UNIVERSITY OF TURKU

ABSTRACT

	Bachelor's thesis
X	Master's thesis
	Licentiate's thesis
	Doctor's thesis

Subject	Information Systems Science	Date	01.06.2019
Author(s)	Adam Bartoszczyk-Brzoskowski	Student number	135890
		Number of pages	91
Title	The purpose and impact of the second payment service directive on cyber security of the payment user and affected parties		
Supervisor(s)	Prof. dr. A.F. Rutkowski; Prof. P. Rousseau		

Abstract

This paper evaluates the impact of the second payment service directive (PSD2) on cyber security of the payment service user. The research includes the selection of academic theory based on literature analysis of 27 academic papers, that helps to determine the purpose of said directive. Additionally, three regulatory acts (2015/2366 (PSD2), EBA/GL/2017/17, EBA/RTS/2017/02) that are the foundation of the second payment service directive are evaluated in search for specific cyber security measures influencing safety of the payment service user. Lastly, a qualitative study based on three institutions (traditional bank, third-party service provider and a legislator) affected by the scope of second payment service directive is provided, where the empirical impact of the regulation is analyzed as well as other additional implications that were a result of the policy introduction to the payment market.

Key words	Second payment service directive, PSD2, cyber security
Further information	

THE PURPOSE AND IMPACT OF THE SECOND PAYMENT SERVICE DIRECTIVE ON CYBER SECURITY OF THE PAYMENT USER AND AFFECTED PARTIES

Master´s Thesis
in International master's in management of IT

Author:
Adam Bartoszczyk-Brzoskowski

First supervisor:
Prof. dr. A.F. Rutkowski
Second supervisor:
Prof. Patrick Rousseau
Reader:
Prof. Hannu Salmela

01.06.2019
Tilburg

Table of contents

List of figures

List of tables

List of abbreviations

AISP	Account Information Service Provider
API	Application Programming Interface
ASPSP	Account Servicing Payment Service Provider
EBA	European Banking Authority
ECB	European Central Bank
EEA	European Economic Area
ERPB	European Retail Payment Board
EU	European Union
FinTech	Financial Technology
GDRP	General Data Protection Regulation
GDT	General Deterrence Theory
ICT	Information and Communication Technology
PISP	Payment Initiation Service Provider
PMT	Protection Motivation Theory
POS	Point-of-Sale
PSD1	First Payment Service Directive
PSD2	Second Payment Service Directive
PSU	Payment Service User
RAT	Routine Activity Theory
RTS	Regulatory Technical Standards
SCA	Strong Customer Authentication
SEPA	Single Euro Payments Area
TPB	Theory of Planned Behavior
TPP	Third Party Providers
TTAT	Technology Threat Avoidance Theory
XS2A	Access to Account

PREFACE

The thesis is part of the International Master in Management of IT (IMMIT) which is a triple master diploma programme. The scope of the research is the second payment service directive (PSD2) and related aspects of cyber security. The choice of this topic is motivated by my personal interest in cyber security in its entirety. Almost every day there are news of security breaches where digital safety of many individuals is being compromised. I believe that the topic of personal cyber security is only going to become more important matter of everybody's life. Therefore, in order to connect it with business aspect, I have decided to explore the implications that the revised payment service directive brings in terms of cyber security. My goal was to understand the changes that said directive had introduced and become more aware payment service user. Particularly, due to my extensive personal use of many FinTech solutions available on the market. The completed research that I am providing you with in this paper is not only a result of my own work, but also help of many amazing people. I would like to thank all participants that have decided to help me conduct the research and answer to my questions from the Dutch ING, Bank of Aruba as well as Polish company BlueMedia. On top of that, I would like to thank my dad Maciek, who gave me a lot of constructive criticism and proved to be irreplaceable reader, my mom Marta for mental support, my girlfriend Krysia for resolving the many doubts I had and others who were there when I needed to talk. I cannot forget about my friends from IMMIT Cohort 11, who made the time spent in the programme so unforgettable, Last but not least my supervisor Prof. dr. A.F. Rutkowski for her work and support when I needed it the most.

1 INTRODUCTION

1.1 Problem indication

As technology is evolving, it is constantly entering new areas of people's life. In the recent years, a major change has also come to the financial world. Digitalization of banking made a huge remark on how consumers spend and manage their money and services introduced throughout the years allowed for more intuitive and simplified operation. The number of digital transactions is increasing drastically. According the report "Digital Payment Market by Type, Solution Type, Deployment Mode, Organization Size And Region - Global Forecast to 2023", the digital payment market is estimated to be USD 38.00 billion as of the years 2018. By the year 2023, it is forecasted to increase the value to USD 86.76 billion with a year-to-year market growth estimated at 18.0%. Some of the key drivers for the growth of digital payment market are promotion of digital payment, increased importance of smartphones in terms of digital payments and increasing demand for higher level of customer service at POS terminals. (MarketsandMarkets (M&M), 2018)

The digitalization of payments has created few events on the payment market. First of all, traditional banks have benefited from advantages of digital era we are living and started to offer services through new channels, including digital banking also present on smartphones. Additionally, emergence of new players on the digital payment market could be observed. New firms offering services previously provided only by the banks have appeared on the market and gained noticeable presence and impact. Most of them belong to the increasingly popular group of FinTechs. The presence of said emerging businesses on the market is unmistakably noticeable, with a compound annual growth rate (CAGR) in the years 2018-2023 estimated at 42.9%. (Orbis Research, 2018) Therefore, the innovative payment service providers have a fair chance at competing with more traditional banks. Payment service providers are obligated to follow regulations implemented by the PSD2, but are also given an opportunity to apply for a license under the PSD2. Licensee is allowed to operate in all EU/EEA member countries, despite having applied for said license in only one country. However, without the license made under PSD2, all payment service providers are prohibited from offering any service starting from 13th of January 2018. (Huiskes & Elsenga, 2017)

The first service payment directive has been introduced on 13 November 2007 by the European Council and is known as PSD 1. Its main purpose was to unify the payment area within European Union and allow for faster and more secure transfers which would resemble the simplicity of domestic payments. The main result was introduction

of the SEPA (Single Euro Payments Area) which is based on the legal framework introduced by the PSD 1. (European Commission, n.d.)

Following the success of PSD 1, the European Commission in response to the changes in financial market mentioned earlier decided to introduce a Second Payment Service Directive (PSD2), which aims to regulate some of the aspects of newly emerged payment service providers. The revised payment service directive (PSD2) has come to force quite recently in January 2016. The deadline for transposition into a national legislation was January 2018 and this date could be in fact treated as introduction of PSD2 in practical sense. The key objectives of the PSD2 are:

- Easier and safer use of internet payment services
- Better consumer protection against fraud, abuse and payment problems
- Promotion of innovative mobile and internet payment services
- Strengthening of consumer rights
- Strengthening of the role of European Banking Authority (EBA) in order to coordinate, supervise and draft technical standards

(European Commission, n.d.)

One of the biggest concerns of the digital transformation of the banking industry and increasingly popular external payment service providers is aspect of cyber security. Cyber security as defined by Merriam-Webster dictionary means “measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack” (Merriam-Webster dictionary, n.d.) The introduction of new ways of accessing and operating digital payments allow at the same time for new forms of threats to arise. As the European Commission has stated in the prelude to PSD2 – “In recent years, the security risks relating to electronic payments have increased. This is due to the growing technical complexity of electronic payments, the continuously growing volumes of electronic payments worldwide and emerging types of payment services. Safe and secure payment services constitute a vital condition for a well- functioning payment services market. Users of payment services should therefore be adequately protected against such risks. Payment services are essential for the functioning of vital economic and social activities.” Therefore, in order to allow for prosperous growth of the digital payments, directives such as PSD2 are necessary to be implemented.

1.2 Problem statement and research questions

Although the directive is quite new, mainly due to the fact it was an important step for the entire banking service market and the European-wide implementation

requirement it is very well documented and explained throughout number of various sources. The academic papers revolting around PSD2 are a little more scarce, however they are present as well. What is missing however is a comprehensive review of the impact of the PSD 2 directive on cyber security of the payment users from a more empirical point of view. The regulations and guidelines are only valuable if they have practical implications and cause tangible changes. In order to fully understand the meaning of the directive, it is worth analyzing its purpose from academic perspective. In-depth analysis utilizing scientific theories allows for a better comprehension of issues it is trying to resolve. As the aspect of cyber security is one of the most important elements of second payment service directive as well as the entire digital world, the main research question derived is as follows:

What are the purpose and implications of PSD2 on cyber security of payment service user and what is it's empirical impact on affected parties?

In order to answer the main research question, additional supplementary research questions need to be evaluated:

Research Question 1: **Which academic theory most accurately reflects the mechanisms and purpose in terms of cyber security of the second payment directive?**

Research Question 2: **What changes in terms of cyber security does the PSD2 introduces to the payment process from perspective of payment user?**

Research Question 3: **What are the empirical changes in terms of cyber security and business practices that the banks, third party providers and others had experienced as a result of implementation of PSD2?**

1.3 Thesis structure

First part of the paper is focused on literature review. All relevant key terms are defined and analyzed with a specific attention on their importance in terms of second payment service directive. Importantly, all parties which are affected by the directive are clearly stated and their role is defined. A more in-depth description and analysis of the directive in question is provided as well to allow for comprehensive understanding of its scope and implications. As nowadays most recent information are published in the first place in the internet, this paper is generously utilizing internet resources in search for most up-to-date and relevant data. However academic sources are also used in

considerable number, especially in aspects which are less rapidly changing. As the paper is concerning regulatory issues, the actual directives are a great source of information, henceforth they are widely used as well.

Following, the paper answers for the first research question by providing an in-depth review of selected literature which deals with aspects of cyber security in order to find underlying purpose for implementation of PSD2 directive and similar regulations which can be implemented in the future. The theories which are found in the selected literature are given and evaluated and later compared to each other. The results of the comparison are presented in the chart for easier reference and conclusion is being made as for the most suitable theory choice.

Next, the paper deals with more concrete aspects of the second payment service directive in terms of its implication for cyber security of payment service user. The specific articles of the directive are being analyzed in order to understand their impact on cyber security. Specifically, the technical aspects and regulations will be analyzed in order to create a list of changes that the PSD2 introduces to the payment process in terms of cyber security. Importantly, the directive is also compared with a EBA regulation which is a related paper.

Lastly, the research will deal with real-life implications of the PSD2 directive and what are the empirical implications resulting from its introduction on affected parties. The research will be conducted as a single case-study, which analyzes an impact of PSD2 with regard to three different parties – bank (represented by Dutch ING); third-party provider (represented by polish company Blue Media) and legislative (represented by security expert of national bank of Aruba).

1.4 Study Relevance

1.4.1 Theoretical relevance

PSD2 is widely discussed topic also in rather popular media outlets. The forecasts for its impact are described quite extensively, however the information is scattered across many sources, with a very limited number of research papers which provide a comprehensive overview of this regulation. Most of said sources also mention cyber security to a very limited extent, hence leaving a literature gap. Therefore, this study fills that gap by providing a comprehensive analysis of PSD2. The aspect of cyber security will be dealt with in the most detailed way, however the entire regulation will be explained accordingly, in order to allow the reader to fully understand its impact and parties which are affected by it. Only when concerned the entire scope implications of the directive, the

paper will be narrowing down the aspect to cyber security. Importantly, the said paper will also be considering different theories which are explaining the purpose of the implementation of said regulations from perspective of cyber security of payment user. This should allow for a better explanation of motives of implementation of cyber security laws such as PSD2, which can be useful for future legislators as well as payment market participants. It is quite likely, that the theoretical analysis of PSD2 directive has not been yet provided otherwise.

1.4.2 Practical relevance

The research conducted in this paper allow for few practical outcomes. First of all, the extensive literature review allows for a clear and comprehensive understanding of the implication of the directive. This can be utilized also by market participants to derive a concrete examples of actions that need to be undertaken to fully benefit from the possibilities given by the directive, but also use it as a checklist for requirements to fulfill. The results of the theoretical analysis should allow for a better understanding of cyber security implications from perspective of the payment user. Therefore, the aspect of payment user behaviors can be later used also for instance in marketing operations. With a better knowledge about user needs, payment service providers can better aim their marketing techniques, as well as use this knowledge to strengthen their selling points in creation of their offer and future services.

Moreover, the results of the research conducted in the further part of the paper should allow businesses to see how analyzed institutions have benefited from introduction of the PSD2. The research conducted will give information on empirical changes and factors that have been observed by industry experts. This should be a good starting point for some businesses operating in the payment services field to compare themselves with some of the analyzed parties. This study is completed with help of three very diverse payment market participants. One of them consists of a traditional bank – ING, based in the Netherlands. The implications for a traditional party such as bank are particularly interesting due to the fact of change management that the institution needs to undertake in order to provide same or increased service value to their customers. Another participant in the research is Bank of Aruba representative who shows the legislation and regulatory point of view on implementation of PSD2. Despite the fact that Bank of Aruba has not yet implemented the second payment service directive, they are intensively working on this process, therefore their perspective can present a lot of valuable information regarding the change from outdated laws and regulations to modern PSD2 directive. Lastly, the third party payment service providers are represented by a company BlueMedia, who acts as a payment initiation service provider and is based in Poland. Their input should allow

for a better perspective on implications of PSD2 from a perspective of FinTech or emerging business.

2 LITERATURE REVIEW

2.1 PSD2 – key related terms

In order to fully understand the objectives of the second payment service directive it is important to understand the parties that are specified in the act as well as the concepts that the regulation in question is introducing. The participants on the payment market have previously been undetermined and underregulated, which resulted in vague ability to supervise them from the perspective of law and law enforcement institutions such as central bank or financial supervision authority agency. Hence, clear definition of payment market parties does not only allow for better understanding of said market participants, but also specifies laws which apply to them.

2.1.1 List of parties defined by PSD2

There are essentially 3 main payment institutions which are described by the directive. Two of them - Payment Initiation Service Providers (PISP) and Account Information Service Providers (AISP) can be grouped together as Third Party Providers (TPP). Outside of that group are Account Servicing Payment Service Providers (ASPSP) which are entities that are holding customer's payment accounts therefore providing also more primary banking services. The following relation can be easily distinguished on the diagram below:

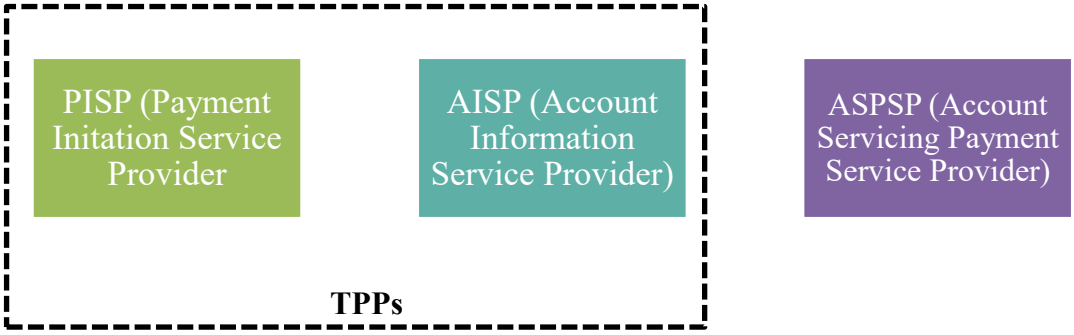

Figure 1 Institutions outlined in PSD2

(Husek, Brich, & Prochazka, 2017)

The PSD2 specifies certain characteristics that the participants in the payment service market possess. In order to fully comprehend their role on the payment market it is worth analyzing their role. A more in-depth definitions of the participants are as follow:

- Account Servicing Payment Service Providers (ASPSP) are financial institutions which hold payment accounts and are issuing payments or are the recipients of such payments. They can be described as the traditional financial entities and consists of mainly traditional banks.
- Payment Service User (PSU) simply is the consumer or retailer, who is the final user of services offered by TPPs or AS PSPs.
- Payment Initiation Service Providers (PISP) is the entity which initiates the payment created by the account owner between the PSU (customer) and ASPSP (usually the bank). They are given permission from PSU to handle online banking payments – they are usually the newly emerging FinTech businesses.
- Account Information Service Providers (AISP) is the entity which is given access to account information by account holder (PSU). Often, they are the same businesses as PISP, as they can both handle information as well as initiate the payments, however it does not necessarily need to be the case.

2.1.2 Application Programming Interface (API)

Before diving into the concept of Access to Account (XS2A) and Open Banking, it is important to understand the underlying technology which allows it to operate. The technology in question is Application Programming Interface, often simply referred to as API.

APIs are one of the drivers which allow for a quick revolution in the fields of cloud computing, mobile applications, Internet of Things (IoT) and many more. (Jensen, 2015) The concept of APIs is very multi-level, however at the very basic it can be defined as – "code that allows two software programs to communicate with each other" (Rouse, Nolle Tom, & Li Thomas, 2017) Moreover, it can be described as a systematic way of sharing data, it allows for an easier collaboration and access to information. (Zachariadis & Ozcan, 2017) The use of APIs in banking, especially in the US, dates decades back. They have been put in use mainly in financial management software, to present billing details at the bank websites as well as they have been utilized extensively by payment card providers such as Visa and MasterCard in their networks. (Brodsky & Oakes, 2017) One of the drivers for recent development and increase in popularity of APIs is the introduction of the smartphone. A lot of mobile apps rely on the APIs in order to exchange data from and to the device. However APIs find a great use not only in mobile applications, but also are widely used in new generation responsive websites. They characterize with a lightweight implementation and simplicity of data exchange format. From a more technical point of view, APIs can be described as a rather small server-side applications. (Jensen, 2015)

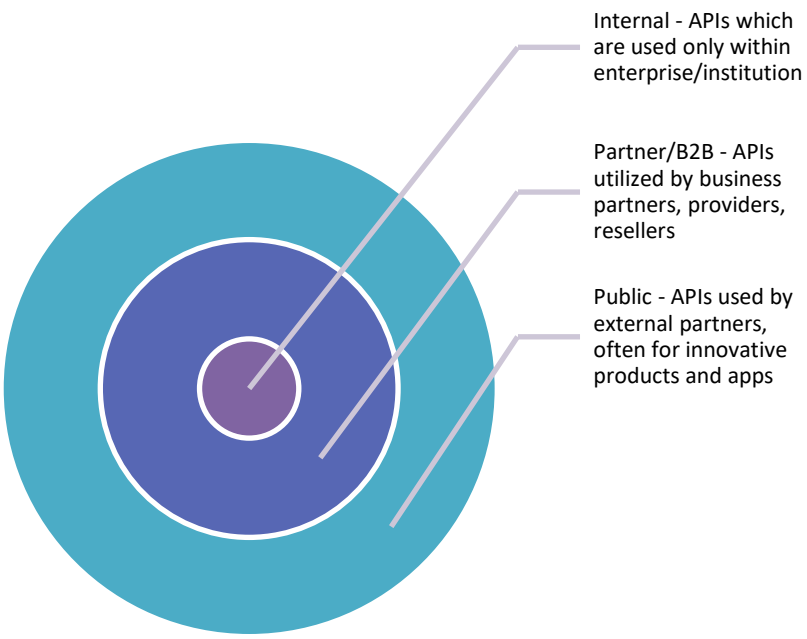

Figure 2 Three types of APIs

(Brodsky & Oakes, 2017)

2.1.3 Access to account (XS2A)

Another aspect which is introduced by PSD2 is Access to account (XS2A). Financial institutions which include banks are obligated by PSD2 to provide access to account to a licensed third-parties. Importantly, the payments which are executed by the third-party providers (TPPs) cannot be anyhow discriminated. What it is basically allowing is bypassing of the "middle-men" in an e-commerce ecosystem. Essentially, XS2A means that for example the merchant can directly connect with customer's bank in order to execute payment which is done through a third-party. This could in the future eliminate the need for in-store point of sale and hence revolutionize the way customers pay for their goods. But this will not only affect purchases in physical stores, but also online shopping. After implementation of all of the aspects of PSD2, instead of purchasing certain products or services using a payment card, payment user can be asked instead to give retailer access to their bank account. After agreeing, the merchant can take the payment user to internet banking site where the user gives required permission to execute the payment. This can be compared to giving permission for using third-party login information in order to access websites (i.e. using Facebook login on websites utilizing Facebook API). The payment user will not provide the merchant with his bank login details, but instead give permission to the exemplar store in order to execute payment on behalf of the user via users bank account. (Sebastian, 2017) The security implications of such solutions will be evaluated in later part of this paper.

