n.d.).

6.3.2 Decrease in revenue & market position

In Accenture’s research analysis of the United Kingdom payments market over 2016, it is predicted that UK banks may lose as much as 43% of their current payments-based revenues by 2020 due to forces in open banking. Figure 3 below indicates this possible decrease in revenue (Light, McFarlane, Barry & Ruotsila 2016). If banks indeed experience a decrease in their payments-based revenues and they are not able to keep up with the pace of innovation, this might endanger their market position.

For example, banks could experience a loss of fees from card-based transactions. Under the Interchange Fee Directive, providers may still charge 0.2% for debit card transactions and 0.3% for credit card transactions (European Commission, 2015b). PSD II introduces a simplified payments chain in which the card network can be disregarded. The change to a real-time transaction process means there is no longer a need for an acquirer or payment network and therefore also no interchange fee to account for anymore. Currently, this risk forms a notable threat for banks, but its impact depends on the level of adoption of PISP services, which is yet unknown (Light et al., 2016).

(%, EUR, Bn.)

![Figure 3: Retail payments revenue evolution in the UK 2015-2020 (Light et al., 2016)](image-url)
6.3.3 Loss of customer ownership & insight

Customer experience is yet to be perceived as one of the most vital elements for success. The bank's relationship with its customer has changed radically over the past years: from physical interactions, to online banking services and finally to mobile real-time payments. The introduction of XS2A poses a risk to banks regarding their customers' experience they have been developing for years. More specifically, the risk entails that banks might lose the direct contact with its customers and becoming more of a utility-type service used by new TPPs. Furthermore, access to customer account data as facilitated by AISP suggests that customers can fulfill their daily banking needs without meaningful engagement and visibility of the brand of the banks (Light et al., 2016).

Also, organizations such as Google or Apple and Fintech entrants focus more nowadays on enhanced products and customer experiences tailored to customer needs. This results in more competition for banks which might threaten their market position. However, the actual risk lies in the fact that TPPs can aggregate and integrate their newly developed services. Access to multiple stand-alone financial services products can be provided via a single platform, integrated with customer’s existing accounts and transactional data. For banks this could result in a loss of customer insight (Light et al., 2016).

6.3.4 Radical changes required to comply with principle-based requirements of RTS

As stated earlier, the RTS on SCA and CSC is the main focus of this research. Cortet et al. (2017) mention in their research that the RTS provides guidance in the form of principle-based requirements, but do not provide banks and other market players with technical specifications. Therefore, additional work is required in order to become compliant and develop technological solutions to complement the principle-based RTS requirements. Pan-European interoperability is the implicit promise of PSD II. Cortet et al. (2017) mention that “… in an open payment market, there would be a single message - and communication interface - standard, complete with operational and governance procedures with full pan-European reach, for innovative and trusted transaction services enabled by third party access to accounts”. Banks could profit from this pan-European interoperability by gaining a positive ROI on PSD II compliance investments. Since concrete technical specifications are missing, the following risks for banks might exist: a) development of unsuitable technological solutions; b) loss of revenue due to high investments in costs and time for R&D; c) losing market share and falling behind on competitors when doing nothing.

Furthermore, radical changes in IT infrastructure are required for banks. The problem is that there are still many banks who use old legacy systems and not modern IT-architecture. Therefore, a risk lies in the
incapability of banks to provide APIs for TPPs (24Solutions, 2016). There are also more operational risks related to the immature processes around APIs. There could be failures in transaction processing for PISPs and AISPs, errors in data provision, accounting errors on business volumes carried out with API developers and so on (Rohan, 2016).

6.3.5 Increase in cyber-attacks due to open interfaces (API)

In line with 6.3.2, where the risk of a possible decrease in revenue is highlighted, another area of risk for banks is the expected increase in cyberattacks due to the introduction of APIs. As a result, this might also affect a bank’s revenue, since cyberattacks lead to an increase in cyber protection costs and/or an increase in recovery costs due to an attack. APIs will therefore become an additional security issue for banks since it processes customer/transactional/financial data (24Solutions, 2016). As per Eroglu et al. (2016), “by providing their APIs to TPPs, banks open up a significantly greater attack surface to potential cyber adversaries and can no longer hide critical applications behind perimeter firewalls”. If a sound architectural approach is missing with security processes that are not quickly able to adapt or respond, banks will become more vulnerable for cyberattacks (Eroglu et al., 2016). Mansfield - Devine (2016) explains in his research that the more doors you open, the bigger is your attack surface. In addition, more players involved means more possibilities for failure. Once TPPs get involved, how do banks mandate that similar security standards are being followed?

Generally, APIs have been considered as relative trustworthy business – to – business (B2B) communication. As a result, controls have not been enforced as strongly as in customer environments. The risk exists that banks do not apply the correct architectural approach when designing APIs. As a result, the security layer might not be able to fully address issues regarding access control, threat detection, confidentiality and integrity, making the API vulnerable to attacks (e.g. DDoS attacks). Concluding, banks might face an increase in cyber-attacks since they must change their current architectural approach to an approach that is suitable for a new sort of API (Eroglu et al., 2016).

