UiO : Faculty of Law
University of Oslo

Payment Services Directive: a better consumer protection in mobile payments

Candidate number: 8005

Submission deadline: 15 May 2015

Number of words: 14400

Table of contents

1 Introduction

Mobile payments and electronic payments have become one of the most important factors in the growth of electronic commerce and e-government application. Mobile devices have radically changed everyday business and consumer life in the field of communication. Mobile phones have achieved full market penetration and rich service levels, making them an ideal channel for payment instruments. At the same time, the mobile payments ecosystem continues to grow and mature rapidly. For stakeholders in the payments industry, it is important to have a good insight into the latest trends within mobile payments and market developments.[1] Consumers have changed significantly their payment habits over the recent years. Mobile devices such as mobile phones are being used worldwide and as a result the consumer is becoming a dependent user of different types of mobile payments systems. Apple, Google and Visa have entered a significant mobile payment initiative in the m-payment business. The financial transactions are made to look easy to process. The use of mobile phone as a wallet or as credit cards have made it even easier to make such transactions. The result of such expansion of e-commerce the consumers are increasingly exposed to various types of cybercrime. Thus e-commerce has massive potential to boost the economy the increasing use of mobile payments raises concerns, including dispute resolution, data security, and privacy. The increase the use of mobile payments are influenced by many factors and different undertakings who see it as a lucrative, unexploited area. Mobile network operators (MNOs) seeking to increase customer numbers, financial institutions, retailers and regulators are all players who are interested in having mobile payments fully integrated into customer's everyday life.

At present, 28% of internet users across the EU are not confident about their ability to use the internet for services like online banking or buying things online. When using the internet for online banking or shopping, the two most common concerns are about someone

[1] http://www.europeanpaymentscouncil.eu/index.cfm/newsletter/article/article.cfm?articles_uuid=DC733ECC-5056-B741-DB33B039AC437E16

taking or misusing personal data (mentioned by 37% of internet users in the EU) and security of online payments (35%).[2]

It is clear that although big advances continue to be made concerning the security of electronic payments, that is not enough on its own. Consumers need to be convinced that electronic payments are no hassle.[3] The cyber security is at the center of European public debate and has become a top priority on the agenda of European legislative bodies. As a result the legislators of the EU are proposing a new legal framework which should provide for the necessary legal certainty for both market players and users.

1.1 Problem

The EU has indicated that in order to ensure *'a better customer protection'* one of the main factors is that these customers must have more trust in mobile payments. However the question is whether it is what the customers really need. According to Ofcom, it is. The use of a mobile payments raises a number of privacy concerns and large amount of undertakings are involved in the process. Despite the increase of mobile transactions the security and privacy concerns might be holding back the global mobile payments market. The Ofcom's International Communications Market report has concluded that the mobile payments market growth has been "relatively low" compared to the mobile banking market in the UK and across other countries.[4] The reason for that is that many consumers across the world have concerns regarding the security of payments made via mobile devices and that the privacy of their personal data had put them off making payments on their own mobile devices. Major data loss issues surrounding such global actors as Paypal have driven many consumers to be suspicious about giving their bank account details to private actors of e-commerce.

---

[2] EU Commission (2013), *Special Eurobarometer 404 – Cyber security*, p. 52, at

[3] IP/03/1265, Electronic payments: Commission conference and study highlight security issues and assess public perception, Brussels, 18th September 2003, http://europa.eu/rapid/press-release_IP-03-1265_en.htm?locale=en

[4] Ofcom, International Communications Market Report, 11 December 2014, http://stakeholders.ofcom.org.uk/binaries/research/cmr/cmr14/icmr/ICMR_2014.pdf

"Our consumer research suggests that the convenience of other payment methods, and concerns about security and privacy, are among the main reasons why those with mobile phones have never made a mobile payment. With the exception of Italy (28%) and Japan (22%), between 36% (in France) and 51% (in China) of non-users across the comparator countries cited security concerns as reason for not making mobile payments."[5]

It should also be noted that in the EU to keep data secure is an essential component of citizens' fundamental right to privacy and failure to ensure security of personal data is enough to breach Article 8 of The Universal Declaration of Human Rights.[6] The Human Rights Court in *I v Finland* concluded that the right to sue for the unlawful disclosure of information is not sufficient protection and that it is "*required to have practical and effective protection to exclude any possibility of unauthorized access occurring*".

The recent news headlines show the problems which third-party payment providers may encounter as even sophisticated security systems can be "hacked" and valuable data acquired by someone who is not supposed to possess it. In 2015 February a news website *Intercept* alleged a hack of the French-Dutch digital security giant and mobile phones SIM card maker, Gemalto, who later admitted that "allegedly" American and British intelligence services were behind a "*particularly sophisticated intrusion*" of its networks several years ago. However Gemalto denied that the alleged hack could have widely compromised encryption it builds into chips in billion mobile phones worldwide. Gemalto claimed to have done a "*thorough*" investigation and that hacks only affected "*the outer parts of networks*". [7] It is yet to be seen if the intrusion did not affect the SIM-cards which most likely could have been the goal. It is important to note that among other services Gemalto is also providing *"proven mobile payment platform, […] which […] offers consumers a*

[5] Ofcom, International Communications Market Report, 11 December 2014, http://stakeholders.ofcom.org.uk/binaries/research/cmr/cmr14/icmr/ICMR_2014.pdf

[6] European Court of Human Rights case I v Finland [2008]

[7] http://www.wsj.com/articles/gemalto-says-hack-didnt-result-in-massive-theft-of-sim-card-keys-1424851298

digital wallet that increases spending, loyalty and engagement".[8] In 2014 Telenor Norge, DNB and Sparebank1 partnered with Gemalto and launched the first NFC wallet in Norway which uses Gemalto's certified secure data centers, ensuring banking-grade security for NFC payments.[9] This can be a huge drawback for the *"spending and loyal"* customers relying on mobile payment systems. The world has been shown again that the security systems even of sophisticated undertakings, who deal with security itself, can be hacked, and as a result a lot of personal information can be accessible to those who may misuse such information.

Thus, what is the 'better consumer protection' for a consumer himself? It is reasonable to say that security is one of the higher priorities for customer in order to make internet or mobile payments. As shown case of Gemalto, even the hardest security can be breached. Therefore, a better consumer protection should also cover situations where fraud was committed. European Central Bank in its '*Third Report on Card Fraud'* revealed that the total value of fraudulent transactions conducted using cards issued within SEPA and acquired worldwide amounted to €1.33 billion in 2012, which represented an increase of 14.8% from 2011.[10] Therefore, the consumer should know what are consequences for a fraudulent transaction on his bank account.

1.2 Purpose of the study

The European Commission claims that they are bringing a "better consumer protection" by introducing PSD2 and Interchange Fees Directive. Therefore the purpose of the thesis is to see whether the new legislation has the potential to give the better protection to a consumer. The legal discussion will be based around PSD2 and Interchange Fees Regulation, and most of other laws regarding the Data Protection will be only discussed

[8] http://www.gemalto.com/mobile/mcommerce/mfs/mobile-payment

[9] Norway goes with Gemalto Trusted Service for mobile NFC payment commercial rollout, http://www.gemalto.com/press/Pages/Norway-goes-with-Gemalto-Trusted-Service-for-mobile-NFC-payment-commercial-rollout.aspx

[10] European Central Bank, Third report on card fraud, http://www.ecb.europa.eu/pub/pdf/other/cardfraudreport201402en.pdf, page 4

briefly because this is a broad area of law and therefore requires a separate piece of research.

1.3 Questions

The thesis is asking whether the PSD2 together with Interchange fees Directive is providing consumer with a better protection. The thesis also trying to identify what is a better customer protection.

2 Methodology

As a main method for the research the documentary analysis is used. The information used is obtained from the existing legal sources. The thesis is based on the research of various written texts on the subject will be utilized and an analysis of any existing literature and legislation. The legal texts used in this thesis include journals, reports, articles, presentation papers, and textbooks.

The research is analyzing the upcoming Directives and Regulations therefore in order to get information about it, the internet resources will play a crucial role. The publications from the European Commission will be a key in determining the current state and development of the laws which are relevant to the topic. Since the laws are under consideration at the time of this thesis writing process, some of the sections of the relevant laws can be already amended.

3 Mobile Payments

Mobile payments have become a more integral part of payments system. The recognition that it must have its on place in European regulatory framework is crucial for the future of innovation and mobile payments in Europe.

"A digital single market cannot function without a framework for trustworthy online payments. This framework must include mobile payments, across Europe, and be built on reliable interoperable systems. The protection of personal data, which come about in such

online transactions, and the ability to preserve private information are of major importance to guarantee trust in an online single market."[11]

3.1 What are mobile payments ?

Laurent Bailay and Bernard Van der Lande propose to define a mobile payment as a "payment for products or services between two parties for which a mobile device, such as a mobile phone, plays a key role in the realization of the payment".[12] In the European Commission's Green Paper[13] the mobile payments are described as payments for which the payment data and the payment instruction are initiated, transmitted or confirmed via a mobile phone or device. This can apply to online or offline purchases of services, digital or physical goods. Mobile payments can be classified into two main categories:

1) Remote m-payments mostly take place through internet/WAP[9] or through premium SMS services which are billed to the payer through the Mobile Network Operator (MNO). Most remote m-payments through the internet are currently based on card payment schemes. Other solutions, based on credit transfers or direct debits, are technically feasible and possibly as secure, efficient and competitive, but seem to have difficulties entering the market.

