SWIFT INSTITUTE

SWIFT INSTITUTE WORKING PAPER NO. 2015-001

THE EVOLUTION OF THIRD PARTY PAYMENT PROVIDERS AND CRYPTOCURRENCIES UNDER THE EU'S UPCOMING PSD2 AND AMLD4

PEGGY VALCKE
NIELS VANDEZANDE
NATHAN VAN DE VELDE

PUBLICATION DATE: 23 SEPTEMBER 2015

Table of Contents

Acknowledgments

This research has been made possible with the support of a grant from the SWIFT Institute.

Furthermore, the research leading up to the results reported here draws from experience gained from the iMinds TRU-BLISS project, a research project co-funded by iMinds, a research institute founded by the Flemish Government.

About

The KU Leuven Centre for IT & IP Law is a research center at the faculty of law of KU Leuven University, founded in July 2014 following the merger of the Interdisciplinary Centre for Law and Information Technology (ICRI) and the Centre of Intellectual Property Rights (CIR). ICRI was founded in 1990 by Prof. Dr. Jos Dumortier and became one of the top five IT law research centers in Europe. CIR was established in 1988 on the initiative of Prof. Dr. Frank Gotzen.
The KU Leuven Centre for IT & IP Law employs over 40 staff members, specialized in legal-ethical aspects of ICT and IP innovation and focus on the fundamental re-thinking of current legal frameworks, necessitated by the rapid evolution of technology in different fields (government, media, copyrights, healthcare, pharmacology, commerce, banking, transport, etc.) It is a member of The Leuven Center on Information and Communication Technology (LICT) and iMinds (www.iminds.be), and was the coordinator of the Belgian Cybercrime Centre of Excellence for Training, Research and Education (www.b-ccentre.be).
The KU Leuven Centre for IT & IP Law has a solid track record as legal partner of large international and interdisciplinary research projects and is internationally renowned for its expertise in the areas of data privacy and information security law, new media and communications law, information rights management and intellectual property rights.

Prof. Dr. Peggy Valcke is full time research professor (BOFZAP) at KU Leuven and teaches media law in the advanced master in Intellectual Property Law at HUBrussel. She joined the Interdisciplinary Centre for Law & ICT (ICRI) in 1996. She is visiting professor at the University of Tilburg and member of the scientific committee of the Florence School of Regulation - Communications and Media. In 2006, she was visiting professor at Central European University in Budapest, Hungary, and lecturer in the Oxford/Annenberg Summer School. Prof. Valcke is recognized as a leading European expert on media and communications law. She has been included in the 2010 Who's Who in the World, is a frequently invited speaker at conferences and expert workshops, and has published widely in national and international journals (in English, French, German and Dutch) on a broad range of topics relating to electronic communications law, media law and competition law.

Niels Vandezande is a legal researcher at the KU Leuven Centre for IT & IP Law - iMinds since 2009. He obtained his LL.B. and LL.M. degrees at the same university, focusing on ICT-law, international law and corporate law. He currently conducts Ph.D. research on the regulatory aspects of virtual currencies under financial and economic law. Working in interdisciplinary applied research projects, his main research interests are in the fields of virtual currencies and electronic payments. He has also gained substantial expertise working on projects related to security & trust issues, as well as regarding privacy and identity management. Since 2010, he has also been a regular contributor to the Belgian news section of Privacy & Informatie.

Nathan Van de Velde is a legal researcher at the KU Leuven Centre for IT & IP Law - iMinds, involved in the TRU-BLISS project (2014-2016) which aims to help banks augment their cyber security readiness. He obtained his Master of Laws in 2012 from the same university, as well as an additional LLM in Intellectual Property Rights & ICT (cum laude) at H.U. Brussels/KU Leuven in 2013. He completed the Schuman traineeship with the Directorate-General for Innovation and Technological Support at the European Parliament in 2014. Before that, he

worked as a legal intern for a Brussels-based Intellectual property practice and worked at a Public Affairs consultancy focusing on Technology, Media and Telecommunications policies.