6.3.6 Alignment of XS2A with the GDPR

As of May 2018, the General Data Protection Regulation (GDPR) came into force. The GDPR is an EU regulation addressing data protection and privacy for all individuals within the European Economic Area (EEA; EU including Iceland, Norway and Liechtenstein). The regulation aims to give people greater power and control over their data and require organizations to be more transparent in how they deal with their customer’s data (European Commission, 2016). New requirements regarding accountability, documentation and privacy by design are accompanied by high fines for organizations in case of non-
compliance (4% of annual turnover of previous year, up till 20mln). As a result, the risk landscape will change significantly (Eroglu et al., 2016).

Due to the introduction of open banking the following changes might have its impact on GDPR compliance for banks:

- There is a significant increase in communication channels (APIs) in which personal identifiable data flows. Under the GDPR, banks need to know which channels are used, where and what personal data flows and what security measures to take. APIs should be designed to maximise privacy and security (privacy by design);
- Banks might face a limited understanding of its client data (also refer to 6.3.3), and, volumes of data are increasing. This might conflict with the GDPR requirements that banks should provide transparency of its customer data and need to know where their data flows. In other words, banks need to maintain a Record of Processing activities (RoPa).

If banks are not able to comply with the above, they face a huge risk of getting fined by not acting in accordance with the requirements as set out in the GDPR. The issues that arise due to the creation of an open banking payments area, might be impacted and amplified if banks fail to align their revised infrastructure with the GDPR (Eroglu et al., 2016).

### 6.4 The possible IT implications of the PSD II requirement regarding strong customer authentication

Now that PSD II mandates banks to provide APIs to TPPs, fraudsters enjoy a proliferation of entry points for attack. The directive tries to control these new fraud challenges by mandating SCA. Under PSD II, SCA is the responsibility of the ASPSP, which are the banks. Primarily, SCA is intended to secure the customer and reduce fraud during payment-related actions. Over the years, banks have invested a lot of time in securing online authentication for services (e.g. online banking). Methods such as two-factor authentication and out-of-band authentication have become common, but do not go without issues. For example, cyberattacks in the form of banking Trojans have evolved by attacking both desktop and mobile platforms to intercept both codes (Mansfield - Devine, 2016). Implementing SCA that complies with the requirements of the RTS and the friction that it poses might cause new risks for banks. What are these possible IT implications for banks regarding the Directive's requirements related to SCA? Similar to what has been described in chapter 6.3., the risks as presented below are meant to be as complete as possible and are derived from the literature.
6.4.1 Threatened customer experience

Under the new payments regulation, banks are obliged to use SCA when customers are accessing their payment account online, initiate an electronic payment transaction or carry out any action through a remote channel which may imply a risk of payment fraud or other abuses (EBA, 2017). SCA means that customers need to perform several, often independent, actions in order to authenticate themselves. As a result, gaining access will become less frictionless for customers, causing reduced customer satisfaction. SCA can be applicable during the entire payment experience and the risk of losing appeal to customers which could eventually lead to a dropping market share is of great significance for banks.

There is a thin line between transaction security and customer experience. In recent years, regulators are striving for greater security, although customers have been often prioritizing experience over security. The impact of the requirements for SCA will radically change the customer experience and journey since two-factor authentication will be required for transactions and account access. One of PSD II’s objectives is to encourage and facilitate innovations. However, these SCA restrictions could potentially limit innovation, rather than stimulating it.

The EBA is aware of the possible friction that SCA causes, and therefore included clauses for exemptions of SCA. These exemptions are much debated, since it is hard to find a balance between security, innovation, user-friendliness and accessibility. In order to rely on any of these exemptions, PSPs must have proper transaction monitoring mechanisms in place which are able to detect unauthorized transactions. This will be discussed more in detail in 6.4.2. This is crucial in reducing customer friction since it creates the foundation of authenticating payment transactions from a risk-based perspective.

6.4.2 Transaction monitoring complexities

As stated above, a risk-based approach will be key to reduce fraud but maintain a certain level of user-friendliness. Therefore, the EBA introduced exemptions to SCA in its RTS for which banks should have transaction monitoring mechanisms in place. These mechanisms are developed to detect unauthorized transactions and include real-time risk monitoring. Banks must identify a transaction as low risk only when it meets certain conditions as discussed in chapter 6.2.3 of this research. A PSP that adequately monitors transactions can intervene during unusual transactions or in case of transaction patterns. However, an incorrect or incomplete transaction monitoring model and control framework may lead to high costs for banks. Also, if banks (or other PSPs) fail to ensure adequate monitoring, they might unconsciously cooperate in terrorist financing or money laundering practices (DNB, 2017). The EBA mandates PSPs to record and monitor all their fraud rates as well as the results of the transaction risk analysis method used.
The risk of incorrect or expensive transaction monitoring practices may also arise from the fact that the obligation is principle based. The DNB describes in its guidance on post-event transaction monitoring that "the practical interpretation of this requirement is not prescribed in detail by laws and regulations, or by the supervisory authority. This guidance provides you with indications on how to set up a transaction monitoring system. It is up to you as a payment services provider to determine how exactly you interpret this. The supervisory authority will assess the result" (DNB, 2017).