2) Proximity payments generally take place directly at the point of sale. Using Near Field Communication (NFC), the leading proximity technology at this stage, payments require specifically equipped phones which can be recognized when put near a reader module at the point of sale (e.g. stores, public transport, parking spaces). This method uses "tap and go" which enables NFC phones communicate with each other and with NFC enabled points of sale, using radio frequency identification. The mobile phones do not have to touch the point of sale or each other to transfer information, i.e. money, but they have to be fairly close within four inches/ten centimeters of each other. Such technologies

[11] Viviane Reding, BEUC multi-stakeholder Forum on "Consumer Privacy and Online Marketing: Market Trends and Policy Perspectives", Brussels , 12 November 2009

[12] Bailly, L.; Van der Lande, B. (2007). Breakthroughs in the European Mobile payment market, White paper, Atos Oringin

[13] European Commission, GREEN PAPER Towards an integrated European market for card, internet and mobile payments, page 5, http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52011DC0941

create the room for "mobile point of sale" (mPOS) abilities where the payment transaction can be executed through a consumer's mobile device.

These definitions, in particular for remote m-payments, suggest that the line between e payments and m-payments is blurred, and may become even more so in the future.

This thesis will target electronic payments initiated through a mobile device. According to European Central Bank, payments initiated through mobile phones etc. are called mobile payments. They are a sub-group of electronic payments.[14]

Despite the convenience of mobile payments there remain some barriers for its expansion. There can be many factors discouraging customers to make a mobile payment. The main factor is fear amongst customers as they are not sure whether the payment is secure. Only one quarter of all respondents think that mobile payment are 100% secure. There is also concern that personal information could be compromised by mobile payments. More than one half of the respondents worry about this when using a mobile payment app. Another factor which is precluding customers from making mobile payments is a lack of adoption of the technology by merchants. One third of consumers would like to make more mobile payments but are prevented from doing so by the small number of merchants offering it.[15] The PSD2 seems to address some of these issues by introducing stronger customer authentication and capping interchange fees. As shown above the data protection is one the biggest concerns, nevertheless the PSD2 is vague on this point, and in addition to that potentially increase the risk of leakage of personal data.

4 EU Mobile Payments Regulatory Framework

In Europe, most mobile payment transactions are covered by the Payment Services Directive and the E-money Directive. The Payment Services Directive requires, among

[14] E-Payments without Frontiers; Issues Paper for the European Central Bank Conference on 10 November 2004, Page 7.

[15] GfK, *GfK's proprietary survey of shopper attitudes and behaviors*, FutureBuy 2014

other things, consumer authentication and authorization procedures before the individual transactions take place, limitations on consumers' liability when using the service, and standard terms covering the parties' contractual duties and liabilities regarding the unauthorized use of financial services. However, there are exceptions to the application of these directives, and there is no other legislation or regulation for transactions that fall outside of the scope of these directives. This is seen as a problem by many European respondents that favor equal protection for mobile and card-based payments. This chapter will discuss the current framework that mobile payments in the EU are regulated by.

4.1 SEPA

"*[A]n integrated market for payment services which is subject to effective competition and where there is no distinction between cross-border and national payments within the euro area*" thus calling "*for the removal of all technical, legal and commercial barriers between the current national payment markets*"[16]

The Single Euro Payments Area (SEPA) stands for a European Union (EU) payments integration initiative. With the introduction of the euro currency in 1999, the political drivers of the SEPA initiative - EU governments, the European Parliament, the European Commission and the European Central Bank (ECB) - have focused on the integration of the euro payments market. Since then, the political drivers have called upon the payments industry to bolster the common currency, by developing a set of harmonised payment schemes and frameworks for electronic euro payments.

- Integrating the multitude of existing national euro credit transfer and euro direct debit schemes into a single set of European payment schemes is a natural step towards making the euro a single and fully operational currency.
- Creating a SEPA for cards aims at ensuring a consistent customer experience when making or accepting payments with cards throughout the euro area.

[16] Press release: Joint statement by the European Commission and the European Central Bank, 4 May 2006

- The SEPA programme seeks to incentivise increased use of electronic payment instruments, while reducing the cost of wholesale cash distribution.
- The European authorities driving the SEPA process have clarified that migration to harmonised SEPA payment schemes and technical standards does not conclude this EU integration project. In a next step, the regulators expect further harmonisation in the area of mobile and online payments.

The jurisdictional scope of the SEPA Schemes currently consists of the 28 EU Member States plus Iceland, Norway, Liechtenstein, Switzerland, Monaco and San Marino. [17]

The payments market is heavily dependent on strict communication standards between agents involved in the market. Therefore, SEPA can first and foremost be viewed as being a standardization initiative. Nevertheless, it must be further emphasized that a unified payments area was originally a political undertaking to which SEPA can be viewed to be a response by the industry in order to meet the political aspirations behind the regulation.
Integration within the European retail payments market has been evident when looking at the past 10 years. While it can be questioned whether all this is due to SEPA, it is very likely that a significant portion of this change is attributable to the aims and ambitions behind the initiative. SEPA would appear to hold the potential for creating a harmonized competitive payments market with the possibility of becoming an innovative platform for future payments related development.

The passage of the Payment Services Directive (PSD) by the European Parliament and the EC is an essential step towards a consistent legal framework for payments hence introducing much improved certainty and clarity to the SEPA project.[18] However, as will be seen, the scope of the PSD is not limited to SEPA transactions but is relevant for all payments in all EU currencies within the EU 27 from 1 November 2009 onwards. The PSD

[17] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCILon payment services in the internal market and amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC
[18] Jere Virtanen, The Single Euro Payments Area: Characteristics, Realization and Future Prospect, 2014, page 7-8

mandates neither the implementation of SEPA payment instruments nor the replacement of existing national euro payment instruments.

4.2 European Commission Directive on E-Money

As online payment systems increased, the European Commission established a context within which e-money providers could operate. The aim of the Directive 2000/46/EC was to harmonize the regulatory supervision of, and increase public confidence in, e/money issuers by providing strict standards that e-money institutions need to follow.

Electronic money institutions was defined in Article 1(3) as an undertaking or other legal person, other than a credit institution, which issues means of payment in the form of electronic money. The E-money Directive updates EU rules on electronic money (e-money) and in particular brings the prudential regime for e-money institutions into line with the requirements for payment institutions in the Payment Services Directive (PSD).[19] According to the report issued by the European Commission it was found that since the implementation of the Directive only nine independent e-money institutions came to existence assumingly it was due to restrictions imposed by the Directive. The new E-Money Directive essentially aims to, enable new, innovative and secure electronic money services to be designed, provide market access to new companies and foster real and effective competition between all market participants.

Recital of the Directive 2009/110/EC suggested that the E-Money Directive 2000/46/EC was responsible for hindering the emergence of a true single market for e-money services. The new E-Money Directive has a wider definition of e-money institution and is defined as a legal person who has been authorized to issue e-money which needs to be read in conjunction with Article 6(1), which provides a lengthy list of other activities that e-money institutions may get involved in. The first Electronic Money Directive ("EMD1"), introduced in 2000, required electronic money institutions ("EMIs") to hold initial capital of €1 million. But in 2009, the PSD enabled payment institutions to launch other types of

[19] Electronic Money Directive 2009 Consultation Paper , 16 December 2010, http://www.finance.gov.ie/sites/default/files/EMDConsultation.pdf

payment services with only €125,000 of initial capital (and later, in 2011, EMD2 reduced the initial capital for EMIs to €350,000) in order to bring EMD more in line with PSD1.[20]
EMD2 introduced new safeguarding requirements where ELMIs are required to safeguard funds in prescribed manner by placing them in a segregated account or holding an insurance policy or bank guarantee. ELMIs will have 5 business days before funds that have not yet cleared must be safeguarded and customers will rank above other creditors in access to safeguarded funds if issuer becomes insolvent.
The EMD2 provides with limited network exemption where E-money used only within "a limited network of services providers or for a limited range of goods or services" is exempt from the rules for e-money, including authorisation requirements for issuers. However the EMD2 provides no definition of "limited network". Geographically, it may cover the whole of Europe, e.g. a single retailer store card. Quantitatively, a limited network of retailers could be numerous e.g. covering a franchise. In addition transactions executed by means of any telecommunication device are exempt, if goods and services purchased are delivered to and are to be used through a telecommunication device provided the operator does not act only as an intermediary between user and supplier.
New redemption requirements are introduced on top of other changes. Redemption can be sought at any time. It may be subject to a fee that is proportionate and commensurate with costs but only of stated in a contract and only where redemption is requested before a contract ends, the customer terminates the contract before the end-date and redemption is requested more than one year after the contract ends. If customers do not reclaim funds after termination of contract, issuer has to safeguard such dormant accounts and such funds will count towards the calculation of capital requirements.