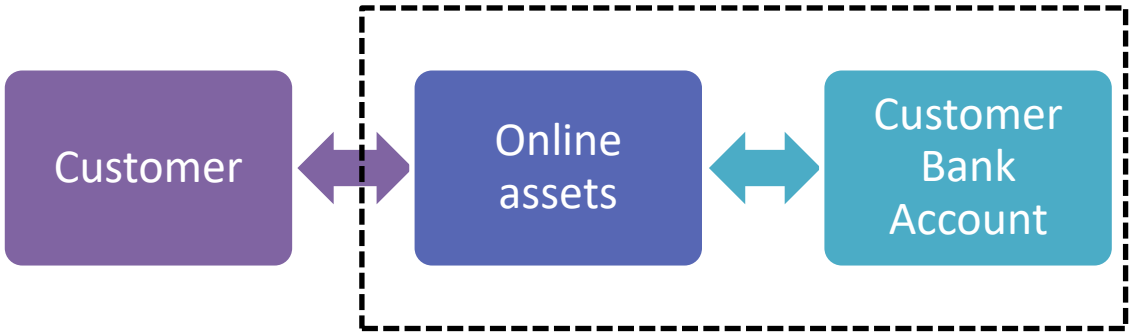

Figure 3 Communication before PSD2 & XS2A

Source: (Hemon-Laurens, 2015)

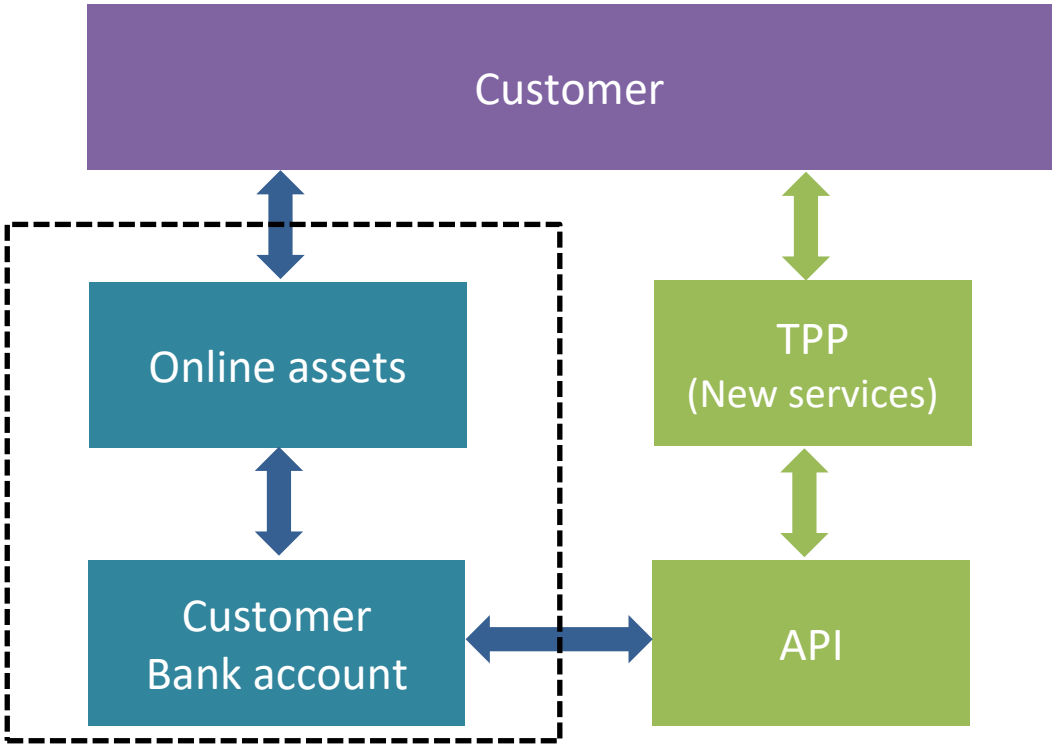

Figure 4 Communication with PSD2 & XS2A

Source: (Hemon-Laurens, 2015)

According to the report by consulting firm Ernst & Young, XS2A is considered by financial institutions to be the most critical aspect of the PSD2, mainly due to the expected implementation efforts, business and technical impacts and risk mitigation efforts that have to be conducted by ASPSPs. However, while implemented, payment initiation service providers (PISP) as well as account information service providers (AISP)

can create new business opportunities for both established and new market participants. This could lead to reengineering, enlarging or improving products and services offered. (Ernst & Young S.A., 2018)

2.1.4 Open-banking

Open banking consists of collaborative model, where banking data is being shared through APIs between two or more unaffiliated parties in order to deliver enhanced marketplace capabilities. It is no different than the concept of Access to Account (XS2A) mentioned earlier, but it is one of the proposed solutions in order to standardize it.

Open Banking is an initiative created by Open Banking Limited, which is a non-profit organization based in UK. However, although it is not operating European-wide, the term Open Banking has become a synonym for access to account solutions. There is a number of potential benefits that are expected resultants of use of Open Banking: creation of new revenue streams, improved customer experience and creation of sustainable service model for markets which were previously underserved. (Brodsky & Oakes, 2017)

2.1.5 Financial Technology (FinTech)

FinTech is a term widely used in connotation with PSD2. Businesses which are affected by PSD2 are often described with a term FinTech, henceforth understanding how they have emerged on the market is valuable in terms of the understanding of the current market of payment providers. It is worth noting as well that thanks to second payment service directive, FinTech can observe even higher rise of growth, mainly thanks to lowering barriers to entry and data-sharing among financial institutions.

The term “Financial Technology” often abbreviated to “FinTech” can be simply explained as use of technology in order to deliver financial solutions. One of the definitions of FinTech was presented by (Kawai, 2016) and it suggests that it is a ”technologically enabled financial innovation. It is giving rise to new business models, applications, processes and products. These could have a material effect on financial markets and institutions and the provision of financial services.” FinTech although it is perceived as a recent trend that goes only to early 2010s has been present in the banking industry much longer, with the term FinTech being traced to early 90s. (Arner, Barberis, & Buckley, 2016) Definition stated earlier, although correct and accurate does not show the whole picture of what FinTech industry actually is nowadays. The increasingly popular FinTech firms can certainly be described as innovative. The main goals are to change the way customers are using banks and increase access to financial services, mainly for customers

familiar with new technologies. Moreover, the individuals and business thanks to FinTech are able to invest and borrow money more easily, the transactions and payments are safer and cheaper. The rate of transactions previously often neglected and sometimes taking even days to execute is now reduced to almost an instance. FinTech industry essentially challenges everything that has been established in the financial world so far and tries to reinvent it. (Mackenzie, 2015) Moreover, there are many FinTech services that distribute insurances, various other financial instruments or other third-party services. The term FinTech can also refer to companies that provide technology to providers of financial services. (Dorfleitner, Hornuf, Schmitt, & Weber, 2017) Interestingly, FinTech businesses are gaining surprisingly high confidence levels from its customers. According to a survey made in 2015, Americans have a higher level of trust in FinTech or overall Technological firms handling their financial information rather than traditional banks. The bank with the highest level of trust which is listed in the study is Wells Fargo, with confidence of 44%. On the other hand, purely technological firm PayPal can boast a trust level reaching 73%, along Amazon (71%), Google (64%) and Apple (57%) all well exceeding trust levels of traditional banks. (McCarthy, 2015)

2.1.6 Neobanks

PSD2 does not directly specifies or defines Neobanks per se, this paper is neither evaluating them in great detail, but in order to understand the full picture of market situation of payment service providers it is good to briefly discuss them.

Essentially, Neobanks are a sub-group of FinTechs and could be assigned Account Servicing Payment Service Providers (ASPSP) characteristics. According to (Minarchenko, 2018) Neobanks are financial institutions which offer a combination of checking accounts, saving accounts and debit cards through digital channels. Importantly, they offer their services only through mobile applications and do not have any physical branches. The applications themselves are often simplified with ease of use in mind. Often, they offer additional features to allow for easier saving and spending habits by implementing expense categorization and ability to easily track incomes and outflows. Therefore, Neobanks are using fully digital platform built from ground-up, hence not only serving as simplified front-end of traditional banking platforms.

The main advantages of Neobanks over traditional brick and mortar established businesses is usually lower interest rates and fees, 24/7 customer support through the mobile app and extremely transparent display of transaction costs. Often the ATM withdrawal costs are also free of extra costs (to certain given limits), there are no costs associated with running the account, the products are based on prepaid services, which eliminate the overdraft fees. Importantly, the transactions are online-only, meaning the balance displayed on the smartphone represents the actual amount of money in the possession on the account. Neobanks have been primarily based with deposit focus in mind, though due to increase in popularity they are starting to slowly evolve into more advanced types of services.

The rate of growth of Neobank companies is also staggering. One of the most popular bank-in-the-app companies – Revolut has gained a status of a unicorn in 2018. This means that their valuation has exceeded 1 billion dollars. (Schwienbacher, 2019) However, it is not the only example of a unicorn among banking-oriented FinTechs. German Neobank N26 at the beginning of 2019 has raised $300 million through series D funding round, which has brought its overall funding to over $500 million and valuation to $2.7 billion mark. (Nonninger, 2019)

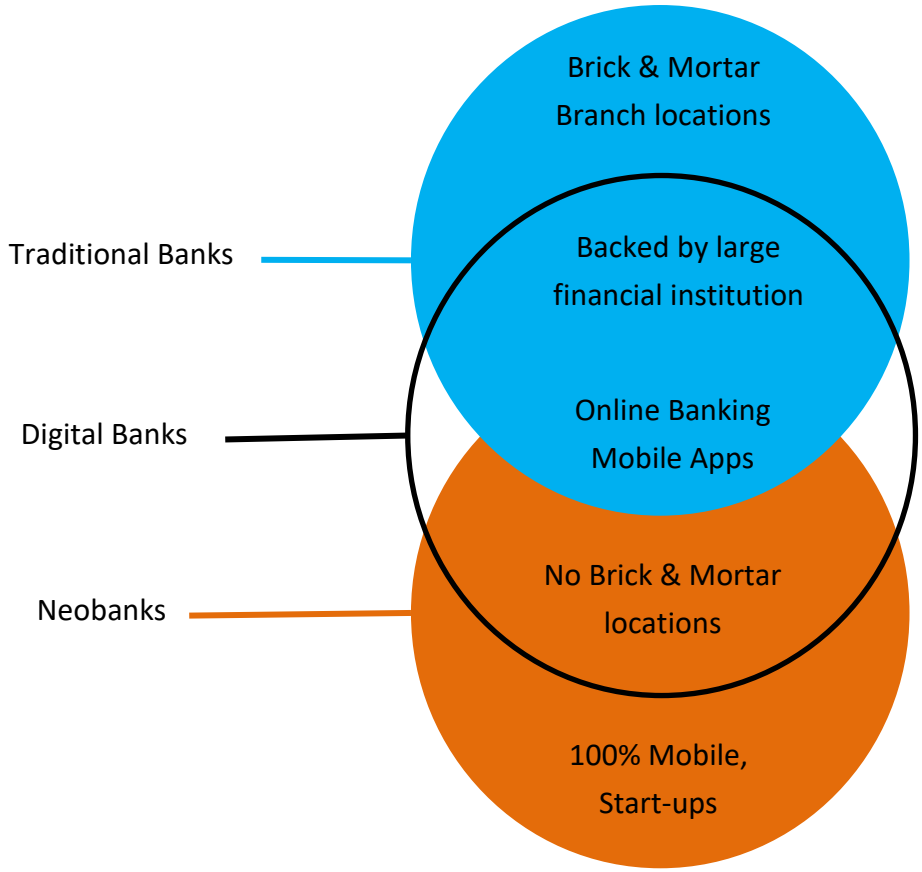

Figure 5 Comparision of Neobanks, Digital Banks and Traditional Banks

Source: (Brockhurts, 2019)

2.2 Cyber security

Understanding of cyber security is quite essential in the process of analyzing regulations which are aiming to improve it. Therefore, before looking at particular examples of changes that the PSD2 introduces in terms of cyber security, clearly defining and comprehending this aspect will be necessary.

According to (Von Solms & Van Niekerk, 2013), cyber security can be described as a set of certain technologies, assurances, best practices, training, actions, risk management approaches, guidelines, security safeguards, security concepts, policies and other tools. The purpose of all of these concepts is protection of the cyber environment, organizations or institutions and importantly user's assets. The said assets can consist of computer devices which are connected to world-wide-web, personnel, computer infrastructure, digital applications, services, systems concerning telecommunication and data stored or transmitted within the cyber environment. Moreover, cybersecurity is aiming to achieve certain level of security properties of the organization. The authors provide three main objectives of security which are: availability, integrity and confidentiality.

A few concepts and characteristics of cyber security given above are essential, however it is also worth to show its origin. All aspects of cyber security measures starts with a legal violation in form of a fraud. As the legal dictionary suggests, frauds is "the intentional use of deceit, a trick or some dishonest means to deprive another of his/her/its money, property or a legal right (...)". ("Legal Dictionary | Law.com," n.d.). Essentially, cyber security is a measure in order to limit fraud which is being committed in digital environment. Previously, fraud was an act committed in physical sense, however due to the increasing digitalization, number of criminal activities committed online have been also rising in popularity.

One of the act of fraud which is being done digitally is cyber-identity theft. Cyber-identity theft is concerning a theft or misappropriation of identity tokens. Some of the common types of online identity tokens consist of email address, websites and authentication mechanisms such as a combination of username and password which is used to access personal information for instance banking account. (Sweeney, 2006) There are number of methods that are used in cyber-identity theft. Some of them are listed by (Paget, 2007) to be "hacking, phishing, pharming, traffic redirectors, advance-fee frauds, fake taxation forms, keyloggers and password stealing". Interestingly, there are number of individuals who despite having their identity tokens stolen, were not aware of the form that the credentials have been leaked. They are aware of the fact that the vulnerable data has been compromised, however many of them are not able to point the source of theft.

It is also believed, that the importance of cyber security is increasing with emergence of FinTech, who's part are third party payment services. With the increasing number of cyber-attacks, financial institutions are obligated to continue to improve their cyber

security frameworks, which can be achieved by gathering, examining and sharing cyber-related data information. (Stewart & Jürjens, 2018) Therefore, the directives such as PSD2 need to address aspects of cybersecurity in order to provide such frameworks on European-wide financial markets.

2.3 The selection of relevant academic theories used in the research

The following academic theories are a result of literature research conducted on several academic journals. The list of articles have been selected through a use of search term – "cyber defense" in some of the journals available. The assumption is that the resultant papers would be related to discipline of cyber security, which is the perspective this paper intends to make in terms of the second payment service directive. Hence, the resultant papers have been analyzed in terms of the theories used and along with the context have been presented in the chart that can be found in the appendix to this paper. From the analyzed scientific works, which were 27 in total, came from 4 academic journals: MIS Quarterly (MISQ), Communications of the Association for Information Systems (CAIS), Journal of the Association for Information Systems (JAIS), Hawaii International Conference on System Sciences (HICSS) and Decision Analysis (DA). It is worth pointing out that the sources that have been selected to not total for the all available papers related to cyber security in those journals. They are however, the pre-selected batch that have been coded for purposes of this work. Hence, the limitation of this strategy can be seen in the range of the theories listed. Nevertheless, the selection of relevant theories is wide enough to create a scientific value in terms of analysis of the second payment service directive. The identified theories, in order to provide them in a more comprehensive and clear manner are listed in the chart below, along main conceptual elements of the theory. Following, the overview of each theory is provided, which should allow for more comprehensive understanding and easier comparison with mechanisms of the PSD2. From all the theories that have been identified and listed in the appendix, the selected five are already a pre-selected range that applies to a bigger extent with the purposes of the second payment service directive.