Due to the fact that new TPPs bring new streams of data, current fraud detection activities of banks should be adapted with new fraud detection rules. Mansfield - Devine (2016) explains in his research that banks are still liable for any fraudulent payments under PSD II, although they are no longer in sole charge and that is where the complexity increases. Banks were used to possess all information needed to establish whether a transaction is fraudulent. Real-time fraud was prevented by using packaged software with fraud scoring models. When customers are no longer logging on to their bank’s website (but via AISPs), the amount of relevant data available to banks will be reduced. Within this light, it will be challenging for banks to provide a secure infrastructure to TPPs. The new transactions through TPPs require revised scores/scoring models that reflect the transaction risk, which will take around two years to develop. In the meantime, banks will need to perform proactive transaction monitoring and develop their own rules to prevent fraud. This is both time and cost consuming (Eroglu, Bhatia, Bhardwaj & McFarlane 2016).

6.5 The PSD II Risk Framework
To present an overview of risks regarding SCA and XS2A which is as complete as possible, the risks as elaborated in chapter 6.3 and 6.4 have been validated with subject matter experts of a multinational professional services firm, performing both assurance and advisory services. The result of the theoretical research, in the form of a PSD II Risk Framework, will be used as input for the case study and can be seen in figure 4 below.
This research is focused on the risks that arise due to the implementation of PSD II with regards to SCA and XS2A. The case study will validate the aforementioned risks and possibly extend the framework when new risks arise based on the empirical research.

Figure 4: The XS2A & SCA Risk Framework
7 Empirical Research

The presented risk framework in chapter 6.5 is created as a result of the theoretical analysis. This research pursues to present a comprehensive, accurate and complete framework of risks which can be used by organizations to build, align or test their mitigating controls around. In order to do so, the framework as introduced above is tested in practice on accurateness and completeness at two Dutch banks who are closely involved with the implementation of PSD II. This chapter will validate the risk framework and update the framework where needed. Also, the risks will be rated on impact and likelihood, resulting in a risk score.

7.1 Validating the Risk Framework

7.1.1 Third Party Access to Accounts

New & changing fraud risks

As per chapter 6.3.1, it is expected that there will be an increase in card-not-present fraud, director- and invoice fraud, new attacks on users of new payments services and new social engineering schemes (Feedzai, n.d.). The results of the empirical analysis indicate that fraud risks are indeed expected to change and possibly increase since the payments chain gets longer and there will be a growth in the number of entry points. Banks were used to control this chain from end-to-end. They have a strong position in the card-schemes, IDEAL payments and within the issuer – merchant banking relationship. Now we are entering an ecosystem with new stakeholders, meaning banks will lose grip on the chain. Dutch banks agreed that the security of payment traffic is their common task and that they are not going to compete with each other with regards to security. Banks however, employ hundreds of people who work on security, but the smaller TPPs, such as FinTechs, might not have similar capacity and will therefore be more vulnerable to fraudsters.

TPPs having a license under the PSD II, does not provide 100% certainty that there will be no attacks. The risk still exists that a PISP will be hacked, resulting in fraudsters changing account numbers and manipulating money flows. Another example of a risk is TPPs having an invalid eIDAS certificate. ASPSPs should identify and authenticate TPPs through eIDAS qualified certificates for electronic seals or website authentication (Cortet et al., 2017). However, how do you prevent TPPs using a bank’s API with a certificate that is misused or withdrawn? Also, eIDAS certificates include a link to a Qualified Trust Service Provider (QTSP) to verify whether the certificate is still signed by the QTSP. There is a risk that the QTSP is compromised and therefore not trustworthy. Dealing with TPPs that use certificates for identification and authentication offers several possible weaknesses and entry points of attack.
In short, the *modus operandi* for fraudsters are changing due to PSD II, resulting in a high likelihood and a high impact for banks. Attackers can aim for the APIs, by hacking the systems and processes of the TPP. However, the weakest link is still the bank’s customer: under the PSD II, customers ‘learn’ that it is acceptable to share credentials with third parties, which opens many doors for fraudsters. Controls to mitigate fraud should not therefore only be focused on technical solutions, but also on soft controls, such as training & awareness.

**Decrease in revenue & market position**

The theoretical research indicated that banks might lose a considerable share of their payment-based revenues due to forces in open banking, which might result in a deteriorated market position. The results of the empirical research are not clear-cut on this. One of the respondents indicated that it depends on the level of adoption of the banks. If they lag with launching apps, online exposure and meeting client needs then they might lose clients. However, the other respondent did not recognize this risk due to several reasons. Banks remain ‘account banks’, also under the PSD II. As a result, they are always the ones who hold and are responsible for the client’s bank account (and not the TPPs). Revenue is generated by having these accounts and doing transactions any not by a bank’s online banking environment. Therefore, there will be no significant loss of revenue related to this aspect. Furthermore, the possible loss of fees from card-based transactions under the Interchange Fee Directive, does most likely not have its impact on traditional banks. Banks do not make money with card transactions, money is earned with the net interest margin and fees on products. Cards are not profitable and therefore banks will not be considerably impacted. The only issue that could impact the bank’s market position is that customers are dissatisfied with the banking services, but this is a general issue and not specifically linked to PSD II. Concluding, as long as the level of adoption of PSD II by banks is sufficient, this risk could potentially be considered as a non-issue and will therefore be removed from the risk framework.

