Radboud University Nijmegen
Faculty of Science

Master's thesis Information Sciences

Payment Service Directive 2

Dutch supervision on the security and data protection of third party access

Author:

Jos Reijers

s4260147

Supervisor:

Prof. Dr. B.P.F. Jacobs

Reader:

Dr. Ir. E. Poll

June 1st 2016

Preface

This thesis is submitted for the degree of Master of Science in Information Sciences at the Radboud University Nijmegen. The research was conducted under the supervision of Prof. Dr. B.P.F. Jacobs and reader Dr. Ir. E. Poll in the department of the Digital Security group between May 2015 and June 2016. I would like to thank both for their assistance, guidance and time.

Jos Reijers,

Nijmegen, June 2016

Summary

Data is the new gold. That statement is often used to describe the new business models that companies are developing. With the introduction of the personal computer and the internet, an explosion of data has taken place and companies are constantly looking for new ways to create wealth from that new found data. The use of data has also reached the financial industry and FinTech companies are beginning to explore the available possibilities of monetising that financial transaction data. This trend could be accelerated through a new European legal framework that will come into force in the near future. That legal framework is the Payment Service Directive 2 (PSD2), which will legally force banks to give third parties access to bank accounts of their customers. This access, which is currently only available to banks, will make financial data and the ability to initiate transactions available to the FinTech industry on a large scale.

This thesis researches whether that access is sufficiently surrounded by supervision to ensure the security and data protection of consumers when the PSD2 is legislated in the Netherlands. Financial data holds very detailed personal information, including our preferences and indirectly a view on our actual behaviour. It tells a lot about our day to day lives and illustrates clearly what choices we make. Therefore, this data is a gold mine for most companies today, but the abuse of it can have a great impact on those same consumers. This is especially the case with marketing, personalised advertising and price discrimination through detailed profiling, but also with the abuse by criminals to commit fraud via identity theft and social engineering. Several controls should be in place to protect consumers against the threats that come from the abuse of that data. Such controls are expected to be included in the PSD2 and enforced through supervision.

The thesis commences with an analysis of the current Payment Service Directive (PSD1) and its implementation in The Netherlands. That provides a historic perspective which is followed by an analysis of its successor, the PSD2. In the analysis of the PSD2, a particular focus is on third party access related to security and data protection. The research also uses specific cases to describe how this third party access could work. An overview of the potential issues that could emerge as a result of this access is also provided. In order to protect consumers appropriately, access to financial data and use of financial systems by any party – banks or third parties – should be supervised by the proper authorities. Therefore the relevant supervisors are identified. Interviews conducted with them gave a good understanding of their current and possible, future role on the supervision of third party access. This makes it possible to verify whether supervision is arranged when access to accounts comes into effect and how that mitigates the potential issues identified earlier, and what challenges lie ahead for those supervisors.

As will be argued in this thesis, the supervision that is mandated in the PSD2 is not sufficiently arranged in the Netherlands yet, and creates a gap in supervision of future TPP's. On the topic of information security, no official supervisor has been appointed (yet), but some work has been done in the financial sector by De Nederlandse Bank (DNB). The lack of an official national supervisor on a generic topic such as information security no longer seems appropriate as our dependence on computer systems is increasing every day and it remains to be seen if DNB has enough resources and the ability to supervise technology focusedcompanies, such as TPP's. On the topic of data protection, the Autoriteit Persoonsgegevens (AP) clearly doesn't have enough resources to supervise as much as they would like to and therefore priorities need to be set. This lack of resources at the AP could result in companies not being penalised for data protection breaches. This means that consumers could be vulnerable to the issues or threats identified in this thesis. In the end this thesis recommends establishing an official national supervisor on cyber security, mandatory data protection and security officers for all organisations that will work with financial transaction data so these gaps can be closed. Other recommendations are better coordination between supervisors which includes an example, and finally the concept of Terms of Services; Didn't Read as an answer to the long, complexand incomprehensible service conditions companies.

The ultimate goal of this thesis is to make a contribution to the coming discussion between supervisors, banks and third parties, and to help find solutions to the potential security and data protection challenges that exist. And in this way make a contribution to a more secure and reliable financial eco-system, and as such foster trust and innovation from which consumers can profit, just as the European Commission envisioned.

Contents

1 Research question & thesis set-up

This paragraph will provide an introduction to the subject of this thesis, followed by the defined research question and it will finish with the thesis set-up.

1.1 Introduction

In ancient history, the library of Alexandria was considered the summum of all human knowledge. If itscontents were converted to a modern digital equivalent, it would not be more than 20GB[1].Nowadays this is comparable to a regular size SD-card or USB stick. In contrast, one of the most prominent technology companies, Google, had a data storage of about 15 exabytes[2] of data in 2013[3].With 7.3 billion people[4] in the world in 2015 this means that Google could have more than 2GB of digital data on each single person on earth which makes data a relevant aspect of our every day life.

The creation of digital data started in the late 1950s. That time marked the beginning of the third industrial revolution, also known as the digital revolution. Analog technology changed to a digital version, and mechanics were being replaced with electronics. The personal computer, the cellular phone and the internet were invented and introduced. This was all driven by the miniaturisation of electronics resulting in more powerful and smaller computers. The third industrial revolution was followed by the information revolution, also known as the information age. It changed society from an industry based economy, to an economy based on computers, data and information. Supported by high-tech and globalising companies this has resulted in the establishment of the knowledge intensive economy we now know today.

The knowledge economy is based on data and is supported by the "datafication" trend. This is a modern technological trend turning many aspects of our life into data and transforming the derived information into new forms of value. Examples of "datafication" are how Twitter datafies thoughts or LinkedIn datafies human resources. Also location information has been datafied through the use of modern smartphones using the GPS sensor to track its whereabouts.

The datafication trend and the high adoption rate of information technology by people has led to an explosion in data. Combined with the reduced cost of processing power and storage capacity, this introduced the resources to use more and more data. In order to create information, harness the knowledge and use the *"wisdom from data"*, a second technological trend emerged, big data. That trend is not focused on deriving exact and precise answers from data, but works with an inferred probability. Exact answers are a challenge with large datasets and the second best answer is a probability calculation. A well-known example is the way the search engine of Google works, namely the PageRank algorithm. When a search is executed, PageRank returns the most relevant results based on the probability that the search term refers to the result. A higher probability means a higher rank in the list.

Using large volumes of data also changed the way we think about data and how it is being used nowadays. With the explosion of data it means that there is much data to work with. This results in better statistical models as they tend to get better with bigger sample sizes. Since big data works with probabilities this improves the overall performance in services that use these technologies.

---

[1] How many gigabytes of data were in the Library of Alexandria? (Irwin, Philip 2015)

[2] One exabytes is equivalent to a billion gigabytes.

[3] If all digital data were stored on punch cards, how big would Google's data warehouse be? (Munroe, Randall 2013)

[4] UN projects world population to reach 8.5 billion by 2030, driven by growth in developing countries. (United Nations 2015)

A second important aspect is a shift in the way companies use data. Previously, data was used to find an exact answer and the related cause, but with big data this has been replaced with finding patterns and correlations in data. Companies are less interested in why you want to buy something and more interested in what you want to buy. With that information they are able to develop better business models.

These technological developments – datafication and big data – have reached the financial industry and are increasingly being considered by companies – banks and technology start-ups – to develop new, innovative services which will lead to new business opportunities and increase their revenues. These developments are also known as FinTech, which stands for Financial Technology. FinTech is often associated with new ideas and concepts which are disruptive in the financial industry and also serve as a contrast to the existing companies, banks, and their services in this industry.

A well-known example of a FinTech innovation is Bitcoin[5]. Bitcoin is a cryptocurrency and an alternative to traditional payment systems. It had a disruptive effect, because it was simpler and cheaper[6] than the established payment systems. It showed clearly that financial services could be delivered without the traditional infrastructure of that banks and without regulation or supervision. At first, most users were attracted by the fact that there was no governmental control or supervision. Supervision is often considered as cumbersome and unnecessary, but it does serve a purpose which is visible in the case of bitcoin too. Bitcoin works with a distributed model in order toverify each transaction. At a certain moment in time a lot of the computer systems, acting as a verification node, were located in China. Those systems together accounted for over 50% of all of the verification nodes in the world. This meant that the owners of those nodes were actually controlling the verification process of every bitcoin transaction. It was thought that through a majority voting system and the spread of control in a distributed model, the stability could be ensured. However this example shows that such systems have vulnerabilities as well and some control, in whatever shape or form, might help to stabilise the system.

As will be explained, the current European legal framework for the financial industry, the Payment Service Directive 1 (PSD1), is not fully equipped to deal with these new technologies and FinTech companies. Topics like supervision, security and data protection are important for consumers in order to trust such new companies and their technology. In order to accommodate those developments and companies, the European Commission (EC) initiated the revision of the PSD1. With that revision the EC created the Payment Service Directive 2 (PSD2). In the PSD2 the legal justification is made to allow the FinTech companies to deliver new and innovative services based on financial data or on its access to accounts which will have to be provisioned by banks. Banks are referred to as Account Servicing Payment Service Providers (AS-PSP's). The companies delivering the services are called Third Party Payment service providers (TPP's). The services they provide consists of the usage of consumer data also referred to as Account Information Services (AIS) and the ability to initiate a payment as known as Payment Initiation Services (PIS). Together commonly referred to as Payment Accounts Access Services (PAAS). By allowing TPP's to enter the market for certain financial services, which is currently dominated by banks, the EC expects more economic growth and thus welfare in the European Union. More players mean more competition which could be visible in a positive effect on pricing. Secondly this development supports innovation and allows for more diversity of services provided to consumers and in that way providing choice.

This increased competition is a positive development for consumers, however care must be taken to maintain a balanced trade-off between the expected benefits of the PSD2 on one side and the security and data protection for consumers on the other side. Companies are going to use their customer data, financial data, as the next evolution on current business models. Along with that, customers most likely will expect higher levels of security and data protection from companies. Supervision on TPP's could help achieve this.

---

[5] *Bitcoin: A Peer-to-Peer Electronic Cash System (Nakamoto, Satoshi 2008)*

[6] *The Innovators Dilemma (Christensen, Clayton 1997)*

1.2 Research Question

The current Payment Services Directive (PSD1) will soon be replaced with the revised Payment Service Directive (PSD2), which in time will be translated into national legislation. The PSD2 will legally allow third party payment service providers (TPP's) access to accounts from customers of the banks trough the so-called Payments Accounts Access Services (PAAS).

This thesis will investigate how that access by TPP's is surrounded by (governmental) supervision in the Netherlands, to ensure the security and data protection[7] for customers with respect to PAAS. This results in the following research question.

> *How is the Dutch governmental supervision of third party payment service providers (TPP's) arranged in the light of the revised Payment Services Directive (PSD2), and*
>
> *(i) does that supervision incorporate the protection against abuse of access (security),*
>
> *(ii) does that supervision incorporate the prevention of the abuse of data[8] (data protection),*
>
> *(iii) if any issues occur at i or ii, provide recommendations to improve supervision.*

[7] Often privacy and data protection have the same meaning, however their definitions are different. Data protection aims to establish conditions with which it is legitimate to process personal data (European Data Protection Supervisor 1995). Privacy is the respect for private life and may be described as the right which prevents public authorities from measures which are privacy invasive, unless certain conditions are met (European Data Protection Supervisor 1950). The thesis uses the definition of data protection.

[8] To clarify the abuse of data terminology in this thesis, a differentiation is used. Illegal use of data is the use of data not permitted by law. The abuse of data is the use of data permitted by law, but with an uninformed customer consent. This means that the customer accepted the terms of services which allows companies to use their data, but the customer does not understand the consequences of it. A data breach is defined as unlawful access to data by someone not belonging to the company that lawfully holds the data.

1.3 Thesis set-up

As the PSD2 is relatively new, involved parties such as supervisors, TPP's and banks are exploring what this means for them and how they should or could take their role. The ultimate goal of this thesis would be to make a contribution to the coming discussion about the PSD2 between supervisors, TPP's and banks to achieve an optimal implementation of the PSD2. All, to ensure a secure and reliable online financial Eco-system. This will foster trust and innovation from which customers in general will profit, just as the EC envisioned. This thesis will answer the research question by using the following structure.

Section two will start with an analysis of the PSD1. It will describe the origin and motivation of the directive and the implementation in Dutch nationals laws. It continues with a summary on remaining gaps in the PSD1 and a short analysis on the Impact Study[9] which was published between the implementation of the PSD1 and the publication of the PSD2. This paper has had a major influence on the creation of the PSD2 (version October 8th 2015).

In the third section the legal text of the PSD2, limited to articles related to either PAAS, TPP's, security or data protection, is analysed. From those articles an interpretation of PAAS will be explored. This section is completed with examples of real-world products that already use the principles and concepts of PAAS, and potential issues on information security and data protection that could emerge as a result of it.

In the fourth section the legal analysis is extended beyond the PSD2 to other relevant European legislation that is coming in the near future and has strong connections with the PSD2. This legislation is the General Data Protection Regulation (GDPR)[10] and the high common level framework on Network and Information Security (NIS)[11].

In section five relevant supervisors concerning the PSD2 and TPP's are identified. For each identified supervisor a description is given on their relationship with TPP's, and what responsibilities can be derived from that. This description is not only based on literature research, but also on interviews with employees of those supervisors. These are background interviews[12] and have been conducted to get a better understanding of the role of a supervisor in general and with respect to the PSD2, and PAAS in particular. They do not necessarily represent the official opinion of the supervisors.

Section six draws conclusions with respect to the research question and the identified issues, followed by recommendations that could remedy these issues, resulting in more secure and safe financial online services, ultimately being beneficial for all consumers. This section and thesis will finish with a personal opinion of the PSD2.

---

[9] Study on the impact of directive 2007/64/EC on payment services in the internal market and on the application of regulation (EC) No 924/2009 on cross-border payments in the community (London Economics, IFF, PaySys Consultancy Gmbh 2013)

[10] Proposal for a regulation of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (European Commission 2012)

[11] Proposal for a directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union (European Commission 2013)

[12] In the second appendix an overview is given of the conducted interviews.

2 History of the PSD1 and its consequences

In this section the history of the first and current Payment Service Directive (PSD1) will be discussed. It will provide the background to introduce its successor, the PSD2 in the next sections. It will start with the history and the motivation for the PSD1, followed by its scope and expected effects. After a relatively short time an evaluation has been made on the impact of the PSD1. That study and some conclusions are also discussed to illustrate issues that remain. The section finishes with the effects of the PSD1 on Dutch law.

2.1 Why did we need the PSD1?

During the time of the inception of the European Union and the creation of the Euro currency in 1992, member states were already profiting from the introduction of the integrated European market, allowing free traffic of individuals, services, capital and goods. This resulted in an increase of economic activity between customers and businesses across the different member states. However, there came an awareness and strong sense with politicians in the member states that the European payment systems did not undergo the necessary transformation to strengthen this pan-European flow of money and the economic growth. At that time there were major differences in the processing of payments with regard to execution times and transaction fees. Domestic payments took only hours and were cheap, and non-domestic, pan-European payments took days and were expensive[13].

It took until 2002 to build up the political pressure to have a more efficient European payment system. This resulted in a European regulation on cross-border payments in euro's[14] where banks were not permitted to impose different fees on cross-border payments within the European Union. This eventually forced banks to at least apply the same rates for European payments as for domestic payments and arrange for a speedy handling of payments.

As expenses on European payments were higher, European banks decided to develop a Single European Payments Area (SEPA) which would reduce costs for cross-border payments to the same level as domestic payments. If there was a single system for both payments the costs would be the same. Therefore the purpose of SEPA is to improve the efficiency of cross-border payments and to turn the fragmented, national markets for euro payments into a single "domestic" market. In order to achieve this, the European Payments Council (EPC)[15] was founded in 2002. The members of the EPC are all European commercial banks. Through the EPC, its members were able to make arrangements on the processing of pan-European payments. These arrangements led to the creation of SEPA.

SEPA was a result from the legal ruling on cross-border payments, but has no legal status by itself. There was no formal legislation that regulated SEPA. As a consequence, there was also no governance on SEPA. For that reason the PSD1[16] has been developed, adopted and implemented into the national laws of the member states of the European Union and other countries that are member of SEPA. It provides the legal foundation for the creation of a European wide, single market for payments.

---

[13] SEPA, How it all Started (Jennekens, Paul 2012)

[14] Regulation No 924/2009 of the European Parliament and of the Council on cross-border payments in the Community and repealing Regulation (EC) No 2560/2001 (European Commission 2009)

[15] About the EPC and its role in the SEPA process (European Payments Council 2002)

[16] Directive 2007/64/Ec of the European Parliament and of the Council on payment services in the internal market (European Commission 2007)

The PSD1 is about establishing a complete and comprehensive set of legal rules applicable to all payment services in the SEPA countries. This includes the supervision of all parties delivering payment services. A second objective of the legal framework was to increase competition by allowing other parties, not being banks or credit institutions, to offer payment services.

The PSD1 went into force on December 25th, 2007 and was to be transposed into national legislation by all SEPA countries by November 1st, 2009. In mid 2015, those countries were the 28 member states of the European Union, the 4 member states of the European Free Trade Association (Iceland, Liechtenstein, Norway and Switzerland), Monaco and San Marino.

Figure 1. SEPA/PSD1 countries.

2.2 What does the PSD1 mean?

Since a legal framework such as the PSD1 is not common to customers, the European Commission (EC) published an explanation[17] to illustrate the benefits and implications they should expect. This publication has been written specifically for the citizens of the European Union and addresses the major topics in plain English. The next paragraphs discuss and explore these major topics.