4.3 European Commission Directive on Payment Services (PSD)

Directive 2007/64/EC on payment services within the internal market stemmed from a European Commission initiative to regulate electronic means of payment within the

[20] Alistair Maughan and Simon Deane-Johns , Review of the European Union's proposal for a new directive on payment services ("PSD2"), 18 February 2014, page 1

European Union. The Directive was passed in 2007 and sought to make electronic payments more efficient and remove barriers to payment systems. The Payment Services Directive was adopted to provide a clear legal framework for the SEPA and payment services in general. The role of SEPA is to provide harmonized euro payment services to be treated as domestic payments within the EU. Together PSD and SEPA aim to create a common legal framework and a standardised environment for euro payment services in the EU.

The Directive sought to be a maximum harmonization measure and at the heart of the legislation lay three core principles:

- To create an authorization scheme for providers of payment systems;
- Harmonize the business rules that apply to payment service providers;
- Open up payment systems within the European Union.

Consumers are dependent on payment services, which is why consumer protection is a corner stone of the PSD. The Directive ensures that the rules on electronic payments – for example, paying by debit card or transferring money – are the same in 30 European countries (all 27 members of the EU and Iceland, Norway, and Liechtenstein). This means that customers were able to make payments throughout Europe as easily and safely as in their home country.

The Directive introduced new liquidity and security regulations for all payment service providers. However, one of the main objectives of the PSD is to open the payment market to new providers, notably through the creation of a new category of payment service providers i.e. the payment institutions, which benefit from a specific legal and prudential environment. Payment institutions are permitted to make and remit payments on behalf of customers but are not allowed to issue credit or issue electronic money.[21]

4.3.1 Payment Service Providers

[21] Andrew Murray, Information Technology law: The law and Society, page 479

Traditionally payment service providers include banks, card networks, and payment processors. However recently, new payment players, often referred to as alternative payment providers (APPs) or payment institutions. Mobile network providers are also a part of a growing leading role in mobile payments in a number of countries. They do so under a range of business models such as mobile centric model[22], bank centric model[23], partial integration model[24], and full collaboration model[25]. Particularly full collaboration model allows such companies as Apple Inc and Google to join a full venture between mobile operators, banks and other payment providers.[26] According to Article 4(9), 'payment service provider' (PSP) means [sic] '*bodies referred to in Article 1(1) and legal and natural persons benefiting from the waiver under Article 26'*. The most significant categories of payment service provider are credit institutions (i.e. banks), electronic money institutions and "payment institutions". For all other categories of PSPs it will be the third and the fourth Title (transparency and rights) of the PSD that are applicable, instead of the second Title (authorization requirements).

The PSD distinguishes between various categories of possible payment service providers:

- Credit institutions, which take deposits from service recipients that can be used to fund payment transactions. These are subject to the strict prudential requirements of the relevant Banking Directive.

[22] Policy Briefing by Robin Simpson, The mobile operator acts independently to deploy mobile payment applications to NFC-enabled mobile devices, MOBILE PAYMENTS AND CONSUMER PROTECTION, January 2014

[23] Under this model, banks develop a mass-market payment mechanism independently, without involving mobile operators or mobile phone manufacturers., Policy Briefing by Robin Simpson, MOBILE PAYMENTS AND CONSUMER PROTECTION, January 2014

[24] This involves a mobile operator creating a bank subsidiary to handle mobile payments, and the subsidiary offers a payment mechanism for vending machines., Policy Briefing by Robin Simpson, MOBILE PAYMENTS AND CONSUMER PROTECTION, January 2014

[25] Under this model a joint venture is formed between mobile operators, banks, and other payment providers; Policy Briefing by Robin Simpson, MOBILE PAYMENTS AND CONSUMER PROTECTION, January 2014

[26] OECD, REPORT ON CONSUMER PROTECTION IN ONLINE AND MOBILE PAYMENTS, page 10, http://www.oecd-ilibrary.org/docserver/download/5k9490gwp7f3.pdf?expires=1430665310&id=id&accname=guest&checksum=7AD8A4EF998F39BED20280A7BC034616

- E-money institutions, which issue electronic money that can be used to fund payment transactions, and which again are subject to austere prudential rules under the E/Money Directive.
- Post office giro institutions, whose status is negatively defined in that they are neither banks nor E-money institutions and which are to provide payment services under national law.

The payment institutions, as mentioned above, form a special category of payments service suppliers that would fall under neither the definition of credit institutions nor that of the electronic money institutions. The underlying reason is that the activities of payment institutions carry only a low level of risk, as no deposit-taking is involved.[27] In other words, Payment institutions are undertakings which provide one or more payment services, such as facilitating deposits and withdrawals from bank accounts, executing direct debits and standing orders, money remittance and certain services provided through mobile phones or other digital and IT devices.

The effect of the European Services Directive 2007/64/EC and the E-Money Directive is that there are now three levels of payment service providers, with banks at the top, e-money institutions in the middle and all other payment providers at the bottom. As a result there are three different capital requirements for the e-money institutions and other payment institutions. However the nature of the electronic payment has taken a different course to that which was anticipated, with continued usage of credit and debit cards.[28]

PSD includes exemptions clauses which outlines the conditions under which the directive will not apply. Thus, Market intelligence suggests that a substantial number of PSPs made use of the exemptions to redesign their current products and services to fall under exemptions and thus escape the Payment Service Directive. For the purpose of the thesis three following exceptions were chosen to be discussed.[29]

[27] Panagiotis Delimatsis, Nils Herger, Financial Regulation At the Crossroads: Implications for Supervision, Institutional Design and Trade, March 2011, page 349

[28] Kevin M Rogers, The Internet and the Law, Palgrave Macmillan, July 2011, page 81

[29] COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT, Brussels, 24.7.2013 SWD(2013) 288 final Volume ½, page 151

4.3.2 Exceptions

"Limited network" (Article 3(k) of PSD) - this exemption is applied to large networks involving high payment volumes and rages of products and services. This exception can be relied on by supplier of goods who, for example, offers a pre-paid card, such as a gift card, with stored value which can only be spent with that retailer. However, some of the service providers have found ways to make sure that they would not be caught by the provision. As a result, this leaves the consumer in the legal uncertainty and out of scope of protection.

"Added value" – under Article 3(l) of PSD certain payment transactions carried out by means of a mobile phone or any other digital or IT device are excluded from the scope of the Directive. As a result, in cases where the activity of the telecommunication operator goes beyond a mere payment transaction since the operator might add intrinsic value to the goods or services purchased which furthermore are delivered to and are to be used only through a digital device (e.g. mobile phones), the concrete payment transaction would not fall within the PSD in accordance with its Article 3(l).

"Mobile phone operators and other digital payment service providers" - the exclusion from the PSD (Article 3(j)) that may exempt at least some of the payment-type services currently offered by technical service providers[30]. This exception is of the relevance with regards to such mobile payment services as, for example, Apple Pay or soon coming Samsung Pay. Consumer potentially do not get protected when using such mobile payment services.

Both directives - E-Money Directive and PSD1 do not apply to services used for acquisition of goods or services 'within a limited network of service providers or for limited range of goods or services'. According to Payment Committee[31] Several Member

[30] A technical service provider is an entity that provides technical services to payment service providers so that the payment service provider can provide payment services to their users. They themselves never enter in relationship with the users directly and are therefore not covered as such by the PSD. *Payment Services Directive 2007/64/EC*, Questions and answers, http://ec.europa.eu/internal_market/payments/docs/framework/transposition/faq_en.pdf

[31] Payment Committee, 'Summary Record of the Sixth meeting of the Payments Committee of 21 March 2012' (2012) <ec.europa.eu> PC/005/12, 3.

States reported that the application of several exceptions had proven rather difficult.[32] The exceptions most frequently referred to were Article 3(k) and Article 3(l). Both exceptions would leave room for conflicting interpretation and abuse. Market participants were reported to increasingly design business models aiming at falling into the negative scope (and therefore not into the directive). As stressed by some Member States, the biggest issue was that service providers would often not even consult the authorities about whether they were covered or not but rely on their own assessment.[33]

4.3.3 Full harmonization

Full harmonization is a great challenge in the context of the PSD. The PSD includes a large amount of provisions which explicitly give Member States discretion as to how implement them in their national legal orders. For example, Member States have discretion to reverse the burden of proof on the information requirements laid down in the PSD in favour of payment service users.[34] The negative impact of the current approach to exemptions is amplified by the fact that a number of Member States decided to amend the wording or the scope of exemptions. In the absence of harmonization of the guidance (whether general or individual) by the competent authorities of Member States, a uniform approach to exemptions does not seem feasible. To counteract these developments, one competent authority pointed out that all Member States' interpretation ought to be the same in order to ensure a level playing-field.[35] Therefore, varying application of a harmonized European regulation contradicts the approach of a single European market.