**Loss of customer ownership & insight**

As per the literature review, the possibly increased level of competition from TPPs operating as AISP might impact a bank’s customer ownership and insight in customer data. The empirical analysis indicates that the entrance of new players (and their solutions) could indeed form a risk for banks, but it will be a risk with a rather low risk level since the likelihood is expected to be low (although the impact can be relatively high). The challenge for banks within this respect is to offer an app with functionalities and customer experience which is valuable for her customers and which is to a certain extent keeping up with the solutions built by AISP.
In contrary to what has been stated above, banking is more than offering these apps and corresponding features. A considerable share of customer insight is generated by a bank’s core business, which is also in line with what is stated in the previous part that banks remain ‘account banks’. Until today, core banking is still about performing activities such as Know Your Customer (KYC), Anti Money Laundering (AML) and activities stemming from the Foreign Account Tax Compliance Act (FATCA). KYC is the process of a business verifying the identity of its clients and assessing potential risks of illegal intentions for the business relationship. Up till now, this is still a physical check (someone physical proving his/her identity by showing a passport). TPPs with the ambition to operate under a banking license, are also required to perform these checks. Summarizing, by means of providing AISP-related services, banks should keep up with the innovations of TPPs to a certain extent since these services possibly increase customer insight. However, the likelihood of the loss of customer ownership and insight is low. As a side note, the UK started a year earlier than the Netherlands with implementing the Directive and up to now there is not yet a killer app developed which makes all traditional apps superfluous. On the other hand, important to understand is that a considerable share of customer ownership and insight will still be gained resulting from a bank’s core business, which is unlikely to be highly impacted by the introduction of PSD II.

Radical changes required to comply with principle-based requirements of RTS

As a result of the literature review it became clear that the RTS provides guidance in the form of principle-based requirements, but does not provide technical specifications. Therefore, it is likely that additional work and radical changes are required in order to become compliant which could lead to a loss of revenue. Banks are therefore forced to form their own opinion, supported by the Dutch BetaalVereniging who helps structuring market initiatives and working groups. As a trend it can be noted that the guidelines as provided by the Berlin Group (but also other initiatives such as Open Banking UK) are commonly used by several banks. The Berlin Group is a pan-European payments interoperability standards and harmonisation initiative with the primary objective of defining open and common scheme- and processor-independent standards in the interbanking domain between the acquiring bank and issuing bank (Berlin Group, 2004). The empirical analysis indicates that complying to the RTS costs a lot of money and time which eventually results in a product (e.g. API) for which banks cannot charge a rate, and can therefore never be profitable. The changes required to comply to the RTS have a high impact on the bank’s PSD II roadmap. For the bigger banks this might not form a high risk. One of the respondents has around 40 employees only to perform the work around XS2A. Smaller banks with less budget and manpower might see this as a bigger issue.

Another element which might form an even bigger risk is that, since the RTS is principle-based which led to a lot of freedom of choice during the implementation, there is also a lot of uncertainty whether the
choices made by banks are the right choices. It took some time before regulators such as the DNB and the ECB understood which choices should be made, or in other words, what are the best-practices for implementation. By the time regulators formed an initial opinion on this, choices have already been made by banks in an early phase of the project and are difficult to change when the regulators judge that the chosen solutions are less suitable. Banks designed and implemented their solutions on a detailed level, which makes it difficult to change when an official market standard arises.

Finally, one of the respondents mentioned that the technical specifications of the APIs will absorb less time than the functional specifications. The technical definition of the APIs will probably take around 2% of the entire workload. In the end, it is all about what is functionally included in the API: which accounts have access, which data will be transferred, what should be included in the description field, etc. The functional scope of the technical implementation will be a matter of debate.

Concluding, the main risks which are linked to the radical changes that are required to comply with the principle-based requirements of the RTS are: a) a lack of budget and manpower will lead to difficulties in investing sufficient time and money, which will form even a bigger risk for the smaller banks and b) due to the fact that regulators did not provide guidelines and approved best-practices in an early stage of the implementation, the risk exists that regulators do not approve the choices made by banks, which are then difficult or even impossible to change in that stage. Both the impact and the likelihood for this risk can be rated as high.

Increase of cyber-attacks due to open interfaces (API)

The introduction of APIs for the purpose of XS2A under PSD II implies that a new channel is introduced. A new channel means a new possibility for attack, which should be secured, tested and monitored. If a TPP has access to the API of a bank, this means there is direct access to the back office of this bank, which forms a great risk in case of misuse. Access control in these APIs are therefore of importance. One of the respondents indicated they designed a central gateway which is well protected. But the question is: how are you going to protect the different layers of security? This should be done by means of secured sessions, measures to prevent DDoS-attacks, pen tests, etc. This will cost considerable time and money. Also, APIs were commonly used as a B2B communication channel by traditional banks, which means the amount of security controls is somewhat lower than at times of external/client communication. As a result, the risk could exist that traditional banks want to build on these ‘legacy’ APIs within the light of PSD II and therefore overlook things and do not provide a secure architecture. Summarizing, the enforcement of providing APIs can be associated with a higher amount of cyber-attacks and there is an additional risk of not having a secure API architecture if banks build on traditional B2B APIs. The likelihood that this risk is being exposed can be rated as medium, while the impact of the increase of cyber-attacks will be high.
Alignment of XS2A with the GDPR