EUROPEAN-WIDE RULES AND INCREASED COMPETITION

The PSD1 advises that the same rules on making payments apply for all customers and businesses for those countries that implemented the PSD1. Having the same rules should have the effect that European payments are just as easy and safe as domestic payments. In this context easy refers to the time and cost a payment takes, which was reduced by the introduction of the PSD1, and reached the same level as domestic payments. Safe refers to the position of the customer who would better protected by lying down rules on refund rights and thus a more protected liability position (see third paragraph).

As the costs and speed of European payments now match domestic payments, it doesn't matter if the customer buys from a domestic or European seller. In that context it enhanced choice for the customer and increased competition between companies and also across members states.

[17] *The Payment Services Directive - What it means for consumers (European Commission 2010)*

Increased competition was also improved by opening the market to other companies in addition tobanks to handle payments. Companies that handle payments on behalf of other companies, in essence delivering payment services[18], are known within the PSD1 as Payment Service Providers (PSP)[19]. Prior to the PSD1, only banks and credit institutions could be seen as a PSP. As a result of increasing online sales, other companies, not being banks, dramatically increased their handling of payments on behalf of web shop owners. These companies would service web shops with the ability to handle several different payment methods, this relieves them from handling payments on their own. These companies were (temporarily) holding the money and acting as a bank, but they didn't have the same legal status. As a result of having no legal status these companies weren't supervised and posed a risk to customers, for example with regard to their refund rights. With the implementation of the PSD1, the legal definition of a PSP is laid down and it extends beyond the traditional companies such as banks, to include those companies delivering payment services. These companies were given a specific name –Payment Institution (PI)[20] – in the PSD1. In the Netherlands Adyen[21] and Global Collect[22] are examples of PI's.

The definition in the PSD1 of a PI includes the requirements that need to be fulfilled in order to acquire the correct legal status. Such requirements cover the financial position of the company by defining the initial capital and additional funding for running the services. By having a certain minimum level of capital, continuity of the services is better ensured. As these PI's will handle and store money from customers there are requirements for the companies on integrity of board members as well. This means that only people that are in good standing should be able to set-up these services and run such companies.

Since all PSP's are subjected to control and supervision, this also applies to a PI. The supervision over these PI's, for example which supervisory body should control them, the right to complain and how liability should be arranged in cases of disputes, are stated in the PSD1. Under certain circumstances a company can apply for an exemption. The requirements for those exemptions and the formal prohibition of providing services without license are also stated in the PSD1.

CLEARER INFORMATION ON PAYMENT SERVICES AND PAYMENTS

The PSD1 provides clearer information for customers on payment services and payments. This is addressed in two ways; more information on payments in shops, including online shops, and information provided by PSP's on their services. More information in shops includes information regarding any applicable charges. Retailers have to provide clear information on the way they charge you for making the payment. However, there are differences between countries. National legislation provides options to encourage or discourage payment methods by either giving a discount or making an additional charge. In all cases it has to be stated clearly and thus be transparent for the customer that some payment methods are more expensive than others.

With the PSD1, PSP's are legally obligated to inform their customers about the applicable terms and conditions of their payment services. It includes information on features such as the procedure of giving consent and refund rights. Additionally for every payment a PSP needs to supply detailed information such as the amount, date and any additional charges.

---

[18] PSD1, Title I, Art. 4, Par. 3, page 11 (European Commission 2007)

[19] PSD1, Title I, Art. 4, Par. 9, page 11 (European Commission 2007)

[20] PSD1, Title I, Art. 4, Par. 4, page 11 (European Commission 2007)

[21] About Adyen (https://www.adyen.com/nl/about-adyen)

[22] GlobalCollect (http://www.globalcollect.com)

By providing more and clearer information to customers, a better and more easy comparison of services between PSP's is possible. A customer will be enabled to choose the best option for itself, including the consideration of costs. Furthermore a customer can expect the same information on payments handled by different PSP's. Having the same information makes it easier to verify a payment on its correctness and costs.

BETTER PROTECTION OF CONSUMERS BY REFUND RIGHTS

The PSD1 contributes to a better protection of the consumer by defining the rules for refund in the case of unauthorised debits (impersonating the owner), overcharging and incorrect processing of payments. In essence rules are laid down that all businesses need to adhere to in case something goes wrong. These rules clarify the position of the consumer and the businesses in terms of responsibility and liability.

For example, in case of an unauthorised debit, the consumer has the right to a refund as long as they notify the provider not later than 13 months after the purchase. This is a considerably long period and one might expect that the customer should have seen the incorrect payment and had the opportunity to act on it. Therefore they have had enough opportunity to get refunded. Together with the European wide rules stated earlier, this creates a framework which the customer can rely on.

IMPORTANT MILESTONES FOR THE PSD1

1992	Establishment of the European Union by the treaty of Maastricht
1992	Establishment of the euro
1999	Introduction of the euro as an electronic currency
2000	Lisbon Agenda to make Europe "the world's most competitive and dynamic knowledge-driven economy" by 2010
2000	Creation of the European Financial Services Action Plan
2001	Regulation EC 2560/2001 on cross-border payments in Euro
2001 - 2004	Consultation period and preparation of the PSD1
2002	Introduction of euro banknotes and coins
2002	Establishment of the European Payments Council
2005	Proposal for the PSD1 by director general internal market commissioner McCreevy
2007	Agreement and enforcement on the PSD1
2009	Deadline for implementation of the PSD1 in national legislation
2009	First update of the PSD1 (EC Regulation 924/2009)
2012	Second update of the PSD1 (EU Regulation 260/2012)
2013	Report on implementation of PSD and its two updates

Table 1: Most important milestones of the PSD1 in chronological order.

2.3 Remaining issues

After the PSD1 was enforced and legislated in the national laws, some issues surfaced and remain unaddressed. These issues will be briefly discussed in this section.

LIMITED GEOGRAPHICAL SCOPE OF THE PSD

The PSD1 originates from European countries and is thus only applicable to those countries. That means that payments to and from countries outside Europe are still slow and expensive compared to the pan-European payments. The PSD1 was also about thriving economic growth and increasing welfare within European member states. Part of that economic growth comes from economic activity with countries outside Europe. With the ongoing globalisation, especially online, it seems that the virtual borders of Europe are the next step for further economic growth.

MARKET HETEROGENEITY

In the PSD1 there is a possibility for nations to encourage or discourage customers from certain payment methods as has been discussed in the previous paragraph. This has made the European market more heterogene, which led to more friction on pan-European payments. One country could promote direct debit transfers while another country would promote credit card transfers. This is not beneficial for customers who are trying to do more pan-European payments because they need to have more payment methods available which increases cost and is more cumbersome to maintain.

RISE OF THIRD PARTY PAYMENT SERVICE PROVIDERS

After the rise of PI's, again a new type of PSP appeared in the market. These new PSP's are also known as a Third Party Payment Service Provider (TPP).

TPP's facilitate online shopping by offering low cost payment solutions on the internet by using the customer's home online banking application with their consent. In Germany Sofort Uberweisung[23] is considered to be such a TPP. It acts as a man-in-the-middle between web shops and banks on behalf of the customer. The web shop is serviced by the TPP and gets its advantage from the fact that the TPP connects to a major number of banks and therefore offers a major group of their customers a convenient, single payment method.

Since these TPP's never hold any funds at any time they currently aren't considered as a type of PSP, which puts them in a non-supervised position. This will lead to confusion with customers because they most likely will expect TPP's to be a PSP's, along with all of the associated rights and obligations. This means that all prior stated benefits and implications of the PSD1 do not apply to TPP's.

2.4 Study on the impact of the PSD1

An impact study[24] of the PSD1 was made in 2013 to assess whether the original goals, as discussed in the previous paragraph, were achieved. The goal of the study was defined as follows; *"The study was required to cover the impact of the PSD1 on the internal market and any problems which may have arisen, to include legal and economic information. Its aim was also to identify areas where amendments might be considered appropriate, regarding a possible revision of the PSD1 and/or the regulation on cross-border payments."*[25]

[23] About Sofort Überweisung (https://www.sofort.com/eng-INT/about/company/)

[24] Study on the impact of directive 2007/64/EC (London Economics, IFF, PaySys Consultancy Gmbh 2013)

[25] Quote from "Study on the impact of directive 2007/64/EC", p. VIII

The impact study is based on four sources of information. These are the legal text of the PSD1, the corresponding national laws, official statistics on payment services and the responses to surveys from key stakeholders. The legal texts are necessary to put the statistics and results from questionnaires in the right context. It needs to be said that this study has some limitations. Firstly because it has been conducted after a relatively short period (2.5 years) at which the PSD1 was fully into force. Therefore it could be that some intended effects might show later than anticipated. Secondly this study did use official statistics but those were limited available, resulting in more focus on a qualitative approach through the knowledge of business experts.

INCREASING COMPETITION BY LEGALLY DEFINING PAYMENT INSTITUTIONS

Unfortunately no substantial impact was observed with respect to the entry of new actors, technological innovation and increased efficiency on the provisioning of payment services. This is confirmed by the statistics on the national business registers. They state that the majority of PI's (~85%)[26] were already active prior to the PSD1. This means that only a small number of PI's were new to the market and started to offer their services.

THIRD PARTY PAYMENT SERVICE PROVIDERS

The rise of online shopping also increased the importance of TPP's as they enable an easy, single payment method for web shops. A PSP is defined in the PSD1, but it doesn't include a TPP and therefore TPP's do not fall within the scope of supervision. The non-regulation of the TPP is not in the best interest of the customer and should be corrected in the PSD2. In essence this impact study verifies the issue which is also mentioned in paragraph 2.3 of this thesis.

SILENT CONSENT

The study also refers to the terms of services that are applicable to payment services. Those terms describe the rights and obligations for customers and PSP's when they engage with each other. It was found that changes in those conditions could be considered as a silent consent and a challenge to those users who do not read the terms or understand their ramifications. As an example, this silent consent allows companies to use their customer data for any purpose, without having the obligation to inform customers. American research[27] has shown that on average a customer would need to spend 244 hours yearly to read all the terms of services once every year for the most frequently visited websites. Therefore it is most likely that customers will never read the terms of services and might not know for what purposes companies are using the data.

In general, this gives companies a legal escape to always get consent from customers without them actually knowing or realising it. A combined opinion of experts in the study proposed to have the PSD2 make an attempt on increased standardisation for the terms of services and limit the derogation of it.

2.5 The effect of the PSD1 on Dutch national law

In this paragraph a closer look will be given to the consequences of the PSD1 on Dutch national law. As a law needs enforcement, this will also identify relevant supervisors. These supervisors will be used in section five to verify the relevance of them related to the PSD2, and to conclude if any gaps remain on supervision. This paragraph will finish with a short explanation on the European Passport construct which allows PSP'sto expand their services easily across Europe.

---

[26] Quote from "Study on the impact of directive 2007/64/EC", p. X

[27] The cost of reading privacy policies (Aleecia M. McDonald, Lorrie Faith Cranor 2008)

The PSD1 was adopted into Dutch national law in 2009 and has impacted two national laws. Firstly, the national law "Wet op het financieel toezicht" (Wft)[28], which is also about the supervision of PSP's. Secondly the Dutch national civil law, "Burgerlijk Wetboek" (Bw)[29] which, among other things, arranges the rights and obligations between customers and service providers. Finally as PSP's are processing personal information so there is a connection with the relevant Dutch data protection law, the "Wet bescherming persoonsgegevens" (Wbp)[30].

WET FINANCIEEL TOEZICHT

Access to financial markets and payment systems is arranged through a licensing scheme. So in order to lawfully accept and process payments, a PSP first needs to acquire a license. With the PSD1 this also applies to payment institutions (PI's) which were now defined as a PSP. This license and the process of acquiring one is overseen by De Nederlandse Bank (DNB)[31]. The requirements are stated in the Wft. These requirements are set to achieve some certainties and guarantees with respect to business continuity and consumer protection.

Because of the definition of PI's as a PSP, they are also automatically subject to on-going prudential supervision[32] by DNB. The Wft also arranges for a set of informative duties for the PI's towards their supervisors. Both instruments allow the supervisors to obtain a realistic overview of the managerial and financial position of the company. As DNB has supervision of PSP's it also maintains a register[33] about them which is publicly available. Through this register it is clear which companies are licensed and which are not.

To give all companies fair and equal access to payment systems a modification to the Wft has been made to ensure this. This modifications states that no discrimination may take place to deny PSP's access to systems. The supervision of this article is mandated to the Autoriteit Consument en Markt (ACM) which makes it a relevant supervisor.

BURGERLIJK WETBOEK

In order to protect the customers against PI's in case of disputes there are rules that govern the rights and obligations. With the introduction of the PI's a change to Dutch national civil law was needed to achieve the same conditions for customers with respect to these PI's. These conditions have been written down in the Burgerlijk Wetboek[34].

WET BESCHERMING PERSOONSGEGEVENS

PSP's provide payment services to customers and by doing so are also processing customer data. This data is also personal and therefore the European directive on data protection is applicable. This is translated into Dutch national law through the Wbp. Supervision is assigned to the Autoriteit Person (AP) and makes it a relevant supervisor.

---

[28] Wet financieel toezicht (Rijksoverheid Nederland 2015) (Retrieved year)

[29] Burgerlijk wetboek (Rijksoverheid Nederland 2015) (Retrieved year)

[30] Wet bescherming persoonsgegevens (Rijksoverheid Nederland 1995)

[31] In specific situations they work together with the Autoriteit Financial Markten (AFM).

[32] Supervision aimed at promoting the financial soundness of financial institutions.

[33] Register of PI's in the Netherlands (http://www.dnb.nl/en/supervision/consumer-and-supervision/registers/WFTBI/index.jsp)

[34] Burgerlijk wetboek, Boek 7, titel 7B

EUROPEAN PASSPORT[35]

Based on several treaties in the European Union, arrangements have been made to allow the free traffic of goods and services between member states. This also extends to the services provided by PI's. Since those services are digital, they can easily cross borders and be made available in other member states. In order to limit the administrative burden to acquire a license in every member state, the "European Passport" construct has been introduced. This is also known as cross-border services. For example, if a PI acquired a Dutch license it is allowed to run the same services in Spain or Germany without applying for a second or third license. There are some prerequisites to the use of the European Passport, but those are limited to the obligation of notifying the appropriate national banks. This means that every member state has incoming and outgoing notifications of either PI's that are expanding their services to other countries or PI's expanding to their country.

The European passport construct will therefore lead to PI's that, for example are active in the Netherlands, but aren't placed under Dutch supervision. The supervision lies within the home country of that PI. Since the PSD1 is a directive and not a regulation, differences could occur in the supervision through differences in national legislation. From a customer perspective this means that although the purchase was made in a Dutch web shop, the payment could have been handled by a Polish PI.

So by having the European passport, multiple PI's could be active in the Netherlands which are differently supervised and have different laws applicable. In the example given, it most likely means that the processing of the customer data was done in Poland under their data protection laws. A customer is probably not aware of this.

2.6 Summary

In summary, this section has introduced the PSD1 which originated from the SEPA initiative. Its goals are a single European wide ruleset on payments, to increase competition on the payment market, clearer information on payments and better protection for customers. Issues that remained after the adoption of the PSD1 have been identified and discussed. These remaining issues are the limited geographical scope, a heterogene market and the rise of TPP's. To verify the effectiveness of the PSD1, the impact study and several conclusions from the study have been discussed. These conclusions are the lack of new PI's entering the market which didn't result in more competition, the lack of supervision of TPP's as they weren't defined in the PSD1, and finally the fact that unclear terms of services are used to get a silent consent from customers. This is followed by a discussion on the Dutch implementation of the PSD1 and the identification of the relevant national supervisors, which are DNB, ACM and AP. The section finishes with elaborating on the possibilities for companies to deliver their services in other European countries by using the European Passport construct.

The remaining issues of the PSD1 and the conclusions from the impact study are expected to be addressed in the PSD2. The next sections will explore if that is the case by trying to answer the following subquestions as part of the research question.

a) Are TPP's placed under supervision in the PSD2, and are the same supervisors as with the PSD1 also relevant and in what way, and can other supervisors be identified?

b) Is the European passport construct incorporated in the PSD2 and does it apply to TPP's, and what are the effects of it on supervision?

c) How is the issue of silent consent addressed in the PSD2, especially with services provided by TPP's?

[35] *Betaalinstellingen: Grensoverschrijdende dienstverlening (De Nederlandse Bank 2012)*

3 Introduction to the PSD2 and exploration of PAAS

This section will start with introducing the Payment Services Directive 2 (PSD2)[36] and discuss a selection of legal articles from it. The selection will zoom in on Payment Account Access Services (PAAS) which is part of the PSD2. PAAS is about access to accounts through the use of a third party, either for acquiring payment information or for payment initiation. Further exploration of PAAS will be done by providing use cases to explain the proposed working. These use cases are completed with examples of companies that already provide PAAS like services. This section finishes with potential issues on security and data protection that might surface as a result of the introduction of the PSD2 and more specific PAAS.

3.1 Introduction to the PSD2

After the implementation of the PSD1, shortcomings were identified that needed to be repaired in its successor, the PSD2. On top of the repairs, several new aspects needed to be accommodated in anticipation of major changes in the way consumers are using payment systems in the digital world. The European Commission (EC) intended for the PSD2 to positively affect innovation on the payment markets again. This time by legally allowing access to accounts with the introduction of PAAS. With that the EC expects that companies will use the opportunities of the PSD2 to develop new services based on PAAS.

On October 8th 2015 the proposal for the PSD2 was adopted by the European Parliament[37]. This will be followed by the formal adoption through the European Union, Council of Ministers and finally by the publication in the official journal of the European Union. After that member states will have a two year period to change national legislation in such a way that it accommodates this directive[38].