2.3.1 Technology threat avoidance theory

The purpose of Technology Threat Avoidance Theory (TTAT) is the explanation of individual IT users engagement in threat avoidance behaviors. In contrast to many studies which are examining IT security from the perspective of organization, TTAT is supplying a framework from the perspective of individual user. The authors of the theory

are Liang and Xue, who achieved it by synthesizing literature from diverse sources such as risk analysis, health care, psychology and information systems. The main principle of TTAT is stating that when individual user is perceiving an IT threat, said user will be motivated to actively avoid that IT threat. User will be taking a safeguarding measures, when they believe that the threat can be indeed avoided by executing said safeguarding measures of procedures. The alternative is that the user in case that the threat is treated as unavoidable for him will be trying to passively avoid it by executing emotion-focused copying, in case that there are no perceived safeguarding measures to be applied. The framework also provides factors that are influencing IT users threat avoidance behavior. As derived from the cybernetic theory, TTAT argues that user indents to increase the distance between their current state and the undesired (unsafe) end state. There are two cognitive processes remarked in the TTAT – threat appraisal and coping appraisal. They are derived from the coping theory. Therefore, the user first assesses the situation of IT threat existence and its degree and later plans the safeguarding actions in order to avoid it. According to the theory, threat perception is based on the perceived probability of the threat occurrence and the scope of the impact of the threat that is consequences of the threat. Moreover, the TTAT suggests that the user has three factors that are used to assess the extent to which the threat can be avoided by implementing safeguarding measures. The factors are: the effectiveness of the safeguarding measure, the costs of the measure and users' self-efficacy of applying the measure. It is important to state a few additional elements of the technology threat avoidance theory that include clarification of the approach-avoidance distinction and the differentiation between the avoidance of malicious threat and acceptance of safeguarding measure. Avoidance and adoption behavior are qualitatively different, therefore the application of one theory in different context could results in inconsistent or even false findings. As an example given by the authors, the study of threat of spyware could not produce the same, consistent findings as study of adoption of anti-spyware. In addition to the multi-theory background of the technology threat avoidance theory, the authors decided to integrate the view of the process theory and variance theory, for testing in process research and variance research purposes. TTAT shows IT user's avoidance behavior in the form of a dynamic positive feedback loop. Emergence of malicious IT in the users environment is the starting point of the loop. Once aware, the user sets the anti-goal strategy which is sourced by the fact of being harmed by malicious IT. Then the coping mechanisms will be involved, as when the user starts to perceive their current state, they will engage it. It is done in order to increase the current state and the undesired end-state. Threat avoidance behavior is expected to continue until the discrepancy becomes too large, hence the threat is expected to disappear. It can be said that the variance theory includes the relevant variables to understand threat appraisal, coping appraisal and coping in the technology threat avoidance theory. More can be observed on the diagram below. (Liang & Xue, 2018)

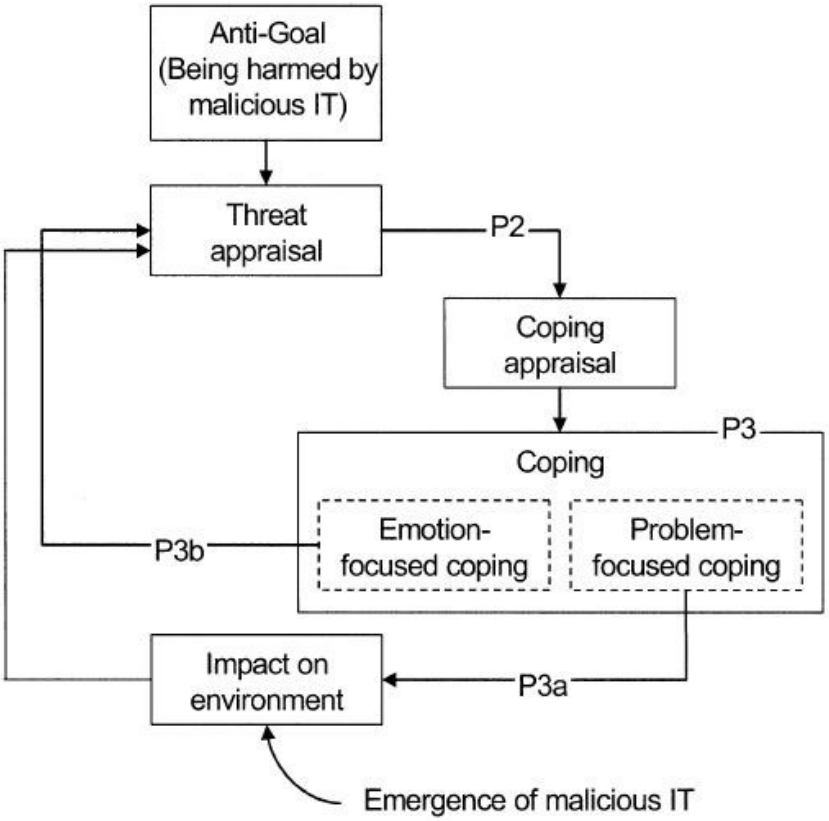

Figure 6 The process of IT threat avoidance

(Khan, 2017)

As the authors have made in the remarks to the theory, the potential practical use of the framework is quite extensive. Interestingly, some applications include security awareness and creation of efficient mechanism for educational purposes of employees and other stakeholders. It allows for a good understanding of likelihood of malicious IT attacks and its negative impact. TTAT also includes some guidelines in terms of IT practice. (Khan, 2017)

2.3.2 General deterrence theory (GDT)

According to the General Deterrence Theory (GDT) "posits that individuals can be dissuaded from committing antisocial acts through the use of countermeasures, which include strong disincentives and sanctions relative to the act" The foundation of the work on the subject is based on the work of (Walke & Straub, 1998). The author argues that the GDT can be used as a guideline in order to eliminate a threat to mitigate the risk associated with occurrence of such threat by implementation of countermeasures. Some of the countermeasures that can be used to eliminate or mitigate risks include training and

education, backups and reprimands. The research view of the GDT is expending currently to also other sources of threats. Example of such would include non-human factors. Therefore, the scope of the GDT theory can be applied also to aspects such as natural disasters and technical failures. Preemptive planning is given as one of the mechanisms for risk mitigation, examples of such could include creation of backups that would prevent data loss or hardware failures.

2.3.3 Routine Activity Theory (RAT)

The theory of Routine Activity also known as RAT includes three main elements that built up the framework – motivated offender, attractive target and the absence of capable guardianship. The factors are converged in space and time. (Cohen & Felson, 1979) The concept of motivated offenders according to the routine activity theory consists of two elements – capability of committing a criminal activity as well as willingness to do so. (Felson & Cohen, 1980) The targets that can be perceived as attractive or vulnerable can be a person or an object. Guardianship has been established to be a person or an object that works effectively in case of deterring offenses from occurring. In some instances, the crime can be stopped just by the fact that the guardianship is present in time and space. Hence, the author of the theory argues that the attractiveness of the target is rendered by situation and specificity of the crime. (Felson, 1995)

Moreover, the Routine Activity Theory considers the macro-level view, the focus is put on patterns of behavior of a victim and the offender in a broad-scale. Additionally, the focus is also concentrated on specific crimes and behaviors or decision of the offender. According to the Routine Activity Theory, the opportunity is the prime driver for committing a crime. Interestingly, the theory also provides a perspective of a victim in that regard, that it is mainly due to the fact of placing yourself in a situation where crime can be committed against you.

Figure 7 Routine Activity Theory (RAT)

Source: (Miller, 2014)

2.3.4 Protection motivation theory (PMT)

The purpose of the protection motivation theory was to help understand and clarify the fear appeals. There are essentially four factors that the protection motivation theory is built upon. The factors consist of: perceived severity of a threating even, perceived probability of the occurrence, vulnerability and the efficacy of the recommended preventive behavior as well as perceived self-efficacy. (Rogers, 1975) There are to elements that the protection motivation theory is stemming from and they include threat appraisal and coping appraisal. First of all, the threat appraisal role is to assess the severity of the situation and hence also asses the seriousness of the situation. The response to the situation is based on the coping appraisal. Moreover, the coping appraisal includes both efficacy and self-efficacy. By efficacy is the ability of an individual to process recommendations or other guidelines in order to mitigate or remove threat. Whereas, the concept of self-efficacy is the possibility of an individual to process the recommendations for an action in a successful manner. (Pechmann, Zhao, Goldberg, & Reibling, 2003)

The protection motivation theory is particularly useful in terms of suggesting optional behaviors changing in order to explain individuals on how to disengage threatening practices. Its role is both educational and motivational. The primary prevention that has

been proposed by the theory is counter measures, such as not participating in events that can lead to threats. The following secondary prevention would be to participate in measures in order to prevent the occurrence of a threat from becoming worse. (Maddux & Rogers, 1983)

2.3.5 Theory of planned behavior

The theory of planned behavior (TPB) is used primarily in psychology. The theory links one's beliefs and behavior. The main elements of the theory state that individual's behavioral intentions and behavior can be shaped by subjective norms and perceived behavioral control. The theory has been developed by Icek Azjen, which have built it upon the predictive power of the theory of reason actions. The difference being, that TPB includes perceived behavioral control. Despite its background in psychology, the theory has found a vast number of applications, such as studies of sustainability, advertising, political campaigns, healthcare, sport management. It was used primarily to research beliefs, attitudes as well as behavioral intentions. The diagram below shows the main principles and constructs of the theory. (Azjen, 1991)

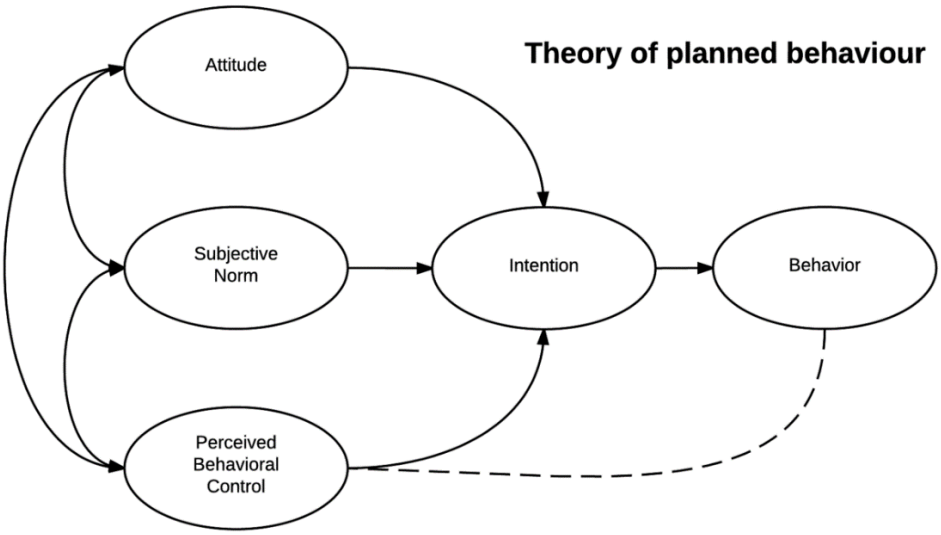

Figure 8 Theory of planned behavior

Source: (Azjen, 1991)

In order to answer the first research question which states "Which academic theory most accurately reflects the mechanisms and purpose in terms of cyber security of the second payment directive?"; the analysis of the theories have been done also in a form of a chart below. The theories have been compared by listing their main aspects as well as the context of the theory. The chart is presenting the theories only in a very brief manner, as detailed overview has been provided in the earlier part of this section.

Table 1 Overview of the theories

Theory	Main aspects of the theory	Application to cybersecurity aspect of PSD2
Technology Threat Avoidance Theory (TTAT)	IT user's engagement in threat avoidance behaviors.	The theory is based on a synthesis of literature, therefore provides vast scientific background, particularly valuable is the fact that IT threats are main element of the theory.
General deterrence theory (GDT)	The individuals behavior can be affected by strong disincentives and sanctions.	Theory present a more single-level point of view on a behavior of an individual. The application in terms of cyber security can be present, however more vaguely.
Routine Activity Theory (RAT)	Importance of motivated offender, attractive target and guardianship.	It is an interesting perspective on the motivation of the attacker and how targets can become less attractive to them by providing safeguarding mechanisms.
Protection motivation theory (PMT)	The motivation of a user in order to implement protection.	The theory allows for interesting observation of motivation to implement cyber security measures in case of fear of threats.
Theory of planned behavior	The link between beliefs and behavior.	The norms and behavioral control impact on individuals behavior, however the context of regulation can be only vaguely connected.

The above table provides in a clearer manner what are the links between the regulatory aspect of second payment service directive and the academic theories which have been selected for research purposes. Hence, the answer the first research question - "**Which academic theory most accurately reflects the mechanisms and purpose in terms of cyber security of the second payment directive?**" the theory that is most interestingly linking the two aspects is Technology Threat Avoidance Theory (TTAT). Of course, the study could be extended to cover wider range of literature, henceforth a wider scope of academic theories, however the limitations have already been mentioned in the earlier part of this section. Nevertheless, the link between threat avoidance and stated application in IT allows it to be the most comprehensive theory explaining the purposes of creation of regulatory acts such as second payment service directive. The PSD2 is concerned with providing and IT user, or particularly a digital payment service user an opportunity to avoid threats in face of dangers in cyber environment. Therefore, elements mentioned in the TTAT have been well suitable for supplementing the regulation purposes. Particularly, the elements of safeguarding measures and behaviors of the user in case of threat identification. The approach of linking theories with practical real-world regulations presented in this paper should allow in future to build legislative acts with a higher degree of understanding of behavior of the most important party involved – the final user.

2.4 Analysis of main objectives of PSD2 and scope of research of said directive and related regulatory acts

In order to start a more detailed analysis of implications of PSD2 on cyber security of payment user, the main objectives of PSD2 are going to be mentioned. Although they have been briefly stated in the introductory part of this paper, it is worth to talk about them in greater detail. According to the report created by the (Ernst & Young S.A., 2018) the main objectives of PSD2 are as follow:

- Digitalization of the payment industry, which can be achieved through integration and increase in efficiency of European payment market, reducing number of exemptions from regulations and reducing market deficiencies.
- Allowing for a more equal opportunity and therefore improving the competition of all payment service providers. Allowing for introduction of new players on the payment market.
- Improving the scope of the previous directive by specifying unregulated payment service providers, transactions and reducing exemptions overall.

- Improving customer protection, which go alongside security and safety of the payments. The means to achieve this include increasing transparency, security of retail payments (i.e by introduction of better authentication mechanism) and efficiency. Additionally, the directive also specifies the liabilities and obligations of the involved parties.
- Reduction of the general cost of payment, mainly through stimulating competition which is to reduce the prices for the final payment services user.

As given above, security is only one of the aspects of the regulation, however for purposes of this thesis it will be the focal point of this research. The further analysis in this section will consist of research of three regulatory acts – the main PSD2 directive, the guidelines issued by the European Banking Authority (EBA/GL/2017/17) as well as the Regulatory Technical Standards (EBA/RTS/2017/02). It is important to include all three sources of regulations, as the PSD2 act specifies that some more technical guidelines need to be provided in a supplementary act by European Banking Authority. Hence, for a full point of view of the implication of the PSD2, one cannot omit the complementary directives and regulations.

2.5 Analysis of articles in directive 2015/2366 (PSD2) from perspective of cyber security of payment user

The second payment service directive number 2015/2366 also known as PSD2 is widely addressing many security concerns related to payment services. Therefore, this section indents to point out the main elements of security regulations that have been mentioned under PSD2, which later should allow for a clearer understanding and creation of a chart to observe all elements introduced by this act. Due to the scope of this paper, the attention will be put on cyber security aspect of said regulations and particularly the impact on the end-customer or in other words the payment service user (PSU). The paper will evaluate some of the broader rules of security concerns, yet with cyber security being prioritized in all instances. The articles have been selected by their specific impact on aspects of cyber security. As cyber security is only one of the aspects addressed by the directive, a certain pre-selection was necessary in order to narrow down the scope of said regulatory act. In case of some articles, additional information from other supplementary sources are provided as well, mainly in order to explain in certain security aspects in greater detail and using a real-world examples. The additional sources are indicated accordingly. The second payment service directive consist of a prelude and core part. Starting with the prelude, the articles in question are as follows:

In the point (7) of the prelude in PSD2, it has been mentioned that the security risks related to electronic payments have increased for number of reasons. Main concerns are the increase in complexity of electronic payments, increasing volume of payments being executed and increase in number of types of payments available.

As stated in point (31); the payment initiation service provider (PISP) is forbidden to hold user funds at any stage. Moreover, it requires full authorization if it indents to hold user funds. This directly effects banking and FinTech businesses to gain full authorization in case of mobile payments. Services such as Google Pay, Apple Pay and such, which indeed allow for long-term use of user funds require additional confirmation by said user in order to operate. This eliminates risk of such services being "activated" and able to execute transactions without full knowledge of the customer. Point (32) also enforce ASPSP to allow such direct access to PISP.

Point (75) aiming at reducing risks of card-based payments addresses the issue of transactions where the amount charged is unknown when the payment service user (PSU) gives its confirmation. The PSP can only block the amount of funds that the user has consent to be blocked. This is particularly important in cases of automatic gas stations, hotel bookings and car rental places. The PSD2 theoretically should disallow instances where certain transactions block funds through payment-cards without a clear information and confirmation from the customer. It has been a rather popular method of securing funds for certain businesses, but potentially dangerous from the perspective of customer funds security.

In point (96), the directive mentions the basic security measures regarding electronic and mobile payments. The security measures as said needs to be appropriate to the risk involved in the payment service. Basically, the payments are required to be secured with personalized security credentials in order to avoid phishing and other types of fraud. The directive suggests typical security measures which includes data encryption on personal device of the payment service user and/or additional confirmation through another channel of communication such as email or text message with one-time password. It is important that such measures should be used when payment imitation service provider (PISP) or account information service provider (AISP) are participating in the information exchange process.

The following part comes from the core section of the directive 2015/2366:

First, the article 66 focuses on rules regarding access to payment account in case of payment service initiation services. Examples of such services are PayPal, iDEAL, PayU and many more of similar nature. Paragraph 3 states the requirements expected from PISP most of which clearly effect cyber security aspect of the transactions.

Paragraph 3 point (b) states that the security credentials of the payment service user cannot be shared with other parties, and importantly are transmitted through safe channels. This is perhaps one of the basic principles effecting cyber security in banking, where login information is key to gain access to user's account. One of the examples of a system that has been misused in the past would be SofortBanking system. It is an example of payment initiation service provider (PISP) which required a user to provide banking information to their banking service through their website without a use of original ASPSP's API. The service would then log to user's banking system in order to initiate a transaction, but it was presumably done or verified by human employees of SofortBanking, hence the login information was accessible to 3rd parties. This service would no longer comply with regulations implied by the PSD2 initiative and certainly this practice could create a danger to cyber security of PSU. (Lech, 2012) Point (c) talks about data privacy during transactions with PISP. According to the directive, information collected about PSU should only be provided to the payee and only with consent of the user. This could probably refer to many forms of data collection methods, that could potentially breach privacy which is part of one's cyber security. This point eliminates the possibility of PISP to collect data about user to later sell it or share it with 3rd parties who could use it for their mainly commercial purposes. Point (d) emphasizes the importance of secure exchange of information and transparency while identifying PIPS to AS PSP in a clear way. This is particularly important, as the bank (AS PSP) needs to verify authenticity of PIPS. This is one of the means to fight phishing, where in quite frequent instances, websites try to imitate popular PIPS in order to extract money from unaware users. Moreover, point (e) talks about storing sensitive payment data of the payment service user. This is yet another example which highly aims at reducing risks from cyber security perspective. In case of potential breach, with PSD2 in place, data stored by PISP can have no impact on safety of the user in case data leak. Point (f) and (g) build upon previous ones especially point (c), as they state the importance of confidentiality of information, especially collection of information unrelated to the needs of service provided, that could potentially be used for customer segregation or use for example in case of personalized advertisements. Unauthorized modification of the amount being transferred, or any other aspects of the transaction stated in point (h) is rather straight forward and perhaps is the most obvious potential form of fraud, hence it needs to no explanation.