---

[32] According to the Swedish Government's legal proposal for the law implementing the PSD, contents of Article 3(l) do not constitute payment services and Sweden has not implemented the mentioned article, in order to avoid superfluous regulation.

[33] Payment Committee, 'Summary Record of the Sixth meeting of the Payments Committee of 21 March 2012' (2012) <ec.europa.eu> PC/005/12, 3.

[34] Stefan Grundmann, Yeşim M. Atamer, Financial Services, Financial Crisis and General European Contract Law: Failure and Challenges of Contracting, Kluwer Law International, 2011, page 234

[35] 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 Contract MARKT/2011/120/H3/ST/OP Final reportPrepared by London Economics and iff in association with PaySys, page 132

From the feedback acquired from research and consultation processes, it became clear that the 2007 Payment Services Directive had not fully reached its intended goals, mainly due to its broadly phrased scope exemptions.[36] The European Commission is concerned that many payment service undertakings have escaped regulation under the current Payment Services Directive. There is, therefore, a need to bring more undertakings within the scope of regulation in order to provide consumer with better consumer protection in the context of mobile payments.

5 European Commission Directive on Payment Services II (PSD2)

On 3 April 2014, in the last month of the 2009-14 term, the European Parliament voted to adopt a number of amendments to the European Commission proposals for a recast Directive on payment services in the internal market, better known as the Payment Services Directive ('PSD2'), and its accompanying Regulation on interchange fees for card-based payment transactions ('the Regulation'). PSD2 may be seen as a response to many of the criticisms, suggestions and issues that have been raised in respect of PSD1 and the wider regulation of payments in the EU. In addition, the European Commission aims to improve the level of consumer protection in place, and also to increase competition. It follows on from the European Commission green paper *'Towards an integrated European market for card, internet and mobile payments'* and is also part of the wider EU proposal for regulatory reform of payment services. In the context of mobile payments, the PSD2 aims to regulate new third party payment service providers and thus support European economic growth. According to the European Commission there is a *"legal vacuum for certain newly emerged Internet service providers, such as third party providers offering online banking*

[36] Niels Vandezande, Between Bitcoins and mobile payments: will the European Commission's new proposal provide more legal certainty?, page 14

payment based initiation…The legal vacuum risks impeding innovation and appropriate market access conditions."[37]

In order to eliminate the '*legal vacuum'* the European Commission aims to implement PSD2 for the introduction of newly emerged payment services by third party account servicing payment service providers who use the payment infrastructures of the already regulated payment service providers. It also addresses the inconsistency of application of existing rules by Member States, which has contributed to the fragmentation of the retailer payment market along national lines. The PSD2 draws more attention towards security issues. PSD2 strengthens the authentication as it is a major aspect of online payments security, payment service providers will have to make assessment of operational and security risks, as well as, occasionally notifying customers of relevant security incidents. Inadequate security is an important impediment to the efficiency of payment systems because, as the number and value of payment transactions has increased over time, the number of security incidents has increased as well. The PSD2 proposals will amend and replace PSD1[38]. They are aimed at levelling the playing field for different types of PSP, filling gaps in consumer protection, improving the security of payments, reducing areas of ambiguity, and ensuring greater consistency of approach to regulation across the EU.[39]

5.1 Negative scope

'*Limited network'* - Within the framework of PSD2 the Commission has closely reviewed the exception for limited networks. This was considered necessary due to the increasing application of the exception to large networks with high payment volumes and a broad spectrum of goods and services extending beyond the purpose of the exception, and thus leading to large payment volumes being outside of regulation and creating a disadvantage in competition for players in regulated markets. The new definition is intended to limit these risks.

---

[37] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC /* COM/2013/0547 final - 2013/0264 (COD) */

[38] European Banking Authorities, Final Guidelines on the Security of Internet Payments, page 27

[39] Hogan Lovells, Briefing on EU proposals for a second Payment Services Directive and new Interchange Regulation, 15 August 2013

Consequently the Commission has extensively revised the wording of the exception. It does no longer apply to services based on instruments, but requires the instruments to be "specific". Furthermore, these instruments need to be "designed to address precise needs" and "used only in a limited way". Apart from that the wording is reorganised, but is not changed substantially; i.e. there are still three exceptions available: (i) being used in a limited way to enable the customer to acquire goods or services only in the premises of the issuer, (ii) instruments within a limited network of service providers which have a direct commercial agreement with the issuer and which result in the customer only being able to acquire a limited range of goods or services and (iii) instruments to be used only to acquire a limited range of goods or services. The unpublished preliminary draft had intended to limit the exception to those instruments to be used in the premises of the issuer or chain store – explicitly not depending on geographic scope.

"*Mobile phone operators and other digital payment service providers*" – as mentioned above under Article 3(l) of PSD1 certain payment transactions carried out by means of a mobile phone or any other digital or IT device are excluded from the scope of the Directive. PSD2 has amended this exclusion so that it applies to: "payment transactions carried out by a provider of electronic communication networks or services where the transaction is provided for a subscriber to the network or service and for purchase of digital content as ancillary services to electronic communications services, regardless of the device used for the purchase or consumption of the content, provided that the value of any single payment transaction does not exceed EUR 50 and the cumulative value of payment transactions does not exceed EUR 200 in any billing month".

Not only does the revised exclusion places strict monetary values on its application, it appears from its wording to apply mainly to telecommunications company operators, insofar that the purchase of digital content must be 'ancillary' to the electronic communications services and the payment amount limits are made with reference to 'subscribers' and 'billing months' – all concepts which more typically apply to telecommunications company operators. Depending on its interpretation the provision could be an impediment for innovation in the case that the provision will be interpreted in a way that could be only applied to telecommunication companies, excluding the others.

"Mobile phone operators and other digital payment service providers" – (Article 3(j) of the PSD1) contained the provision which excludes 'technical service providers'– on the grounds that they did not come into the possession of the funds. PSD2 seeks to limit this exclusion for operators who are treated as 'payment initiation services' and 'account information services'. Thus, operators who had sought to previously rely upon this exclusion and new services which have entered the market on this basis will need to carry out careful analysis as to whether they will now need to become regulated under PSD2. This will be particularly important for determining whether a payment service support operator falls within the scope of providing 'payment initiation services'. This proposed new regulated activity will cover: "a payment service enabling access to a payment account provided by a third party payment service provider, where the payer can be actively involved in the payment initiation or the third party payment service provider's software, or where payment instruments can be used by the payer or the payee to transmit the payer's credentials to the account servicing payment service provider." The wording suggests that the PSD2 will be able to capture more undertakings with different business models, depending on how exactly they have set up their operations to assist a third party payment service provider in executing payment transactions.

5.2 Payment Account Access Services

A new provider called a 'third party payment service provider' (TPP) which offers payment initiation services to consumers and merchants, often without entering into the possession of the funds to be transferred[40] is introduced as well as two new types of services that TPP's and other PSPs can provide account information services and payment initiation services.

The reason behind the introduction of the "third party payment service providers" is that according to European Commission's report new players have emerged in the market (TPPs) offering low cost payment solutions on the internet using the customers' home online banking application, with their agreement, and informing merchants that the money

[40] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC, (Preamble, para. 18).

is on its way, thereby facilitating online shopping. Some players also offer consolidated information on different accounts of a payments service user ('account information services'). Whilst these new actors bring undeniable benefits for payments users in general –merchants and consumers alike- and competition in the market, a series of issues about security, access to information on payment accounts or data privacy need to be addressed at EU level, alongside their possible licensing and supervision as payment institutions under the PSD.[41]

In order to understand what it has to do with a customer in terms of mobile payments it is essential to understand what TPPs actually are what they do. The section bellow will analyze the sometimes vague definition of the TPP and what is the role of it.

5.3 Third Party Payment Service Providers

So what is TPP? According to Article 4 (11) of the PSD2, the definition for this provider is as follows:

'*third party payment service provider*" means a payment service provider pursuing business activities referred to in point 7 of Annex I'

Services listed in point 7 of Annex I are: 'Services based on access to payment accounts provided by a payment service provider who is the account servicing payment service provider, in the form of:

a) Payment initiation services (PIS), these newly-to-be regulated providers would be able to re-use personal customer online banking security details in order to enter the customer's account and initiate a payment on the customer's behalf.[42]
b) Account information services.(AIS) '

What does a TPP do? Article 4(32) and (33) holds the answer (at least to some extent!):

[41] "REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the application of Directive 2007/64/EC on payment services in the internal market and on Regulation (EC) No 924/2009 on cross-border payments in the Community". Eur-lex.europa.eu. 2013-07-24.