This paragraph will highlight the most relevant legal articles from the PSD2 related to PAAS. Based on the main research question, only those articles that are related to either security, data protection or supervision are selected. This will provide a good understanding of the terminology and will be used in the next paragraph, to explore the concepts of PAAS and its components.

Definitions (art. 4)

This article is about the legal definitions regarding PAAS. The Payment Initiation Service Provider (PISP) and the Account Information Service Provider (AISP), together commonly known as Third Party payment service Providers (TPP)[39] are introduced and defined. The PISP provides services to facilitate payments by establishing a software bridge between the website of a merchant and the online banking platform of the customer. PISP's offer a cheap alternative to card payments for both merchants and customers. AISP's will allow a customer to have a holistic user-friendly overview of payments for a single or for multiple accounts supported by downloaded payment data from banks. This results in a complete overview on the customers financial position. Additionally, the information from payments can be used to develop new features, for example a notification when a payment is received. These services are also defined in the same article under the names Payment Initiation Service (PIS) and Account Information Services (AIS). Below is an excerpt of the exact definitions from article 4 of the PSD2.

---

[36] *Supplementary report on the proposal for a directive of the European Parliament and of the Council on payment services in the internal market, PSD2 (European Commision 2015)*

[37] *Press release by EC on "Revised Directive on Payment Services (PSD2)" (http://ec.europa.eu/finance/payments/framework/index_en.htm)*

[38] *A European directive will be transposed into national laws, while a regulation directly replaces the relevant national law.*

[39] *A Third Party Payment service provider (TPP) is not the same as a Trusted Third Party (TTP).*

4. ”payment institution" means a legal person that has been granted authorisation in accordance with Article 11 to provide and execute payment services throughout the Union;

15. "payment initiation service” (PIS) means a service to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider;

16. "account information service” (AIS) means an online service to provide consolidated information on one or more payment accounts held by the payment service user with either another payment service provider or with more than one payment service provider;

17. "account servicing payment service provider” (AS-PSP) means a payment service provider providing and maintaining a payment account for a payer;

18. "payment initiation service provider” (PISP) means a payment service provider pursuing business activities as referred to in point (7) of Annex I[40];

19. "account information service provider” (AISP) means a payment service provider pursuing business activities as referred to in point (8) of Annex I[41];

Table 2: Definitions from art. 4 of the PSD2

Designation of competent authorities (art. 22)

In this article the European Banking Authority (EBA) is appointed as the competent authority on a European level for TPP's. It also defines the primary competent authorities in the home member states, which are the national banks. Furthermore it stipulates that if there are other relevant authorities they should cooperate with each other in order to obtain optimal supervision.

By legally defining TPP's and the associated services (AIS & PIS), and assigning the competent authorities to supervise them, TPP's are effectively placed under supervision when the PSD2 comes into force. This answers the question from the previous section on the supervision of TPP's, but also implies that a new European supervisor, the EBA, will become directly relevant for national supervisors. EBA will guide them to develop the necessary policies that will help the translation of the PSD2 in national laws. From this article it also becomes clear that multiple supervisors will be active to supervise TPP's. Section five will zoom in on the EBA and those other national supervisors and their roles.

Supervision (art. 23)

Article 23 expands on supervision, and is about the empowerment of the competent authorities. It ensures that they have legal capabilities to intervene when appropriate or necessary. So in case of an incident they can impose a penalty or punishment that should prevent future incidents from happening.

Rules on access to payment account in the case of payment initiation services (Art. 66)

This is the legal base that will allow TPP's to access the accounts of customers at their banks (AS-PSP's) so they can enable PIS services to their customers. For such access, both parties, TPP's and banks need to work together and this article obligates banks to cooperate. It also summarises under what circumstances access is allowed and elaborates on the obligations and rights for both parties, TPP's and banks.

---

[40] In Annex I of the PSD2, only PIS is mentioned and refers to definition 15 in article 4.

[41] In Annex I of the PSD2, only AIS is mentioned and refers to definition 16 in article 4.

This article also describes the obligations surrounding the confidentiality of security features, such as personal logon codes and the identification of the TPP to the banks. It states that there shall be no discrimination in terms of timing or priority of payments initiated through the use of a TPP. In other words a bank may not interfere with any actions or payments initiated by a TPP. There are certain exceptions, for example fraud detection. If a bank suspects the payment is done by a fraudster it may hold or refuse it. In all other cases it has to let it pass.

Rules on access to payment account in the case of account information services (Art. 67)

The same as in article 66 applies here, but in this case for TPP's that deliver AIS services. Interesting to note is that a customer needs to give explicit consent to TPP's to access the payment information at their bank. For payment initiation this seems obvious, but for accounts information services this definition can be read in a way that accepting the terms of service implies an explicit consent – or, as already mentioned a silent consent – which is an issue as will be shown in the next paragraph.

Data protection (Art. 94)

Data protection is arranged by having the Data protection directive[42] applicable. Processing of personal data by a TPP should always be done in alignment with the Data protection directive. This means that the customer has to give consent for the processing of personal data and the TPP needs to have a clear purpose for collecting and using it. A specific exemption on this applies to fraud monitoring. The PSD2 will legally allow the processing of personal information for the purpose of mitigating fraud without having the obligation to inform customers or to get their consent. This is mainly applicable for PIS services and means that customers who enrol for PIS services implicitly agree to the processing of personal data. The consent is generalised for all customers and enabled through this directive. Finally a reservation on the scope of the use of payment data is made by applying the term data minimisation. It states that only data which is relevant to the service may be used.

Management of operational and security risks (Art. 95)

In this article it is stated that payment service providers need to take precautions to secure their services and systems. This includes a notification process on major security incidents. When a TPP is hacked it is obligated to publish the incident and inform relevant competent authorities. It also states that the competent authorities will review the security on a yearly base or shorter when required.

Incident reporting (Art. 96)

In addition to the previous article, this article is also about the notification of security incidents. It explains in detail when and who should be informed in case of major security incidents. This will be the[43] on security in the home member state, but also the European competent authority for the PSD2, the EBA. The EBA will be responsible for issuing guidelines on the content of such a notification in terms of classification of the incident and the format of the report.

---

[42] Data protection directive 95/46/EC (European Commission 1995)

[43] A competent authority is different from a supervisor. A supervisor has enforcement capabilities derived from legislation and the competent authority doesn't have this. The EBA is an authority that sets policies and standards, but cannot enforce this on companies. To do that a national supervisor is needed, which for the Netherlands is De Nederlandse Bank. (DNB) Often the terms supervisor and competent authority are interchanged, but in this thesis, the prior given difference is used.

Authentication (Art. 97)

This article has a strong focus on security by stating the mandatory use of strong (customer) authentication, also known as two-factor authentication[44]. It also states that a TPP should either arrange authentication itself in its services or is allowed to use the authentication means of the banks, redirecting the customer to the bank for authentication. This means that a TPP may rely on other authentication schemes instead of maintaining one itself. It also stipulates that in case of PIS not only strong authentication is required, but also elements like payment amount and the beneficiary need to be a part of the payment authorisation. Essentially a method known as "What you see is what you sign" [45] is applied to authorise the payment.

Regulatory technical standards on authentication and communication (Art .98)

The EBA has been appointed as the competent authority on a European level, in particular for PAAS. This article lays the first steps on requirements for the Regulatory Technical Standards (RTS) on security and data protection. These RTS will be developed and maintained by the EBA. It defines guiding principles that must be used as a starting point for developing other policies, standards and guidelines that will help national supervisors to develop their control instruments to supervise TPP's on the topics of security and data protection.

---

[44] Two factor authentication refers to the fact that a customer need to fulfil two requirements to successfully log on. Usually something you know (PIN code) and something you have (debit card). An example of one factor authentication is only something you know like a password. Adding an out of band message, like SMS makes it two factor.

[45] See What You Sign: Secure Implementations of Digital Signatures (A. Weber 1998)

3.2 Exploration of PAAS and its potential issues

PAAS is all about access to accounts either for gathering information on payments or for the initiation of a new payment using a TPP. In this paragraph the legal definitions of PAAS are used to explore use cases of AIS and PIS services. These cases will illustrate how these services should work. Since this development is not entirely new, there are already some companies that are using the same concepts and ideas. Those examples will help the understanding of these services and how they interact with customers. For both AIS and PIS, several issues are identified which will be discussed to address the possible risks which customers will face when engaging with such services.

ACCOUNT INFORMATION SERVICES — USE CASE

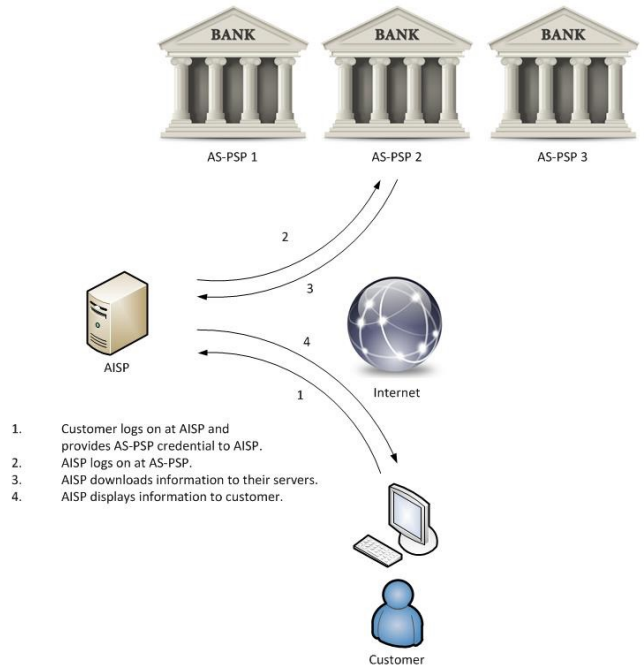

Figure 2. Schematic overview of Account Information Services (AIS)

A customer will first need to enrol himself/herself as a user with the TPP before being able to use the services. After that, a connection between the TPP and the bank (AS-PSP) on behalf of the customer will be initiated. Based on the implementation of the TPP, a customer uses the authentication means provided by the TPP or by the bank to which (s)he wants to connect. The TPP will then start the transfer of financial information. The information is then processed to deliver the service. Several variations of this service could be developed by altering the type and amount of information requested. Examples are, periodic balance check, alerts on financial events, categorised payments and data analytics.

The AIS service is about a "consolidated" way of displaying financial information. Consolidated refers to the fact that a growing number of customers have accounts with multiple banks. In the current landscape of online banking this requires customers to log in to all those portals and then aggregate that information to acquire a consolidated overview. The AIS service is extended to encompass access to multiple accounts with multiple banks. This provides a way to get a total financial overview for customers.

ACCOUNT INFORMATION SERVICES — EXAMPLES

Several companies already use this kind of access to accounts in order to deliver their services. Two examples are briefly described to get a good understanding of how AIS is already being used nowadays.

AFAS Personal[46]

A Dutch AIS product is AFAS Personal. It provides an overview of the customers financial situation for one or more accounts, serviced by different banks. Based on the gathered information additional features in the software are available to the user, such as categorising transactions, comparison of spendings with peer-groups, incoming money versus spendings, etc. The way AFAS Personal acquires the information is either by a manual upload from the user (previously downloaded at the banks) or by relaying bank credentials of the consumer through the AFAS Personal webpage.

BilllGuard[47]

BillGuard is the second example of a company that uses payment data. Their service is focused on detecting fraudulent transactions and unnecessary spendings. For this to work they acquire the transaction information and process it through algorithms in order to find anomalies that could be considered as an unnecessary spending or possibly fraudulent. They do not deliver their services entirely by themselves. Their services are built from multiple components delivered by different parties, for example Yodlee[48]. This means that TPP's are not the only third party that could see the customers payment data. Based on the operating model, for example by partnering with other companies, the information is shared with more companies than the primary service provider. The way BillGuards acquires the payment data is by relaying the credentials of the customer to the bank.

ACCOUNT INFORMATION SERVICES — POTENTIAL ISSUES

The AIS service is all about acquiring data, analysing it and presenting it in a certain, convenient way to customers. Since it is about data placed under control of other parties, this inevitably also introduces new risks. Those risks and related issues are discussed next, and are centred around access to and the processing of data, and can be divided into four major topics. These are the possible negative public opinion on the use of payment data for commercial purposes, authentication, the abuse of payment data, and data breaches.

Negative public opinion on the use of payment data for commercial purposes

Increasing the opportunities for competition by introducing PAAS is one of the goals of the PSD2. More competition will lead to more choice for customers, which could result in more and better services. This could be beneficial for customers. However in the Netherlands the average customer doesn't seem to be ready yet for the developments as proposed in the PSD2, illustrated by the following three cases.

The first case[49] has been raised by the Dutch bank ING in 2014. They were planning *"to explore if customers would be interested in receiving tailored discounts from third parties in line with their spending behaviour"*[50]. The announcement of the idea has been picked up by media and raised a lot of negative comments from customers and media. Because of these negative reactions ING decided not to move forward with this.

---

[46] *AFAS Personal (https://www.afaspersonal.nl)*

[47] *BillGuard (https://www.billguard.com/)*

[48] *Yodlee (http://www.yodlee.com)*

[49] *ING and the use of customer data (http://www.ing.com/About-us/ING-and-the-use-of-customer-data.htm)*

[50] *This sentence is quoted from a press release is therefore in italic (See footnote 42).*

The second case has been raised through research[51] performed by De Nederlandse Bank (DNB) in 2015. The topic of the research is to assess what the general attitude of Dutch citizens is towards the commercial use of payment data. The main conclusion is that Dutch citizens will only slightly accept that use of data by banks and even less by other parties. A second more general conclusion is that the use of data is more acceptable for certain specific purposes such as duty of care, security and improvements of the service.

The negative reaction to the proposal in the first case and the research from DNB in the second case show that the general public in the Netherlands – future customers of TPP's – isn't ready for these kind of services. At the same time proposed legislation on a European level has been developed to encourage and promote the use of payment data for new services.

The third case[52] has been raised by the Autoriteit Persoonsgegevens (AP) against Facebook in 2014. The case is about Facebook changing their terms of services on privacy. These changes became effective on January 30th 2015. The new terms will allow Facebook to use their customer data for commercial purposes. For example, it will allow them to sell your likes and your pictures. Most likely this data will go to data brokers or advertisement companies that will devise more relevant advertisements to increase their revenues.

The reason for this investigation is most likely the dominant position of Facebook on social media in the Netherlands and the societal effect of such changes. This investigation should lead to the understanding of the ramifications and the AP asked Facebook to clarify their intentions on this matter. In this case it needs to be seen if the AP will allow these new terms because they might violate the Dutch national law on data protection. In December 2015 the investigation was still open. As Facebook has a global presence this change also affects other European countries. In Germany a similar case has reached the courts, and ruled in favour of the national German legislation. This means that the terms of services violate their privacy laws and Facebook now has other terms of services in Germany that won't allow them to use customer data commercially.

This case clearly illustrates that supervisors intervene when major changes occur that negatively affect society as a whole. Secondly, this case shows that through the establishment of certain terms of services a company can circumvent the data protection legislation. This circumvention is possible because the legal "informed consent" is hidden in the terms of services. By accepting these, customers are actually giving a silent consent to the commercial use of their data.

Authentication, the customer or the TPP?

An example of an AIS product is AFAS Personal as described in the previous paragraph. In the past it has used the relaying of customer credentials as a method for authenticating itself to the bank (AS-PSP) on behalf of the customer. Through a court ruling[53] in the Netherlands that method has been forbidden. This introduces the next problem. If the PSD2 will legally allow AIS services, in what way will a TPP acquire the payment data in terms of authentication as the relaying of credentials has been forbidden?

The PSD2 provides two options. Customers will authenticate themselves at the bank – which is arranged in the PSD2 through article 97 sub 5 – which allows TPP's to redirect customers to the bank and let them authenticate there. Secondly, the TPP relay the bank credentials from their site to the site of the bank.

---

[51] Opvattingen van nederlanders ten aanzien van het gebruik van betaalgegevens door banken en andere partijen (DNB 2015)

[52] CBP onderzoekt nieuwe privacy voorwaarden Facebook (CBP 2015)

[53] Vonnis in kortgeding van 30 juli 2014 AFAS v.s. ING (Rechtbank Midden-Nederland 2014)

The first option will leave the full control of access to the account at the customer but has the disadvantage that customers need to authenticate themselves for each bank separately and possibly for each update. This will most likely give a bad user experience and will attract fewer customers to the product or services. The second option will transfer the control on access to the account from the customer to the TPP. By applying a federated type of access, customers will express that they are comfortable with a TPP acquiring their payment data on behalf of them. If the granted authorisation would be valid for more than a single download, it effectively introduces a dual control on the access to the account for both the customer and the TPP. This introduces the risk that a TPP can act autonomously on accounts without informing the customers, either because of intentional business reasons (abuse of data) or unintentional security reasons (data breach).

Abuse of payment data

The abuse of payment data should be seen from the perspective of what payment data can tell about people and the possibilities this provides to companies and their business models. The abuse is applicable when companies do not ask for consent or try to get a silent consent, and use the data for other purposes than that they have been telling their customers. Or they did tell, but in such way that it is not comprehensible or takes a disproportional amount of time to understand. In summary customers often do not know which data is collected and for what purposes.