Article 67 aims to regulate similar aspects of cyber security and importantly privacy in regard to payment account information service providers. Similarly, in paragraph 2, as in case of PISP, service providers need to limit their operations only to ones authorized by the user, only where PSU full consent is given (point (a)). Third parties cannot gain access to any credentials of the user, and the transfer of such has to be performed in a secure way (point (b)). The information sourced by AISP needs to be limited to those

requested by the user (d), cannot be sensitive (e) and cannot be used or stored by AISP (f).

Article 97 and 98 contain the most important regulations regarding the authentication of the PSU, with article 97 containing some of the authentication requirements and article 98 guidelines for more in-depth analysis of security and communication that will be further developed by European Banking Authority in separate act. From user's perspective, authentication is perhaps one of the only and certainly most important aspects of risk mitigation in terms of cyber security. Henceforth, the following paragraph will evaluate in detail said regulations with cyber security as the main aspect given in the PSD2 directive.

As article 97, paragraph 1 states, that the user's authentication needs to be required in every instance where user is accessing its payment account online, initiates an electronic payment transaction as well as make any action through a remote channel which could result in payment fraud or other abuse. This is particularly interesting as quick payment options are still available for card payments, often requiring only a log-in to merchant's site, but do not require additional authorization to make a payment. This is a system used for example by Amazon. The website saves essentially all credentials of banking card and on authorized computer do not require any further details to proceed with transaction. It is worth pointing out that such option is possible only with card being selected as a payment method. Interestingly, according to Arno Voerman (2016), in this matter PSD 2 has not full addressed credit card providers and allowed for such loophole in security. Credit cards, according to the Association of Credit Card Issuers Europe (ACCIE) are not caught in scope of Article 97 by arguing that payment by card is not a transfer of funds and the transaction is initiated in the moment when user presents its card to the merchant (and is verified at that moment). Due to the extent of use of card payments online, this is certainly one of the aspects of regulation which does not fully cover the real world needs of cyber security. Of course, the limit of online transactions amount could help mitigate the risk of abuse, however it is also not specified in the directive, which deals with banking cards in a very limited scope. Paragraph 2 specifies that the transaction should be authenticate using a dynamically linked elements which clearly states the specific amount and a specific payee that are taking part in the transaction. Such details are necessary in order to identify transactions and appropriate payees without a potential confusion that could arise from a more generic forms of authentication without one-of-a-kind authentication details involved. Paragraph 3 only mentions that the confidentiality and integrity of PSU personalized security credentials should be "adequate".

Article 98 very briefly states the requirements expected from guidelines created by European Banking Authority, and how it must follow criteria given in Article 97. However, paragraph 2 states also additional goals expected from said guidelines, such as

development of user-friendly, accessible and innovative means of payment (e). More information is provided by EBA/GL/2017/17.

2.6 Analysis of the directive EBA/GL/2017/17 in terms of cyber security of payment user

As a result of article 95 of PSD2, the European Banking Authority (EBA) needs to develop with cooperation with European Central Bank (ECB) guidelines concerning the security measures for operation of payment services. Therefore, this act is complementary to PSD2 and needs to be analyzed in detail to achieve a full scope of implications of the second payment service directive impact on cyber security of the payment user. Due to a wider scope of the EBA guidelines regulations, only aspect of the cyber security will be evaluated and analyzed in the following section. The articles have been selected by their relatedness to the field of cyber security, particularly affecting the final payment user, therefore some irrelevant ones might have been skipped in the process.

Guideline 2, states the requirements regarding the governance of the payment service providers. The establishment of effective operational and security risk management framework has been constituted as a necessary step. The said framework needs to be revised and approved on yearly basis by management body. The most important point stated in this article is 2.2 point d) which talks about the requirement of establishing necessary procedures in order to identify, measure and manage risks related to the payment service providers activities. The resultant is creation of framework to deal with risk management of payment service operation. Moreover, in case of outsourcing, article 2.7 states that it is a responsibility of PSP to ensure that the outsource operations have according security measures in place, similar to the ones placed domestically.

Guideline 3, talks about the risk assessment, in the first two articles 3.1 and 3.2 the main concern is the updating of the business functions, key roles and supporting processes. The EBA emphasized quite extensively the need for organization of business structures in order to provide appropriate level of security. Moreover, as part of that organization structure, the elements of ICT systems that deals with information assets particularly infrastructure, configuration and interconnections with other internal and external systems should also be identified, established and regularly updated by the payment service providers.

Guideline 4 is concerned with the aspect of protection and particularly access control. Article 4.2 states the requirement of two-factor authentication, network segmentation and multiple-firewalls in order to provide a “defense in-depth” approach. Article 4.6 that during the provision of payment services, the collection, routing, processing and storing

of payment user data should be adequate, limited and relevant. The following article 4.7 states the requirement for checking the possible updates for the software used in payment-related procedures. Article 4.8 mentions the cyber security aspects from the perspective of physical security along with articles 4.8 to 4.13. The brief meaning of this section of the guidelines requires the payment service providers to maintain adequate levels of physical and logical access to the ICT systems, while emphasizing that it should only be provided to personnel requiring such provision or business requirement. This should limit the possibility of human factor compromising the cyber security protection measures in place. Elements such as roles-based access, logging and review of the systems activity are also mentioned to support that point along with strong authentication and anomaly detection systems. Particular precaution mechanism should be put in place in case of remote administrative access to critical ICT components, with a very strong authentication put in place in order to avoid potential threats of security breaches.

The following Guide 5 states the requirements in term of monitoring and threat detection. Article 5.1 talks about the implementation of monitoring functions in order to detect anomalies in payment services provision. The monitoring should include all business functions of the operations as well as supporting processes, which basically mean that it covers the entire business unit. Additionally, the monitoring process should be able to detect breaches of confidentiality, integrity and availability of information assets. Moreover, the protection measures regarding the software and hardware should also be implemented. As article 5.3 states, the detective measures should cover all publicly know vulnerabilities and identified information leaks, malicious code or other security threats. Software and hardware updates has also been given as an example of precaution measures for said threats. Articles 5.4 to 5.6 are concerned with security incidents reporting and monitoring, which also impact payment user cyber security. Starting with establishing criteria and appropriate thresholds for threat categorization and classification, along with a warning indicators system, such mechanisms should allow for early detection of operational and security incidents. Moreover, payment service providers according to the EBA act are obligated to establish organization processes and structures in order to provide consistent monitoring, handling and follow-up in case of security incidents. According to the act, the senior management should be informed about operational or security incidents through an established procedure reporting system.

Guideline 6 states the requirements regarding the business continuity. Although most points are concerned with the business aspect of consumer protection, it is still worth to mention some which might have cyber security implications. Article 6.1 talks about precaution plans and business management plans in the event of sever business disruption, which are required by the EBA. The business disruption, although unspecified could potentially apply for cyber security attacks and similar events. The following articles 6.2 and 6.3 are providing requirements that needs to be fulfilled in case of emergencies that

might disturb critical business operation. Particularly, the banking authority requires payment service providers to implement mitigation strategies in case of termination of the payment services or termination of the existing contract. The main goal is to provide continues operation for the pending payment transactions already put in place. Interestingly, EBA in their guidelines suggest payment service providers in article 6.4 to implement wide range of possible emergency scenarios, including those extreme but plausible. Article 6.5 talks about the implementation of response and recovery plans as part of the preparation for the previously stated scenarios. The main focus should include: critical functions, processes, systems, transactions and interdependencies. Moreover, the scenario response plans should be adequately documented and readily accessible in the emergency situation to all business units. Adequate updating and improving of the plans is necessary on timely basis, as the threats in digital environment are constantly changing. Point 6.6 states that the testing of said continuity plans should occur yearly. The same goes for frequency of updating of said plans, which according to article 6.7 should also be completed on at least yearly basis. Lastly, article 6.10 mentions the requirement for a communication in case of a crisis. The payment service providers are required to have effective communication measures in place, in order to inform in a timely manner all important stakeholders, both internal and external as well as other external service providers dependent on the operation.

Guideline 7 focuses on the testing of security measures. First of all, the article 7.1 requires payment service providers to implement a testing framework for their security measures. The testing framework should take into consideration adoption of threats, vulnerabilities and other risks which have been spotted through risk-monitoring activities. Article 7.2 mentions the need for additional tests in case of changes in the procedures, changes in infrastructure or security incidents. The testing framework, according to article 7.3 and 7.4 should include the payment terminals, other devices used for provision of payment services and devices that are used for authentication of the PSU. The test should be performed by the independent testers, in order to provide effectiveness and robustness of the procedures, while ensuring that the tester has sufficient skill, knowledge and expertise to execute such tests. Moreover, the personnel involved in the testing procedures cannot be at the same time involved in the development of testing procedures, which aims to reduce security risks. The requirements for such on-going tests performed by the payment service providers in terms of frequency are identical as described in the guidelines article 3.2, which basically mean that they have to be performed on annual basis.

Guidelines 8 are concerning the situational awareness and continuous learning mechanisms. Article 8.1 and 8.2 talk about the need for identification and constant monitoring of threats that could endanger any part of operation, moreover, the later article requires the payment service providers to use security incidents as material for future improvement of their security measures. Therefore, this point can be understand as

consideration of key lessons based on analysis of security incidents and translating that into future advancement in the field of cyber security. Points 8.4 to 8.6 are considering the training of personnel that is working for payment service provider affected by that regulation. The training program should be established in order to teach staff earlier mentioned protocol, safety measures and requirements in terms of security of the business. Moreover, the EBA requires the payment service providers to ensure that the personnel which is occupying key roles in the business process is identified and will receive targeted information security training. The frequency requirement is also put in place and should be provided on a yearly basis or on more occasion if necessary. Lastly, the establishment of security awareness programs is also specified by the European banking authority, with an aim of easier detection of unusual activities and incidents.

Lastly, the guideline 9 states the relationship between the payment service user and payment service provider. It is important from the perspective of the cyber security as payment provider needs to inform the user regarding potential security risks, must present guidance in case of security measures failure and overall provide assistance in case of emergency. The requirements of said are stated in the article 9.1. The following article states the requirement of keeping the guidance and assistance procedures up-to-date, as new threats and vulnerabilities are appearing. Interestingly, EBA in point 9.2 gives payment service user a permission to disable certain aspects of services that are provided by the payment service user, where such product functionalities exists. That could for instance mean, that certain methods of payment can be disabled if the payment user wishes to do so and therefore have intention to increase his cyber security by that. The spending limits are also subject to regulation by the payment service user, and such mechanism to adjust them needs to be implemented by the payment service provider. This could indeed allow to minimize damages in face of cyber threats. The payment service user is expected to receive information of failed transfer or any other abnormal activity on his payment account, to be able to respond to the potential malicious of fraudulent behavior. As article 9.6 says, the updates to security protocols and regulations should be clearly displayed to the payment user or the PSU should be informed about them through selected channels of communication. Lastly, as article 9.7 the regulations imposed by EBA are requiring payment service providers to supply payment user with information and means of contact in case of questions regarding observed anomalies or security concerns.

2.7 Analysis of the Regulatory Technical Standards (RTS) EBA/RTS/2017/02 from perspective of cyber security of payment user

In this section, the paper will evaluate the key objectives and aspects of the Regulatory Technical Standards (RTS). The evaluation will be based on the memo issued by the (European Commission, 2017), which has been determined to be a comprehensive source of all important information regarding the directive EBA/RTS/2017/02. However, some supplementary information will be provided by article by (Hay, 2017).

The main security measures stated in the RTS consist of ensuring consumer protection, competition as well as leveling playing field in a rapidly changing market environment. Increasing the level of security of digital payments is given as one of the means of achieving consumer protection. The RTS is introducing set of security requirements which are mandatory guidelines for payment service providers, particularly in the process of payments or services which are payment-related. As previously stated, the service providers can include banks as well as other payment institutions. The objective of RTS is also to define the requirements for strong customer authentication (SCA), as well as to give a list of exemptions in which the providers do not need to follow this regulations. The regulatory technical standard is at the same time tasked with objective of brining more competition and fostering innovation at the retail payment market. The scope of RTS is identical to the scope of PSD2, which limits it to cover mainly payment accounts, but also newly specified payment initiation services and account information services.

It is important to distinguish between the applicability of each regulation, despite them being heavily dependable on each other. As already stated in earlier part of this paper, the PSD2 has started applying in all European member states as of 13 January 2018. However, the security measures which are stated in the RTS have a different date of implementation which is 18 months after the core directive. This is a matter subject to the Council and the European Parliament, nevertheless the estimated time-frame of RTS applicability is September 2019.

One of the most important aspect in terms of security in both PSD2 as well as related RTS is the concept of Strong Customer Authentication (SCA). It is aiming to increase the protection of electronic payments and other types of transactions i.e. online banking and online purchases. The requirements stated in the RTS is enforcing all payment market participants to use strong customer authentication as the basic principle of accessing the payment users accounts. The security aspect of SCA is based upon three independent elements that are known to the payment user, and identity confirmation is done using at least two of them. These elements consist of something that the payment user:

- Know (such as a PIN code or more sophisticated password)

- Own (this could include a physical card, a smartphone)
- Is (which basically translates to any type of biometrics i.e. iris scan or fingerprint)

Although this is a common practice to utilize similar authentication methods in other types of transactions, while it comes to online purchases there are still security limitations applicable. Examples of standard transactions that makes use of SCA could include using a point-of-sale terminals in stores and confirming a card payment by typing personal PIN number. With only a number of exemptions, the payments by card needs to go through a similar security process as SCA. One of such mechanisms include 3D-Secure used by some card providers, which two-factor authorization proves enough to comply with SCA requirements imposed. Some vendors have also implemented a solution of dynamic CVV, however card payments are only partly falling under the scope of RTS, hence this brief note.

The requirement of SCA is already applied in few European countries on basis of online transactions, examples include Belgium, the Netherlands and Sweden. The application of SCA for remote transactions in other European countries is purely voluntary at this moment. As the result of the RTS implementation of SCA, this authentication method is going to be mandatory for all online payments as well as accessing payment user's account. Payment service provider, including banks, will be obligated to create a necessary infrastructure for SCA implementation. However, for the regulations stated above, it is important to distinguish the liability of the bank in case of implementation of the security measures. As the recital 14 of RTS says, "PIS Providers have the right to rely on the authentication procedures provided", therefore it is to a big extent up to the bank to authenticate their customer, and not the other way around. Therefore, for instance PISPs will be obligated to pass the control of the bank, and will not be able to implement their own authentication procedures in their place. Hence, the TPPs will not be able to order the bank to proceed with their authentication, done on their terms.

Along with the strong customer authentication, the improvement to fraud management will have to be made. For a smooth operation, consumers and merchants will have to be equipped with necessary tools in order to operate in the SCA environment. There is a possibility of exemption from the SCA regulatory form of authentication, in case of security mechanism that are equally safe and secure. However, one of the requirements for the exemption from the SCA scheme is to provide transaction monitoring mechanisms that can guarantee certain low level of fraud. As a result of the SCA implementation, all payment service providers will have to conduct testing, auditing and implementation procedures that are confirming application of required security measures. Importantly, in case of fraudulent payment that has been conducted, payment user will be entitled to a full reimbursement of the costs that could be a result of such activity. Particularly in case of online payments, additional precaution mechanism will be put in place.

Some of them include linking the online transaction amount with beneficiary of the payment using a generated one-time password. Thanks to this security measure, the information that can be potentially stolen in case of hacking cannot be re-used for purposes of initiating another transaction. Such measures have already been implemented in Belgium, where the number of online frauds have drastically reduced in number. The implementation of SCA is linked with implementation of RTS regulations, therefore its introduction in a full scope is scheduled for September 2019. The time given between introduction of PSD2 and requirements listed in the RTS should allow for a smooth transition in case of payment service providers and particularly traditional banks. Change of security measures can be a delicate procedure, therefore the extended time-frame. Interestingly, RTS is also concerned with security of corporate payments, which are often executed in batches. The new regulations are considering the communication host-to-host, for example in cases where the communication takes place between an IT system of a bank and IT system of a company. There are other types of authentication than SCA that are implemented, however they will also be part of the certification process regulated by RTS and approved by national supervisors. However, this is misaligning with the concept of article 4.1 of RTS, that states that "The authentication code shall be accepted only once.", which works only in case of single payments. The assumption is that while RTS allows TPPs to initiate a series of payments, the original authorization code which has been applied only once in the process of SCA approval works for all the consequent transactions. Nevertheless, the provision of article 4.1 of access "only once" is not fully met.

Since the aspect of exemptions have been mentioned previously, it is important to briefly state what are the more tangible situations in which the exemptions can be applied. First of all, contactless card payments, despite their digital nature are exempted from the SCA regulation for single-transaction of a value up to 50 euro. The SCA requirement has also been voided in case of "trusted beneficiaries". As comment 79 states "The exemption for trusted beneficiaries only applies to payment transactions made on an online account by the payer. The PISP cannot create a list of trusted beneficiaries.". SCA also does not need to apply for low-value payments up to 30 euro with a total value of transactions set at 100 euro, which is aligned with the contactless card payments. Some additional exemptions apply in particular cases of transport payments and parking terminals.

The effect of SCA on e-commerce is despite negative voices forecasted to be positive. The commission is aiming to reduce the distress of implementation of SCA through development of trust in the system, which should foster growth of the market for digital payments. At the same time, the goal of the regulation is to reduce fraud affecting online payments.

The RTS will also consider subject of common and secure communication. It is based on a framework established by a PSD2 of new third-party payment services that are linked to consumer payment account. The services include PISP and AISP. Therefore,

the RTS regulation is aiming to specify the requirements for a common and secure standard of data transfer and communication between bank and FinTechs. As a result, consumer and companies will be provided with an option to grant access to their payment data to third party service providers (TPPs). Said TPPs can not only consist of FinTechs but also other banks where the data exchange can also be beneficiary for service portfolio. It is important to mention, that the data which is granted by the customer requires a conscious consent. Third-party providers, which are given access to the specific data, will be limited by the scope of that consent. Therefore no data outside of the given scope can be accessed by TPPs without prior authorization. The responsibility of the banks is to create a new channels of communication, that will allow TPPs to access said data. The channel needs to allow for a clear identification of each participant, as well as it should allow for a constant communication through securing messaging. It is up to the traditional banks how they plan to establish this communication, it can be done through existing customer online banking interface, but banks can also decide to create new ones. Contingency safeguards needs to be implemented as well, according to RTS regulations. The mechanism are also called “fall back mechanisms” and their purpose is to provide continuity of service and fair market competition.