As per the literature review, under the GDPR banks need to know which channels are used, where and what personal data flows and what security measure should be taken; in other words: banks should provide full transparency on its customer data. As a result of the empirical analysis, a lot of time is spent by banks on complying with the GDPR. The important question in this matter is: until what extent are the banks accountable for the personal data of its customers? Based on the interviews we learned that, from the respondent’s viewpoint, banks are accountable for the data they have in their system, which should not be shared with TPPs without consent. Consent is the crucial factor within this matter. The data can be protected until the front door of the banks (e.g. by means of encryption), but thereafter a shift of responsibility takes place to the TPPs. With regards to consent, the banks are responsible for performing an identity check on the customer who requests to share its bank accounts with TPPs and making sure consent is given in a right manner (explicit, without delay). However, customers cannot withdraw its consent at the banks, this must be arranged at the respective TPP. Also, banks have no control over what the TPP does with the personal data of its customers. However, banks are still responsible for designing their APIs in such a way, that maximises privacy and security. Concluding, banks should have certain basic privacy measures in place, such as maintaining their RoPa, having sufficient privacy & security by design measures implemented, performing Privacy Impact Assessments (PIAs) on their high-risk process within the light of PSD II. However, the likelihood of facing GDPR related complexities for banks will be rated as medium (if consent mechanisms are implemented properly). This risk might be even more relevant for the TPPs since a responsibility shift takes place after the customer provided its consent. However, the impact will be rated as high since banks are dealing with financial information which is, under the GDPR, considered as sensitive information which requires more strict measures.

7.1.2 Strong Customer Authentication

Threatened customer experience

As outlined in chapter 6.4.1, carrying out transactions and gaining access to accounts under the PSD II can become less frictionless due to the requirements around SCA. The RTS’s prescriptive approach to SCA is likely to have a negative impact on the customer experience. However, research results indicate that the argument of offering clients a secure payment environment appears to outweigh the risk of a threatened customer experience. Also, banks currently choose to focus on complying to the requirements of the directive, instead of starting a complex, expensive and time-consuming process of implementing SCA exemptions. As a result, banks make limited use of the opportunity to use the exemptions on SCA to control the possible threatened customer experience. Based on the interviews, there are only a few exemptions which are applied within the organizations of the respondents, such as the contactless
exemption and payments to self (1 out of 2 respondents). Another argument that was raised is that we are shifting to a digital economy in which we often use our mobile phone to perform a considerable share of our financials (doing payments, checking accounts etc.). This mobile phone is per default SCA (something you know: a pin code, something you have: a phone). Clients seem to prefer consistency over ease of use.

Summarizing, in general the banks do acknowledge the risk of a threatened customer experience due to implementing SCA in its payment related activities. However, there seems to be a certain risk acceptance since there are arguments which outweigh this risk: a) offering clients a secure payments environment, b) the digitalization of the economy (consistency over ease of use), c) the importance of complying to the directive and d) the complexity and costs of implementing the exemptions. Both the impact and the likelihood of the risk are rated low.

Transaction monitoring complexities

Complexities with regards to transaction monitoring are acknowledged as a risk resulting from the implementation of the PSD II. This complexity exists due to the fact that first, a system should be developed, where after rules are described, implemented and connected to the entire infrastructure. Often, card payments are hosted on a different system than online payments, which requires a cross-reference between these two systems. But do you know who your client is, based on the card number in your fraud-system? Those relationships should all be established. Therefore, the merchant bank should also provide details on IP-address and locations. The process steps and all related implications should not be underestimated when implementing proper transaction monitoring mechanisms. Also, current transaction monitoring mechanisms require considerable changes since new streams of data are entering the organization.

Another complexity that should be considered is the at times of writing yet undecided discussion related to the card schemes and liability of the merchant and the issuing bank. What if, during card-not-present payments, the merchant indicates low levels of fraud based on their Transaction Risk Analysis (TRA) performed? Low levels of fraud would allow the use of single factor authentication. However, the issuing bank has the final say. The question that then rises is: is the issuer allowed to overrule/overwrite the merchant’s decision, and does the merchant automatically accepts the liability shift in that case? Within the field of card payments, the liability shift when deciding on SCA by means of transaction monitoring is deemed to be complex. The European Payment Institution Federation (EPIF), representing the interests of the non-bank payment sector at the European level, is currently becoming more active in the debate regarding Transaction Risk Analysis (TRA) to enable single factor accounts payments online.
In general, the likelihood that the banks are facing the risk of transaction monitoring complexities is high and the impact can be rated as medium since it is expected that over the course of time, discussions will be closed resulting in new best practices and guidance which might help parties dealing with these complexities.

7.2 Extending the Risk Framework
The goal of this research is to create a complete overview of risks related to SCA and XS2A. The risks derived from the theoretical framework are validated in the empirical analysis. However, besides validating the risk framework, it could also be extended when new risks arise as an outcome of empirical research. The empirical research clearly indicated one risk that did not derive from the theoretical research. This risk is linked to SCA and will be discussed below.

New phishing possibilities when using embedded approach
There are three types of SCA, the embedded approach, redirect approach and decoupled authentication. When using the embedded approach, the process is fully automated and the payment is initiated on behalf of the PSU. To enable this, users must share their credentials with the TPP who authenticates and initiates the payment (embedded into their interaction with the ASPSP). An example of such a TPP is Sofort. In order to mitigate risks, for example when sharing credentials, these TPPs fall under the PSD II and require a license (since they are identified as PISP). On the contrary, by means of the redirect approach the customer (PSU) is redirected, e.g. via a web interface, to perform SCA between the PSU and the ASPSP. The best-known example of a redirect approach is iDEAL. In this sense iDEAL is not considered as a PISP, since the users are controlling the flow and initiating the payment themselves (therefore no PSD II license is required to perform such services). The third method, decoupled authentication means that the second factor of the authentication is decoupled from the first one and can therefore be provided on a different device (European Payment Commission, n.d.). The redirect and embedded approach are presented in figure 5 below.