[42] Ruth Wandhöfer, Transaction Banking and the Impact of Regulatory Change Basel III and Other Challenges for the Global Economy, October 2014, page 35

Article 4(32) '*payment initiation service means a payment service enabling access to a payment account provided by a third party payment services provider, where the payer can be actively involved in the payment initiation or the third party payment service provider's software, or where payment instruments can be used by the payer or the payee to transmit the payer's credentials to the account servicing payment service provider*;'

Article 4(33) *''account information service' means a payment service where consolidated and user-friendly information is provided to a payment service user on one or several payment accounts held by the payment service user with one or several account servicing payment service providers;'*

The wording suggests that the TPP is an undertaking which provides services that facilitate e-commerce payments by establishing a software bridge between the website of the merchant and the online banking platform of the consumer in order to initiate Internet payments on the basis of credit transfers or direct debits.[43] TPP's include companies that enable online purchases such as *Sofort* (Germany), *Ideal* (The Netherlands), *Trustly* (Scandinavia) and *Apple Pay*. However, as TPPs are currently not subject to Directive 2007/64/EC, they are not necessarily supervised by a competent authority and do not follow the requirements of Directive 2007/64/EC.[44] Thus, the PSD2 addresses this legal vacuum and brings the TPPs under the scope of EU regulatory framework. This can be considered as a step forward in the context of better consumer protection. However, the fact that TPPs will be making a transaction instead of the consumer results in that the TPP will have to be able to see customers personal information such as: the amount of savings, the monthly salary, what types of payments the customer recently made, their investments and so on. This invites data mining (gathering any type of useful data about customer), which the PIS TPP could potentially sell to interested parties or re-use for the commercial purposes. Even though the proposed Article 58 (2c) requires TPPs not to store '*sensitive*

[43]Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC, (Preamble, para. 18).
[44] Ibid, (Preamble, para. 18).

payment data or personalized security[45]' which implies that they have access to this information, it is silent on other types of customer data.[46] Needless to say, such access should be highly secure to ensure authentication data is properly protected and cannot be reused by third party. This potentially could trigger data protection laws which will be discussed more closely later in the thesis.

Under Article 58 of PSD2 EU Member States will have to:

- Ensure that payers have the right to use a payment initiation service provider (PISP) to obtain payment initiation services;
- Require the account servicing PSPs domiciled in their jurisdiction to:

  "(a) provide facilities to securely communicate with [PISPs]in accordance with article 87a, paragraph 1(d);

  (b) immediately after the receipt of the payment order from a [PISP,] provide information on the initiation of the payment transaction to the [PISP]; and

  (c) treat payment orders transmitted through the services of a [PISP] without any discrimination, in particular in terms of timing, priority or charges vis-à-vis payment orders transmitted directly by the payer himself, unless objectively justified"; and

- (When the payer gives its explicit consent for a payment to be executed in accordance with Article 57), require their account servicing PSPs:

  "(a) not to hold … the payer's funds in connection with the provision of the payment initiation services;

  (b) to ensure that any information about the payment service user, obtained when providing payment initiation services, is not accessible to other parties;

  (c) every time a payment is initiated, to authenticate itself towards the account servicing [PSP] of the account owner and communicate with the account servicing [PSP], the payer and the payee in a secure way, in accordance with article 87a, paragraph 1(d)

[45] means *"personalised features provided by the [PSP] to a customer for the purposes of authentication*" (see article 4(22a) of PSD2).

[46] Ruth Wandhöfer, Transaction Banking and the Impact of Regulatory Change Basel III and Other Challenges for the Global Economy, October 2014, page 189

(d) not to store sensitive payment data of the payment service user and not to request from the payment service user any data other than those necessary to initiate the payment;

(e) not to use, access and store any data for purposes other than for performing the payment initiation services explicitly requested by the payer; and

(f) not to modify the amount, the recipient or any other feature of the transaction".

Thus, all payment service providers, be they banks, payment institutions or TPPs, will need to prove that they have certain security measures in place ensuring safe and secure payments. An assessment of the operational and security risks at stake and the measures taken will need to be done on a yearly basis. Payment service providers also have to ensure strong customer authentication for payments with a payment instrument that is not present at the point of sale (e.g. internet payments) as set out in the Directive.

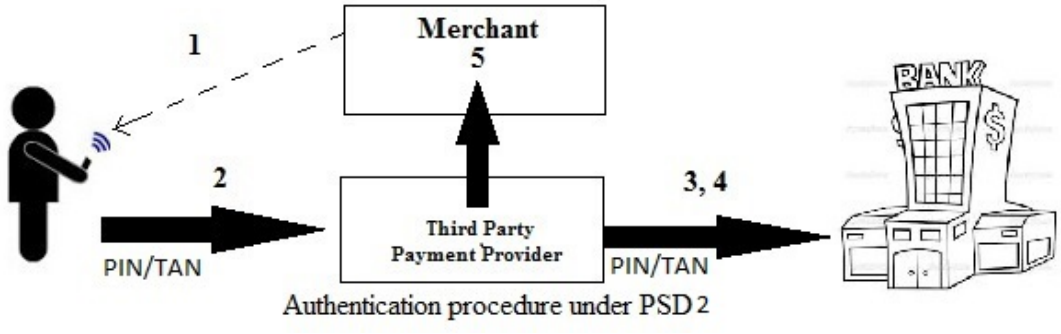
5.4 Strong Customer Authentication

Authentication means a procedure that allows the PSP to verify a customer's identity. A great concern that customer has when making an online payment is security of his payment and that no one else has the access to his/her account.

EU Commission and European Central Bank ECB are particularly engaged to make internet payments more secure. The ECB formed a forum of European central banks and supervisory authorities, called SecuRe Pay, to discuss and eventually agree on a set of rules for the enhancing of security of internet payments, one of the most important of such rules being the strong customer authentication when making internet payments or accessing payment data. The rules were finally issued as recommendations of the ECB in January 2014. The EU Commission included in July 2014 the same basic rule on strong customer authentication within its proposal for a Second Payment Services Directive (PSD2).

Strong customer authentication is defined by the Commission *as "a procedure for the validation of the identification of a natural or legal person based on the use of two or more elements categorized as knowledge, possession and inherence that are independent, in that*

the breach of one does not compromise the reliability of the others and is designed in such a way as to protect the confidentiality of the authentication data".[47]



ECB Recommendations for the security of Internet Payments provides that strong customer authentication is a procedure based on the use of two or more of the following elements – categorized as knowledge, ownership and inherence: (i) something only the user knows (e.g a static password, code or personal identification number); (ii) something only the user possesses (e.g a token, smart cars or mobile device); and (iii) something the user is (e.g. a biometric characteristic, such as a fingerprint).[48] At least one of the elements should be non-reusable and non-replicable (except for inherence), and not capable of being surreptitiously stolen via the internet. The strong authentication procedure should be designed in such a way as to protect the confidentiality of the authentication data

Therefore as a result, if PSP fails to apply strong customer authentication then they would be required to compensate PSPs or intermediaries involved in a transaction for any loss incurred or sums paid by those other businesses.[49] PSPs that fail to apply strong customer authentication for payments made online or over the phone cannot require payers to "*bear any financial consequences* [50] " unless those payers themselves act fraudulently.

[47] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC /* COM/2013/0547 final - 2013/0264 (COD), Article 4 Definitions, nr 22.

[48] European Central Bank, ECB Recommendations for the Security of Internet Payments, page 5

[49] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC, Article 82(2)

[50] Ibid, Article 66(2)

It is essential in terms of mobile payments to ensure an adequate security measures, strong customer authentication is a very important aspect of the changes introduced by the PSD. It is not completely clear what actually constitutes a "*stronger customer authentication*" however for example fingerprint in conjunction with password could potentially fit the definition strong customer authentication. It can be doubted that the stronger authentication provisions would slow the pace of innovation of sophisticated cybercrime. However, it is reasonable to say that ensuring a high level of security is another step towards a better customer protection.

5.5 Dispute Resolution

When one makes a mobile payment it is often unclear how the person could resolve his issues in case something goes wrong when making a transaction. This large number of players can lead to an unclear division of responsibilities among the various entities and the vendor selling the good or service that, in turn, makes it more difficult for consumer dispute resolution and redress as a result consumers can have difficulties in determining their rights and the responsible parties. Thus, in order to solve this problem the OECD in its "*Consumer Policy Guidance on Mobile and Online Payments*" recommended that to ensure that customers have adequate access to dispute resolution and redress the governments, payment providers, merchants and other stakeholders should develop low-cost, easy to use alternative dispute resolution and redress mechanisms which would, inter alia, facilitate resolving claims over payments involving low-value transactions. Such mechanisms could include the development of effective online dispute resolution systems. Alternative dispute resolution and redress mechanisms should not prevent parties from pursuing other forms of redress, as permitted by applicable law.[51] Thus this indicates that third party payment providers should establish their own comprehensive alternative dispute resolution mechanism which would be easily accessible by customers.

[51] OECD(2014), 'Consumer Policy Guidance on Mobile and Online Payments', OECD Digital Economy Papers, No. 236, OECD Publishing. http://dx.doi.org/10.1787/5jz432cl1ns7-en, page 22

Regulation (EC) No 593/2008 of the European Parliament and of the Council[52] states that the weaker contractual party should be protected by conflict-of-law rules that are more favorable to their interest than the general rules and the protection afforded to consumers by the mandatory rules of law of the country in which they have their habitual residence may not be undermined by any contractual terms on laws applicable.