The RTS regulation specifies certain restriction when it comes to dedicated communication interfaces. According to said directive, all communication interfaces will be undertaking a 3-month testing period in “prototype” conditions as well as following 3 month “live” testing in more real world market conditions. The purpose of the test it quality assurance of interfaces which are developed by the account servicing payment service providers (ASPSPs) such as banks. The dedicated interface is required to provide certain level of availability and performance, and should be similar in that regard to interfaces which are offered to customers and company payment users to accessing their payment accounts online. Moreover, the dedicated interface should create no barriers in the provision of information to payment initiation service providers (PISPs) or account information service providers (AISPs). RTS also requires payment service providers that are developing such communication interfaces to develop and define key performance indicators and service level targets, in case they decide to create such solutions. The performance indicators should be similar to those set already for online payments and banking platforms which are used by the final service customers. This should allow for a similar quality assurance as that expected from online banking services. The only exemption from this procedure can occur, when the payment service provider will put in place an interface which is fulfilling regulatory technical and its defined quality criteria of national authorities. The national authorities will have to consult this grant of exemption with the European Banking Authority (EBA). Moreover, one of the objectives of EBA is to ensure that the national authorities will interpret the quality of dedicated interfaces in a similar way. This will allow for easier supervision of their implementation in the future. The

regulations allow national authority to revoke previously given exemption to dedicated communication interface. If the interface does not operate under the criteria given by RTS, after two consecutive weeks of such disoperation the national authority can revoke the permission. The national authority is obligated to contact and inform EBA about such event. Additionally, the industry groups decided to create a consortium and work together on a common standards of interfaces. The example could include the Berlin Group. The European Retail Payment Board (ERPB) has established a working group in order to facilitate that process. Therefore, the ability to derive own standards is still possible, however there are going to be some standards that the payment providers can base it on.

The protection of personal data is an issue which is addressed by PSD2 as well as the data protection directive also known as General Data Protection Regulation (GDPR). Although the topic of GDPR will not be addressed in this paper, some aspects of data protection that are issued by RTS will be included. As previously stated, the processing of data requires a specific consent given by the payment service user. The payment service providers are restricted to the data that the payment user has conceived to and that is necessary to provide service requested by the user. Data that has not been approved by the user cannot be accessed or processed. The provision of services that are accessing payment service user data are strictly regulated by PSD2. This could include initiating a payment from the payment user account, or collecting/aggregating information for purposes of finance management of one or multiple payment account. The use of said services will only be able to be provided with a request of the payment user, and an explicit permission needs to be given. Another aspect of security is the need of informing the payment service customers about the processing of their data. This should allow for a more transparent display of data processing events. Importantly, as the regulations are complementary, laws imposed by GDRP also applies for data processed under the RTS regulation. Hence, the user will have rights such as right to access or right to be forgotten. Importantly, all payment service providers which are defined by the PSD2 and RTS regulations will have to comply with GDRP regulations as well, when they process personal data of the payment service user.

As the PSD2 is stating the specific circumstances and consent requirements that the third party providers need to receive in order to process payment user data, the new regulations are also specifying use of mechanisms in order to avoid “screen scraping”. The process of screen scraping take place through access to customer interface with the payment user security credentials. Hence, the TPPs that are utilizing the technique of screen scrapping can access customer’s data without further identification through an official bank channel. The new regulations are aimed to stop the ability to use this mechanism, mainly to prevent unauthorized data access. Instead, the TPPs will receive an official channel created by the banks, with accordance to the regulations specified in RTS and PSD2. The identification of each party will be one of the key elements of the interface,

making sure that secure communication can be established at all times. The proprietary banking interface can be re-used and adjusted to accommodate new functionality, or new interface can be created. The regulations specified by the RTS are providing detailed guidelines in terms of safeguards that the banks need to install if dedicated interface would be a preferred option. However, according to some market specialists (Hay, 2017), some of the issues of screen scraping might still remain, as the use of dedicated interface remind a process of screen scraping to some extent. Nevertheless, the process of signing the identity should provide extra security.

During the transition period between the implementation of PSD2 and implementation of RTS regulations the banks need to focus on upgrading their payments systems to accommodate all of the above requirements. This will also affect the strong customer authentication (SCA) which has been given ground in the PSD2 directive, however more specific guidelines are provided only in the RTS. Therefore, the transition period will apply to this as well.

2.8 The analysis of cyber security measures across all three regulations

In order to fully answer the second research question: "What changes in terms of cyber security does the PSD2 introduces to the payment process from perspective of payment user?" a comparison chart based on each regulatory act evaluated above needs to be created to visually display each aspect of cyber security in place. It is worth pointing out that due to the extent of the analysis that was provided in the earlier section of this work, only elements with high and medium impact on the cyber security of the payment user are going to be mentioned. The minor implications although in some cases stated in the analysis do not possess sufficient value for the general summary. The selection has been done by assessing the implications of the security measures and choosing only aspects with a high or medium degree impact.

Table 2 Main cyber security measrues

Regulatory directive	Security measure	Key security elements	Main implication on security of payment user
2015/2366 (PSD2)	Full authorization to hold user funds	Confirmation of the action	Potentially lack of unintended fund use without clear consent of the payment user

2015/2366 (PSD2)	Elimination of "blind" payments	Before transaction exact amount need to be know	Blocking a possibility of fraudulent behavior of certain websites and institutions
2015/2366 (PSD2)	Requirements of security measures of mobile devices	Personalized credentials and two step authorization	Additional level of security provided
2015/2366 (PSD2)	Eliminating possibility of sharing credentials	Credential security	Impact on account access
2015/2366 (PSD2)	TPPs operations limited to those with clear consent	Service awareness	Less unknown sources of threats
2015/2366 (PSD2)	User authentication on every instance of account access	Confirmation of action of the user	Impact on account access
EBA/GL/2017/17	Security framework for payment providers	Implication of procedures in case of risk events	Limitation of occurrences that create cyber fraud threat and systematic error elimination
EBA/GL/2017/17	"Defense in-depth"	Two factor authentication, network segmentation, multiple-firewalls	Additional layers of security should impact general level of payment user's confidence
EBA/GL/2017/17	Adequate collection of data	Limitation of data abuse	Limited confidential data leaks
EBA/GL/2017/17	Adequate level of access to ICT systems	Human oriented cyber threats	Access to account safety improvement
EBA/GL/2017/17	Improved threat detection systems	Limitation of cyber security breaches	General improvement of security in terms of remote attacks
EBA/GL/2017/17	Required software and hardware updates	Attack from the identified threats	Improvement of safety unrelated to payment user behavior

EBA/GL/2017/17	Business continuity regulations	Attack which holds funds	Less likely situation of freezing funds during process
EBA/GL/2017/17	Creation of emergency scenarios	Threat response	Faster resolving of cyber security issues in a systematic way
EBA/GL/2017/17	Crisis communication	Threat informing	User can react to threat better when informed about it in the first place, i.e. change password
EBA/GL/2017/17	Security measure testing	Precaution mechanisms	Testing of security measure impact directly the quality of security of end payment user
EBA/GL/2017/17	Training programs and constant improvement based on experience	Precaution mechanism	Improvement of systems safety that is used by the payment user
EBA/GL/2017/17	Assistance in case of threats	Guiding mechanism	Gives users knowledge on responses in case of cyber threat encounter
EBA/RTS/2017/02	Strong Customer Authentication (SCA)	Authentication mechanism	Allows user for a much stronger authentication while accessing account or making other payment-related action
EBA/RTS/2017/02	One-time passwords	Additional transfer verification and identification	Block the ability of a hacker to re-use information extracted from one transaction on others
EBA/RTS/2017/02	Standard and secure data transfer between payment institutions	Communication safety	Reduction of potential cyber breach in the scope of inter-institutional communication

EBA/RTS/2017/02	Extended testing of interfaces	Communication safety	Provision of fully evaluated mechanism, reduction of errors and bugs
EBA/RTS/2017/02	Additional data processing consent	Additional level of security in terms of authorization	Less chance for unauthorized behavior in payment services
EBA/RTS/2017/02	Elimination of screen scrapping mechanisms	Cleared identification of communication channels	Elimination of channels to commit fraud on user's account

As based on the chart above, the implications in term of cyber security that are a resultant of PSD2 or supplementary regulatory acts is extensive. The various precaution mechanism, regulations and guidelines are certainly going to impact the security of payment user greatly. The scope of the regulations implemented by the directive in question particularly shows that previously a lot of matters remained underregulated or unspecified. Obviously, there was an element of volunteer security measures that third-party providers or other payment service providers could implement on their own, nevertheless a specific act that imposes such requirements upon them provides the payment user with higher level of trust and safety. It is important to mention that despite availability of the acts, one should be aware of the dates of their introduction or coming in force. As for PSD2 it has already been implemented in all member states, however the supplementary acts are still in the transition period, therefore some of the regulations at the time of writing this paper might still not come in force in some countries or institutions.

3 RESEARCH METHOD

The purpose of this chapter is to explain the research method used in this paper. First of all, the research design has been explained, with motivation for the type of research that has been applied as well as background information about the methods used. Following, the data sample section evaluates the participants of the study as well as their relevance to the research. Next, the data collection section introduces the methods of how the data has been gathered. Consequently, the explanation of the data analysis is provided. Lastly, the chapter finishes with conclusion and final remarks.

3.1 Research design

Due to the fact, that the structure of this paper is naturally divided by research questions asked in the introduction, the research method explaining how the specific questions are address has to be provided. The first two research questions that is "Which academic theory most accurately reflects the mechanisms and purpose in terms of cyber security of the second payment directive?" and "What changes in terms of cyber security does the PSD2 introduces to the payment process from perspective of payment user?" are answered with a help of literature and secondary data, whereas the answer for the last research question is given through an empirical study. Therefore, the first two research questions utilizes a method of literature synthesis to derive results. Last research question is answered with a help of a qualitative case study.

The literature and secondary data regarding the purposes, mechanisms and specific information regarding the second payment service directive was extensive and easily accessible. The only problem consisted of scattering of information through various academic and secondary sources such as journals, official directives, expert articles and more. Therefore, the logical step of structuring the scattered data was to perform a literature synthesis process.

According to (Kamiański & Szubka, 1989) literature synthesis is one of the three exploratory methods in science. Usually, the work with papers based on this method is progressing in two stages. The first consist of analysis of the collected data in order to distinguish the most important terms and problematic aspects of the explored topic. At this stage, researchers are using the analytical-comparison method. The second stage of the research is based on more regular form of information analysis, which goal is to establish facts, ideas and their meaning in terms of the explored topic. Within the scope of document analysis, one should supplement their work with internal and external analysis. According to (Łobocki, 2000), the internal analysis is based on exploring the content of the documents, appropriate understanding of said and explanation, particularly by

separating the first-plan contextual elements, leading thoughts and connections between them. Whereas, the external analysis of the documents is supplementary to the internal analysis. Its goal is to establish the time, conditions and environment in which the documents have been created and its influence on occurrence of certain events. The text analysis should be complemented with general synthesis process, which provides more general point of view of the research and explains it in a broader scope, after analysis of the individual elements of the data review.

On the other hand, the third research question "What are the empirical changes in terms of cyber security and business practices that the banks, third party providers and others had experienced as a result of implementation of PSD2?" does not have sufficient literature conducted to provide a comprehensive review to answer the question. Therefore, to address this issue a single case study research has been performed. (Stebbins, 2012) states that in case of insufficient research performed on certain topic, an explorative case study should be made. Explorative research allows to explain certain events by providing answers to why, how and when specific occurrences happened. It also provides an option to do so by supplementing the research with different viewpoints. It is one of the methods to achieve deeper understanding or insight of the topic researched. The construction of the research based on explorative case study aims to explain certain events rather than predict the outcomes. Moreover, the single case study in question is also used in prospective research, which means that it includes cases that are meeting certain established criteria. Additionally, single case study is also interpretive, as the results of the research conducted are subjective to analysis of the researcher. The data collected is based on qualitative research method, which means that the data collected is non-numerical.

As case study can include various sources such as interviews, observations and additional documents, it proves to be a good option to provide a comprehensive overview of the question researched. Nevertheless, in order to create correct questions to answer the research question certain preparatory steps have to be completed. According to (Cooper, Schindler, & Sun, 2006), literature review consist of comprehensive source of the overview information that can be used to formulate them. Hence, the questions created for purposes of this study are derived from previously conducted literature review.

To strengthen the choice of research method, as (Yin, 1994) argues, the use of case study is particularly useful in terms of real-life context especially in explore complex matters. Research and analysis that is conducted in a descriptive manner proves a good method of investigating certain phenomenon.

3.2 Data sample

As previously stated, the research is based on a single case study. The data that has been collected comes from three various sources that represent three different payment market participants – the traditional bank, third-party payment service provider and the legislative institution. Therefore, next the overview of the concerned organizations is provided.

3.2.1 Overview of the ING

ING as abbreviated from *Internationale Nederlanden Groep* is a Dutch multinational bank with headquarters in Amsterdam. The business portfolio includes retail banking, direct banking, commercial banking, investment banking, asset management as well as insurance services. The bank boasts a high number of active customers in the range of 37 million world-wide. As of 2017, the bank also has over 54,000 employees in different branches. (*2017 Annual Report ING Groep N.V.*, n.d.)

3.2.2 Overview of the Bank of Aruba

The Central Bank of Aruba started its operation as of 1986, at the time of independence of Aruba from the Kingdom of the Netherlands. Previously, Aruba has been a part of what is known as Netherlands Antilles. Currently, the bank is responsible for provision of the monetary policies, supervision of financial system, bank-notes issuing, governance banking and exchange and supervision of flow of foreign payments. (“Centrale Bank van Aruba - CBA,” n.d.)

3.2.3 Overview of the BlueMedia

BlueMedia acts mainly as a payment initiation service provider with a 500 000 daily customers for their services. They are present on the market for 20 years, however their current operation has shifter drastically from earlier business profile. Their yearly turn-over is above 9 billion PLN which is equivalent of about 2.1 billion euros. They also provide other highly diversified services in payments, banking, identification, insurance, public sector and payment systems. (“O nas - Bluemedia,” n.d.)

3.2.4 Interview method

There were 3 interviews conducted in total. The interviews were done with representatives of different payment service market participants to provide a broader picture of the implications that are the question of the research. The total duration of the interviews was 43 minutes and 49 seconds. The interviews took place between the and 22nd and 28th of May. Overview of the participants is provided in the following section of this document. The number of interviews, although limited, was able to provide sufficient information to analyze the implications for the parties represented and derive interesting conclusion.

3.2.5 Interview participants

Traditional banking institution:

Current Product Manager at ING, with a history in the payment services. Worked closely in the past on the first service payment service directive, with a job related to the field of second payment service directive, however not directly involved in the implementation of latter. Currently involved in the robotics process automation for payment processes.

Legislative intuition:

Manager of the Information Security Department at Central Bank of Aruba and member of the national security task-force, with vast academic and work experience in the field of cyber security. Additionally, the person has been actively involved into the process of implementation planning of second payment service directive for purposes of Aruba.

Third party service provider institution:

Product manager at payment initiation service provider BlueMedia. With a relevant work experience regarding the implementation and development of services that were affected by the second payment service directive. Currently focused on works related to development of payment gate, KIP and TPP.

3.2.6 Interview remarks

As stated earlier, the interview took place in a period of one week. The transcribing of the interviews was performed right after finishing the conversation which helped to understand all the aspects explored in a more concise manner. All of the interviews have provided the research with equally valuable data and there is little in terms of discrepancy between them in terms of the scope of the talks. However, the duration of some interviews differed slightly, due to the ability of the participants to answer the questions as well as their schedule arrangements. All participants have mentioned that the regulations imposed by the second payment service directive had a big influence on their institutions. As can be seen in the in the analysis of the results in the later part, not all aspects that were asked in the interviews have yield the same degree of answers. This is assumed to be a reason for data vulnerability and strategic meaning of this information for their respective organizations. Despite the limitation, the questions seems to provide enough precision for the people interviewed to understand their meaning and provide answers that are relevant. The background information that was provided with some of the questions also seems to be helpful during the interviews as it specifies the scope that the research is trying to explore. The opening questions allowed for a better understanding if the person interviewed can indeed be a suitable choice for this research. The last question was very open-ended and allowed for more freedom of answer for the participants. All the participants stated that the information that is being shared can be used for this research and can be used for needs of this paper. All participants also identified themselves as experts in the field and consisted of high-tier employees.

3.3 Data collection

3.3.1 Primary data

The purpose of the case study conducted through interviews is to collect relevant information from payment service market participants to answer the third research question of this paper. In order to provide sufficient answer, the impact of implementation of second payment service directive had to be analyzed in the scope of the entire institution, as well as key business operations. The interviewees were asked all the questions that were part of the questionnaire. In some instances, the interview has answered the previous following question already through a monolog started by a previous question. In this case, the following question was still asked in order to gather additional data that the participant might have forgotten to mention. The general goal of the interviews was to answer the

research question from three different perspective of different payment market participants. The answers were also planned to be assessed in terms of differences and similarities that the payment service directive have made on each organization. Later, the conclusion could be drawn as for what empirical changes the directive actually bring in the real-world scenario. Particularly, aspect of cyber security, business model implications, potential partnership and finally mandatory data-sharing was aimed to be analyzed in the selected institutions. The interviewer has included background information in the question in order to narrow down the scope and guide the conversation into critical aspects. Therefore the questionnaire can be described as semi-structured. Some participants have been informed before the interviews about the scope of the talks, which resulted in potential preparation of said. Particularly interview with BlueMedia has been scheduled in a longer run and the interviewee had confirmed that talks with PSD2 related division of the institution took place.

All of the interviews had been recorded for purposes of transcription. All of the interviews took place through a long-distance communication that is telephone or Skype.

3.3.2 Secondary data

As some of the participants provided additional information after the interviews to supplement this research, the paper uses also some secondary data to answer the third research question. This data consisted mainly of internal information that is accessible only to the employees of said organizations. Additionally, some information have been sourced from publicly accessible sources to provide a broader-scope of certain topics.

The documents were provided in English and Polish, due to the international scope of the interviewed institutions. The elements that have been used in Polish have been directly translated. The translations have been literal, as to preserve the highest amount of details and stay close to the original. However, due to the fact that the author of the paper is Polish native, the language barrier did not create any obstacles.

3.4 Data analysis

Two of the three interviews are conducted in English, as this is a universal language that the participants are most comfortable with. However, due to the fact that one interviewed party is based in Poland, and the author of this paper is Polish for simplification of the data gathering process the interview was conducted in Polish and later translated into English.

After the completion of the interviews, the entire conversations that were recorded have been transcribed for better analysis purposes. The transcriptions are included in the appendix to this paper. The transcription has been performed through an online software TEMI. The results of the automatic transcription were then manually checked and errors were corrected. The transcription process has been performed to maintain maximus details of the conversation. Certain world such used for pauses, such as “a” or “um” have been removed as they did not add any value and decreased the clarity. No participants had issues with including their interviews to the paper. Due to the limited number of interviews performed as well as their length, the analysis has been performed on a raw material provided. The analysis was performed question based, however due to the free nature of the conversation, some participants have mentioned elements that were related also to other questions stated. Therefore, the interviews should be look at as a whole rather than analyzed per question.