As can be seen with services provided by Google or Facebook, these are never actually free of charge but customers pay with their data. This data often finds its way to data brokers, or in case of Google is used to show relevant advertisements. Therefore personal e-mails in Google Gmail are related to the advertisements shown. So Google knows what your e-mails are about and will choose advertisements based on that. That is their business model; sell advertisements. Reading e-mail and using information of their online search engine allows Google to construct a complete profile about your online behaviour. This ranges from the intentions you express through your search behaviour up to personal communication through your e-mail. It is obvious that although online search behaviour does tell a lot about someone it remains an intention. Searching for a specific disease doesn't imply that you have it. For example, this search for information could have been done for someone else. Moving to e-mail it becomes more personal. Having an e-mail to a doctor confirming an appointment reveals that your current health state is reason to visit a doctor. This still doesn't prove you have an illness. Payment data[54] adds a new dimension, because payment data goes beyond intentions and verifies earlier shown behaviour. The fact that someone spends money on medicines means that there are good reasons to believe that (s)he is indeed suffering from it and wants a cure for it. With that, payment data is more than about intentions. It is about the actual behaviour of people and depicts choices they make during their life. From payment data conclusions can be deduced that people would consider as private and the use of it could be considered a serious infringement in your personal life.

In order to get an impression of the types of information that will become available for TPP's based on AIS services, a small experiment[55] has been conducted. Banks often offer the possibility to download the history of payments in a common format such as comma separated. For this experiment a payment statement was taken from a single account number for a 15 month period. Below are some remarkable types of information that are available in this data set. The items are categorised around several topics, such as personal identifiable (PII), medical, location, behavioural and social information. With each item a short description is given. Appendix 1 contains a more detailed description.

---

[54] Payment data is defined as a one or more financial transaction as shown on a bank statement. This includes a timestamp, customer account number, beneficiary account number, amount and description.

[55] This experiment has been conducted by the author on his own payment data (n=1) and is meant to illustrate what types of data might be available. It should not be seen as statistically relevant and in order to achieve statistical relevance a larger population should be used.

Topic	*Type*	*Description*
PII	Names & addresses	Names and addresses appear in multiple payments.
PII	Social security numbers	Payments related to taxes contain a social security number.
PII	Credit card numbers	Each month the credit card is settled, this reveals the credit card number.
PII	License plate number	Invoices on taxes for cars contain the license plate number.
Financial	Income/Wage	A monthly recurring credit transaction from the same account is usually the wage and also shows the employer.
Financial	Spending categories	Based on description of payments several spending categories can be defined.
Special	Medical	Online shopping for medicines reveal a treatment for a disease.
Special	Religious	Payments to religious institutions, for example a church reveal your religious beliefs.
Other	Location	ATM payments hold location information revealing a pattern of life.
Other	Behavioural	Life events can be deduced from a payment description, such as a marriage or burglary.
Other	Social	Consumer to consumer transactions allow for an overview on relevant social connections.

Table 3: Types of information from payment data

Finally a more general risk on data protection, an odd variation on the abuse of data and not specifically related to the PSD2, isn't addressed in either data protection legislation or terms of services that companies have. This risk arises when a company or TPP goes bankrupt. When this happens all assets that have any economic value will be used by the curator to settle the remaining debts. Nowadays this would include the data of customers. So to a certain extend a company can protect the data of their customers, but if something goes wrong with their business model that same data might become available to the highest bidder when it goes bankrupt. Although not explicitly mentioned it is assumed that with the PSD2 and PAAS, mostly startup companies will enter the market as new players to offer AIS (and PIS) services. These startups are often referred to as FinTech[56] startups. The major goal of these startups is to create a large customer base as quickly as possible, based on an optimal user experience. However the fail rate of these startups is high as well. This could put customer data at risk each time a start-up fails.

[56] *FinTech stands for computer programs and other technology used to support or enable banking and financial services. (Oxford dictionaries 2015) Startup companies are most associated with information technology, hence the assumption that startups are most likely to also engage on PAAS.*

Data breaches

Data breaches are the fourth major topic on potential issues with AIS. According to Verizon[57], the financial losses due to data breaches reached around 400 million dollars from 700 million compromised records globally in 2015. Financial services have been in the top 3 industry on data breaches several years in a row according to the report. This means that financial information was and still is very valuable and worth stealing. As online services are becoming the primary method of purchase, it will increase the creation of payment data resulting in more data to steal, and the introduction of TPP's results in more parties to steal from. So by introducing TPP's, new targets will be added to the list of fraudsters and cyber criminals.

As mentioned previously it is assumed that with the PSD2 and PAAS, mostly FinTech startup companies will enter the market as new players to offer AIS (and PIS) services. Often, security and data protection are considered as non-functional requirements by these start-ups. This means that these requirements do not directly contribute to the product but are needed to run it securely. These requirements are usually moved to a final stage in the development process or aren't developed at all. This will result in less protected services and TPP's which are prone to get hacked. And even if they do get the security right, the numbers of Verizon suggest it is hard job not to get hacked at all. When taking into account that an attacker knows what kind of information a TPP holds, it could become a determined attacker. If that is the case then it's usually a matter of time before a company gets hacked and the data flows to the underground markets. So the potential issues are that startup companies are known to invest less on security and data protection in favour of investments that lead to a better customer experience which increases their customer base, and that all companies are outnumbered in defending customer payment data when dealing with determined attackers. This will result in an elevated risk of exposing payment data to criminals who either will use it to commit fraud or sell it to other criminals.

Another type of data breach could be a state-sponsored data breach. TPP's will create a central repository of payment data which will provide a single entry point to a large payment data set. Governmental agencies could leverage this single entry point to extract information,and by-pass the banks as their current main supplier. Other governmental agencies, concerned with national security, could also leverage this to acquire more detailed information on persons who they are interested in without having to go to the bank. Creating a single repository of valuable data will attract criminals, but also state-sponsored attackers, whatever their goals are.

A final issue on the source of payment data will become prevalent when the data is found on the internet as a result of a breach. As both parties – TPP's and banks – are legally entitled to process and store payment data it becomes very difficult to prove who breached the information. This could become an issue between the TPP and the bank as they both could state they didn't loose it. This leaves the customer with a problem, but more important, no improvement can be made since it is unclear who needs to improve.

[57] *2015 Data breaches investigations report (Verizon 2015)*

PAYMENT INITIATION SERVICES - USE CASE

With Payment Initiation Services (PIS) an additional online payment method will become available. This will be available next to the traditional online payment methods such as PayPal and credit cards. The schematic overview below shows how PIS should work and is based on a purchase at an online web shop.

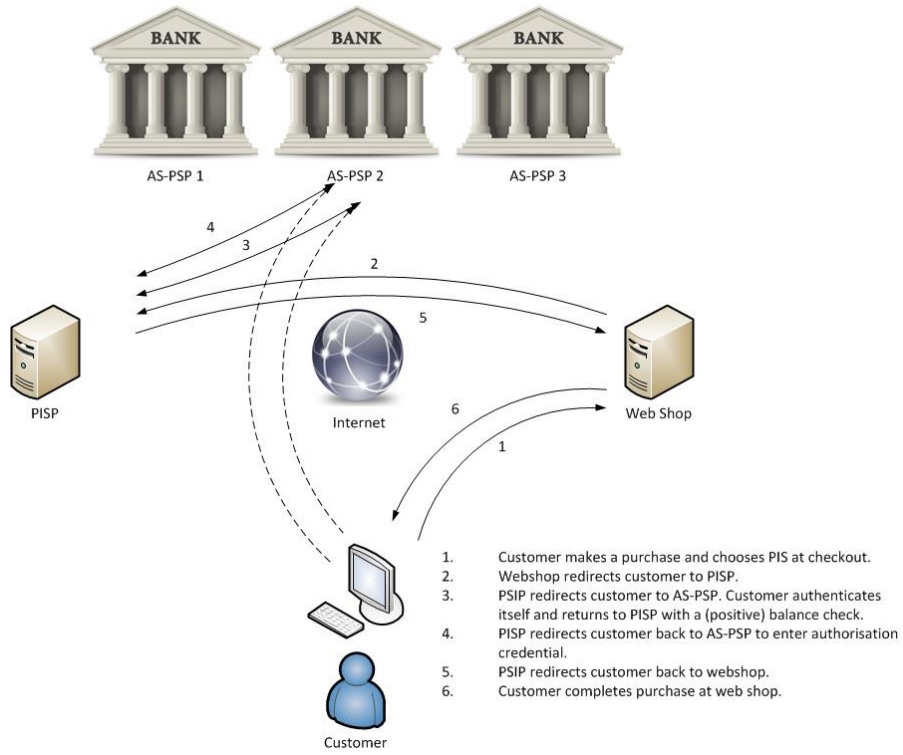

Figure 3. Schematic overview of Payment Initiation Services (PIS)

For an online purchase the flow of events is usually as follows. After customers have made their choice on the product or service in the web shop, they proceed to the checkout and can choose for a PIS service to pay. The details of the purchase are transferred to a TPP, which on its turn will either redirect the customer to the bank (AS-PSP) for authentication or relay the customer credentials. In the first scenario (redirection) the customer is redirected from the web shop to the TPP and then to the bank site to enter the login credentials. The returned information will enable the TPP to check if the current purchase can be made based on the account balance. In the next step, signing credentials are entered at the bank site in order to authorise the payment. The process ends with redirecting the customer to the web shop to finalise the payment and the purchase order. In the second scenario the TPP will relay the customer credentials from the bank and the payment can be completed.

PAYMENT INITIATION SERVICES - EXAMPLES

Within the different European member states various payment schemes have emerged in order to facilitate easy online payments. In some countries there has been a major adaptation of a single payment instrument and in other countries a scattered use of instruments remained[58]. In the Netherlands the dominant system is iDEAL and can be considered a PIS. In Germany a service called Sofort Uberweisung is popular, which is also an example of PIS.

[58] *Online payment methods in Europe (Expert Market 2015)*

iDEAL[59]

iDEAL is a Dutch payment system. It is developed and owned jointly by the major Dutch banks in order to facilitate online shopping.In this scenario the TPP is Currence who is the owner of iDEAL scheme on behalf of the banks. It is based on a four-corner model with a customer, issuer (bank of customer), acquirer (bank of the merchant) and the merchant (web shop). When customers proceed to checkout they are redirected to the bank of their choice and have the details of the payment pre-filled. They only need to authorise the payment. The issuing bank informs the acquiring bank which on its turn informs the merchant. The merchant then knows the transaction is completed and can continue the processing of the order. All major Dutch banks provide a dedicated channel for these types of payments. The speed of the payment is almost real-time. This means that any payment done trough iDEAL is guaranteed at the moment a customer authorises it . The payment cannot be stopped and therefore this method is very efficient for merchants who want to have a fast confirmation on the payments which enables a fully automated order handling. This guarantee on payments has had a major contribution to the high adoption rate of iDEAL in the Netherlands.

Sofort Uberweisung[60]

The European Payment Institutions Federation stated in July 2013 that Sofort AG is the largest European, bank-independent third-party provider of PIS with their Sofort Uberweisung (SU) product, and has been providing this service since 2004. SU provides web shop owners multiple connectors to different banks in Europe which allows them to handle payments. When the customer proceeds to checkout and chooses SU as payment method, the customer is redirected to a secured page of SU which has the details of the payment already entered. After that, the customer needs to choose the country and the bank. Depending on the chosen bank, several fields are presented such as account and card number. It then asks for the first credential. This is a logon credential which is used to enter the online banking portal of the bank, check the balance for the current transaction and if other similar transactions (from SU) have failed in the past 30 days. After that an authorisation screen is shown in which the customer needs to enter a second credential to authorise the payment. Finally Sofort will show a summary and redirect the customer to the web shop. In this example, SU relays personal authentication and authorisation codes from customers to banks.

PAYMENT INITIATION SERVICES - POTENTIAL ISSUES

PIS is about initiating payments and transferring money. Money has always attracted criminals as they follow the money in the real world and with the increase of online purchases also in the digital world. PIS will therefore most likely become victim of the classical threats associated with online payment services such as malware and phishing. From the PSD2 it is clear that an emphasise is put on strong customer authentication. However the value of this defensive measure is declining, and by itself is not enough to protect customers against thieves and fraudsters. Another issue that arises with the introduction of new online payment services is that there are always people who will stretch the rules of these services, allowing them to create other use cases.

In this paragraph potential issues related to PIS are discussed. These revolve around abusing fraud monitoring as data processing purpose to monitor everything, the classic threat against online banking and two examples that stretch the rules. The examples are autonomous PIS services and circumventing compliance controls with PIS.

---

[59] *Betalen met iDEAL (Currence 2015)*

[60] *Zo werkt Sofort (Sofort 2015)*

Abusing fraud monitoring as data processing purpose to monitor everything

Article 94 in the PSD2 is about data protection. In that article an exemption is made on acquiring consent for the processing of personal information for the purpose of fraud monitoring. In order to mitigate fraud TPP's are allowed to process personal information without having the consent of the customer. This will most likely result in the unawareness of customers that their data is being used for this purpose and everything can be monitored.

Although the purpose of fraud monitoring is beneficial for customers, care must be taken that this will not lead to the abuse of personal data. Correct supervision on this theme and transparency could help reduce this risk, which will be investigated in section five.

Defense against classic cybercrime threats (phishing & malware)

Current providers of online payments face cybercrime threats on a daily basis. This has been going on several years now and is publicly reported on in the Netherlands since 2011 by the Nederlandse Vereniging van Banken (NVB). Cybercrime has caused some major financial damages. In the Netherlands, all banks together suffered 3.1 million euros damage in the first half of 2015[61]. In 2011 this was a staggering 35 million euros. So it seems that customers of banks are still interesting enough to make a positive business case for fraudsters, but revenues have been declining since 2011 as the trend shows a declining amount of financial losses. The introduction of a TPP to the payment market will provide a new target for criminals to focus on. The change for customers by allowing them to choose between classic and new services will provide criminals the opportunity to start phishing. For example they will leverage the advertisement campaign of a TPP to initiate a spread of phishing e-mails and try to persuade customers to give away their personal information and with that commit fraud.

Banks have been gaining experience in fighting cybercrime since 2011. It remains to be seen if TPP's are aware of these threats and will develop their services in such a way that they will limit or prevent the damages for customers from phishing or malware frauds. This doubt is caused by the focus on strong customer authentication in the PSD2. All major Dutch banks have implemented strong customer authentication, but still there have been substantial financial losses. This means that current cybercrime threats are able to circumvent strong customer authentication. Therefore banks rely on other, additional mitigating measures to limit the damages caused by frauds. An example of such a measure is fraud monitoring. This defensive measure does not directly add value to the PIS service and could be considered as a non-functional requirement. Therefore TPP's could choose to develop this at a later stage and putting customers at risk.

Autonomous PIS services

Another scenario for PIS could emerge and would be developed on top of AIS services. It entails the opportunity to transfer money from one account to another (checking vs. savings) or from an account at the primary bank to an account at another bank. For example a customer uses an AIS service in which the interest rates on accounts are incorporated. The service can detect that another bank where the customer also holds an account, provides a better interest rate. It will then ask the customer to transfer the money through a PIS service to obtain the better interest rate. Thinking this further trough one could imagine a scenario where a customer will authorise the TPP to obtain a maximum amount of interest over a certain period of time and let it work autonomously.

[61] *Factsheet Veiligheid en fraude (NVB 2015)*

The threats in this scenario would be that in contrast of an earlier statement the TPP will become responsible for the funds of the customer as the customer will transfer the control of funds to the algorithm provided by the TPP. Besides the liability problem there could also be a stability problem as well. If these TPP's would reach a critical mass of users that let their money flow autonomously, it could result in an uncontrolled flow of money ultimately crashing online banking systems and possibly voiding the funds of the account holders. This threat is inspired by the Flash crash in 2010 on the US Stock markets[62]. An error in the algorithm caused the stock markets to crash and stopped the market from functioning.

Circumventing compliance controls with PIS

A second scenario could be that from an AIS portal a customer would like to pay other parties, not being a web shop, for example a utility company. Such a payment is usually initiated trough the use of the online portal of the bank. However in this scenario the online portal of the TPP is used. This would allow the customer to make his/her payment without requiring to log on directly to the bank portal.

Although this scenario looks very similar to online payments done through the bank portal, the difference is in the fact that the bank only authorises the payment and may not interfere with it, except for fraud monitoring. So when a bank thinks the transaction is fraudulent it is legally allowed to stop it. This implies that several responsibilities are transferred from banks to TPP's, such as Anti-Money Laundering monitoring (AML) and sanction monitoring. This second scenario could therefore be used to circumvent compliance controls that banks have and which are imposed on them through legislation. This legislation, for example on AML, is also applicable to TPP's. This is confirmed through article 5.1 sub k in the PSD2, where a Payment Service Provider (PSP), hence a TTP, is put under the legal obligation of adhering to the European directive on AML. As stated earlier it is anticipated that the FinTech start-up companies will be the first movers in this new domain. As start-up companies have a strong focus on gaining a large customer base they might have a lesser focus on this obligation.

[62] *Findings regarding the market events of May 6, 2010 (Flash Crash) (U.S. Commodity Futures Trading Commission, U.S. Securities & Exchange Commission 2010)*

3.3 Summary

In this section the PSD2, and in particular PAAS, has been introduced and discussed based on the relevant legal text. After that more focus has been placed on PAAS by providing use cases for Account Information Services (AIS) and Payment Initiation Services (PIS), along with examples like AFAS Personal, BillGuard, iDEAL and Sofort Uberweising. These companies or products already offer services that use the concepts of PAAS. For both AIS and PIS potential issues have been identified and discussed that could threaten the protection of customers and their personal payment data. Below is a summary of the identified issues.

AIS Issues	***PIS Issues***
Negative public opinion on the use of payment data for commercial purposes	*Abusing fraud monitoring as data processing purpose for monitoring everything*
Who authenticates, the customer or the TPP?	*Defense against classic cybercrime threats (phishing & malware)*
Abuse of payment data	*Autonomous PIS services*
Data breaches	*Circumventing compliance controls with PIS*

Table 4: Potential issues on AIS and PIS

In this section questions from the previous section have been answered. In summary; TPP's are placed within range of supervisors and the EBA has been identified as a relevant European supervisor for TPP's. The EBA and other supervisors will be discussed in section five. Information on the European passport construct is lacking in the PSD2. However the introduction of the PSD2 does mention the "passporting" and that it should be allowed. This means that the European passport construct is also valid in the PSD2 and applies for PAAS services as well. The ramifications from this for supervisors will also be addressed in section five.