![Figure 5: The Embedded & Redirect approach explained (European Payment Commission, n.d.)](image-url)
There are several parties that debate that the redirect approach interrupts the customer journey and hence they see the convention ratio drop which is bad for their turnover and therefore the suggest that the PSD II ecosystem will not work. Article 32(3) of the RTS on SCA states that ASPSPs should ensure that a dedicated interface does not create obstacles to TPPs providing their services, and that this may include redirection of TPPs to ASPSP’s authentication or other functions (EBA, 2017). However, what if the authorities agree that the redirect approach does create obstacles and therefore the embedded approach will be the preferred method? When using the embedded approach, the data of customers is entered in the TPP environment, which is sent to the bank via an API. However, this opens the door for phishing: how does a customer know whether they give their credentials to a valid TPP that has been registered? How does the bank know that the TPPs set up proper processes and protocols around the collection of these credentials? Banks have been educating their customers to not share credentials with third parties for years to limit the risk of phishing. Therefore, both respondents prefer the redirect approach, which is not the most seamless approach (since the customer will be redirected to the ASPSPs environment), but it is the approach which allows banks to perform security checks to ensure that no malicious TPPs access the customer’s bank account. The client must provide its consent/approve in the environment of the banks, before it can proceed with the TPP. Concluding, the risk of the embedded approach being possibly assigned as the preferred method increases the possibilities of phishing and is therefore currently considered as one of the biggest risks with a high likelihood and a high impact. This debate is at times of writing yet undecided.

7.3 Redefining the extended Risk Framework

The output of the theoretical research is an initial risk framework focused on XS2A and SCA. As part of the empirical analysis, this framework is, as stated before, validated on completeness and accurateness. The output of the empirical research is a redefined risk framework which is the result of both the theoretical and empirical research combined. This redefined risk framework will be presented below. As a result of the empirical analysis, almost all risks proved to be valid:

- The empirical analysis clearly indicated that a distinction should be made between inherent and residual risks. The banks already put a lot effort in mitigating the risks, leading to lower scored residual risks. Therefore it should be noted that the risk framework as presented in this research focuses on inherent risks;
- One risk appears to be less or even not applicable and will therefore be removed from the risk framework;
- One risk was initially not included in the risk framework but appears to be a valid risk and will therefore be added to the framework;
Based on the empirical research, some risks appear to be more relevant than others. Therefore, the risks of the framework will be scored low-medium-high based on an initial estimate of likelihood and impact. The risk matrix in table 2 will be used to assess the risks.

Table 2: Risk matrix based on likelihood & impact

Table 3 Provides a systematic overview of the redefined risk framework, including the validated, removed and added risks. Consequently, the risks are granted with an impact score, based on an initial estimate of its impact and likelihood.

<table>
<thead>
<tr>
<th>Risk</th>
<th>Validated / Added / Removed</th>
<th>Likelihood X Impact</th>
<th>Risk Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threatened customer experience</td>
<td>Validated</td>
<td>Low X Low</td>
<td>Low</td>
</tr>
<tr>
<td>Transaction Monitoring Complexities</td>
<td>Validated</td>
<td>High X Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Increase of cyber-attacks due to embedded approach</td>
<td>Added</td>
<td>High X High</td>
<td>High</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Risk</th>
<th>Validated / Added / Removed</th>
<th>Likelihood X Impact</th>
<th>Risk Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>New &amp; changing fraud risks</td>
<td>Validated</td>
<td>High X High</td>
<td>High</td>
</tr>
<tr>
<td>Decrease in revenue &amp; market position</td>
<td>Removed</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Loss of customer ownership and insight</td>
<td>Validated</td>
<td>Low X Medium</td>
<td>Low</td>
</tr>
<tr>
<td>Principle-based requirements of RTS</td>
<td>Validated</td>
<td>High X Medium</td>
<td>High</td>
</tr>
<tr>
<td>Increase of cyber-attacks due to APIs</td>
<td>Validated</td>
<td>Medium X High</td>
<td>Medium</td>
</tr>
<tr>
<td>Alignment of XS2A with GDPR</td>
<td>Validated</td>
<td>Medium X High</td>
<td>Medium</td>
</tr>
</tbody>
</table>

Finally, figure 6 includes the final risk framework, consisting of an overview of the risks linked to SCA and XS2A, including a risk score which is based on an initial assessment of the impact and the likelihood of the risk.
Figure 6: The validated risk framework on SCA and XS2A
8 Conclusion

With the arrival of the PSD II, the traditional payment landscape is facing disruptions. Banks are no longer responsible for the entire payments value chain resulting in reduced control. Also, new players entering the market implies new entries for attack. This research examined the risks for banks related to SCA and XS2A, which resulted in a risk framework which can be used by banks as a basis to mitigate their risks.

8.1 Answering sub-questions

In order to formulate an answer to the central research question, four sub-questions were formulated. An answer to these sub-questions is given below.