4 RESULTS

In this section, the results of the interviews previously described will be analyzed. The structure will follow the structure of the questionnaire and therefore will be divided into six main concepts that are investigated in the research. The concepts include: changes in the security standards that are affecting final user of the payment service, implementation of the strong customer authentication, creation of new services, creation of new partnerships, data sharing, additional changes resulting from implementation of the second payment service directive. Each concept will be evaluated separately and will include three sub-sections based on the data collected from each of the three institutions that are participating in this research. Following, the results will be discussed to bring the main elements that have been discovered.

4.1 Changes in security standards affecting payment service customer

ING:

The expert from the ING has provided very limited information when it comes to the technical changes in terms of cyber security resulting from implementation of the second payment service directive. Elements that have been mentioned however were the improvement of cyber security infrastructure, nevertheless no specific examples have been given. Moreover, the participant have stated – "Well, the most important change for ING is that we are opening the account information to third party providers" while asked for the aspects of cyber security. It can be assumed that by that, the area where ING is possible foreseeing cyber security threats can be related to this specific aspect of PSD2. The information about opening up those channels have been compared with the fact that previously said channels were exclusively available to the internal banking infrastructure. The fact that the information is going to flow through different digital devices, such as mobiles have also been mentioned. Additionally the interviewee have stated that "(…) we used APIs that were new to the ING and we worked a lot on making that available in a secure way, adhering to all the security standards, (...), that you need to apply." Based on that statement, it can be concluded that APIs have enforced additional changes to the security aspect of operations in ING that resulted in implementation of new cyber security measures.

Bank of Aruba:

In terms of cyber security, the representative of the Bank of Aruba have confirmed that the implications coming from the PSD2 have affected all aspects that have been mentioned in the question. That includes changes to: IT security infrastructure, internal security policies, security incident management procedures, contingency procedures, outsourcing security policies and implementations of new forms of security authorization. Moreover, the expert have mentioned that as a result of the implementation of PSD2 the cyber security measurements would also include building of a new, different infrastructure for facilitating payments. No specific technical examples have been given, however the perspective of this expert is providing an overview of changes that will be implement in the future. The situation of Aruba implies that the PSD2 policy is in the process of implementation and preparation that has not yet been completed. However, the range of changes that it take is perhaps the most broad among given institutions.

Blue Media:

First and foremost, the representative of Blue Media has addressed the changes that the institution had to implement due to the implementation of PSD2. The expert had confirmed that all elements that have been mentioned in the question had indeed been modified in order to comply with the new regulation. Unfortunately, specific technical details of changes could not be provided due to the data vulnerability.

4.2 Implementation of Strong Customer Authentication

ING:

The expert has declined to provide more information in regard to cyber security, therefore the implementation aspect of Strong Customer Authentication has to be omitted from perspective of the interviewee. However, thanks to the secondary data provided by said participant more perspective on the approach of ING can be analyzed. According to the documentation, the implementation of SCA for ING is an important and valuable regulation. Thanks to that, the cybersecurity of their customers can increase due to the fact that the practice of “screen scrapping” is no longer possible for the third-party payment providers, however the changes in terms of implementation have not been mentioned.

Bank of Aruba:

The Bank of Aruba representative have stated that the implementation of Strong Customer Authentication does not lay in their field of operation. As the participant is

representative of the legislative side, their responsibility is to supervise such implementation in other dependent institutions. However, the expert has also stated “I can foresee that it will have impact on safekeeping of all these factors”, which can be taken as a confirmation of importance of the SCA in terms of cyber security.

Blue Media:

The interviewee has stated that “It is certainly an important aspect for us, as we value the safety of our customers a lot.” This emphasizes the importance of this specific aspect of PSD2 in terms of cyber security for the analyzed institution. It is worth pointing out that according to the expert, the process of implementation is still on-going, that is, it has not been yet fully completed. Moreover, the expert had mentioned that the works on the SCA are in the “conceptual” stage.

4.3 Creation of new services

ING:

According to the interviewee, creation of new services is an important aspect of their strategy and the participant have confirmed that PSD2 indeed led to creation of new services. The expert has said that “We are working together with the FinTechs to see how their solutions can be integrated with the account information that we can provide so that you can imagine that there will be a lot of platforms that can now really enhance services because they can provide more end-to-end service including banking services without the need to go to any kind of proprietary channel of a bank.” Therefore, some of the services that have been indicated here include banking platforms and solutions that are currently offered by the FinTechs and could be soon extended to the customers of ING. The participant have also stated that ING intention is to be present in terms of branding on said platforms, therefore maintaining recognizable brand image in terms of new service development. Interestingly, some examples of new services that were given consisted of use of APIs for smart speakers. Due to the opening-up of the channels, the expert showed interest of ING in the area of smart devices.

From the secondary source documentation, the ING has stated that the development of the “Payconiq” payment service that operates in Belgium has been “paved” by the PSD2 regulation, therefore it allowed for easier implementation.

Bank of Aruba:

Due to the fact that the PSD2 implementation is not a complete process in the situation of Aruba, the impact on provision of new services is hard to assess. However, the interviewee has mentioned that "indeed a new payment service providers would want to join in", therefore indicating that an increase of competition on the payment market in Aruba is expected to increase. Some examples of FinTech companies have also been given, such as Google and Facebook.

Blue Media:

The answer provided by the interviewee was very brief, however it encapsulated the result the overall impact of PSD2 on this aspect. The interviewee has confirmed that indeed the introduction of PSD2 had stimulated creation of new services in terms of account information services and payment initiation services. There were no specific examples provided though. Moreover, the interviewee had stated that the institution is currently working on new services that are adjusted to the changes for after 14th of September (RTS implementation deadline).

4.4 Creation of new partnerships

ING

The expert has explicitly stated that "So we are also working together with these major players and that's all now becoming possible because of this standardized way of working and because of PSD2". Therefore it can be confirmed that the impact of PSD2 has indeed positively affected the creation of new partnerships. In case of most services that were indicated in the previous section, the element of partnership was mentioned as well. Moreover, on several occasion the participant has mentioned the new possibility of information exchange with other banks and third party providers. The participant has also mentioned the willingness of ING to be a part of more collaborative market platforms, and example given consisted of mortgage comparison platform. The representative of ING has also addressed concerns from the new market situation which is a potential lack of identity on the payment market.

Bank of Aruba

The interviewee has confirmed that the implementation of PSD2 is expected to create new partnerships in the payment market of Aruba. Nevertheless, the implementation of this regulatory act is not given as the only impact that might stimulate that event, rather the implementation of new payment rails that is undertaken in the nation of Aruba.

Blue Media

In case of creation of new partnership relationships, the interviewee had indeed confirmed the impact of PSD2 in this aspect. The partnership creation had been pointed at the account information services in particular and an example of telecom companies had been provided. Another example had consisted of partnership with another Polish PISP "PayU", however the details of the scope of partnership had not been disclosed.

4.5 Data sharing

ING

Data sharing has been extensively mentioned throughout the interview. On several occasions the interviewee have stated that it is a very important measure for ING. The interviewee have mentioned that ING is in the process of development of APIs based on the regulations imposed by PSD2. The participant have also addressed that the idea of Open Banking goes beyond payment services and ING would like to utilize those opportunities that come with it.

Bank of Aruba

In case of data sharing, the interviewee has stated that the represented institution would most likely be implementing new forms of APIs, that are potentially developed specifically for their purpose. Moreover, the security aspect of data sharing has also been addressed. The example given was concerning untrusted third-party providers and the responsibility of the bank to maintain data safety. Hence, the expert has identified an issue that data sharing technology might still require additional cyber security measures that the traditional banks would need to implement in order to prevent other untrusted organization to gain access to them through data sharing. The aspect of data privacy law in Europe (GDRP) has also been given as despite being limited to Europe it does effect European citizens world-wide. Therefore, the institutions in Aruba as historically related to Europe would need to consider this aspect as well.

Blue Media

The development of APIs had been indicated as important. The interviewee had stated that the company is "currently working on quite intensively" on this aspect of regulations. Moreover, the expert has stated that the use of APIs would include those issued by the traditional banks as well as development in their own solutions.

4.6 Additional changes resulting from implementation of the PSD2

ING

The implications that have been stated by the ING representative includes the financial impact that are resultant of implementation of all measures related to PSD2. The statement was rather general, but it would imply that the highest costs would be associated with development of new channels, assuming forms of APIs and others. The interviewee has also stated that the general banking environment is going to drastically change, particularly in the form of providing services to the banking customers. The expert have also mentioned "(…) much less, (…) proprietary environment", that is the traditional banking brick and mortar market share. Instead, it was suggested that the banking industry will shift towards much more open environment, where the emphasize will be put on the actual service and development of new services rather than the front-end. The future of ING has been indicated to go towards the idea of a platform that is collection of different services where PSD2 is one of the stimulants that encourages this approach.

Bank of Aruba

The main aspect that has been additionally mentioned by the expert of Bank of Aruba is addressing the idea of a Sandbox. The purpose would be to be able to observe their operation in a controlled environment that allows for adjustment of regulations and security measures. Particularly, the third-party providers and new ventures have been stated as for the use of such Sandbox. Interestingly, another important security aspect have been mentioned in the last part of the interview. The interviewee has stated "Also from a technical perspective, what are these people, offering to the user? Where is the user data? Is there enough transparency for the end user as to where his data is? And also something that's also very tricky in case of a breach who is responsible for what (…) so where does the responsibility end and the other starts, because I think, the bank can also have a say in this." This aspect is particularly interesting, as in terms of changes of regulations, the PSD2 does indeed specify a lot of said security concerns. Therefore it can be assumed that the use of Sandbox and evaluation of service providers can be beneficial for implementation and changes that the PSD2 brings in terms of cyber security.

Blue Media

Additional changes that have been a result of implementation of PSD2 were confirmed. Examples given by the interviewee includes development of new business strategies. Moreover, the expert has stated "generally we perceive PSD2 as sort of the incubator for changes that might come," The impact of said regulation had also been described as major. It has also been stated that the evaluated institution is "looking for opportunities and threats and try to respond to them accordingly". This can also be linked with cyber

security threats that could be perceived by such payment market participants, however no definite statements as such have been made.

4.7 Result discussion

The purpose of this section is to describe the results implications and how they address the research question stated. Due to the lack of literature that could allow for comparison of the results with other studies conducted, the discussion will focus purely on context of the research on the scope of this paper.

The research question that the study was trying to address was What are the empirical changes in terms of cyber security and business practices that the banks, third party providers and others had experienced as a result of implementation of PSD2?". As can be observed, the scope of the research question did not limit the investigation to only the aspect of cyber security in terms of the PSD2 regulation. Moreover, it extended to show other empirical implications that could go along the changes of cyber security measures with the intention to observe the link between them.

Hence, the analysis of the results allowed for statement that the aspect of cyber security indeed plays a crucial role for all of the studied institutions. Nevertheless, the specific implications of that impact were hard to observe on the results provided earlier. The discrepancy between the institutions was quite clear, all of the three institutions are at the same time representatives of different payment market participants showed very far going differences in approach, plans and experiences related to the second payment service directive. Moreover, it is worth pointing out that the institutions were all in different stages of implementing said regulations and could provide very diversified opinions about them. In terms of cyber security, the results also varied in terms of the knowledge of participants and their involvement in implementation of said. The detailed technical changes that were expected to be observed turned out to be extremely hard to obtain, mainly due to the fact that such data can be described as vulnerable for business operation of investigated organizations, as well as limited willingness of participants to elaborate more in this aspect. However, all of the interviewees showed a high willingness to share information about future plans, growth, development of new services and other aspects that could be described as more general.

The research however can make some general brief answers to the questions asked. First of all, the impact of the payment service directive on the cyber security of the payment user can be described as significant and far going. All of the researched organizations basically could confirm that statement. Moreover, in terms of SCA, Bank of Aruba and Blue Media indeed confirmed the importance of that measure for cyber security of the payment user and for their operation. The implications of PSD2 on additional

aspects such as development of new services, business relations can also be described as existent and rather significant. Lastly, the data sharing has collected interesting results as one hand it has been observed to be a very important aspect of the PSD2 from empirical perspective of the organizations research, but also has been identified as a potential threat in terms of cyber security. Therefore, the implication of data sharing could be further studied to see what are those implications and potential threats.

Based on the results, it is very hard to make general statements in case of different institutions in order to apply this research on a wider scope of the payment market participants. However, the results still turned out to be rather interesting and could possess a value from business perspective.

5 CONCLUSION

5.1 Main findings

The main findings include answers to the three research questions stated in the beginning of the paper, as well as, the problem statement.

First of all, the first research question was trying to present the theory that could explain the purpose of the second payment service directive from the perspective of the payment user. Therefore, in the result of the study a Technology Threat Avoidance Theory (TTAT) has been derived as the most suitable choice to explain the underlying purposes of the directive in question. It has been observed as presenting very interesting perspective on a second payment service directive, as a result of the study, it has been concluded that the theory could prove useful not only in explanation of the purposes but also in future development of similar regulatory acts.

Secondly, the study aimed to answer the research question concerning the changes that the second payment service directive, as well as supplementary policies, have brought in terms of cyber security to the payment service user. It can be concluded that the changes were severe. As a result of the analysis of three very extensive regulatory acts have been presented in a form of a table containing the most important implications (according to the author). Overall, thanks to the implementation of said regulatory acts, safety of the payment services user has drastically improved and will further improve as some acts are still pending and will be mandatory for service providers in the near future.

Thirdly, the research question was attempting to address the empirical implications that the second payment service directive had on payment service users in terms of cyber security, and provide additional information about the impact on other aspects of analyzed institutions. Concluding, the cyber security aspect of the payment service directive on payment users has been established to be significant. Moreover, all of the institutions have stated that the changes that the PSD2 is bringing in terms of cyber security are important. Additionally, the changes from previous policies to the ones imposed by PSD2 in terms of cyber security according to two out of three institutions have included all of the aspects mentioned in the questionnaire that is: IT security infrastructure, internal security policies, security incident management procedures, contingency procedures, outsourcing policies and implementation of new form of authentication. Moreover, the aspect of Strong Customer Authentication (SCA), which has been previously established to be one of the key objectives of the PSD2 regulation in terms of cyber security improvement also turned out to be significant in perspective of the studied institutions. Two out of three organizations have also mentioned that they will have to introduces changes to some aspects of security measures in order to comply with said safety mechanism.

Interesting observations have also been observed in other aspects of payment service providers business other than cybersecurity. The introduction of PSD2 has led to introduction of new services in all three studied organizations or dependent entities. Particularly interesting was the impact of PSD2 on development and importance of FinTechs which has also been mentioned by two of three institutions directly, as one could be assigned as FinTech by itself. Introduction of PSD2 has led to creation of new partnerships also for all studied organizations, or in case of Bank of Aruba its almost certainly going to create new partnerships in the future. Data sharing has been identified as one of the most important aspects of PSD2, particularly by traditional bank representative, however all participants have confirmed its importance. Data sharing has also been perceived as a potential threat, again mainly by the traditional bank representative. Additional remarks that were given at the end of the study include use of Sandbox environment to test new payment market participants, positive impact of PSD2 on business development and indication of drastic changes to the banking environment in general which result from implementation of second payment service directive.

5.2 Research Validity

In order to validate the research, the four different aspects of the qualitative method used are going to be evaluated as according to (Guba, 1981). These aspects include: credibility, transferability, dependability and confirmability.

The purpose of credibility is to check if the results obtained are believable. The use of a standard questionnaire for each interviewed participant is believed to increase said aspect. Moreover, the interviews conducted have been transcribed and the provided in the appendix to this paper. The translation of one of three interviews that had been conducted in Polish rather than English has been done by the author of this paper who is a native of Polish language, therefore the translation should maintain high level of original information provided.

The second aspect of research validity, that is transferability will be discussed next. The meaning of this aspect is how the results derived in this research can be applied in different context. As the representatives of the participants were providing information from perspective of the entire organization the transferability has certainly increased. Some of the data collected can also be used on evaluation of wider impact of PSD2 rather than only the perspective of cyber security.

The third aspect is dependability, which explains the ability to replicate the study on while conducting similar research. In this paper, the study has been conducted on three very diverse institutions which will be indeed hard to transfer to other context. Moreover, the time frame of this research, that is after the implementation of PSD2, however before

the deadline for certain supplementary regulations also proves a unique perspective of this research. Nevertheless, dependability has been increased by providing of detailed methodology and participant introduction which therefore allows for creation of similar study. More to that, the data collected in this study is believed to be useful to complement data collected on different organizations through similar study.

Lastly, confirmability explains the degree of the influence that outside parties had on the results of this study. The interviewees were not related by any means, therefore is no possibility for any communication. The interviews were also recorded and transcribed which creates a hard evidence. Any other aspects of work on this paper by outside party has been determined to be minimal to not say non-existent.

5.3 Limitations and future study recommendations

The research has number of limitations that need to be addressed. To start, the first research question method of literature analysis is based on 27 academic sources, which do not represent the entire scope of the research papers that are available in selected journals. In order to provide a more comprehensive analysis, one should conduct a broader study to include the remaining literature, the selection process could also include more factors that could provide easier comparison of the theories rather than concluding the research on literature review.

The second research question that was answered with a help of literature synthesis also need to clarify certain limitations in the process. Beginning with the scope of literature synthesis, the number of academic sources is limited due to recent character of the regulation in question. Therefore, the synthesis had to include sources from less reliable websites, rather than focus purely on academic papers. Therefore, some aspects could suffer on quality of data that it was based on. Moreover, the analysis of the regulations due to its size proved to be very time consuming and difficult task. As only one author has worked on it, certain elements of cyber security regulations that were researched using said regulatory acts could be omitted.

The third research question was answered by a single case study based on qualitative research method. The most significant limitation included the scope of the research, three institutions that were evaluated cannot represent the entire payment service market properly and can hardly scale within their own type of organization. Moreover, each institution had only one expert interviewed which added the limitation in that regard. The questionnaire, due to limited number of participants in the study could not be adjusted through a pilot study on benchmark market participant. Some of the aspects that have been asked in the study were not fully implemented in participating institutions.

Moreover, the interviewees had a tendency to avoid answering the questions with a concrete examples, despite being asked to provide such.

Despite interesting data gathered, it would certainly be beneficial for the study to have a higher number of interviews and to increase the scope of the participating organizations. In order to provide a cleared formulation of the questionnaire, a pilot study on a benchmark participant could be performed as well. It would be interesting to see the results after implementation of all the supplementary regulations to PSD2, which are coming to power in the near future. Certainly, the data gathered could include much more "delicate" information if the study would be conducted by someone working within one of the organizations affected by implementation of PSD2. Lastly, over time more literature on the topic could become available, therefore providing a better comparison material to aid this research.