Out-of-court complaint and redress procedures for the settlement of disputes are covered by Articles 88-90 of the PSDII. Article 88 deals with complains and requires that procedures would be set up for submitting complaints to the competent authorities with regard to payment service providers' alleged infringements if the Directive. In addition, the reply from the competent authorities will have to inform the complainant of the existence of the out-of-court complaint and redress procedures set up in accordance with Article 91.[53]

Article 89 of the Directive provides that the Member States shall designate competent authorities to ensure and monitor effective compliance with the Directive. It is also required that MS shall notify the commission of the designated competent authorities within one year after entry into force of this Directive.

The PSDII has included the provision governing internal dispute resolution [54] which clearly states that "*Member States shall ensure that payment service providers put in place adequate and effective consumer complaint resolution procedures for the settlement of complaints of payment service users concerning the rights and obligations arising under this Directive.*"[55] Therefore, current reform and emergence of PSDII will be bringing more

[52]Regulation (EC) No 593/2008 of the European parliament\ and of the Council of 17 June 2008 on the law applicable to contractual obligations (ROME I) (OJ L 177, 4.7.2008, p.6).

[53] Adequate and effective out-of-court complaint and redress procedures for the settlement of disputes between payment service users and payment service providers concerning the rights and obligations arising under this Directive shall bee stablished. The Member State bodies shall cooperate for the resolution of cross-border disputes.

[54] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC, Art 90

[55] Ibid, Art 90

clarity to the consumer regarding the dispute resolution. Consumers will also gain a stronger position in case of disputes with their bank and other payment service providers: the new rules will oblige banks to answer in written form to any complaint within 15 business days. However it is yet to be seen whether 15 business day limit for responding and addressing the points raised will be enough for the payment service provider.

The proposed PSD Directive also entitles the payer to a refund if the authorisation did not specify the exact amount of the payment transaction, and when the amount of the payment transaction exceeded the amount the payer could reasonably have expected.[56] In addition, the payer can request the refund for a period of eight weeks from the date on which the funds were debited. Then within 10 business days of receiving a request for a refund, the PSP shall either refund the full amount of the payment or provide justification for refusing the refund, indicating the bodies to which the payer may refer the matter if not accepting the justification provided.[57]

6 The Interchange Fees Regulation

According to the European Commission undistorted competition leads to innovation. However, the problems in the card markets are spilling over into the new markets of internet and mobile payments. Most payment schemes in the EU were established before the current levels of interchange fees. And many investments in innovative payments (e.g. terminals for mobile payments), are made on the acceptance side by banks and retailers that pay the interchange fees - not by those that receive them.[58]

The Interchange fees Regulation is a part of the package which will come together with PSD2. The Council adopted on 20 April 2015 a regulation capping interchange fees for payments made with debit and credit cards. The Interchange Fees Regulation aims to bring more innovation. The idea is that the regulation will open the gateway for more competition which eventually means lower prices for customers.

[56] Ibid, Art 67

[57] Ibid, Article 68

[58] European Commission, The interchange fees regulation, page 2, http://ec.europa.eu/competition/publications/factsheet_interchange_fees_en.pdf

However what was exactly wrong that the Commission decided to bring forward a regulation in order to deal with it? When a customer pays for a purchase in a store using a credit or debit card, the bank that serves the store (the "acquiring bank") pays a fee to the bank that issued the payment card to the consumer (the "issuing bank"). A so-called "interchange fee" is then deducted from the final amount that the store merchant receives from the acquiring bank for the transaction. Today, only competition rules limit the fees set by banks and payment card schemes, which are hidden from the consumer and neither retailers nor consumers can influence. When retailers pass these costs on to consumers this can of course lead to inflated prices. In its MasterCard judgment[59] of September 2014, the European Court of Justice made clear that such interchange fees are a violation of EU antitrust rules. The Regulation aims to help the card payments industry move from its current business practices to a new more competitive system, to the benefit of consumers, merchants and banks.[60] The justification generally used for interchange fees is that they are used to stimulate card issuing and use; banks would use part of the fees to incentivize card use through bonuses (air miles, etc.). However not everything is as perfect. The cardholders are encouraged to use cards that generate higher fees, and card companies compete primarily to attract issuing banks by offering high(er) interchange fees. This means that the competition between the payment card schemes cost more for retailers who eventually will increase the prices for a product making the customer pay more. The problem is that it is difficult for the new market entrants to enter the market because banks expect at least the same revenues from them as for normal card payment. Therefore it leads to a situation where customers and merchants are not able to use more efficient and innovative payment means. Thus, because European cards market is quite fragmented and interchange fees vary widely. The competition enforcement cannot deal with the current imbalance for a level playing field to emerge in a comprehensive and timely way. As a result a regulation was seen as the best mean in order to achieve harmonization.

[59] European Court of Justice, MasterCard case (case C-382/12P)

[60] European Commission - Press release, Commission welcomes European Parliament vote to cap interchange fees and improve competition for card-based payments, Brussels, 10 March 2015

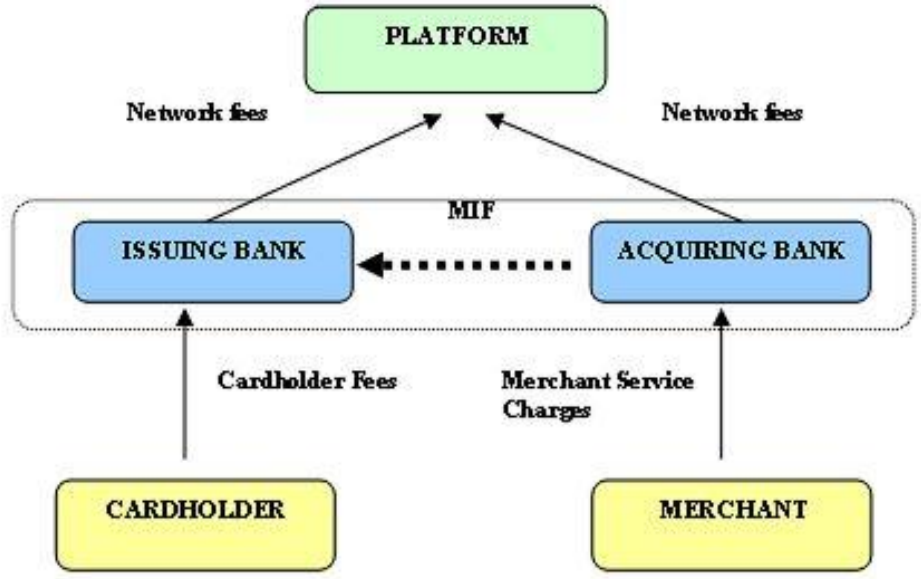


Illustration of the operation of a four-party scheme, including the transfer of the multilateral interchange fee[61]

The commissioner Margrethe Vestager, in charge of competition policy, said: *"For too long, uncompetitive and hidden bank interchange fees have increased costs of merchants and consumers. Today's vote has brought us another step closer to putting an end to this. This legislation will put a cap on interchange fees, make them more transparent and remove a hurdle to rolling out innovative payment technologies. It is good for consumers, good for business and good for innovation and growth in Europe. As cards are the most widely used means of online payment, this Regulation is also an important building block to complete the European Digital Single Market."*[62]

[61] European Commission - Press release, Commission welcomes European Parliament vote to cap interchange fees and improve competition for card-based payments, Brussels, 10 March 2015

[62] European Commission, Press release, Commission welcomes European Parliament vote to cap interchange fees and improve competition for card-based payments, Brussels, 10 March 2015

The 0.2% and 0.3% caps[63] were proposed by schemes in competition proceedings and appear practical as providing legal certainty while not threatening the viability of these schemes. These levels are based on an estimate of the fee at which a merchant would be indifferent between being paid by card or in cash.[64] The caps (0.2/0.3%) which are presented by the Regulation are below the levels which are in most of Member States. Therefore the affect, which the regulation will bring, should be felt significantly by consumers in these Member states where the interchange fees were high. These new rules brings more transparency and should encourage competition. A transparent mechanism should allow the retailers to be aware level of fees paid when accepting cards.

Thus, if the Regulation reaches its potential the consumers would not have to pay more and would have more choice when deciding which payment provider they should use. For example in Netherlands, the cheap online payment solution (Ideal) was adopted widely by the retailers mostly because interchange fees in Netherlands are actually 0.2%.

6.1 Benefits for Customer

The package consisting of Payment Services Directive 2 and Interchange Fees Regulation is a promising step forward, however what would be the actual benefits for the consumer if the goals targeted by the European Commission would become a reality?

It has already been discussed above that PSD2 together with Interchange fees Regulation will cap the card charges imposed on merchants, which will bring more flexibility for merchants to choose payment services as a result the consumer will become a winning party too, since merchants will not have surcharge consumers in order not to suffer loss. The card payments work best when the interests of all stakeholders are equally balanced. The reduction of multilateral interchange fees would make it cheaper for the retailers in terms of card payments. However, it can also happen that as the consumer's issuing bank

[63] European Commission, *Payment Services Directive and Interchange fees Regulation: frequently asked questions*, page 8

[64] The figures have been developed using data from the central banks of Belgium, the Netherlands and Sweden on the cost of payment instruments.

will see a substantial reduction of its payment related revenues, it may no longer be able to cover its cost on growing base of card transactions. This situation may force to reconstruct their fee models, increasing the total bill consumers have to pay. Thus, it is not clear how the market will react.