I. What is the need to replace the PSD I Directive by the PSD II Directive?

PSD II is introduced by the European Commission to modernise its predecessor PSD I and to take into account new types of (until that time unregulated) payment services. Bringing these new services within the scope of PSD II significantly increased transparency, innovation and security. Furthermore, PSD I led to both regulatory arbitrage and legal uncertainty, and thus, updated definitions in the revised Directive (PSD II) would ensure a level playing field between different providers. More specifically, PSD II is providing a legal framework to strengthen consumer protection, drive competition and facilitate innovation by further opening the payments market. It provides a more integrated approach to financial services regulation. PSD II also enhances cooperation and information exchange between authorities and introduces enhanced mandatory security measures for all PSPs. To solve the shortcomings of PSD I and to keep up with the rapidly evolving payments landscape, the introduction of PSD II was inevitable.

II. What are the main requirements of the PSD II Directive?

On top of the already existing players within the payments field (PSP, PSU & ASPSP), PSD II introduces (requirements for) two new types of TPPs (the AISP and the PISP). Under the PSD II, an AISP can provide a consolidated overview of all payments accounts of a customer on an online platform, even if those accounts are held on multiple PSPs. PISPs act as a link between a payer’s bank account and a merchant’s banking platform. All players must comply with the, for them relevant, requirements of the PSD II. A large share of the requirements of PSD II can be linked back to XS2A and SCA. Regarding the former, PSD II enables access to customer’s bank accounts to both financial and non-financial institutions. Banks are now forced by law to give TPPs access to customer accounts if the customer has given its consent. The industry considers APIs as the best technical solution to allow all PISPs and AISP to connect to ASPSPs in a secure and effective manner.
Another important element of PSD II is the introduction of a new legal requirement regarding SCA in payer-not-present context. SCA is required when customers are accessing their payment account online, initiate an electronic payment transaction or carry out any action through a remote channel which may imply a risk of payment fraud or other abuses. To improve confidence in transactions over the internet, a proper balance between the interests in enhanced security in remote payments and needs of user-friendliness and accessibility is established. PSD II has done so by introducing seven exemptions on SCA.

Finally, two other requirements as included in the Directive which cannot be linked back to XS2A and SCA but are relevant to this research are: PSPs must ensure that when applying SCA, it includes elements that dynamically link the transaction to a specific amount and payee and PSPs must have adequate security measures in place to protect the confidentiality and integrity of PSUs personalized security credentials.

III. What are the possible IT implications of the PSD II requirement regarding third party access to accounts?

The theoretical research indicated that fraud risks are changing due to the introduction of PSD II. Now TPPs can act as intermediaries between customers and banks, banks might lose the grip on customer data where they traditionally relied on to make fraud-related decisions. It can be difficult for banks to judge the reliability and identify potential fraudulent TPPs. Also, there will be a fast increase in entry-points for attack for fraudsters, since banks are required to provide APIs to TPPs. Furthermore, the literature review indicated that banks may lose a share of their current payments-based revenue which might impact their market position. Another potential risk is the loss of customer ownership and insight. More specifically, the actual risk lies in the fact that TPPs are able to aggregate and integrate their newly developed services. Access to multiple stand-alone financial services products can be provided via a single platform, integrated with customer’s existing accounts and transactional data. For banks this could result in a loss of customer insight. Another risk is related to the principle-based requirements of the RTS which are lacking technical specifications. Radical changes in IT infrastructure are required for banks. Therefore, the following sub-risks for banks might exist: a) development of unsuitable technological solutions; b) loss of revenue due to high investments in costs and time for R&D; c) losing market share and falling behind on competitors when doing nothing. The final two risks linked to XS2A are a possible increase in cyber-attacks due to open interfaces and the mis-alignment with the GDPR. Regarding the former, if a sound architectural approach is missing with security processes that are not quickly able to adapt or respond, banks will become more vulnerable for cyberattacks. Regarding the latter, due to the increase in communication channels, banks should know which channels are used, where and what personal data flows and what security measures to take. Non-compliance could result in high fines.
IV. What are the possible IT implications of the PSD II requirement regarding strong customer authentication?

Under PSD II, SCA is intended to secure the customer and reduce fraud during payment-related actions. However, implementing SCA that complies with the requirements of the RTS and the friction that it possibly poses causes new or revised risk for banks. These risks are related to a threatened customer journey and complexities in transaction monitoring. When applying SCA, gaining access will become less frictionless for customers, possibly causing reduced customer satisfaction. The EBA is aware of the friction that SCA could cause, and therefore included clauses for exemptions of SCA. These exemptions are much debated, since it is hard to find a balance between security, innovation, user-friendliness and accessibility. Furthermore, an incorrect or incomplete transaction monitoring model and control framework may lead to high costs for banks. Also, if banks (or other PSPs) fail to ensure adequate monitoring, they might unconsciously cooperate in terrorist financing or money laundering practices. The new transactions through TPPs require revised scores/scoring models in monitoring mechanisms that reflect the transaction risk, which will take around two years to develop and is therefore time and cost consuming.

8.2 Answering central question

Based on the analysis of the previous chapters and the answers to the four sub-questions, an answer is formulated to the central question below. This is a combined result of both the theoretical and empirical analysis. The risks described below refer to the inherent risks related to XS2A and SCA banks might face.

What are the possible risks of the introduction of the second Payment Service Directive in terms of third party access to accounts and strong customer authentication?