List of Tables

List of Figures

1. Introduction

HISTORICAL BACKGROUND - The late 1990's and early 2000's have brought a number of developments within the financial world that gave rise to new actors within payment systems. On the one hand, there are the issuers of electronic money, or e-money. The European Union (EU) has subjected these entities to specific regulation by means of the E-money Directive.[1] On the other hand, there are the entities that provide payment services. For these actors, the EU adopted the Payment Services Directive aimed at harmonizing market access for non-credit institution actors in order to create a level-playing field, instill more competition in national markets, and reflect market developments.[2]

LEGISLATIVE DEVELOPMENTS - In more recent years, however, a new type of entity has developed: third party payment providers. These actors allow consumers to, for instance, make online payments without the need for a credit card by establishing a "*link between the payer and the online merchant via the payer's online banking module*".[3] A number of third party payment providers have become very successful within the EU, important examples being SOFORT in Germany, iDEAL in the Netherlands and Trustly in Sweden. These third party payment providers do not require the consumer to open an account directly with them. Instead, they gather information on the consumer's existing bank accounts and present that information in an integrated manner.[4] However, in doing so these entities gain possession of a significant amount of sensitive information, for instance by providing a gateway from which consumers log in to their bank accounts using their unique identifiers and credentials. As a result, these entities are drawing increasingly more attention from legislators and regulators. After all, the sensitive information they possess and process poses a significant risk for abuse in money laundering schemes, terrorist financing, or other illicit activities.

NEW PAYMENT METHODS - Another notable development is that of alternative payment methods. These are payment systems that do not rely on the classic actors usually found within payment systems – such as banks or payment service providers – and that may go as far as to substitute the use of accepted legal tender for that of alternative currencies. A prime example here are cryptocurrencies such as bitcoin. The bitcoin ecosystem is decentralized, meaning that no single entity controls the system. Moreover, its use of unique pseudonymous transaction identifiers can provide a certain level of anonymity for its users.

---

[1] Directive 2000/46/EC of the European Parliament and of the Council of 18 September 2000 on the taking up, pursuit of and prudential supervision of the business of electronic money institutions, *OJ* L 275 of 27 December 2000, 39-43. This directive was replaced in 2009: Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC, *OJ* L 267 of 10 October 2009, 7-17 (hereinafter: Second E-money Directive or EMD2).

[2] European Commission (2005) "Proposal for a directive of the European Parliament and of the Council on payment services in the internal market and amending Directives 97/7/EC, 2000/12/EC and 2002/65/EC", *COM(2005) 603 final*, 7. This legislative proposal eventually became the Payment Services Directive or PSD: Directive 2007/64/EC of the European Parliament and of the Council of 13 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 of 5 December 2007, 1-36.

[3] European Commission (2013) "MEMO: Payment Services Directive and Interchange fees Regulation: frequently asked questions", *MEMO-13-719*.

[4] These are so-called "account information services". European Commission (2013) "MEMO: Payment Services Directive and Interchange fees Regulation: frequently asked questions", *MEMO-13-719*.

These characteristics have made cryptocurrencies a favored payment alternative for those that eschew established financial actors and currency. Consequently, this has also made cryptocurrencies a target of those engaged in drug trafficking and money laundering.[5]

[5] As evidenced in the recent conviction in the Silk Road case: Greenberg, A. (2014) "Silk Road Mastermind Ross Ulbricht Convicted of All 7 Charges", *Wired*, 4 February 2015.

2. State of the art

THIRD PARTY PAYMENT SERVICES - Despite the rising popularity of third party payment providers and the sensitivity of their activities through the data they process, they are not covered by the scope of the current Payment Services Directive. As a result, these entities are presently not regulated at the level of the EU. The European Commission has therefore proposed a new set of rules – in the form of a Second Payment Services Directive (PSD2) – to cover what is referred to as "third party payment providers", "payment initiation services" and "account information services".[6] This initiative would essentially bring such third party payment providers under the same standards of regulation and supervision as existing payment service providers. Moreover, the Commission's proposal also includes a number of requirements relating to stronger security measures, emphasizing the need for strong authentication mechanisms.