It is important for the customer to feel safe in cases of fraud. The PSD2 promises better consumer rights, enhance protection and promote legal certainty. The result of that is the introduction of unconditional refund right. This means that the consumer will be able to ask for a unconditional refund even in the case of a disputed payment transaction. The are some exceptions to the rule, the exception will apply where the merchant has already fulfilled the contract and the corresponding good or service has already been consumed. Nevertheless, the consumer should not be a weaker party any longer, according to PSD2 the consumer gets a stronger position in the case of disputes with their banks and payment service providers. It was sought that a consumer would not have to wait for an answer for a long time. The big payment service providers and banks are having greater resources in order to deal with disputes leaving the customer in a uncertain and weak position. The PSD2 would bring 15 business days answer limit which should be conformed with by the banks and payment service providers.

Furthermore, the PSD2 obliges Member States to ensure that a competent authorities dealing with complains would be designated. This brings more clarity for the consumer, the payment service providers should ensure that there is a complaints procedure for consumers that they can use before seeking out-of-court redress or before launching court proceedings. This brings more clarity for the consumers who are often avoiding the complicated and long lasting in-court procedures.

One of the bigger changes that PSD2 brings is so called “strong customer authentication” which should ensure a higher level of payment security in terms in the context of mobile payments. Thus, according to the PSD2 all the service payment providers, be they banks, payment institutions or TPPs, will need to prove that they have certain security measures in place ensuring safe and secure payments. An assessment of the operational and security risks at stake and the measures taken will need to be done on a yearly basis. The PSPs will be obliged to provide strong customer authentication for payments with a payment

instrument that is not present at the point of sale. This is one of the key points for customers when making a mobile payment.

To sum up, the changes should be regarded as actually improving the situation for the consumer. It will have to be seen whether those changes will not make the costumers pay more. The payment service providers will have to implement better security mechanism in order to ensure strong customer authentication, however this may result in some costs for PSPs, which could be as easily passed on merchants and eventually to a consumer.[65]

7 Directive 95/46/EC

The Directive 95/46/EC is out of scope of this thesis, however it is important do have a little insight into what the European laws have to offer in terms of data protection. Data protection is an important topic concerning mobile payments. It is enough to remember that PSD2 enables TTPs to access the accounts information in order to process a payment.

The existing 1995 Directive sets the overarching framework for data protection in the EU and sets out certain core principles concerning the processing of personal data. Under the existing directive there is a specific requirement under Article 17.1 for Member States to implement “appropriate technical and organisational measures” and ensure ”a level of security appropriate to the risks represented by the processing and the nature of the data to be protected”. This is a clear obligation to deploy encryption technologies.

For the purposes of this thesis the notion of “personal data” will be as defined in Article 2a of the Directive :

"any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;"

[65] European Commission, Payment Services Directive and Interchange fees Regulation: frequently asked questions, http://europa.eu/rapid/press-release_MEMO-13-719_en.htm

Information about the customer provided or obtained during the enrolment process and activation of the mobile payment service contains a lot of such data which identifies natural person, therefore they are obliged to take all possible measures to protect personal data depending on whether the undertaking is the “data controller” or “data processor”. The responsibility for compliance rests on the shoulders of the "controller" as he would be responsible for the compliance with data protection laws. [66]

It is crucial to establish who is taking place of a data controller for the relevant personal. The data controller is characterised in Article 2 (d) as the party that “*determines the purposes and means of processing of personal data*” and the data processor processes ”*personal data on behalf of the controller*”. Processing means "*any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction*".[67]

In some cases determination of who is whom can be quite challenging especially where the mobile payments solution simply involves an extension of web-based payment solution offered by financial institutions, it will usually be the financial institutions that will be acting as data controllers. In some cases there are few parties which are data controllers.

Article 12 (a), (b) “*right of access*”, where the data subject has the right that the data controller communicates ”*an intelligible form of the data undergoing processing*” and the right of ”*rectification, erasure and blocking of data*”. Even if in Article 12 only the data controller is addressed, the data controller would need to demand appropriate requirements

[66] *EU Directive 95/46/EC,* Article 2d*, “the natural or artificial person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data”,*

[67] EU Directive 95/46/EC, Art. 2 b

from the data processor in form of a contract, even if the data processor is not addressed in the Directive. The obligation for such a contract is mentioned in Article 17. 3. [68]

In order to reduce the number of incident while processing which the Directive explicitly states that data controller must "*implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access ... and against all other unlawful forms of processing*".[69]

However, the payment information usually always includes information relating to an individual. Therefore the question is whether the customer can feel safe regarding the transfer of his personal information. The EU is determined to protect the privacy of its citizens therefore under the Directive the country which does not offer adequate protection will be met with restrictions.[70] A transfer of personal data to another country constitutes data processing so the EU National Data Protection Authority of the Member State (MS) must be notified where the transfer is being done.

"....the transfer to a third country of personal data ....may take place only if.... the third country in question ensures an adequate level of protection." (Article 25 of Directive 95/46/EC)"

Nevertheless, the data transfer to a third country, which does not have adequate protection, is still possible if there is unambiguous consent from the data subject, the transfer is necessary for the performance, implementation or conclusion of certain contractual transactions, the transfer is in the public interest or the vital interests of the data subject or the transfer is made from a public register.[71] Thus, no formalities or restrictions would

[68] The Infrastructure Level of Cloud Computing as a Basis for Privacy and Security of Software Services, Ina Schiering and Jan Kretschmer, page 91
[69] *EU Directive 95/46/EC,* Article 17, 1
[70] Ibid, Article 25(4)
[71] Ibid, Article 26,

apply if the data is transferred across EU or EEA or other third countries recognized by European Commission.

The current EU Data Protection Directive 95/46/EC does not consider important aspects like globalization and technological developments like social networks and cloud computing sufficiently and determined that new guidelines for data protection and privacy were required. Therefore, as a result the General Data Protection Directive was proposed in order to deal with today's issues regarding data protection.

The draft Data Protection Regulation provides in its explanatory memorandum that:

"Rapid technological developments have brought new challenges for the protection of personal data. The scale of data sharing and collecting has increased dramatically (...). Building trust in the online environment is key to economic development. Lack of trust makes consumers hesitate to buy online and adopt new services. This risks slowing down the development of innovative uses of new technologies".

Key principles of the European data protection framework include the consent of the data subject as well as a legitimate interest from data processor and data controller to process data. It is questionable whether these concepts have been taken into account in the current draft of the PSD2 that strangely enough allows for the sharing of personal banking credentials to allow the initiation of payments by third party providers (TPPs). [72]

The regulation applies if the data controller or processor (organization) or the data subject (person) is based in the EU. Furthermore (and unlike the current Directive) the Regulation also applies to organizations based outside the European Union if they process personal data of EU residents. According to the European Commission:

"personal data is any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a photo, an email

[72] SÉVERINE ANCIBERRO AND SÉBASTIEN DE BROUWER, EU Payments Legislative Package: Strong Concerns of European Banks, http://www.europeanpaymentscouncil.eu/index.cfm/newsletter/article/?articles_uuid=C2D4B9AF-5056-B741-DBA0A3E20D1C5ABB

address, bank details, posts on social networking websites, medical information, or a computer's IP address."[73]

Thus, to summarize, the Directive 95/46/EC does not seem to be suitable for current advancements of technology. The proposed Regulation is meant to tackle these issues and, as a result, includes increased responsibility and accountability for those processing personal data, companies and organizations must notify the national supervisory authority of serious breaches as soon as possible, strengthened independent and national protection authorities.

8 Apple Pay case scenario

In order to have an overview over what is to be expected from third-party mobile payment provider, we could take newly emerged Apple Pay service provided by Apple Inc. Apple Pay was launched in October some weeks after the release of the iPhone 6, the service allows consumers to make debit and credit card purchases using device-specific Device Account Numbers (DANs). The card numbers themselves are not stored, meaning that a customer need only cancel their DANs—not the payment cards—should they happen to lose their phone. In our case scenario we will try to get an insight on how a payment service provider would be bound by EU legal framework and what kind of legislation would actually apply to it. Thus, Apple Pay might be caught by few Directives and Regulations in the EU.

8.1 E-Money Directive

In order for Apple Pay to be subject to E-Money regulations, Apple Pay must be issuing "e-money". E-money is defined under Article 2(2) of the E-Money Directive:
'electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions as defined in point 5 of Article 4 of Directive 2007/64/EC, and which is accepted by a natural or legal person other than the electronic money issuer'.

[73] European Commission's press release announcing the proposed comprehensive reform of data protection rules. 25 January 2012. Retrieved 3 January 2013.