4 Upcoming legislation on data protection & security

In this section other upcoming European legislation will be reviewed which is connected to the PSD2, PAAS and TPP's. It will complete the legal analysis and possibly provide solutions to the issues raised in the previous section. Two European legal proposals are relevant which are the General Data Protection Regulation (GDPR)[63] and the high common level framework for Network and Information Security (NIS)[64]. The GDPR is relevant, because it will become the new legal framework on data protection. The NIS is also relevant, because it will be the first legal text which is primarily focused on network and information security. Both proposals will be briefly introduced, followed by a discussion on their relationship with the PSD2 and what impact they can have on TPP's and their supervision.

4.1 General Data Protection Regulation

The current European directive[65] on data protection dates from 1995. Since then, the society has changed a lot with respect to data protection. Aspects like globalisation and technical progress are not well enough covered by the current directive on a European level and not by law on a national level. To better address those developments, a proposal for a new data protection regulation has been drafted and is now on its way to be finalised. The major differences between the current directive and the draft regulation cover several aspects, such as the type of legislation, its scope, a conscious opt-in consent model, the introduction of the data protection officer, a data breach notification and the right to be forgotten.

There is a difference in the type of legislation. It will change from a directive to a regulation. A directive means that additional national legislation is needed to translate the directive into national law. A regulation is more prescriptive and dictates that all European member states must adhere to it, without exception. This change will result in a single, harmonised set of legal rules on data protection in all member states. All local and national legislation on this topic will be voided at the moment the GDPR comes into force.

Also the scope of the regulation will change. The protection of data of European citizens is dominantly present in the GDPR and is not restricted to European companies or countries. All companies that process personal information of European citizens must comply with the new regulation. For example, technology companies from the United States must also adhere to this regulation even though their customer data will not reside in a European data centre, or the company is based outside Europe.

Another important aspect of the regulation is the conscious opt-in[66] consent for the collection and use of personal data. The regulation will force all companies – that process personal information – to acquire the customers consent through an opt-in construction. This means that customers explicitly need to authorise companies to process their data. Customers cannot give an implicit consent anymore by remaining passive.

---

[63] Proposal for a regulation of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, GDPR (European Commission 2012)

[64] Proposal for a directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, NIS (European Commission 2013)

[65] Data Protection Directive 95/46/EC (European Commission 1995)

[66] Opt-in refers to the fact of choosing to take part in an activity, arrangement, etc., rather than being forced to take part.

This passive, implicit consent has often been used in the past by companies through the opt-out[67] consent. For example, a customer starts to use a certain service and is automatically enrolled in another service as well. The only way to end the second service was to explicitly terminate it. With the GDPR a customer needs to give consent for both services, and companies must also be able to reproduce the consent which was given by customers. Therefore companies do not only need to acquire the consent but register and store it as well so it can be used later on, for example in a dispute to get clarity on the consent.

With the GDPR a Data Protection Officer (DPO) is introduced. This officer will act independently from the company hierarchical structure. Most likely this officer will not be governed by the executive board, but by the competent national authority. A DPO is therefore a local, company specific supervisor on data protection. In the Netherlands, companies can already choose to appoint a DPO also known as the "Functionaris voor de gegevensbescherming"[68]. This would allow companies to benefit from the previous mentioned advantages already, however only a limited number of companies have chosen to do so. This can be deduced from the number of entries in the official register[69] for Dutch DPO's.

Data breaches are often in the news nowadays. Therefore a data breach notification has been incorporated into the regulation to better protect customers by at least informing the stakeholders of the breach. Companies will have the legal obligation to notify their customers and the supervisor– without delay – about a data breach that has taken place. So when something goes wrong with customer data, the customers and supervisors at least know something went wrong and have the ability to act on it. For example customers could change their passwords to prevent further unauthorised access, and supervisors can choose to impose fines or they could incorporate the lessons learned from the incident trough updates of policies and guidelines, possibly preventing future incidents.

Finally a much debated change in the regulation is the right to be forgotten. It provides customers the right to request for the erasure of personal data at companies. This right can already be exercised based on a legal ruling in the case of Google v. Spain[70] and will be formalised with this regulation.

RELATIONSHIP BETWEEN GDPR, PSD2 AND TPP'S

Through article 94 in the PSD2 there is a direct link between the PSD2 and the current data protection directive. In that article it is stated that the current data protection directive is applicable entirely. This will be continued when the GDPR comes into effect, since it will replace all legislation on data protection. Derived therefrom TPP's will need to comply with the GDPR as well. The important changes for TPP's based on the prior described aspects are the conscious opt-in consent, the introduction of the DPO, the data breach notification and the right to be forgotten.

Both the GDPR and the PSD2 refer to consent as an informed choice by customers. An informed choice implies two things, informed and choice. Informed intends to make customers aware of the consequences of their choices, and to have customers clearly understand what data is being collected and how it will be used. Once they know that, they can either choose to accept or decline. Registering that choice in case of acceptance is the actual consent. The PSD2 and the GDPR are still very general about the information level a customer must have in order to be considered an informed customer that makes an informed choice.

---

[67] Opt-out refers to the fact of being forced to take part in an activity, arrangement, etc., rather than choosing to take part.

[68] Functionaris voor de gegevens bescherming (CBP 2016)

[69] Dutch register for DPO's (AP 2016)
https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/functionaris-voor-de-gegevensbescherming

[70] Judgement in Case C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González (Court of Justice of the European Union 2014)

This gives companies the opportunity to use their terms of service to get a conscious opt-in consent. It has been stated earlier that most people do not read and do not understand the terms of services which results in a non-informed choice by customers.

The introduction of the DPO could improve the local supervision within companies and thus TPP's. The independent status of this officer could be beneficial to data protection and more specifically to the prevention of the abuse of data. The officer should not allow the use of customer data without having a clear purpose and consent for it, just as it is stated in the legislation. Having a DPO appointed, companies will most likely give more consideration to the alignment of their business models and the processing of personal data. This alignment and the control performed by the DPO will help to prevent the abuse of data. However care must be taken that the position of the officer will stay independent, because (s)he has to deal with multiple stakeholders that have different, possibly contradicting interests. Another important issue with respect to the introduction of the DPO is the scoping on types of companies that will be obligated to have such a DPO. Currently the introduction of the DPO is limited to multi-national corporations or companies having over 200 employees. This leaves the smaller companies out of scope. Exempting the smaller companies will become a bigger issue when more small technology startups will develop services based on the PSD2 and process personal data on a large scale.

Data breach notification is expected to have a positive effect on the security of personal data, because severe sanctions can be imposed on companies that experience a breach. An example of such a sanction is a fine based on the percentage of the total turn-over. The risk of getting a high fine will most likely lead to a more thorough consideration at companies whether to even start with the processing of personal data. And if companies choose to do so, they will be more aware of the associated risks on data protection, which in turn should result in a greater and clearer motivation to secure their processing systems well enough to prevent breaches.

In the Netherlands, a change in national law[71] on January 1st 2016 already accommodates such a data breach notification. So TPP's in the Netherlands are obliged to notify the Autoriteit Persoonsgegevens (AP) in case of a data breach. However that doesn't mean that Dutch customers will always be informed about a breach. If the TPP resides in another country and uses the European passport construct, it could be that this TPP is not obliged to report the data breach. The enforcement of the GDPR will harmonise the legal rules on data protection and therefore also on data breach notification which becomes mandatory in all European countries and improves data protection throughout Europe. The GDPR ensures that Dutch consumersor the national DPA will be informed of all breaches at TPP's, independent from the originating country.

The right to be forgotten will allow customers to request removal of their data from a data processing or storage facility. With the current data-driven society, enormous amounts of data are being generated daily by everyone. Especially digital natives – young people that grew up with internet – are creating a huge trail of data. Nowadays it is nearly impossible to remove that data. This feature – the right to be forgotten – in the regulation will provide customers the possibility to act on it, by having it erased. However this right will be very hard to implement for companies in their applications and systems. The main reason lies in the complexity of modern computer systems. A single piece of data will flow through multiple separate servers and could be stored on multiple locations. The ability to erase all instances of that single piece of data requires companies to have a good understanding of all locations on that same data, logically and physically.

[71] *Meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid CBP (Eerste kamer der Staten Generaal 2015)*

This flow should be considered as the primary flow of that data, but there are also secondary flows such as backups and aggregated data. When a customer chooses to exercise their right this usually only includes the primary flow of data and not the secondary flow. A second reason is that companies still want to use the data for data analytics. Therefore companies often do not erase the data but make it inaccessible to customers. This gives customers the impression it is deleted and erased, but actually it isn't visible to them anymore. This "procedure of erasure" is often stated in the terms of services which customers are not likely to read. Customers could therefore get a false sense of the erasure quality or level.

The current information in the PSD2 lacks guidance on the right to be forgotten and how it should be implemented and executed. This could mean that TPP's will not be ready nor have the ability to erase the data when a user requests it, and will most likely result in making the data of that user inaccessible – which is not the same as erasure – and allows companies to keep using it. Failure to comply to a single request could become a problem for the TPP including their other customers. A consequence of the failure to erase the data of a single user, could lead to the erasure of the data of all users. That also complies with the request only being far more extensive than necessary. This puts the TPP in a problematic position, because erasure of all data, would include the data of all customers. Also the ones that didn't apply for erasure. Those customers could become victim of the inability of the TPP to act on this appropriately. So depending on the ability to act on the right to be forgotten, a TPP could render its services useless with a single erasure request affecting all customers, also customers that are not involved in this matter.

4.2 Proposal for a directive on Network and Information Security

The dependence on the security of information systems becomes bigger, because more people are using them in almost every aspect of their lives. Without these information systems, companies and possibly nations could come to a hold and stop functioning. Major security incidents – either caused intentionally or unintentionally – have occurred in the past, and they all impacted the reliability of these systems and services in one way or another. In order to prevent or minimise the impact of such incidents, a minimum level of Network and Information Security (NIS) is being set up. A tangible result on this topic is the proposal for a high common level framework on NIS, drafted by the European Commission in 2013.

An important aspect of this proposal is the establishment of a national strategy on NIS, including the designation of a competent national authority. In the Netherlands this proposed authority is the National Cyber Security Centre (NCSC)[72]. Another aspect is that many organisations must also have some kind of measurement on the effectiveness of information security controls. A suggestion is made by introducing a well-known standard, the ISO27001[73] as a starting point. When the NCSC starts acting as an authority and uses the ISO standard as a security baseline it can improve security in general.

RELATIONSHIP BETWEEN NIS, PSD2 AND TPP'S

The old proposal of the PSD2 – the version prior to October 8th 2015 – contained two articles that refer to the NIS proposal. The related articles in the NIS proposal are about the establishment of the national competent authority, security incident notification and measurements on the effectiveness of security controls.

By referring specifically to these articles it is clear that the national competent authority on NIS is expected to play a role in supervising TPP's, and the NIS framework will provide a solid base for information security on services provided by TPP's. Customers will profit from this in two ways. TPP's will get guidance on how to set up their security properly and secondly by introducing an authority – the NCSC in the Netherlands – on this topic. By setting up this role, it means that a minimum level of NIS can be reached through enforcement of legislation.

---

[72] *About the NCSC (National Cyber Security Center 2015)*

[73] *ISO/IEC 27001 Information security management (ISO 2013)*

Section five will elaborate more on the expected role of the NCSC and it will propose to also have the NCSC as the Dutch supervisor on NIS and thus the supervisor on security for TPP's.

Similar to the data breach notification in the GDPR, a security incident notification in the NIS framework will become relevant, also affecting TPP's. This will be beneficial for customers since companies are obliged to be transparent and clear on any security issues that arise with their services. The increased awareness could be a result from such an obligation, and could lead to better security precautions and processes at TPP's and elsewhere, for example at banks.

The effectiveness of security is difficult to grasp and quantify, but by introducing and using a well-known standard – the ISO27001 – a certain indication of the effectiveness might be gained. The objective nature of a standard will also allow for a comparison between companies in a single country, or between countries, ultimately providing an indication of the security level at TPP's in Europe. However a standard could be considered objective, it doesn't imply that is also adequate. Care must be taken not to depend too much on standards alone.

As the final revised text of the PSD2 – version October 8th 2015 – doesn't contain a reference to the articles in the NIS proposal, it doesn't mean the link should be considered absent. It is expected that a national competent authority on NIS definitely will have an added value in general, but also from the specific perspective of the PSD2 and TPP's.

4.3 Summary

In this section two European legal proposals have been introduced namely the GDPR and the NIS. The GDPR revises the legal framework on data protection in Europe. The NIS framework aims to achieve a minimum level of network and information security and introduces a national competent authority on this theme.

The key elements for the GDPR related to the PSD2 and TPP's are the conscious opt-in consent, the introduction of the DPO, the data breach notification and the right to be forgotten. From the analysis of the GDPR it becomes clear that the conscious opt-in consent is broadly defined, and allows companies to circumvent the obligation to inform customers appropriately.

The other three key elements most likely will help customers in protecting their data. These are; local supervision through the DPO which could prevent problems by careful consideration on which data to process and for what reason, a notification to customers in case of a data breach and finally the option to erase their data. This erasure also prevents future problems and limits the impact of an incident.

The key element for NIS is the appointment of a national competent authority, which will be the NCSC in the Netherlands. This is a first step in achieving a minimum security level and the ability to focus on that level. Having a dedicated authority and possibly also a supervisor– the NCSC is proposed to become this supervisor in the next section – on a generic topic such as security will improve security. It will help companies and therefore also TPP's to better secure their products, resulting in fewer security incidents and more reliable services.

5 Supervision of Third Party Payment Service Providers

Changing the legal framework – moving from the PSD1 to the PSD2 – is a start for changing the rules based on which companies provide services to customers.However, additional effort is needed to enforce the legislation, achieve its intended effects and to prevent undesirable situations. That effort has to be made by supervisors as they measure the extent to which companies are adhering to the legal framework. Customers expect supervisors to control companies on their behalf. The trust of customersand the trustworthiness of companies are often derived from this supervisory work.

This section will shift focus from the content of the PSD2 – which has been discussed in previous sections – to the supervisors that will control and oversee TPP's. Authorities and supervisors which are relevant to TPP's – on topics of governance, security and data protection – will be identified. This will provide an overview of supervision of TPP's which is presented in the first paragraph. The subsequent paragraphs will describe each supervisor through a short summary of its mission and vision, the relationship between the supervisor and TPP's, and potential challenges they might face.

5.1 Overview of supervision of TPP's

Supervision of TPP's at a European level is concentrated within the European Banking Authority (EBA)[74]. It will act as the primary authority and provide the first guidance on the process of getting the PSD2 correctly implemented in national law in all European countries. It will deal primarily with national banks as its peers. In the Netherlands this will be De Nederlandse Bank (DNB)[75]. A second national supervisor, which deals with the aspect of data protection, is Autoriteit Persoonsgegevens (AP)[76]. The AP can be assisted by a local supervisor for companies, the Data Protection Officer (DPO). The third national supervisor is the Autoriteit Consument & Markt (ACM). Amongst other things, it also supervises the relationship between the customer and companies, in this thesis the TPP's.

The fourth and final national supervisor is the proposed national competent authority on information security. This is the National Cyber Security Centre (NCSC) in the Netherlands. Through a proposed directive on Network and Information Security as discussed in section four, the NCSC will become the competent authority on information security. As a result of this, the NCSC could be considered as a future supervisor on information security and thus also TPP's. Since the roots of the NCSC lie within information security, this addition is expected to be an enhancement for supervision of TPP's from which other supervisors can benefit, but it can also be an improvement in general from which society can benefit.

[74] A competent authority is different from a supervisor. A supervisor has enforcement capabilities derived from legislation and the competent authority doesn't have this. The NCSC is a future authority on securitythat sets policies and standards, but cannot enforce this on companies. To do that a national supervisor is needed. Often the terms supervisor and competent authority are interchanged, but in this thesis, the prior given difference is used.

[75] DNB often cooperates with the Autoriteit Financiële Markten (AFM), but in this research no link was found that connected the AFM to TPP's.

[76] Autoriteit Persoonsgegevens (AP) is formerly known as the College Bescherming Persoonsgegevens (CBP).

In summary, EBA will set the policy which will be enforced by the four Dutch national supervisors, and possibly aided by a local supervisor for companies on data protection as shown in the schematic overview below.

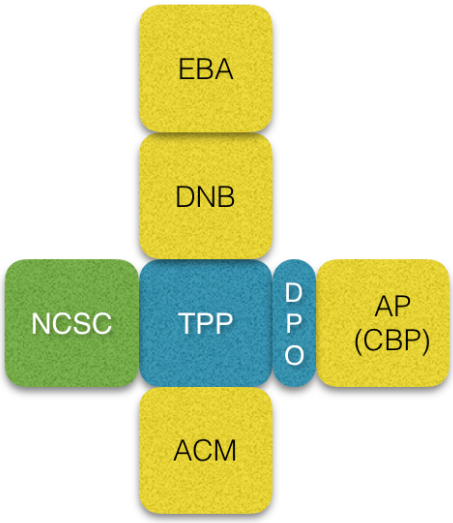

Figure 4:Schematic overview of supervision of TPP's (Blue is the TPP itself including the data protection officer (DPO), yellow are existing supervisors and green is a proposed supervisor)

5.2 European Banking Authority

The European Banking Authority (EBA)[77] was established in 2011 as part of the European System of Financial Supervision (ESFS)[78], which was initiated by the events[79] in the financial markets from 2008 onwards. The EBA is an independent European authority and its main task is to contribute to the creation of the European Single Rulebook[80] which is the basis for the Single Supervisory Mechanism[81] that should lead to stability in the financial sector, aligning with the policy set out by the European Central Bank (ECB).