6 MANAGEMENT SUMMARY

The second payment service directive has broad impact on many aspects of cyber security, operation of third-party service payment providers, traditional banks and last but not least payment service users. Despite vast literature, documentation and publicly available regulatory acts, the information regarding its purpose, impact on cyber-security of the payment user as well as empirical implications on the stakeholders of the second payment service directive is limited. Therefore, this paper provides interesting observations and comprehensive answers to all of the previously stated issues. An overview of the research questions as well as the main finding has been provided in the table below.

Table 3 Management summary

Research Question	Research Method	Main findings
RQ1: Which academic theory most accurately reflects the mechanisms and purpose in terms of cyber security of the second payment directive?	Literature review based on 27 academic papers.	The selection of Technology Threat Avoidance Theory (TTAT) as the most interesting and suitable theory to explain the underlying purposes of the PSD2.
RQ2: What changes in terms of cyber security does the PSD2 introduces to the payment process from perspective of payment user?	Literature synthesis based on extensive literature review, including many articles, internet sources, academic papers as well as three regulatory acts (2015/2366 (PSD2), EBA/GL/2017/17, EBA/RTS/2017/02)	The impact of the PSD2 as well as supplementary acts is significant on the security of the payment service user and among many other implications resulting from their implementation there is also number of cyber security measures affecting payment user introduced.
RQ3: What are the empirical changes in terms of cyber security and business practices that the banks, third party providers and others had experienced as a result of implementation of PSD2?	Single case study based on three diversified stakeholders of the PSD2, which includes a traditional bank, third-party service provider (PISP) and legislator.	The results showed that the institutions did implement changes or will implement changes related to cyber security measures as a result of PSD2 and that the said regulation also impacted other areas of their operations.

BIBLIOGRAPHY

2017 Annual Report ING Groep N.V. (n.d.). Retrieved from https://www.ing.com/web/file?uuid=984d63ab-14e4-4a37-abcd-8326d8196f76&owner=b03bc017-e0db-4b5d-abbf-003b12934429&contentid=42779

Arner, D. W., Barberis, J., & Buckley, R. P. (2016). *The Evolution of FinTech: A New Post-Crisis Paradigm*. *1*(1), 1271–1319. https://doi.org/10.3868/s050-004-015-0003-8

Azjen, I. (1991). The Theory of Planned Behavior. *Community Dental Health*, *25*(2), 107–114. https://doi.org/10.1922/CDH_2120VandenBroucke08

Brockhurts, J. (2019). Market Ripe For Neobank Success. Retrieved May 26, 2019, from https://www.nielsen.com/au/en/insights/news/2019/market-ripe-for-neobank-success.html

Brodsky, L., & Oakes, L. (2017). Data Sharing and Open Banking. *McKinsey on Payments*, (July), 16–23. Retrieved from https://www.mckinsey.it/sites/default/files/data-sharing-and-open-banking.pdf

Centrale Bank van Aruba - CBA. (n.d.). Retrieved May 30, 2019, from https://www.cbaruba.org/cba/getPage.do?page=ABOUT_US_MAIN_FUNCTIONS

Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, *44*(4), 588. https://doi.org/10.2307/2094589

Cooper, D. R., Schindler, P. S., & Sun, J. (2006). *Business research methods*.

Dorfleitner, G., Hornuf, L., Schmitt, M., & Weber, M. (2017). Definition of FinTech and Description of the FinTech Industry Currently. *FinTech in Germany*, 5–10. https://doi.org/10.1007/978-3-319-54666-7

Ernst & Young S.A. (2018). *The revised Payment Service Directive (PSD2). What you need to know*. (December 2015), 8.

European Commission. (n.d.). Payment services. Retrieved from https://ec.europa.eu/info/business-economy-euro/banking-and-finance/consumer-finance-and-payments/payment-services/payment-services_en

European Commission. (2017). Payment Services Directive (PSD2): Regulatory Technical Standards (RTS) enabling consumers to benefit from safer and more innovative electronic payments. *Press Release*, (November 27th), 2–5. Retrieved from http://europa.eu/rapid/press-release_MEMO-17-4961_en.html

Felson, M. (1995). Those who discourage crime. *Crime and Place*, *4*, 53–66.

Felson, M., & Cohen, L. E. (1980). Human ecology and crime: A routine activity approach. *Human Ecology*, *8*(4), 389–406. https://doi.org/10.1007/BF01561001

Guba, E. G. (1981). Criteria for Assessing the Trustworthiness o f Naturalistic Inquiries Egon G. Guba. *Educational Communication and Technology*, *29*(2), 75–91. https://doi.org/10.1007/BF02766777

Hay, T. (2017). The PSD2 Final RTS: 10 Things You Need to Know. Retrieved May 29, 2019, from https://gomedici.com/psd2-final-rts-10-things-you-need-to-know/

Hemon-Laurens, A. (2015). Banks Beware: the Impact of PSD2 and XS2A - Accelerating Digital Disruption | Quadient. Retrieved May 28, 2019, from https://www.quadient.com/blog/banks-beware-impact-psd2-and-xs2a-accelerating-digital-disruption

Huiskes, A., & Elsenga, O. (2017). *Payment Services Directive 2 for FinTech & Payment Service Providers Accelerate your growth journey*. 7.

Husek, S., Brich, P., & Prochazka, J. (2017). *How to flourish in an uncertain future: Open banking and PSD2*. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/cz/Documents/financial-services/cz-open-banking-and-psd2.pdf

Jensen, C. T. (2015). *APIs For Dummies, IBM Limited Edition* (C. A. Burchfield, Ed.). John Wiley & Sons, Inc.

Kamiański, S., & Szubka, T. (1989). *Jak Filozofować? Studia z metodologii filozofii klasycznej*. Retrieved from https://philpapers.org/rec/KAMJFS

Kawai, Y. (2016). June 2016 Issue 53 From the Secretary General. *IAIS International Association Insurance Supervisors*, (53), 12.

Khan, A. (2017). Technology Threat Avoidance Theory (TTAT) - IS Theory. Retrieved May 29, 2019, from https://is.theorizeit.org/wiki/Technology_Threat_Avoidance_Theory_(TTAT)

Lech, K. (2012). System płatności Sofort? Jeżeli dbasz o bezpieczeństwo, to lepiej uważaj! Retrieved April 7, 2019, from https://www.pcworld.pl/news/System-platnosci-Sofort-Jezeli-dbasz-o-bezpieczenstwo-to-lepiej-uwazaj,382840.html

Legal Dictionary | Law.com. (n.d.). Retrieved May 27, 2019, from http://dictionary.law.com/default.aspx?selected=785

Liang, H., & Xue, Y. (2018). *Avoidance of Information Technology Threats: a theoretical perspective*. *33*(1), 71–90.

Łobocki, M. (2000). *Metody i techniki badań pedagogicznych*. Retrieved from http://www.publio.pl/files/samples/2e/5a/68/51731/Metody_Demo.pdf

Mackenzie, A. (2015). The fintech revolution. *London Business School Review*, (3), 50–53.

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, *19*(5), 469–479. https://doi.org/10.1016/0022-1031(83)90023-9

MarketsandMarkets (M&M). (2018). *Digital Payment Market by Type, Solution Type, Deployment Mode, Organization Size And Region - Global Forecast to 2023*. Retrieved from https://www.reportlinker.com/p05587810/Digital-Payment-Market-by-Type-Solution-Type-Deployment-Mode-Organization-Size-And-Region-Global-Forecast-to.html

McCarthy, N. (2015). Americans Trust Tech Firms More Than Banks For Finance [Infographic]. Retrieved April 6, 2019, from 2015-06-24 website: https://www.forbes.com/sites/niallmccarthy/2015/06/24/americans-trust-tech-firms-more-than-banks-for-finance-infographic/#26251b6a4e94

Merriam-Webster dictionary. (n.d.). Cyber Security Definition. Retrieved from https://www.merriam-webster.com/dictionary/cybersecurity

Miller, J. M. (Ed.). (2014). *The Encyclopedia of Theoretical Criminology*. https://doi.org/10.1002/9781118517390

Minarchenko, I. L. S. (2018). *The future of Neobanks in the development of banking sector*. 335–336.

Nonninger, L. (2019). German neobank N26 raises $300 million in Series D funding - Business Insider. Retrieved April 6, 2019, from https://www.businessinsider.com/n26-series-d-funding-unicorn-status-2019-1?IR=T

O nas - Bluemedia. (n.d.). Retrieved May 30, 2019, from https://bluemedia.pl/o-nas

Orbis Research. (2018). Global Third Party Payment Market Growth, Opportunities, Trends and Forecast 2018-2023. Retrieved from https://www.marketwatch.com/press-release/global-third-party-payment-market-growth-opportunities-trends-and-forecast-2018-2023-2018-09-07

Paget, F. (2007). Identity theft. McAfee Avert Labs technical white paper No 1. Retrieved from http://www.mcafee.com/ us/local_content/white_papers/wp_id_theft_ en.pdf

Pechmann, C., Zhao, G., Goldberg, M. E., & Reibling, E. T. (2003). What to Convey in Antismoking Advertisements for Adolescents: The use of Protection Motivation Theory to Identify Effective Message Themes. *Journal of Marketing*, *67*(2), 1–18. https://doi.org/10.1509/jmkg.67.2.1.18607

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change1. *The Journal of Psychology*, *91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Rouse, M., Nolle Tom, & Li Thomas. (2017). What is application program interface (API)? - Definition from WhatIs.com. Retrieved May 26, 2019, from https://searchmicroservices.techtarget.com/definition/application-program-interface-API

Schwienbacher, A. (2019). Equity crowdfunding: anything to celebrate? *Venture Capital*, *21*(1), 65–74. https://doi.org/10.1080/13691066.2018.1559010

Sebastian. (2017). Introduction to Part Two. In *Disputing Strategies in Medieval Scandinavia* (pp. 141–160). https://doi.org/10.1163/9789004221598_007

Stebbins, R. (2012). Exploratory Research in the Social Sciences. In *Exploratory Research in the Social Sciences*. https://doi.org/10.4135/9781412984249

Stewart, H., & Jürjens, J. (2018). Data security and consumer trust in FinTech innovation in Germany. *Information and Computer Security*, *26*(1), 109–128. https://doi.org/10.1108/ICS-06-2017-0039

Sweeney, L. (2006). *Protecting Job Seekers from identity theft*. (April), 74–78.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers and Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Walke, R. J., & Straub, D. W. (1998). Coping with systems risk: Security planning models for management decision making. *Management Information Systems Quarterly*, *22*(4), 441.

Yin, R. K. (1994). Discovering the Future of the Case Study Method in Evaluation Research. *American Journal of Evaluation*, *15*(3), 283–290. https://doi.org/10.1177/109821409401500309

Zachariadis, M., & Ozcan, P. (2017). The API Economy and Digital Transformation in Financial Services: The Case of Open Banking. *Ssrn*. https://doi.org/10.2139/ssrn.2975199

APPENDIX

6.1 Questionnaire

OPENING QUESTIONS:

1. What is your role in the financial sector? Are you a representative of payment service provider (bank, third-party provider), payment user or legislator? Could you briefly describe what do you do?

2. Are you familiar with Second Payment Service Directive? If yes please describe briefly what was the scope of your work with PSD2.

CORE QUESTIONS:

1. Payments and access to the account safety is emphasized as one of the key objectives of the second payment directive (PSD2). As a result of its implementation, did your organization introduce any changes to existing security standards affecting final users of your services? If yes which ones? (Examples could include IT security infrastructure, internal security policies, security incident management procedure, contingency procedures, new forms of security authorization)

2. One of the key objectives of PSD2 is to increase level of security and confidence of electronic payments. It requires payment service providers such as banks to develop strong customer authentication (SCA) which combine at least two independent elements - physical such as card or mobile phone, knowledge (passwords) or biometric feature, such as fingerprint before making a payment. Have your organization had to implement, update or modify in any other way existing security solution in order to comply with PSD2 regulation? If yes, could you briefly describe what was the scope of the change?

3. PSD2 led to increased competition on the financial market. New players knows as Third-party providers have emerged to compete with traditional banks. Therefore, have your organization developed any kind of new services which were a resultant of the new market situation? This could include new forms of payments, mobile apps, forms of authorization etc.

4. Third-party providers do not necessarily need to consist of competitors and in many cases can supplement the offer of traditional bank. Have your organization created new partnerships or implemented services of third-party providers that could be a result of implementation of PSD2 directive?

5. PSD2 also enforces the data sharing between the banks and third-party providers, it is done mainly through Application Programming Interface (API). What were the

implications of this data sharing law on your organization? Does your organization utilizes existing API (i.e. Open Banking) or developed their own?

6. Are there any other changes or practical implications that your organization has undertaken which were a result from implementation of PSD2? Could you briefly state them?

6.2 List of analyzed articles

Table 4 Overview of academic papers

Journal	Title	Theory	Context
MISQ	Avoidance of Information Technology Threats: A Theoretical Perspective	TTAT [p. 72] Malicious vs Virtuous IT [p. 73], Cybernetic Theory [p 73] Copying theory, process theory, variance theory.	What stimulates user to undertake safeguarding measures, realize threat, avoidance and adoption in face of cyber security. User motivation.
MISQ	CyberGate: A Design Framework and System for Text Analysis of Computer-Mediated Communication	N/A	In-depth explanation of what it takes to analyze CMC and how it was done by the authors.
MISQ	Brand Positioning Strategy Using Search Engine Marketing	N/A	Study of web search engines and its effect on consumer behaviour, the study showed number of factors that have been influenced by change in website positioning.
MISQ	Cybercrime Deterrence and International Legislation: Evidence from Distributed Denial of Service Attacks	General deterrence theory (GDT), Routine Activity Theory (RAT)	Evaluation of hackers behavior in case of COC
MISQ	Circuits of Power: A Study of Mandated Compliance to an Information Systems Security De Jure Standard in a Government Organization	N/A	The paper tests few hypothesis related to adoption of ISS mainly in case of gov. Agencies

MISQ	Practicing Safe Computing: A Multimedia Empirical Examination of Home Computer User Security Behavioral Intentions	Protection motivation theory (PMT) [p. 617]	The perspective of human factor in a form of home computer users in terms of cyber security. How they make the weakest point in cyber defense.
CAIS	An Empirical Examination of IT-Enabled Emergency Response: The Cases of Hurricane Katrina and Hurricane Rita	N/A	The value of response, how to response to a threat. In the context of hurricane threat. Information systems used for threat response.
CAIS	Digital Steganography—An Introduction to Techniques and Tools	N/A	How different forms of stenography and more importantly data injections can be used also in cyber-attacks. Mechanism are audio files, image files, video files and other.
CAIS	Information Systems and Health Care XIII: Examining the Critical Requirements, Design Approaches and Evaluation Methods for a Public Health Emergency Response System	N/A	Emergency Response system, similar to later Chen article.
CAIS	Examining Inefficiencies and Consumer Uncertainty in E-Commerce	Economics of Information Theory and Transaction Cost Theory. [p. 527]	Uncertainties' with online shopping. Cyber security as one of the issues of e-commerce [p. 528] Digital vs real world, many comparisons.
CAIS	Country-Level Determinants of E-Government Maturity	N/A	Factors for development of e-governance, factors of measuring the maturity etc.
CAIS	Multiple Indicators and Multiple Causes (MIMIC) Models as a Mixed-Modeling Technique: A Tutorial and an Annotated Example	PBM Model	Highly scientific comparison of MIMIC models
CAIS	Unveiling the Mask of Phishing: Threats, Preventive Measures, and Responsibilities	N/A	Phishing, especially in banking. Bogus websites, Trojans, Web-based delivery, Pharming - many more listed around p. 549

CAIS	A Knowledge Management Approach to Identify Victims of Human Sex Trafficking	System development method [p. 608]	Use of socials for human trafficking (luring), mainly with a use of ads.
JAIS	Preventing State-Led Cyberattacks Using the Bright Internet and Internet Peace Principles	N/A	Bright Internet initiative;
JAIS	Jump-Starting the Internet Revolution: How Structural Conduciveness and Global Connections Help Diffuse the Internet	N/A	Empirical examination of the influence of globalization on Internet capacity/development
JAIS	The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies	User technology acceptance model, theory of planned behavior	Analysis of motivation to prevent cyber-attacks of computer users.
JAIS	Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective	Technology Threat Avoidance Theory [p. 395 and more 396]	How malicious software motivates user to avoid IT Threats.
JAIS	ICT Challenges and Opportunities in Building a "Bright Society"	N/A	Focused mainly on cyberbullying, some other elements of ICT issues also are given.
JAIS	Robbing Peter to Pay Paul: Surrendering Privacy for Security's Sake in an Identity Ecosystem	N/A	The article talks about trade-off of privacy and security on example of specific identity ecosystems.
JAIS	A Lifetime of Theory and Action on the Ethical Use of Computers: A Dialogue with Enid Mumford	N/A	Case studies regarding 4 principles presented in a form of interview with Enid Muford.
HICSS	Perverse Effects in Defense of Computer Systems: When More Is Less	N/A	The article shows many situations where perverse effect occurs - technological, cyber defense, human etc.
EIJS	Dispositional and situational factors: influences on information security policy violations	N/A	How likely it is to violate security measures by users.
EJIS	Third-degree conflicts: information warfare	N/A	Background information on information warfare and comparison with other types of physical warfare.

EIJS	If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security	N/A	How organizations motivate individuals to take precautions in accordance with security measures enforced.
DA	Information Security Investment When Hackers Disseminate Knowledge	N/A	Differential game framework;
DA	Exploitation of Ambiguous Cues to Infer Terrorist Activity	N/A	The article present a model on hypothetical scenario of nuclear terrorist attack and its implications.

6.3 Interview 1 Transcript - ING

Interviewer: 01:07 The first question is, what is your role in the financial sector, are you a representative of payment service provider such as bank, third-party payment provider, payment user or legislator. Could you briefly describe what do you do?

ING: 01:37 I'm a product manager at ING, which is a bank, which is quite famous worldwide and we also engage a lot with the third parties. And I've gotten history in payments, but lately I am doing something else. So that might also complicate, that it will be, maybe it will be hard for me to answer all your questions, but I used to be very heavily involved in a payment sector, but lately I'm doing robotics process automation also for payment processes. So yeah, that's my role.

Interviewer: 02:22 Okay, perfect. Well, are you familiar with the second payment service directive? And if you are, then could you please describe briefly what was the scope of your work with the PSD2?