Regarding XS2A, the modus operandi for fraudsters are changing due to PSD II, resulting in a risk with high likelihood and impact for banks. Fraudsters can aim for the APIs, by hacking the systems and processes of the TPP. Furthermore, the literature indicated that banks may lose a share of their current payments-based revenue which might impact their market position. However, the empirical analysis showed that under the PSD II, banks still remain 'account banks'. As a result, they are always the ones who holds and are responsible for the client’s bank account. Cards in itself are not profitable, banks earn money with the net interest margin and fees on products. Therefore the decrease in revenue and market position is considered as a non-issue.

This research indicates that the entrance of new players (and their solutions) could result in a loss of customer ownership and insight. By providing AISP-related services, banks should keep up with the innovations of TPPs to a certain extent since these services possibly increase customer insight. On the other hand, it is important to understand that a considerable share of customer ownership and insight will still be gained resulting from a bank’s core business, which is unlikely to be highly impacted by the
introduction of PSD II. More importantly, the radical changes that are required to comply with the principle-based requirements of the RTS forms a bigger risk. A lack of budget and manpower will possibly lead to difficulties in investing sufficient time and money. Also, the risk exists that regulators do not approve the choices made by banks, which are difficult or even impossible to change after implementation.

Another potential risk is related to a possible increase of cyber-attacks due to the requirement of providing open interfaces (APIs). New channels imply new possibilities for attack and should be sufficiently secured, tested and monitored. Also, the risk increases when banks build on traditional B2B APIs (legacy) which could result in not having a secure API-architecture in place. Finally, misalignment between XS2A and the GDPR is another potential risk. Banks should have certain basic privacy measures in place to prevent high fines. As long as banks make sure they have proper consent mechanisms in place, the likelihood of this risk is controllable.

Three main risks can be linked to SCA. First, the banks do acknowledge the risk of a threatened customer experience due to enforcing SCA. However, there seems to be a certain risk acceptance since there are arguments which outweigh this risk: a) offering clients a secure payments environment, b) the digitalization of the economy, c) the importance of complying to the directive and d) the complexity and costs of implementing the exemptions. Second, transaction monitoring complexities exist due to the fact that first a system should be developed, where after rules are described, implemented and connected to the entire infrastructure. These complexities could lead to misunderstandings, excessive costs and time-consuming activities to implement proper mechanisms. The final risk that was not identified during the theoretical analysis, but during the empirical analysis is related to the new phishing possibilities when using the embedded approach. When using the embedded approach, the data of customers is entered in the TPP environment, which is sent to the bank via an API. Since banks do not know whether TPPs set up proper processes and protocols and the customer does not know whether its credentials are shared with a valid TPP, phishing possibilities are increased.

The output of the theoretical research is an initial risk framework focused on XS2A and SCA. As part of the empirical analysis, this framework is validated on completeness and accurateness. The final output is a redefined risk framework which is the result of both the theoretical and empirical research combined. Based on the empirical analysis, one risk appeared to be not applicable and is removed from the initial risk framework. One risk was initially not included in the risk framework but appeared to be a valid risk and is added to the framework. Some risks appear to be more relevant than others. Therefore, the risks of the risk framework are scored based on likelihood and impact. The following risks appear to be most important: increase in cyber-attacks when using the embedded approach, new and changing fraud methods/entry points for attack and the radical changes required (in infrastructure) due to the principle-
based requirements of the RTS. The final risk framework can be used by banks as a starting point to mitigate the risks associated to XS2A and SCA.

8.3 Directions for further research

This study has a few limitations which should be addressed in further research. Given the limited scope of two banks, the generalizability of the conclusion is limited. To improve on this, it might be good to enlarge the sample size in further research. Also, this research mainly focused on the risks that banks face with regards to XS2A and SCA. Identifying risks is only one step within the risk management process. Further research should be conducted on the mitigating measures that banks can take to control the risks. Furthermore, this research focused on an analysis of the identified risks, resulting in an initial risk score based on the impact and likelihood. Further research should proceed with this approach, extending on this initial risk assessment. More specifically, the risks as identified in this research should be more thoroughly assessed and rated on elements such as confidentiality, integrity, availability (resulting in an impact rating) and inherent versus residual risks. Finally, since the RTS requirements are mainly principle-based, further research should be conducted on the technical specifications and the suitability of solutions to provide more guidance and best practices for banks or other players within the light of the RTS and PSD II.

8.4 Personal reflection

In this past half year, I have gained comprehensive insights in the wonderful world of payments. I have realized we are on, or actually already over, the edge of a new era. Many current legislations do not properly reflect the need of this digitized world anymore. This is the main reason we see several revised Regulations and Directives, among which PSD II. I have learned that it takes some time to find sufficient scientific literature for a Directive that has been introduced so recently. Most focus is put on guidance documents written by regulators and opinion articles of expert organizations. Doing this research a year later might have changed the results slightly, since new insights are still on the rise. Related to this, certain risks as included in this framework, are related to discussions which are still undecided by the local regulators (such as the Embedded vs Redirect approach discussion). Therefore, the framework might change over the course of time, when there is more clarity on the right implementation of the principle based requirements of the Directive.
9 Literature List


24Solutions (2016). Whitepaper PSD II - What are the implications, problems, possibilities, challenges and opportunities.