The task of the EBA related to the PSD2, is to provide guidance on the translation of the PSD2 into national supervisory policies. To execute this task, the EBA can produce a number of regulatory and non-regulatory documents including Regulatory Technical Standards (RTS), guidelines, recommendations, opinions and reports. The RTS are legal documents which specify certain aspects of an EU directive or regulation. The final RTS are endorsed and adopted by the European Commission and are thus legally binding in all member states. This gives the EBA executive supervisory powers to influence other supervisors, andthose supervisors will influence companies, including TPP's.

---

[77] About the EBA (European Banking Authority 2015)

[78] The European System of Financial Supervision (ESFS) is the framework for financial supervision in the European Union in operation since 2011.

[79] An Analysis of the Financial Crisis of 2008: Causes and Solutions (Murphy, Austin 2008)

[80] The European single rulebook aims to provide a single set of harmonised prudential rules which institutions throughout the EU must respect.

[81] The single supervisory mechanism transfer national supervisory power to the European Central Bank to allow more control from a central supervisor. This mechanism came in effect as of November 2014.

RELATIONSHIP BETWEEN EBA & TPP'S

The EBA will have a great influence on the security and data protection controls that TPP's must undertake to allow them to run their services, and it will become the leading European authority on the interpretation of the PSD2 and, in particular, PAAS. It will be responsible for setting the minimum level of security and data protection for TPP's across Europe. Its main contribution will be the draft of the RTS which will set standards across all member states for the implementation of the PSD2. The RTS will be based on the earlier published documents by the ECB[82] [83] which are a first attempt at drafting the RTS. Through its working program several actions are planned to give direction to general developments on the implementation of the PSD2, but also to specific key elements with respect to the newly defined services, such as AIS and PIS.

The EBA will also establish and maintain a central register for those companies who have acquired a license – issued by the relevant national bank – to act as a TPP. In this way a central overview of all TPP's in Europe will be possible. TPP's are able to use the European passport construct to extend their services to other European countries. The central register will probably be fed by European countries through their national registers. In the Netherlands a register is maintained by DNB. This will most likely serve as a basis for the Dutch contribution to the European register, possibly with some modifications to accommodate TPP's.

The EBA also has a role in receiving notifications from TPP's on security incidents and data breaches and relay them to the appropriate supervisors in the member states. This notification function, combined with the public registers, give EBA the best position to assess the European impact when security at a TPP which serves customers across Europe, is breached. The EBA will have the opportunity to enable parties throughout Europe to help mitigate the impact of severe incidents and add value as a central information hub.

5.3 De Nederlandse Bank

De Nederlandse Bank (DNB)[84] is the main Dutch national supervisor for the financial sector. It derives its mandate from the law on financial supervision, also known as the Wet financieel toezicht (Wft), and works primarily on building trust for society in financial systems, which is the base for price stability and prosperity in the Netherlands. Besides the goals of price stability and stable financial systems, it also has role in performing supervision of Payment Service Providers (PSP's), including TPP's when the PSD2 comes into force.

The way supervision of PSP's is arranged by DNB is through a system of licenses, public registers and prudential supervision. The system of licenses works as a safeguard on the financial health of a company and proper management when it starts. The license ensures that a company has the ability to fulfil its financial obligations for an initial period of time, which is especially important for those companies that enter the market. The second important theme in the licensing system is the screening of people that will manage and control the company. This is meant to prevent unsuitable individuals from gaining an opportunity to de-fraud companies or customers. In essence this means that when people don't have the right credentials or aren't in good standing, they are not allowed to run such companies. DNB also maintains several public registers on PSP's and reported incidents. In this way it is transparent for a customer whose organisation acquired a license and whose organisation has been reported on in case of an incident. The prudential supervision is based on the financial administration and financial performance of an organisation, and thus mainly focused on the solvency and liquidity of a company.

---

[82] Public note on security of payment accounts access services (European Central Bank 2014)

[83] Final Recommendations on the security of payment accounts access services (European Central Bank 2014)

[84] Over DNB (De Nederlandse Bank 2015)

RELATIONSHIP BETWEEN DNB & TPP'S

In the PSD1, the DNB is positioned as the main supervisor of financial organisations in the Netherlands. As the PSD2 is the successor of the PSD1, it implicitly is also appointed as the national supervisor for the PSD2. This means that with respect to the PSD2, DNB will get additional parties (TPP's) to supervise. According to the current set-up of supervision, these TPP's will have to acquire a license, will be placed in the national registers and will be subject to prudential supervision. In the near future DNB will get guidance in terms of the RTS from the EBA on which it needs to act. The first thing that needs to be done is that governments must convert European wide directives and the RTS into national legislation. The second item is the implementation of supervision of TPP's in their working programs and ongoing prudential supervision.

On the topic of information security, DNB can profit from earlier work[85] [86] and apply that to TPP's. Since 2010, DNB has been conducting investigations at financial organisations to assess the quality level of information security and their maturity level. In 2014 and 2015 the framework has been adjusted to demand a higher maturity level of companies on certain aspects of information security. This adjusted framework has been verified on a selection of companies[87], which had to perform a self-assessment and return the results to the DNB. For other non-challenged companies, DNB expects that those companies will take their responsibility themselves.

CHALLENGES

In the PSD2 it is stated that TPP's will be supervised as a regular financial organisation. In the Netherlands this means that a TPP will fall under the supervision of DNB. DNB mostly deals with prudential supervision which is historically focused on the financial position of a company, as already explained. In case of TPP's there is no real financial position since the money of a customer is never under control of the TPP. Therefore the traditional prudential supervision is expected to be less effective. Prudential supervision needs to be adapted to the changes that are introduced by the PSD2.

The second challenge is about the application for a license[88]. The application process has a prudential perspective and less to do with security and data protection. It remains to be seen if customers are best served with DNB acting as a sole arbiter, and in that position has to check if a TPP has the appropriate security and data protection controls, and it should be given the license. DNB has done some work on this already, but it should consider if this is enough and if this is the right focus for a financial supervisor. Or, it could consider to join forces with other organisations that have a stronger relation with information security, such as the National Cyber Security Center (NCSC).

In section three a scenario has been put forward that transfers the control of the funds of customers to TPP's, the autonomous PIS services scenario.When such services become active, TPP's will have the control of funds in order to maximise profits. This will create a new risk profile of a TPP, changing it from a small participant of the financial system to a single point of failure. When it reaches a critical user base it could control a large amount of funds. DNB needs to closely follow the innovative solutions to prevent this situation, and if it doesn't put controls in place, this could impact financial services resulting in an uncontrolled flow of money.

---

[85] Toetsingskader Informatiebeveiliging voor DNB thema-onderzoek 2014 (DNB 2014)
http://www.toezicht.dnb.nl/3/50-203304.jsp

[86]Resultaten onderzoeksthema Pentesten (DNB 2013)
http://www.toezicht.dnb.nl/2/50-229818.jsp

[87] Toelichting op Toetsingskader Informatiebeveiliging 2014 (DNB 2014)
http://www.toezicht.dnb.nl/binaries/50-230767.pdf

[88] Vereisten voor een vergunning van een betaalinstelling (DNB 2015)
http://www.toezicht.dnb.nl/2/50-228425.jsp

DNB also has to be vigilant to the second proposed scenario. That scenario is about the TPP becoming a normal payment provider and provides services to make regular payments as well, not limited to payments in online web shops. This will attract customers that seek ways to circumvent bank controls, such as Anti-Money Laundering (AML) and money paid to beneficiaries in sanctioned countries. DNB needs to monitor TPP's on its services and verify if this scenario is offered as well, and also needs to check if AML and Sanction screening is present. Banks are not allowed to intervene on payments initiated by TPP's and therefore might not be responsible for the payments, possibly resulting in the financing of criminals. If this would be a sole responsibility of the banks and not of the TPP's, than it wouldn't be an equal competition anymore as banks need to do more than TPP's.

5.4 Autoriteit Persoonsgegevens

Autoriteit Persoonsgegevens (AP), formerly known as College Bescherming Persoonsgegevens (CBP)[89], states its mission as executing the supervision of "the protection of personal data". It regards this protection as a fundamental right and sees it as being something that should apply to every citizen and should be protected at all times.

The main task of the AP is to supervise the processing of personal data within all organisations and companies in the Netherlands, and check if the storage and processing is compliant with the relevant national law, the Wet Bescherming Persoonsgegevens (Wbp). The approach of the AP is to explain its interpretation of protection, and its main supervisory task is to address violations of the law of data protection by doing investigations on a case by case basis. Furthermore the AP raises awareness in all parts of society and advises the Dutch government on new data protection laws and regulations. Part of that awareness is achieved by publishing all results of its investigations and by keeping a register on all companies that process personal data. In this way consumers have the opportunity to obtain more information about the processing of personal data by organisations and any related investigations into those companies.

Supervision by the AP is mainly about conducting investigations for assessing the level of (in) compliance of organisations with the law. It is equipped with tools for enforcement, for example a Co-operation Order or a Conditional Fine. These investigations can be started by the AP itself or on the request of another party which have expressed a complaint. In essence this means that every consumer or organisation can report an issue. Based upon the impact and current priorities, the AP determines whether to investigate the issue or not.

Since there are a lot of organisations that process personal data and the AP is limited in resources, organisations are allowed to arrange certain supervisory tasks themselves by appointing someone in the role of Data Protection Officer[90] (DPO). This role inherits some of the powers of the AP by law but those are limited to performing supervision and don't include enforcement. If an organisation appoints a DPO, the AP will be less involved in the supervision, because this is partially transferred to the DPO. The DPO's main task is to supervise the processing of personal data and to verify if it complies with the law and take appropriate action when there is an issue. Other tasks include administering the collection of all data processing facilities within the organisation. If no DPO is present, all processing must be reported directly to the AP. Furthermore the DPO is also tasked with responding to questions and complaints from either employees and customers, and finally (s)he has to promote and advise on *"Privacy by Design"* within day to day business and projects. The AP demands some skills of the DPO. Those are that (s)he needs to be reliable and has sufficient knowledge about data protection and the relevant legislation. All officers that are appointed are also put into a public register that is held and maintained by the AP.

[89] *Over het CBP (College Bescherming Persoonsgegevens 2015)*

[90] *The Data protection officer is also known in Dutch as the Functionaris voor de gegevensbescherming.*

In order to keep an overview of all organisations that process personal data and for what reason, the AP keeps a public register[91] for notifications on processing operations. By law, all organisations are obliged to notify the AP of the processing of personal data, and risk receiving a fine if they do not comply. That notification includes the name of the processor, the purpose, the people involved, the receivers of information and if the information will be transported outside the European Union or not. Because of this obligation, the register provides a central point of information for data processing on a national level. Customers can view all organisations that process personal information and thus get a good overview on what data is being collected.

Since the legislative text about data protection can be difficult to understand, the AP provides additional information on how to read the legal text and how to apply it in the right way[92]. Furthermore it also provides more general information on data protection, for example how to protect your own data or how to request information from organisations that have been processing it. When new legislative proposals or drafts are being made up, the government has the obligation to take the advice of the AP into consideration.

As of January 1st 2016 the Dutch law on data protection has changed. It now incorporates a mandatory obligation to inform the AP in case of a data breach. Several guidelines have been issued on when to report a breach in terms of impact, in what timeframe and the content of the notification. This is also addressed in the coming General Data Protection Regulation (GDPR) as discussed in section four. As a result of this change in Dutch law, Dutch companies are now forced to be transparent about any data breach they experience.

RELATIONSHIP BETWEEN AP & TPP'S

In article 94 of the PSD2 it is stated that any processing of personal data must be carried out in accordance with the European data protection directive (95/46/EC), and derived from that, also in accordance with the Dutch national law (Wbp). Since the AP is the supervisor on this matter in the Netherlands, it means that the AP will also become responsible for the supervision of TPP's with respect to the processing of personal data.

CHALLENGES

The supervision of data protection performed by AP is arranged in a reactive way. Companies that process personal data are obliged by law to report what personal data they are going to process, and for what purposes. From the analysis of the supervisory role of the AP it became clear that there is no active policy or action by it to find companies that do process personal information but haven't reported it and thus are violating the law. Only after the AP receives complaints or through some other channel receives indications that something is wrong, will it start an investigation. Given the increase of the processing of personal data and the growing number of incidents of either abuse of data or data breaches, a passive approach no longer seems to be appropriate.

Secondly, by applying a reactive form of supervision there is a risk that data will be used in a wrong way. This means that a company initially reported the purpose and scope of the processing of that data, but due to changed business interests used it for other purposes as well, but did not report the change. This results in a broader use than originally intended. Although this broader use should have been reported as well, it is expected that this is often forgotten by companies or worse, neglected. Although this is not specifically related to the PSD2, the PSD2 will open up access to payment data and as seen in previous sections, it introduces a vast amount of opportunities to use this data.

---

[91] Meldingenregister (https://www.collegebeschermingpersoonsgegevens.nl/asp/orsearch.asp)

[92] Richtsnoer beveiliging persoonsgegevens (CBP 2013)

As a result, the chances of data being used for other purposes might increase, and having a reactive form of supervision could let other uses go unnoticed.

It is also clear the AP is limited in its capacity and thus has limited opportunities for investigations. This could become a problem with the revised European and national legislation on data protection (GDPR), the introduction of the data breach notification, and the additional parties to supervise, such as TPP's. As stated in the previous sections the value of payment data is big, resulting in an easy case for data abuse and data breaches. Care must be taken that the supervisor for data protection will not be flooded with work or investigations as it already is limited in its capacity. This problem is confirmed by the director of the AP in a television broadcast[93] on December 2nd 2015. In that broadcast he mentions that the AP needs to quintuple in human resources in order to keep up with all changes. Since government is cutting on expenses and is less willingly to invest in the AP, he states that the AP will probably need to let companies go that cross the line.

Inevitably this could mean that TPP's are placed under control but it remains to be seen if that supervision is sufficient. A partial solution can be found in the GDPR on the topic of the DPO. The introduction of a mandatory DPO will be of much benefit for customers since their independent position could prevent problems. This could reduce the number of incidents of abuse of data and data breaches, and reduces the workload for the AP. As mentioned before, this is already an option in the Netherlands.

5.5 Autoriteit Consument en Markt

The Autoriteit Consument en Markt (ACM)[94] is a Dutch national supervisor on consumer related topics. The ACM is relatively new and was formed in 2013[95] by the merger of several former supervisors which were the Onafhankelijke Post en Telecommunicatie Autoriteit (OPTA), the Nederlandse Mededingings autoriteit (NMa) and the Consumenten Autoriteit (CA). The ACM promotes chances and choices for companies and consumers which includes innovation on new products and services. The main focus of the ACM for consumers is to enhance their knowledge of their rights and empower them to make informed choices. The focus for corporations is to improve their transparency on the provided services. They need to be clear about the conditions of their services and what consequences could follow from the use of it. As a result of the merger, the ACM still monitors specific markets such as energy, telecommunications, transport and postal services. In addition to those markets, it also supervises – in general – the fair corporate competition.

The activity of the ACM revolves around three themes; investigations, prevent/clarify/end and warn/penalise. The ACM has the power to independently start an investigation either based on external or internal signals. When something is discovered from this investigation, the ACM has several instruments to make companies comply. For example a "bindende aanwijzing" which tells the company how it should interpret the law correctly so there can be no more misunderstanding. This is usually combined with a "last onder dwangsom". This is to stop the offence by means of a fine. Finally the ACM has the ability to warn the general public about companies that do not comply in order to make the public more aware and to prevent further damages.

---

[93] Television broadcast by VARA Zembla with the title "Data: het nieuwe goud" broadcasted on December 2nd 2015. The director of the AP, Mr. J. Kohnstamm appears at 35:40 in the broadcast (http://zembla.vara.nl/seizoenen/2015/afleveringen/02-12-2015).

[94] Over de Autoriteit Consument en Markt (Autoriteit Consument en Markt 2015)

[95] Instellingswet Autoriteit Consument en Markt (Rijksoverheid 2013)

RELATIONSHIP BETWEEN ACM & TPP'S

The ACM is connected to TPP's through art 35, 66 and 67 of the PSD2. Article 35 is about the rules on access to payment systems, and articles 66 and 67 elaborate on that in the context of Account Information Services (AIS) and Payment Initiation Services (PIS). Those rules are meant to achieve fair access for all payment providers and treat them equally. The ACM will supervise this process.

A second important indirect link between the ACM and TPP's exist in the protection of customer rights. TPP's will provide services and need to be transparent about their terms. Based on this information customers will make choices on whether or not to start using these services. So it is very important that customers are well informed and understand the consequences of their choices. However there are many examples that display how companies are using these terms to get a silent consent for the use of personal data that isn't aligned with the service, but which is only aiding the business model. This also a conclusion from the impact study of the PSD1 as discussed in section two. This is why the ACM focuses on empowering customers so they become more aware of the data they share with companies. As seen in previous sections, reading and understanding the terms of services of all online services would take a disproportionate amount of time of consumers. The ACM therefore doesn't focus on the terms of services, but asks customers to focus on the data being shared. This could empower the customer and provides the opportunity for an informed choice and should help remedy the issue of silent consent.

Another interesting observation has been made by the ACM, which is described next. The introduction of the PSD2 – in particular Payment Account Access Services (PAAS) – and in general the obligation for banks to share financial data with third parties based on legal grounds, holds a risk. The obligation of sharing data through third party access could lead to "one way sharing". Major non-European technology companies, such as Google, Amazon and Facebook would be able to enforce – with customer consent – access to payment data and enrich that with their own data. However TPP's or banks cannot enforce similar access to data of Google or Facebook. Data can have a major competitive advantage which makes the incentive for companies to keep the data for themselves bigger. The position of companies in the chain of information is essential to acquire unique access to certain data.