ING:	02:38	Yeah, I worked on the predecessors, the euro back in the days with SEPA, with the PSD1 and for PSD2, I'm not really heavily involved. I'm familiar with Open Banking a little bit and how we are trying to organize ourselves within ING to be prepared for the PSD2 a as a bank.
Interviewer:	03:15	Okay, perfect. Well most of my questions are PSD2 related so I would still appreciate if you just answer to the best of your knowledge and that's absolutely fine. Let's move on with the core questions then. So as you know, payment and access to the account safety is emphasized as one of the key objectives of the second payment service directive. And as a result of its implementation, did your organization introduce any changes to existing security standards affecting final user of the service? And, if yes, which ones? I can give you some of the examples as well to guide the question. And those examples could include: IT security infrastructure, internal security policies, security incident management procedures, contingency procedures, new forms of security authorization.
ING:	04:21	Well, the most important change for ING is that we are opening the account information to third party providers, so until now, we have our own channels and information about accounts was restricted to our own channels for Internet brunches, mobile. As of now we are opening this to third party provider. So that's the most important change for us. That we need to provide an API for other parties, also other banks, but also, to other providers to make it the most of all to share account information that until now was really only within our own system. So that means that we used APIs that were new to the ING and we worked a lot on making that available in a secure way, adhering to all the security standards, that you need to, that you need to apply. On the other hand, we are also of course, seeing the opportunities for PSD2 that we can also start providing account information from other banks to our customers. So the multi-thing principle now becomes much easier to provide to our customers, being at the retail and wholesale. So yeah, we, we did a lot on our infrastructure and also on the security. I don't have all the details, but indeed, we need to provide the PSD2 APIs. That was the most important change for us. And on the other hand, we are also going to use third party or other banks APIs to also provide this to our customers.

Interviewer:	06:28	Is there anything else that, you know, about the security aspect that has been changed, in terms of PSD2? Basically, do you have a knowledge of any, any changes when it comes to security that has been implemented because of the PSD2?
ING:	07:04	No, I'm afraid I don't have that knowledge. No.
Interviewer:	07:07	Okay. That's all right . Let's move to the question number three then. PSD2 led to increased competition on the financial market and new players known as the Third party provides have emerged to compete with traditional banks. Therefore, have your organization developed any kind of new services which were a result of the new market situation? This could include new forms of payments and mobile apps, forms of authorization.
ING:	07:47	Yes, we did. We are working together with the FinTechs to see how their solutions can be integrated with the account information that we can provide so that you can imagine that there will be a lot of platforms that can now really enhanced services because they can provide more end to end service including banking services without the need to go to any kind of proprietary channel of a bank. So we are looking together with FinTechs to see how can we deliver the services, because of course you can imagine that our concern is that in the end this account information will be fully out of our hands. And the window to the customer, will then belong to another party like a Google or Amazon or Apple. And, and we are only becoming a factory without a face to the customer. So that's why we are trying to make sure that we will be there with our own branding and our own products in this portals that people go to. We also on the other hand, we like to extend our service, not only with account information and payment information, but also services added on top of that. So also there we are reaching out to FinTechs and hopefully we can also create these kinds of portals and platforms where people will go to. And, for instance we create this API, and yeah, we cannot really afford, ignore the power of these big companies like Amazon and Google. So we are also, connecting our PSD2 APIs with for instance smart speakers. So we would like to be available via Google Home or Amazon Echo so that a customer can ask for his balance just by sitting on the kitchen table and asking Google what the balance is. So we are also working together with

these major players and that's all now becoming possible because of this standardized way of working and because of PSD2.

Interviewer: 10:16 Okay, great. That's very useful answer. That basically answers also my, another question which was if there are any partnerships created thanks to the third party providers integration which is a result of PSD2. So you've already mentioned the, the Amazon and Google and Apple. So this one side. Do you have any other examples on mind perhaps?

ING: 10:52 Yeah, I think we are also dealing with these platforms. So, I do not have the concrete examples, but for instance, if you would create a kind of mortgage comparison platform, and ING would also have stake in there, we would then be able not only to add our own PSD2 information, but also again, account information from other banks available in that portal and then, you can still have an ING endorsed solution can then be made available. So, I mean we are, it's again the same thing that we would not only like to be only providing our information. But we would also like to benefit from the open market that you will now see by teaming up with these kind of platform initiatives for their mortgage comparisons or instant loans. For instance, that you would be able to provide the loan to a consumer by also just checking in real-time the dependence that he has with another thing. Those are things that were impossible before PSD2 and are now becoming available.

Interviewer: 12:08 Okay. I think that answers my question pretty well. Two more questions I've got. First of all, well you've already mentioned open banking as one of the API that ING is utilizing is the only one that? Well, is ING, your organization participating in development of the Open Banking API or is it developing their own? Could you elaborate a little bit on that?

ING: 12:45 We are building our own PSD2 APIs, so our own development. We are extending the scope like open banking, so it's not only PSD2. So not only payments related, APIs that we are building, but we're also trying to put together more APIs that in the end can be opened for our customers. So it's open banking is more than and payments and we are, I think also

developing our own standards, not our own ones. But we are developing our own KPIs there as well. But I don't have a lot of detailed information about that, I'm afraid.

Interviewer: 13:35 Okay. Well, the last question would be very open ended. We've talked about some elements such as the APIs, such as the other implications of basically opening up the format of the banking and sharing the information. Are there any other changes or practical implications that you have observed in your organization that are a result of the PSD2 implementation? Could you briefly state them?

ING: 14:11 I think this will change the way that we are now serving our customers because we have invested a lot in these different channels and every bank has invested a lot in different channels. It's costing millions of euros of a development and maintenance. And I think what you will see in the next years, and we are already starting to prepare for that. That we will have much less, I think this proprietary environment where customers will go, we will have much more open environment where customers will go to and that will mean that we will not invest more in the frond-end but in creating this services and also using these services. So I think that that is going to be the main thing for the future. And that's why ING is also trying to become a portal, a proprietary platform that a lot of people go to, or at least be part of the platform where people go and that's the big change and we will invest less in our own channels and we will invest more in this platform idea and I think PSD2 the most concrete example right now.

Interviewer: 15:31 Okay, great. I think that's all I basically need in terms of the implications of PSD2 in your organization.

ING: 15:45 What I could do is I can check on our intranet for more PSD2 related information. And if I get some interesting stuff that's really answering your questions in a more detailed way. I will share this to you this afternoon. Maybe I can help you a little bit more with some more specific information. Let's see what I can find.

Interviewer:	16:12	That will be absolutely great and obviously I appreciate that help a lot. Especially if you can get some information in terms of a cyber security that is particularly useful for my research. And, I do understand that this is a very, very vulnerable data that, well it's very a well a well that you cannot really say any specific information obviously, I would very much be interested, especially in information which would be basically what was the cyber security implication of PSD2, meaning it does not have to be exact solution or our cyber security measure.
ING:	17:12	I will, I will see what I can find. But of course you have to imagine that our channels were of course, kind of for Fort Knox kind of. Yeah. Nobody could get it of course. And now we are opening. So, so we are, we need to defend our data and our apartments in another way. But yeah, if you ask me specific what we did, I would try to rectify.

6.4 Interview 2 Transcript – Bank of Aruba

Interviewer:	01:04	Well let's start with the opening question then. What is your role in the financial sector? Are you representative of payment service provider such as bank, third party provider or legislator? And could you briefly describe what do you do?
Bank of Aruba:	01:20	So basically, I have two functions. So a legislator definitely and we do a lot of supervision and also in the payments infrastructure for the financial sector as well.
Interviewer:	01:41	Okay, perfect. Well another question, are you familiar with second payment services directive? If yes, please describe briefly what was the scope of your work with PSD2?

Bank of Aruba:	01:53	So yes, I am currently for our domain. I'm in the group that is presenting a version of the PSD2, for our, our nation or our island in this case. So I am pretty much, on the legislative side, to present this for our country.
Interviewer:	02:23	Okay, perfect. Well we'll have the core questions then. Payments and access to the account safety is emphasized as one of the key objectives of the second payment directive PSD2, as a result of its implementation, did your organization introduce or is planning to introduce any changes to existing security standards affecting final user of your services? If yes, which ones and examples could include IT Security infrastructure, an internal security policies, security incident management procedures, contingency procedures, new forms of security authorization.
Bank of Aruba:	03:03	So basically all of the above. It does strike from policy right down to the, oh, you forgot outsourcing policy as well. So outsourcing from internal security policies, from, the IT infrastructure as well. So we are planning to build in a different infrastructure for supporting of such a payment facilities. If it's a dictates that we would you be using them as well.
Interviewer:	03:41	Okay. Uh, well that's very brief, but let's stick to that for now. One of the key objectives of PSD2 is to increase level of security and confidence of electronic payments. It requires payment service providers such as bank to develop strong customer authentication SCA, which combines at least two independent elements, physical such as a card or mobile phone, knowledge, passwords or biometric features such as fingerprint before making any payment. Have your organization had to implement, update or modify in any other way existing security regulations in order to comply with this PSD2 regulation? If yes, could you briefly describe what was the scope?
Bank of Aruba:	04:27	We, we are not, going to roll out for ourselves a payment scheme or payment service as we are a regulator. But of course we are, it is our duty to make sure that the financial sector, which encapsulates banks and other financial institutes, do that in a safe and consistent manner. So for us as an organization, I don't see us in the near future really having to do with that. But in the future I think it is our duty to ensure that the financial sector here does comply with that. And

I can, I can foresee that it will have impact on safekeeping of all these factors. Cause you mentioned a password biometrics and, and another factor if you wish. So the safe keeping of these of this information is also very crucial cause it'll flow now through a third party before it reaches the bank where it was initially already intended to be and also be kept safe.

Interviewer: 05:40 Okay. Perfect. Well, PSD2 led to increased competition on the financial market. New players known as third party providers have emerged to compete with traditional banks. Therefore have your organization developed any kind of new services, which were a result of the new market situation. And this could include new forms of payments, mobile apps forms of authorization, et cetera.

Bank of Aruba: 06:07 In the market where we are we don't have the legislation yet, but what we do foresee that might happen is that indeed a new payment service providers would want to join in. And we will need to actually open the doors to them as well. So for our organization directly, no, but we do foresee that maybe, neighboring islands or neighboring nations would, would want to participate or even maybe the bigger ones like Google and Facebook I think is also turning to banking now as well. I read this morning.

Interviewer: 06:50 Okay. Well, Third party providers not necessarily need to consist of competitors and in many cases can supplement the offer of traditional bank. Have you organization created new partnerships or implement services offered by the providers that could be a result of implementation of PSD2 directive or is planning to in that case?

Bank of Aruba: 07:14 I think a yes because we have, currently we are responsible for the payment rails are the national payment rails and we have acquired a third party to a for example, assist those with the modernization of this. It's not PSD2 as you would see it in its in its pure form. However, it is the first step, to making payments transparent for all parties as well. I think the

		next step would be that, that through this third party you'll have API's becoming available for which they, they could provide or hook their services onto it.
Interviewer:	07:56	Okay. That's actually, what sort of relates to my next question. Which is, that PSD2 also enforces the data sharing between the banks and the third party providers and it is mainly done through application programming interface API. What would the implications of the this data sharing law in your organization or in this case are presumably going to be and is your organization utilizes existing APIs such as OpenBanking, or is planning to use develop their own?
Bank of Aruba:	08:34	I think it's going to be new APIs. I think specifically developed for us, if we go down that path of using APIs, it'll be specifically developed for our purpose. And, and the first part of your question please.
Interviewer:	08:50	Yes. Well the first, what was the implication this data sharing law on your organization? So basically what could that mean in case of the data sharing that is going to be implemented.
Bank of Aruba:	09:07	That means a lot, I think, if you see how data is, so going back, basically you just share your information with the bank, keep it there for your financial, lifetime or life cycle that you are with this bank. Now you are opening the door through a different vendor to get to your information and that should be given I think on a case by case basis. So that should be a technical advance going to the bank back and forth where the bank also should come back to you and say, okay, are you really sure you want me to share this data with a company, A, B, or C? And do you want me to keep reminding you every time they ask for your data or they offer you something through this information so it will open the doors of the banks. I'm not really sure that they are comfortable with this, but they need to have better measures in place once that starts happening, especially with the law on privacy, also applicable in Europe. And for Europeans living abroad as well. So it's not that if you're not in Europe that it doesn't apply to you.

Interviewer:	10:28	Okay. Yes, please. If you have anything to add then.
Bank of Aruba:	10:34	No, I think it'll be just major, major implications and, and technical is not even the beginning of, of the complexity that it adds.
Interviewer:	10:46	Okay. Well, last question is more of an open ended and I think in a case of your organization, there's much more to add in this. Are there any other changes or other practical implications that your organization has undertaken which would result from implementation of PSD2 and could you briefly state them?
Bank of Aruba:	11:23	I think in our specific, context as a regulator, we will need to be ready for maybe a sandbox solution, where we can host, for example, these upcoming spin ups or third parties or a new ventures even, in order to see how we could regulate, their actions and products better. I don't, I do think it's a good movement. It does shake up the banking industry a lot, but it needs to be understood. Also from a technical perspective, what are these people, offering to the user? Um, where is the user data? Is there enough transparency for the end user as to where his data is? And, and also something that's also very tricky in case of a breach who is responsible for what, you know, so where does the responsibility end and the other starts, because I think, sorry, the bank can also have a say in this. If you know of a shady service, for example, that requesting your customers' data that you have worked so hard to protect, and if you know that it's not safe, on the other hand, you're not just freely going to give it away without a warning. So it's, it means a lot to technically really, really does. And from a regulator perspective, everybody is basically looking at you for guidance. So we need to make sure that we are on the ball with that.
Interviewer:	13:10	Okay. well that pretty much answers all my questions. Well, I'm not, I'm not sure if there's anything else that could be a direct, impact on, on the organization that, you haven't mentioned before as well. Basically, it's a, it's a pretty broad topic, so it's probably going to unfold a little in the process as well.

Bank of Aruba:	13:43	So we can learn from that as well. Yeah,
Interviewer:	13:48	Yeah, exactly. Well, but that's going to be a little bit later, I suppose. Yeah. Well, okay, well thank you very much then.
Bank of Aruba:	14:19	Okay, cool. Glad that I could help.

6.5 Interview 3 Transcript – BlueMedia

Interviewer:	00:54	Well, since you have limited time let's move on with the opening questions. What is your role in the financial sector? Are you representative of payment service provider such as bank, third party provider or legislator? Could you briefly describe what do you do?
Blue Media:	01:25	So, my general occupation is a Product Manager at Blue Media. Although the scope of the actual functions is a bit bigger, I can say that pretty much I am responsible for development of the payment gate, so the main sort of service we provide, but also KIP and TPP.
Interviewer:	02:22	Okay, great. Well next question, are you familiar with second payment services directive? If yes, please describe briefly what was the scope of your work with PSD2?

Blue Media:	02:40	So yes, I have learned about PSD2 while I was already working in Blue Media. I have been working there for some time already, but I think I worked with it more since maybe two years ago. I have also participated in the workshops and conferences that were related to the PSD2 and we have quite extensive internal documentation of that.
Interviewer:	03:27	Okay, perfect. Well we'll move on the the core questions then. Payments and access to the account safety is emphasized as one of the key objectives of the second payment service directive PSD2 and as a result of its implementation, have your organization any changes to existing security standards affecting final user of your services? If that is correct, which ones? And maybe I can give few examples that could be IT Security infrastructure, Internal security policies, security incident management procedures, contingency procedures, new forms of security authorization.
Blue Media:	04:01	Well, we had to adjust in some scope pretty much all of the things that you have mentioned. I am not really able to disclose the particular changes that we have implemented, as this is very delicate information, but we have slightly adjusted them. But on top of that, well, we are also just developing all aspects of security despite the regulations and we do bear in mind the current market regulations and rules.
Interviewer:	04:45	Okay. Well, I understand that you cannot really provide me with more, so it’s ok. The next question. One of the key objectives of PSD2 is to increase level of security and confidence of electronic payments. It requires payment service providers such as bank to develop strong customer authentication SCA, which combines at least two independent elements, physical such as a card or mobile phone, knowledge, passwords or biometric features such as fingerprint before making any payment. Have your organization had to implement, update or modify in any other way existing security regulations in order to comply with this PSD2 regulation? If yes, could you briefly describe what was the scope?
Blue Media:	05:27	We are constantly in the process of implementing changes when it comes to Strong Customer Authentication. It is certainly an important aspect for us, as we value the safety of our customers a lot. So this is an important element. But, at

this time we are working on it in more sort of conceptual way. We have not yet implemented it fully, so I would call it a conceptual stage.

Interviewer: 06:14 Okay. Perfect. Well, PSD2 led to increased competition on the financial market. New players known as third party providers have emerged to compete with traditional banks. Therefore have your organization developed any kind of new services, which were a result of the new market situation. And this could include new forms of payments, mobile apps forms of authorization and so on.

Blue Media: 06:47 I can answer yes to this question. We did implement types of service functions of AIS and PIS from before 14th of September. And we are working on new services that will be adjusted to changes for after 14th of September.

Interviewer: 07:32 Okay, thank you. Next question then, third party providers not necessarily need to consist of competitors and in many cases can supplement the offer of traditional bank. Did you, well your organization created new partnerships or implement services offered by the providers that could be a result of implementation of PSD2 directive?

Blue Media: 07:55 I think, well yes. We did made some new relations in terms of AIS and the opportunities that have come with it. It is mainly for the telecom industry, but also well we will have a closer relation with one other service provider, I think its ok if I mention that it will be PayU. But I cannot disclose much more information.

Interviewer: 08:34 Okay. That's already very useful information. Well, the following question then that is, PSD2 also enforces the data sharing between the banks and the third party providers and traditional banks. It is mainly done through application programming interface API. What are the implications of this data sharing law in your organization and is your organization utilizes existing APIs such as OpenBanking, or is going to develop their own?

Blue Media:	08:57	Ok, that is something that we are currently working on quite intensively. We are utilizing both the traditional bank APIs which are shared by the ASPSPs and we are building our own. This is one of the elements that we believe that the market is heading towards, so yes, it is a big part of our current operations. So the impact is quite severe I would say overall of the data sharing in our case.
Interviewer:	10:02	Okay. Well, this is already the last question and it is more open ended. Are there any other changes or other empirical implications that your organization has undertaken which would result from implementation of PSD2 and could you briefly describe them?
Blue Media:	10:26	Yes, we of course have experienced some. It allows for more business development strategies, generally we perceive PSD2 as sort of the incubator for changes that might come, sort of like the starting point for more changes. So it is very important to our organization to look through it very well and look where else we can develop and grow. For now, I can just say that we are researching the market mainly, looking for opportunities and threats and try to respond to them accordingly.
Interviewer:	11:30	Okay. That was the last of it. Well, is there anything else that you could add?
Blue Media:	11:42	Well, due to the profile of our company I can only share general information I am afraid. But hope it was enough to help.
Interviewer:	12:03	Sure, I mean thank you a lot. Thank you for taking your time. Hope you have a great day and thanks again.
Blue Media:	12:18	Okay, thank you. Bye.