However, Apple Pay does not issue e-money, therefore it could be simply a facilitator for the processing of payments by sending secure payment information. If Apple would be issuing e-money it would have to ensure that ApplePay complies with the EU's E-Money directive which imposes license requirements on each undertaking seeking to issue e-money and/or to offer payment services within the EU. Whether and to which extent this will apply to Apple Pay depends on the details of the technology used and the payment flows involved.

8.2 Payments Service Directive (PSD)

Article 3(j) stipulates that the PSD does not apply to:
"services provided by technical service providers, which support the provision of payment services, without them entering at any time into possession of the funds to be transferred, including processing and storage of data, trust and privacy protection services, data and entity authentication, information technology (IT) and communication network provision, provision and maintenance of terminals and devices used for payment services;"

Thus, Apple Pay appears to be a pass-through wallet holding third party issuer's cards, Apple is likely to be relying on the exemption for services provided by "technical service providers", which support the provision of payment services, without the provider entering at any time into possession of the funds to be transferred.

The Commission has shown significant improvements in the areas such as surcharging, transparency, security and the introduction of the TPPs which now falls under regulatory scope. However there is no clear answer whether the PSD2 is bringing a better consumer protection. On one hand the PSD2 has put more organizations under its scope. One the other hand the failure, whether it is misuse of personal data by PSP's or increased prices for covering the costs of additional security measures by PSP's, would result that more customers would be affected by it. What is clear is that PSD2 is an improvement over the original PSD thus, rendering PSD2 a more proper instrument for making customers more

likely to use mobile payments. The time will show whether the potential dangers will call for a PSD3.

8.3 Payments Service Directive II (PSD2)

PSD2 is likely to include such services within its scope when it comes into effect by 2017. The draft Article 4(32) of PSD II seemingly catches such services provided by Apple:

'payment initiation service' means a payment service enabling access to a payment account provided by a third party payment service provider, where the payer can be actively involved in the payment initiation or the third party payment service provider's software, or where payment instruments can be used by the payer or the payee to transmit the payer's credentials to the account servicing payment service provider;'

This should enhance new low cost e-payment solutions on the internet while ensuring appropriate security, data protection and liability standards.[74] Under PSD II the third-party payment initiation service would be required to be licensed, registered and supervised, like any other payment institution. They would be subject to their own information and transparency requirements, as well as the new requirements on internet payment security. PSD2 allows such payment initiation services as Apple Pay to share personal banking credentials to allow the initiation of payments by third party providers (TPPs), however to do so Apple would have to structure its services in a particular way to come within the scope of PSD2 and operate within constraints around the use of data set by PSD2.

8.4 General Data Protection Regulation

Apple would also need to ensure that the collection and processing of the users' personal (payment) data are justified under European data protection laws. It seems likely that the user data used by Apple Pay will fall within the broad definition of 'personal data' contained in European data protection legislation and Apple will most likely be considered to be a data controller of the data collected and used by Apple Pay.

[74] PSDII Title I-V and Annex I point 7

8.5 Overview

Thus, most of the current EU laws would not cover such TPPs as Apple Pay, however the PSD2 has different approach to it. This is mostly because of introduction of 'payment initiation services' which captures Apple Pay. This means that Apple Pay would have to comply with European regulations regulating mobile payments. The analysis shows that PSD is the only instrument which is able to ensure that TPPs are under control of the European regulatory framework in the context of mobile payments. The legal vacuum which was present at the presence of the original PSD is now filled with a more delicate regulatory instrument.

9 Conclusion

The PSD2 together with Interchange Fees Regulation makes a great effort in order to increase harmonization of mobile payments across the European Union. There are some areas, though, where a full harmonization has not been suggested yet. There are some key points where the current draft of the PSD2 does not bring any confidence for a customer. In order to increase customer protection the PSD2 allows third party service providers to access the account holders personal data. In order to protect customer and their money, security details, whteher static or dynamic, once usable or re-usable, should not be shared with any party apart from the entity which issued these credentials. Only then it will be possible to protect customers and their data. Furthermore, as mentioned above it should be sought that the PSD2 would not only benefit the customers but also the payment service providers. This would be an encouragement for the new payment service providers to enter the market, which eventually would result in more competition and higher prices. It may be save to say the PSD2 could be a right answer for the increase of e-commerce in the European Union, however it will all depend how the market players and users will benefit from the PSD. The balance between customer rights and the PSPs obligations should not tilt towards one or another, this can result in higher costs on both sides, leaving no winners. The Commission has shown significant improvements in the areas such as surcharging, transparency, security and the introduction of the TPPs which now falls under regulatory

scope. However there is no clear answer whether the PSD2 is bringing a better consumer protection. On one hand the PSD2 has put more organizations under its scope. One the other hand the failure, whether it is misuse of personal data by PSP's or increased prices for covering the costs of additional security measures by PSP's, would result that more customers would be affected by it. What is clear is that PSD2 is an improvement over the original PSD thus, rendering PSD2 a more proper instrument for making customers more likely to use mobile payments. The time will show whether the potential dangers will call for a PSD3.

Table of reference

Key Legislation

The Payment Services Directive 2007/64/EC of the European Parliament and of the Council of 13th November 2007, on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC. OJ L 319/1 of 5.12.2007.

Directive 2007/64/EC of the European Parliament and of the Council 13 November 2007on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC

Electronic Money Directive 2009/110/EC of the European Parliament and of the Council on the taking up, pursuit and prudential supervision of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC, OJ L 267 of 10.10.2009

Proposal for a Regulation on the European Parliament and of the Council on interchange fees for card-based payment transactions, COM/2013/0550 final - 2013/0265 (COD)

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Literature (Journals and Reports)

Books

Alistair Maughan and Simon Deane-Johns , *Review of the European Union's proposal for a new directive on payment services ("PSD2"),* 18 February 2014

Andrew Murray, *Information Technology law: The law and Society*, 22 August 2013

Stefan Grundmann, Yeşim M. Atamer, *Financial Services, Financial Crisis and General European Contract Law: Failure and Challenges of Contracting*, Kluwer Law International, 2011

Kevin M Rogers, *The Internet and the Law, Palgrave Macmillan*, Palgrave Macmillan, July 2011

Niels Vandezande, *Between Bitcoins and mobile payments: will the European Commission's new proposal provide more legal certainty?,* September 2014, International Journal of Law & Information Technology;Autumn2014, Vol. 22 Issue 3

Ruth Wandhöfer, *Transaction Banking and the Impact of Regulatory Change Basel III and Other Challenges for the Global Economy*, Palgrave Macmillan, October 2014

European Commission, GREEN PAPER, *Towards an integrated European market for card, internet and mobile payments*, 11/01/2012

Reports

Report from the Commission to the European Parliament and the Council on the application of Directive 2007/64/EC on payment services in the internal market and on Regulation (EC) No 924/2009 on cross-border payments in the Community". Eur-lex.europa.eu. 2013-07-24.

European Central Bank, *ECB Recommendations for the Security of Internet Payments*

COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT, Brussels, 24.7.2013 SWD(2013) 288 final Volume ½

OECD Report: *The Future of Money, Paris 2002*
http://www.oecd.org/sti/futures/35391062.pdf

OECD (2014), *"Consumer Policy Guidance on Mobile and Online Payments*", OECD Economy Papers, No. 236, OECD Publishing. http://dx.doi.org/10.1787/5jz432cl1ns7-en.

OECD (2012), "*Report on Consumer Protection in Online and Mobile Payments"*, OECD Digital Economy Papers No. 204, OECD Publishing.
http://dx.doi.org/10.1787/5k9490gwp7f3-en

Ofcom, *International Communications Market Report*, 11 December 2014, http://stakeholders.ofcom.org.uk/binaries/research/cmr/cmr14/icmr/ICMR_2014.pdf

Study on the impact of the 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 Contract MARKT/2011/120/H3/ST/OP Final report Prepared by London Economics and iff in association with PaySys

<u>Other Sources</u>

European Commission's press release announcing the proposed comprehensive reform of data protection rules. 25 January 2012. Retrieved 3 January 2013

Jere Virtanen, *The Single Euro Payments Area: Characteristics,* Realization and Future Prospect, 2014

Bailly, L.; Van der Lande, B. (2007), *Breakthroughs in the European Mobile payment market*, White paper, Atos Oringin

SÉVERINE ANCIBERRO AND SÉBASTIEN DE BROUWER*, EU Payments Legislative*

Package: Strong Concerns of European Banks, http://www.europeanpaymentscouncil.eu/index.cfm/newsletter/article/?articles_uuid=C2D4B9AF-5056-B741-DBA0A3E20D1C5ABB

Policy Briefing by Robin Simpson, *The mobile operator acts independently to deploy mobile payment applications to NFC-enabled mobile devices,* MOBILE PAYMENTS AND CONSUMER PROTECTION, January 2014

Ina Schiering and Jan Kretschmer, *The Infrastructure Level of Cloud Computing as a Basis for Privacy and Security of Software Services*, 7th IFIP WG 9.2, 9.6/11.7, 11.4, 11.6/PrimeLife International Summer School, Trento, Italy, September 5-9, 2011, Revised Selected Papers