An example is the case of small American banks that didn't start to offer credit cards, but instead outsourced it to other major companies such as MasterCard and Visa. By outsourcing those services they do not have access to the data that is being generated and cannot use it to offer new personalised services. Visa and MasterCard acquired an ideal position in the chain and are changing their businesses slowly from the processing of payments to the collection of data. They could sell that data through a license scheme but instead they are holding on to it for themselves. MasterCard Advisors collects and analyses 65 billion transactions of 1.5 billion cardholders in 210 countries to map business and consumer trends. These trends are then sold to the highest bidder. An example of such trend is that it is most likely that people that stop for gas around 4 PM in the afternoon, will also spend between 35 and 40 dollar in a supermarket in the next hour. So it is possible that in the future credit card companies will stop commissioning transactions and process them for free, but in exchange will acquire access to data, with which they can analyse even more and extensive[96].

[96] *De Big Data Revolutie, Mayer-Schonberger, Viktor en Cukier, 2014, p.181.*

5.6 National Cyber Security Centre

The National Cyber Security Centre (NCSC)[97] was formed in 2012 out of the Dutch national GovCERT organisation. The NCSC is organisationally placed within the ministry of Safety and Justice and falls under the responsibility of the national coordinator on terrorism and safety. The core tasks are security incident response, situational awareness, reinforcement of incident management and acting as a liaison platform for security partners. Those partners are mostly governmental, but also come from the vital infrastructure, such as energy companies and banks.

The NCSC acts as the central Dutch hub for information on cybersecurity and its mission is to contribute to the improvement of the cyber resilience in the Netherlands. It is expected that this will contribute to a more secure and safe digital society. The NCSC also has international connections. Therefore it is the main point for communications on any cyber intelligence or threat nationally and acts as single point of contact internationally. Finally it can act as a crisis manager in case of a cyber incident at the Dutch government, for example as with the DigiNotar case[98].

RELATIONSHIP BETWEEN NCSC & TPP'S

The establishment of the NCSC as the Dutch competent authority on security through the proposal for a high common level framework on Network and Information Security (NIS) provides an indirect link with the PSD2 and TPP's. The NCSC could have a role in supervising TPP's on security, possibly collaborating with other national supervisors, for example with DNB or AP on the interpretation, implementation and control of the Regulatory Technical Standards issued by the EBA.

CHALLENGES

Through contact[99] with the NCSC it became clear that it also expects to become the national competent authority on NIS in the Netherlands. However it doesn't have any ambitions to develop itself as a supervisor as there are already sector and branch related supervisors, for example DNB in the case of financial institutions. Even so – as stated earlier – our dependance on information technology is growing. Therefore it seems only logical that there will be a dedicated supervisor for security which is not related to a specific sector. Security is a general theme just as data protection is. For data protection there is a separate supervisor and the NCSC could be that supervisor for security. So by adding NCSC as a supervisor on TPP's, it will improve supervision on security in general, and in this thesis, more specific for TPP's. The NCSC has proven to be experienced through several years of work as a responder to security incidents. This experience could be used by other supervisors such as the AP and the DNB, to help them strengthen their supervision.

In the previous sections several issues with the PSD2 and TPP's have been identified. Among these were the security breaches (part of data breaches) and the classic security threats, such as phishing and malware. Since there are already preparations being made to legally oblige companies to report on major security incidents, this needs to be managed within countries and the NCSC seems an appropriate candidate to handle this in the Netherlands. Similar in the way the AP handles data breach notifications. Security incidents often are not specifically related to a sector but are a problem for all industries, and sharing information is essential to control the impact of such incidents. This sharing of information could be solved be either really good a cooperation between sector related supervisors or by a non-sector specific, central, national supervisor.

---

[97] Over het National Cyber Security Center (National Cyber Security Center 2015)

[98] Dossier Diginotar (https://www.ncsc.nl/actueel/dossiers/diginotar.html, NCSC 2011)

[99] As stated in section one, all relevant supervisors have been contacted. The information gathered is mostly used as background information, but here a reference is used.

The cybercrime directed towards banks and its customers in the Netherlands is declining in the last few years and almost every incident of cybercrime is reimbursed except for those with gross negligence. This means that banks have invested a fair amount of time and money to keep the threats from phishing and malware attacks at a minimum. In order to keep customers safe, a similar level of security against these threats from TPP's should be expected.

Although DNB has made progress on this and the EBA is working on it as well, the help of the NCSC could take this topic to the next level in the Netherlands by giving it the proper attention from an experienced perspective, and adding more resources to the topic.

From numerous security incidents and the classic threats it is clear that security is a major topic for providing reliable services. This reliability is strengthened by applying the lessons learned from incidents from the past, and with that the NCSC can add value in a supervisory role and can contribute to progress on security supervision in the Netherlands.

5.7 Summary

In this section an overview is given on the relevant supervisors which will play a role in supervising TPP's. Those supervisors are the DNB, AP, ACM. The EBA is the primary European authority which will start the implementation of the PSD2 and PAAS by issuing the Regulatory Technical Standards.

The DNB is the main Dutch national supervisor on Payment Service Providers (banks) and it will include TPP's when the PSD2 comes into force. Their supervision is arranged on a licensing system that will apply to TPP's, public registers and ongoing prudential supervision. The main challenge for DNB is if it will be able to modify its traditional approach of prudential supervision to an approach that fits the new technological reality. Re-using its earlier work on the maturity of information security at financial organisations, and collaborating more with other supervisors could enhance the supervision of TPP's.

The AP is tasked with supervision of the processing of personal data at TPP's. The AP is facing major legislative changes with the prospect of the GDPR, but also with national changes on the mandatory reporting of data breaches. The introduction of TPP's – which are extra parties to supervise and who will control very valuable data – will put even more stress on the capacity of the AP. As noted by the director of the AP, it needs to grow massively, but are not funded to do so by the Dutch government. This will result in a gap in the supervision of TPP's and the AP could be forced to let companies go that don't comply with the law. This will leave customers of TPP's and their data vulnerable.

The ACM is concerned about the informed choices customers of TPP's should make. The main concern is that customers are not able to oversee the consequences of their choices well enough. Although the approach of empowering the customer seems promising, it is still too early to tell if this would also works in the case of TPP's, as their services will be using very valuable and personal data.

Finally, I introduce the NCSC as a new official supervisor. It will become the national competent authority on security, and its strength lies within the incident response domain and with giving advice on security. I suggest it should step up to the next level, and become a supervisor. As a supervisor, it could enforce security and help other supervisors, for example DNB. Other supervisors have a different origin which makes the appointment of the NCSC complimentary to the current supervisors. It would also add more capacity to the existing supervisory staff.

6 Conclusions and Recommendations

The previous sections are about the origin, motivation and contents of the Payment Service Directive 2 (PSD2), in particular Payment Account Access Services (PAAS), and the associated supervision of TPP's. This section draws conclusions based on the main research question from section one, and includes several recommendations to address the challenges that have been identified. This section and thesis finish with a personal opinion of the author on the biggest risk of PAAS and on a strategic side-effect of the PSD2.

6.1 Conclusions

TPP's will be allowed to access consumer bank accounts[100] as a result of the revised legal framework on payments, the PSD2. The topic of this thesis is to investigate if and in what way supervision of those TPP's in the Netherlands is arranged, with a particular focus on information security and data protection. This has resulted in the following main research question and in two additional minor research questions.

How is the Dutch governmental supervision of third party payment service providers (TPP's) arranged in the light of the revised Payment Services Directive (PSD2).

From section three it became clear that there is a legal basis in the PSD2 for supervising TPP's. There are already supervisors in place and actively supervising financial organisations. Their scope will be extended to encompass TPP's. So, once the PSD2 comes into force there will be supervisors available to monitor TPP's. From section five it became clear that the following existing supervisors for TPP's in the Netherlands are relevant;

a) De Nederlandse Bank (DNB)
b) Autoriteit Persoonsgegevens (AP)
c) Autoriteit Consument & Markt (ACM)

In the PSD2, TPP's are considered a specific type of Payment Service Provider and thus are in scope for supervision by the main national supervisor of financial organisations, which is DNB. As TPP's process personal information they are also subject to the supervision of the AP for data protection. Finally, as TPP's offer services to customers they fall under the supervision of the ACM. On a European level, an important position is given to the European Banking Authority (EBA). The EBA is primarily tasked with providing guidance to national supervisors on implementing the PSD2 and PAAS.

How is the Dutch governmental supervision of third party payment service providers (TPP's) arranged in the light of the revised Payment Services Directive (PSD2), ***and does that supervision incorporate the protection against abuse of access (security).***

No official supervisor has yet been appointed for information security in general, nor in the PSD2. The absence of an official national supervisor on information security creates a gap in supervision in general. Having a supervisor that can enforce sound security hygiene and force companies to cover the basics, is essential to prevent security incidents and reduce the impact. This gap is partially closed in the Dutch financial sector by DNB as it has made progress on this topic since 2010.

[100] *In the Netherlands banks have a distinction between corporate accounts and consumer accounts. This thesis takes the perspective of consumer accounts.*

Since then it developed a high-level framework on information security[101] and a self assessment tool on the maturity level of security at financial institutions. However this framework has only been verified at a subset of financial organisations through a self-assessment tool. It is not clear if this will be useful and applicable for TPP's as well and if a self-assessment way of supervision will be sufficient. Relying on FinTech companies to arrange the proper security themselves is likely to fail as argued in section three. DNB is also limited in resources and appointing the NCSC as a supervisor will make more resources available which should improve supervision of security.

TPP's should also be aware that they will create a concentration of financial information and payment data. Centralising financial information at TPP's can make them an interesting target for adversaries, being either criminal or state-sponsored. This concentration and the associated value of payment data are good drivers for demanding a high security level and a dedicated supervisor on security for the financial sector, including TPP's and banks.

In the PSD2 a focus is placed on strong customer authentication. Although this is an improvement on the current level of authentication of online applications, it is also clear from publications [102] that strong customer authentication is already being bypassed by malware attacks. That is why this control should not be considered as a single final solution, but it is merely one of multiple controls. Another important control is fraud monitoring, which is a general control that can adapt. Because of its ability to adapt fast and without significant additional costs, it will endure longer, even after other controls have been defeated. Authentication means have changed and evolved as well, however those changes take more time and cost significantly more than monitoring because it impacts both customer experience and the IT systems. However, fraud monitoring didn't get as much attention and detail in the PSD2 as strong customer authentication did. The PSD2 only states that TPP's should have fraud monitoring in place. Having proper fraud monitoring reduces the risk for customers and it should have gotten the same attention level in the PSD2. This could be repaired by giving it the proper attention in the coming Regulatory Technical Standards which are to be drafted by the EBA.

How is the Dutch governmental supervision of third party payment service providers (TPP's) arranged in the light of the revised Payment Services Directive (PSD2), ***and does that supervision incorporate the prevention of the abuse of data (data protection).***

Supervision on data protection in the Netherlands is arranged and executed by the AP. As TPP's will be processing personal information, data protection is also applicable to them. However, there are some concerns about the scope and the effectiveness of this supervision. The scope of the AP is influenced by the behaviour of the customer itself. Once customers accept the terms of services, TPP's are legally allowed to use their data, and this positions TPP's beyond the reach of the AP. The concern of effectiveness is related to the staffing of the AP. Its staffing hasn't been keeping pace with the increased importance of online services and the dependence on them by large portions of society. This means that online services used to be a small portion to supervise, but over time have become the major topic and therefore should be equally matched in resources. Too many incidents remain out of reach of the AP because of this lack of resources. This diminishes overall supervision on data protection.

So in conclusion, the supervision that is mandated in the PSD2 is not sufficiently arranged in the Netherlands yet and creates a gap in supervision of future TPP's on the topics of security and data protection.

---

[101] *Toetsingskader Informatiebeveiliging voor DNB thema-onderzoek 2014 (DNB 2014)* http://www.toezicht.dnb.nl/3/50-203304.jsp

[102] *Malware bypasses 2-factor authentication* http://www.bankinfosecurity.com/malware-bypasses-2-factor-authentication-a-7090/op-1

6.2 Recommendations

This paragraph will present and briefly discuss recommendations for supervisors and TPP's to address the most important challenges, and thereby answer the third minor question from section one.

How is the Dutch governmental supervision of third party payment service providers (TPP's) arranged in the light of the revised Payment Services Directive (PSD2), and

(i) does that supervision incorporate the protection against abuse of access (security),
(ii) does that supervision incorporate the prevention of the abuse of data (data protection)
(iii) if any issues occur at i or ii, provide recommendations to improve supervision.

Although some recommendations have a broad scope and are generally applicable, they are given from a PSD2 and TPP perspective. Since the PSD2 is new development and TPP's are a new participant of the financial system, much is unclear now, but these recommendations are also general so they will still remain valuable whichever direction the Dutch development of the PSD2, PAAS and TPP's goes.

RECOMMENDATION 1 - APPOINT THE NCSC AS THE NATIONAL SUPERVISOR ON SECURITY
Similar to data protection, security is a generic aspect of information systems and is gaining importance. For data protection a dedicated supervisor – Autoriteit Persoonsgegevens (AP) – is established along with enforcement powers. I propose to appoint an official national supervisor on security, which should get a similar status as the current supervisor on data protection so it can enforce a minimal security level and impose fines on those companies that do not comply. Since the National Cyber Security Center (NCSC) will become the national competent authority on security, it only seems obvious to let it become the supervisor on security in the Netherlands as well. This will also create the possibility for DNB to transfer their work on information security and focus on its core topics.

RECOMMENDATION 2 - INTRODUCE A MANDATORY DATA PROTECTION OFFICER
The lack of resources and the reactive approach of the AP could be compensated by empowering TPP's with a mandatory and dedicated Data Protection Officer. This is already partially envisioned in the GDPR. It will not only relieve the pressure on the AP, but it will also enhance the overall data protection coverage at companies in the Netherlands. Assigning a DPO at every company will provide a more complete overview on all data processing, because the main task of the DPO is to collect and report any processing of personal data within their company. The DPO has an independent role and holds a formal legal position. (S)he is therefore not controlled by the executive management, so they cannot interfere with their work. Finally the DPO should be very close to the business to monitor possible changes in products and services that might interfere with the appropriate use of data. In the Netherlands a DPO is merely an option and companies should be forced to use this option. As good data protection starts with the earliest designs of products and services (data protection-by-design), it is recommended that the DPO is appointed quick after the establishment of a company or when a company starts developing services. This could slow down the product development, especially for start-up companies, but it could increase the level of data protection significantly.

RECOMMENDATION 3 - INTRODUCE A MANDATORY INFORMATION SECURITY OFFICER

Similar to the DPO, legislators should consider developing a formal Information Security Officer (ISO) role with the same legal status as a DPO. As stated earlier, information security is also very important to run services securely. A common way to control this in companies nowadays, is to appoint an ISO. Leveraging this role to a formal and independent status will provide the same benefits as the DPO. This will most likely benefit the security at companies and thus also at TPP's, and it will reduce the pressure on the new supervisor on security, the NCSC. As good security starts with the earliest designs of products and services (security-by-design), it is also recommended that the ISO is appointed quick after the establishment of a company or when a company starts developing services. This could also slow down developments at FinTech start-ups as stated in the previous recommendation.

RECOMMENDATION 4 - STRENGTHEN COOPERATION BETWEEN SUPERVISORS

There should be more coordination between supervisors from the moment a TPP applies for a license. A potential set-up could be that De Nederlandse Bank (DNB) takes the lead at the start of the license application. It would asses the traditional requirements and check the organisation and its people on integrity. In addition, it should request assistance from the AP on the aspect of data protection, and assistance from the NCSC on the aspect of security. The Autoriteit Consument & Markt (ACM) should be consulted on the terms of services. In this way, all supervisors will leverage their own strengths at a single point. Since DNB acts as a gate keeper through its license procedure, this set-up can prevent gaps in supervision, even before these TPP's start servicing their customers.

RECOMMENDATION 5 - SIMPLIFY THE TERMS OF SERVICES

Terms of services are the legal base for providing services and explain in detail what companies are really doing with customer data. Because this is a mandatory document and it is legally binding, it tends to be very long and complex. Therefore customers do not read it and so they don't know what obligations and rights derive from that. This issue is becoming more important as technology companies increase the use of data, but also because that data is reaching a more personal level (financial data). A recommendation to overcome the complexity and size of these terms of conditions is ToS;Dr (tosdr.org). The acronym stands for Terms of Services; Didn't Read, and it expresses the behaviour that the majority of customers are showing nowadays. The idea is simple, let knowledgeable people – legal expert opinions – score the terms of services of companies on issues of security and data protection. These are then reduced from 80 pages to several bullets. Experts rate and label the terms of services and data protection statements. The rate they can give is from very good (Class A) to very bad (Class E). Examples of labels are that a company doesn't actually delete data, but renders it inaccessible, or that the copyright license is broader than necessary resulting in the opportunity for companies to use the data for their other, possibly commercial purposes. Since the ACM is positioned to protect the interests of consumers I recommend that the ACM should take the lead in promoting ToS;Dr in the Netherlands.

6.3 Personal opinion

This paragraph will present the author's personal opinion on the PSD2 and Payment Account Access Services (PAAS). This opinion is about the biggest risk of PAAS and about a more strategic side-effect of the PSD2 on corporate competition.

With the introduction of the PSD2 and access to accounts, valuable financial information will reside outside the protected framework without sufficient supervision. The biggest risk with the introduction of the PSD2 and TPP's will be the abuse and illegal use of financial data. Major technology companies already have access to a lot of data, such as search terms, blogs and social connections. The author's main concern is that access to financial data – data that describes consumers behaviour and not only intentions and interests – will allow these companies to develop highly precise profiles. It will provide those companies the ability to choose the information shown to consumers, and derived from that, influence the choices consumers make. This means these companies can better predict and steer what people want, when they want it and how they want it. But do people know that they are being conditioned this way and would they still use their services if they would actually understand this? Also the trend of FinTech seems promising but holds a great risk. A lot of startup companies are likely to fail and have a focus on added value and not on security or data protection. With a high fail rate of those companies, financial data is likely to end up in unexpected places as consumer data will be sold to the highest bidder when it fails. Startup companies also tend to focus on customer experiences and aim to maximise their user base. This is to manage their exit strategy so they can cash in on their investment. Having proper security and data protection controls will slow down their development and is counterproductive, and will most likely will be left undeveloped. Therefore it remains to be seen if FinTech startups can and will match the high standard of security and data protection which financial data needs. Instead of opening up the access all at once it would have been better to gradually allow access for those technology companies and gain experience with it and the ability to control this development.

The author thinks the abuse and illegal use of data is possible for two reasons. Companies deceive customers through the use of an uninformed consent or a silent consent which is based on long and complex terms of services. Customers don't know what data will be gathered by a TPP or what that data will be used for. They are given the relevant information, but they aren't able to comprehend it. This is often because terms of service are deliberately being obfuscated by companies to hide their real goals and intentions. The second reason is that the control to counter this, supervision, is not adequately equipped with resources and will need to settle for less protection of consumers. So in conclusion, consumers often do not know what data is being gathered and for what purposes, and supervisors cannot control or supervise the use of it to the extent needed. With the PSD2 and PAAS banks will be forced to add more valuable data to the system, which will provide the opportunity to others to abuse it without any repercussions.

On a more strategic level, the enforced "one-way" sharing of financial data will weaken European companies and will strengthen non-European information giants. The PSD2 forces European banks to open up their systems and allow the access of other, FinTech startups companies to develop new services based on consumer data or the ability to initiate a transaction. Major technology companies will also be given this opportunity – they have the ability (money and technology) and the possibility (PSD2) – to acquire payment data and monetise that. This seems more beneficial for the major technology companies or information giants than for the banks. This is because these giants will be able to create the most complete profile of a customer based on search, social and soon, financial data. This puts them in the top position of the information value chain. However, in the other direction, banks cannot acquire the data of those giants since the PSD2 only forces banks to open their systems, and doesn't force information giants to open up their systems. The key point here is that by allowing third party access, several major global information giants are more likely to benefit from the PSD2 than European banks. It is ironic that the European Commission is undermining their own European banks with the PSD2 and at the same time supports the already dominant non-European technology and information giants.

Appendices

Appendix 1 Transaction analysis

In order to get an impression of the types of information that will become available for TPP's based on Account Information Services (AIS) services, a small experiment[103] has been conducted. Banks often offer the possibility to download the history of payments in a common format such as comma separated. For this experiment a payment statement was downloaded from a single account number for a 15 month period. The relevant fields in the data set are the timestamp, account number, beneficiary account number, description and amount. Below are some remarkable types of information that are available in this data set. They are categorised around several topics, such as personal identifiable (PII), medical, location, behavioural and social information. In addition to the information found in the data set, an associated threat for each type is provided as well.

Personal identifiable information - Names and addresses

A single account can hold multiple identities through the use of multiple debit cards. In the Netherlands it is quite common to have a so-called "en/of" account. Multiple persons share an account to which they have access. By stating the card sequence number in every transaction, different patterns can be seen for each card. This will reveal multiple identities on a single account. Several transactions to saving accounts reveal the entire structure of a family, including the number of children. Also the home address is visible within the description of several transactions.

Threats that could be associated with this are targeted marketing, not only aimed at adults but at children as well. The home address in combination with account balance could be interesting for burglars under the assumption that more money online, relates to more expensive goods offline. Finally, social engineering becomes easier since there is more information available about the account holder(s).

Personal identifiable information - Social security number

To collect taxes, the government either receives payment by citizens or refunds citizens. Refund transaction contain the social security number – in the Netherlands also known as the Burger Service Nummer (BSN) – and is visible in the description. This number is used to identify citizens for all kinds of purposes, especially when dealing with governmental departments and services. Its use and storage are strictly regulated.

Once a fraudster gets hold of the payment data, they also know the social security number which (s)he could use to commit identity theft, followed by fraud[104]. A second issue could arise because of the strict rules which apply when working with social security numbers. So if the TPP decides to use the social security number, for example as an userID, this would violate the more strict data protection rules.

[103] *This experiment has been conducted by the author on his own payment data (n=1) and is meant to illustrate what types of data might be available. It should not be seen as statistically relevant and in order to achieve statistical relevance a larger population should be used.*

[104] *Burgerservicenummer (BSN) (College Bescherming Persoonsgegevens 2015)*

Personal identifiable information - Credit card numbers

Credit cards are not the main payment method in the Netherlands, but they are owned and used by a reasonable size of the population. Each month the spending of the card are settled with the regular account. In that settlement the credit card number is visible.

Credit card information is usually stolen through malware on Point Of Sale (POS) terminals, along with the expiry date and the security code, and then sold in the underground economy. The payment data only shows the credit card number and this will limit the threat, because a fraudster also needs the expiry date and the security code to complete a transaction. This information is on the card and not in the payment data.

Personal identifiable information - License plate numbers

In the Netherlands citizens have to pay taxes to be allowed to drive a car on the road. The collection of those taxes is also in the payment data which shows the number plate as a reference. From public records of the Rijksdienst Wegverkeer (RDW) more information can be collected on the car such as the original price and the number of seats.

From the house address and the license plate, someone could start following people, even when they use their car and start travelling. For example when a stalker buys this information on their victim. Also the value of the car can be estimated, which in some cases could be interesting for thieves. For example this could be the case with very rare, old or expensive cars.

Financial - Income

A primary account is almost always used to receive the wages from the employer. A list of all credited transactions will provide an overview of the amount of money which is coming in. This makes clear what the total income is and at what company the account holder works.

The employer could be of interest to several types of criminals or intelligence agencies. The income combined with spending could reveal leverage points for extortion or blackmail.

Financial - Spending categories

All spending can be categorised, and identifies the preferences of the account holder in terms of favourite shops, food, energy, sporting clubs, etc. . The way people spend their money provides a very detailed description of them. One example would be on how much someone spends on their house. Mortgages are loans that need to be paid back with interest to the bank that provided them. From the payment of interest one could determine the total amount of the mortgages that the account holder has and related to that the value of the property they are currently living in. In essence a wealth calculation is possible.

As the spending provides a very detailed description of your interests, habits and travels it allows for targeted social engineering and advertisements. The key element here is that payment data does not only reveal intentions, but also actual behaviour.

Special - Medical

The increasing trend of online shopping for medicines is visible in payment data. From these medical purchases several causes could be deduced that have resulted in this purchase. But also a transaction to a personal coach on food could lead to the conclusion that the account holder is under the impression that (s)he has a problem with their weight.

Health insurance companies could use this information to discriminate between healthy and non-healthy customers and ask them different fee's for their insurance.

Special - Religion

A transaction has been identified that was done to a religious institution. From that, the religion of the account holder can be determined which is special type of personal information.

No specific threat can be associated with it at this time, but religion seems to a driver on the terrorists attacks in Paris in 2015 and in Brussels in 2016.

Location

The transaction description also holds location information on where that transaction has taken place. This holds for Automated Teller Machines (ATM's) but also for Point of Sale (POS) terminals. With a reasonable amount of transactions within the data set a certain pattern of life can be established. This pattern shows places that someone visits frequently and might predict where someone will travel in the near future.

As travels provide a very detailed description of someone's whereabouts, it allows for targeted social engineering and even a planned burglary when nobody is at home. Figure 5 shows an example of the location analysis.

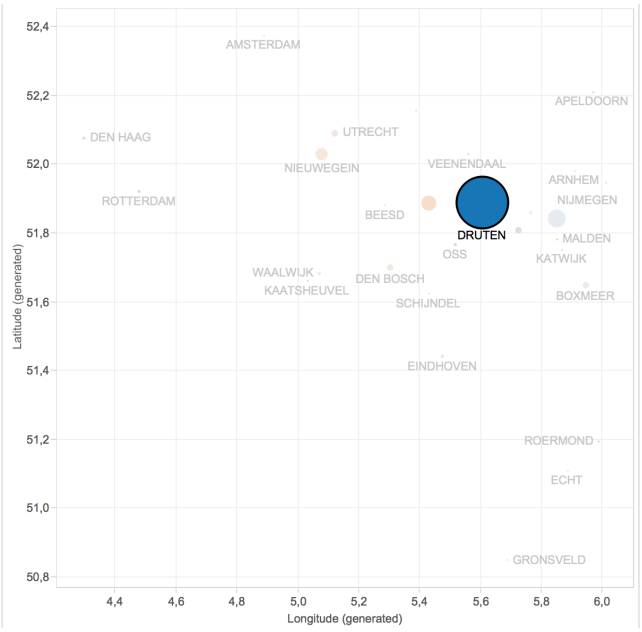

Figure 5: This figure shows the geographic location deduced from the transaction descriptions. Different colours mean different locations either being a city or a village. The size is the number of occurrences. As Druten is the largest shape it should be clear where the author lives.

Behavioural

In this set several important life events happened which were recorded through transactions. For example a reference was found to a marriage. Most likely one of the two identities in this data set got married.

There was also a credit transaction from an insurance company which noted a refund caused by a burglary. Furthermore It can also be seen that an identity is receiving an education at a university and finally, someone went skiing.

As your behaviour provides a very detailed description of your habits it allows for targeted social engineering and advertisements.

Social

Most transactions are business to consumer and vice versa. However a limited number of transactions are consumer to consumer. From those transactions a social network can be created. In this data set several identities become visible from consumer to consumer transactions. From the number of transactions and/or associated value one could derive the intensity of that relationship. When we assume that more transactions or more value in those transactions resemble a more intense relationship, a graph can be drawn to visualise the social connection, and this information might also be an indicator for emotional distance (family, friends, co-workers, acquaintances and online buyers through eBay).

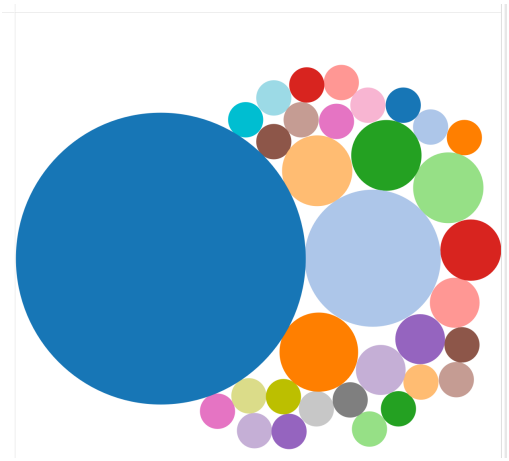

Figure 6: This figure shows the different identities by colour that were extracted as a beneficiary from the transaction history. The size is the number of occurrences. The largest identity is the account holder, the second largest a first degree family member and the third a very close friend.

Knowledge of the social connections allows for targeted social engineering since the consumer has placed a certain trust in the counter party based on the prior successful transaction. When the fraudster uses such a known and trusted identity, the victim will lower the natural safeguards and the chances of success increase.

Appendix 2 Interview of supervisors

Supervisor	**Date**	**Form**
De Nederlandse Bank	18-09-2015	On-site
Autoriteit Consument & Markt	14-10-2015	Telephone
Autoriteit Persoonsgegevens	08-09-2015	On-site
National Cyber Security Centre	30-10-2015	E-mail

Appendix 3 AIS and PIS issues related to supervisors

In this table the identified issues from section three are plotted against the identified supervisors from section five.

	DNB	***AP***	***ACM***	***NCSC***
AIS Issues				
Negative public opinion on the use of payment data for commercial purposes	V		V	
Who authenticates, the customer or the TPP?	V			
Abuse of payment data		V	V	
Data breaches				V
PIS Issues				
Abusing fraud monitoring as data processing purpose for monitoring everything		V		
Defense against classic cybercrime threats (phishing & malware)				V
Autonomous PIS services	V			
Circumventing compliance controls with PIS	V			

Bibliography

Philip Irwin, *How many gigabytes of data were in the Library of Alexandria?*(2015), *available at* https://www.quora.com/How-many-gigabytes-of-data-were-in-the-Library-of-Alexandria.

Randall Munroe, If all digital data were stored on punch cards, how big would Google's data warehouse be?(2013), available at https://what-if.xkcd.com/63/.

United Nations, UN projects world population to reach 8.5 billion by 2030, driven by growth in developing countries(2015), available at http://www.un.org/apps/news/story.asp?NewsID=51526.

Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System(2008), available at https://bitcoin.org/bitcoin.pdf.

European Data Protection Supervisor, *Definition of data protection*(1995), *available at* https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Dataprotection.

European Data Protection Supervisor, Convention for the Protection of Human Rights and Fundamental Freedoms (1950).

Study on the impact of directive 2007/64/EC (PSD1). (2013).

European Commission, Proposal for a regulation of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulatio (2012).

European Commission, Proposal for a directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union (2013).

Paul Jennekens, *SEPA, How it all started*, Equens. History of SEPA (2012), *available at* http://blog.equens.com/eu/2012/09/sepa-how-it-all-started/.

European Commission, Regulation No 924/2009 of the European Parliament and of the Council on cross-border payments in the Community and repealing Regulation (EC) No 2560/2001 (2009).

European Payments Council, *About EPC*(2002), *available at* http://www.europeanpaymentscouncil.eu/index.cfm/about-epc/role-of-the-epc-in-the-sepa-process/.

European Commission, *Directive 2007/64/EC (PSD1)*(2007), *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32007L0064&from=EN.

European Commission, *The Payment Service Directive - What it means for consumers*. Consumer brochure on Payment Services. (2010), *available at* http://ec.europa.eu/finance/payments/docs/framework/psd_consumers/psd_en.pdf.

Lorrie Faith Cranor Aleecia M. McDonald, *The Cost of Reading Privacy Policies*, (2008).

Rijksoverheid Nederland, Wet financieel toezicht (2015).

Rijksoverheid Nederland, Algemene bestuurswet (2015).

Rijksoverheid Nederland, Wet bescherming persoonsgegevens (1995).

De Nederlandse Bank, *Payment institutions: Cross-border services*(2012), *available at* http://www.toezicht.dnb.nl/2/50-224497.jsp.

European Commision, Revised Payment Services Directive (2015).

European Commission, Data Protection Directive 95/46/EC (1995).

A. Weber, *See What You Sign: Secure Implementations of Digital Signatures*, Proceedings of the International Conference on Intelligence and Services in Networks (1998).

DNB, Opvattingen van nederlanders ten aanzien van het gebruik van betaalgegevens door banken en andere partijen, (2015).

CBP, *CBP onderzoekt nieuwe privacyvoorwaarden Facebook*(2015), *available at* https://cbpweb.nl/nl/nieuws/cbp-onderzoekt-nieuwe-privacyvoorwaarden-facebook.

Rechtbank Midden-Nederland, Vonnis in kortgeding van 30 juli 2014 AFAS v.s. ING § ECLI:NL:RBMNE:2014:3250 (Rechtbank Midden-Nederland 2014).

2015 Data breach investigations report. (2015).

Expert Market, *Online payment methods in Europe*(2015), *available at* http://www.expertmarket.co.uk/sites/default/files/filemanager/Payment_methods_online.

Currence, *Betalen met iDEAL*(2015), *available at* https://www.ideal.nl/betalen/.

Sofort, *Zo werkt Sofort*(2015), *available at* https://www.sofort.com/dut-NL/consumenten/sb/sofort-banking-werkwijz/.

NVB, Factsheet Veiligheid en fraude (2015).

Finding regarding the market events of May 6, 2010 (Flash Crash). (2010).

European Commission, Proposal for a regulation of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (2012).

European Commission, Proposal for a directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union (NIS) (2013).

CBP, *Functionaris voor de gegevensbescherming*(2016), *available at* https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/functionaris-voor-de-gegevensbescherming.

Court of Justice of the European Union, Judgement in Case C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González (2014).

Eerste kamer der Staten Generaal, Meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid CBP, (2015).

National Cyber Security Center, Over het National Cyber Security Center(2015), available at https://www.ncsc.nl/organisatie.

ISO, *ISO/IEC 27001 - Information security management*(2013), *available at* http://www.iso.org/iso/home/standards/management-standards/iso27001.htm.

European Banking Authority, *About the EBA*(2015), *available at* http://www.eba.europa.eu/about-us.

An Analysis of the Financial Crisis of 2008: Causes and Solutions. (2008).

European Central Bank, Public note on security of payment accounts access services, (2014).

Final Recommendations on the security of payment accounts access services. (2014).

De Nederlandse Bank, *Over DNB*(2015), *available at* http://www.dnb.nl/over-dnb/index.jsp.

College Bescherming Persoonsgegevens, Over het College Bescherming Persoonsgegevens(2015), available at https://www.cbpweb.nl.

CBP, Richtsnoer Beveiliging persoonsgegevens (2013).

Autoriteit Consument en Markt, *Over de Autoriteit Consument en Markt*(2015), *available at* https://www.acm.nl/nl/organisatie/missie-visie-strategie/onze-missie/.

Rijksoverheid, Instellingswet Autoriteit Consument en Markt (2013).

College Bescherming Persoonsgegevens, *Burgerservicenummer (BSN)*(2015), *available at* https://cbpweb.nl/nl/onderwerpen/identificatie/burgerservicenummer-bsn.

TNO, Marktrapportage Elektrosniche Communicatie 2014, (2014).