LEGISLATIVE PROPOSAL - However, as the legislative procedure regarding this proposal is still ongoing, the precise scope of the eventual directive – if adopted – remains unclear. It is therefore as of yet uncertain whether this proposal will succeed in bringing the wide range of different third party payment providers under the fold of regulatory scrutiny. Moreover, it is unclear what the precise relation will be for third party payment providers under the PSD2 and the recently adopted Fourth Anti-Money Laundering Directive (AMLD4).[7]

CRYPTOCURRENCIES - Additionally, the legislator has as of yet remained largely silent on the topic of alternative payment systems, in particular cryptocurrencies. Within the EU, existing research has established that the application of the E-money and Payment Services Directives to cryptocurrencies is problematic, if not downright impossible.[8] However, it remains unclear how such cryptocurrencies should then be qualified from the perspective of financial law. Moreover, the service providers engaged in cryptocurrencies – mostly in the form of exchange platforms – have proven untrustworthy, and are often mired in dubious activities.[9] Similarly, the response of legislators and regulators remains to be seen. While it is becoming increasingly more evident that clear rules are needed here, the current state of the legislative procedures regarding the PSD2 and the AMLD4 do not make any reference to a possible inclusion of cryptocurrencies under their scope. At this moment, only an inclusion under the next revision of the E-money Directive seems to be on the cards.[10]

---

[6] European Commission (2015) "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/2013/547 final.*

[7] European Commission (2013) "Proposal for a directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing", *COM/2013/045 final* (hereinafter: Proposal AMLD4).

[8] Vandezande, N. (2014) "Between Bitcoins and mobile payments: will the European Commission's new proposal provide more legal certainty?", *International Journal of Law and Information Technology, 22*(3), 295-310.

[9] As evidenced in the closing of Mt.Gox with allegations of theft and money laundering, theft at Bitstamp, money laundering at BitInstant, etc. Popper, N., Abrams, R. (2014) "Apparent Theft at Mt. Gox Shakes Bitcoin World", *New York Times*, 25 February 2014; Hackett, R. (2015) "Hackers steal $5 million from major bitcoin exchange", *Forbes*, 5 January 2015; Wile, R. (2014) "CEO of bitcoin exchange arrested", *Business Insider*, 27 January 2014.

[10] Payment Systems Market Expert Group (2014) "Minutes of the meeting of 22 October 2014", *PSMEG 008/14.*

3. Research objectives

DUAL OBJECTIVE - Our research paper has a dual objective: (1) to analyze which third party payment providers are covered by the upcoming PSD2 and AMLD4, the consequences thereof, as well as to what extent such coverage goes; and (2) to analyze the potential for the regulation of cryptocurrency in terms of combatting money laundering and terrorist financing.

ANALYSIS OF EU REGULATORY FRAMEWORK - The objective of this analysis is to identify whether the core third party payment providers can be covered by the PSD2 and AMLD4, and whether industry and regulatory guidelines are adequately implemented. Similarly, in assessing the potential for regulation of cryptocurrencies, it will be made clear to what extent cryptocurrency service providers can be made subject to the regulation regarding anti-money laundering (AML) and combatting the financing of terrorism (CFT).

COMPARATIVE ANALYSIS - While the primary focus of the research is put on legislative initiatives within the EU, it is the goal to assess whether the findings can be extrapolated to facilitate global cooperation in this field. Given the global reach of third party payment providers, a global outlook is pivotal in establishing effective AML and CFT initiatives.

4. Methodology

LEGAL THEORETICAL LITERATURE STUDY - Given the focus of the proposed research on the prospects for regulation of third party payment providers – including cryptocurrency service providers – within the EU, the core method used for this paper is a legal theoretical literature study. Furthermore, the paper will build on the knowledge regarding AML and CFT regulation gained by the authors through an interdisciplinary research project which they are currently leading and which involves members of the Belgian banking sector.[11] This cooperation also allows the authors to gain a better understanding of the perceived risks regarding third party payment providers within that sector. In addition, a comparative analysis with the US and Asia will be conducted. The analysis of the US is based on a literature study. For the comparative analysis with the Asian market, the authors had to rely on secondary sources as the relevant texts are not readily available in English.

TWO RESEARCH TRACKS - Overall, the research will be conducted along two parallel tracks, each corresponding to one of the core objectives: (1) third party payment providers under PSD2 and AMLD4; (2) regulation of cryptocurrencies and their service providers.

THIRD PARTY PAYMENT PROVIDERS - The first research track (Section 5) will start with a critical assessment of the scope of the PSD2 and AMLD4 in their current state of the legislative procedure.[12] This will serve to identify whether the broad range of rather different third party payment providers can adequately be covered by the scope of the proposed directives, or whether gaps will remain in the upcoming legal frameworks. In doing so, the core third party payment providers are identified. As noted, the authors can build upon their experience and contacts within the financial sector in identifying those players and the risks they pose regarding money laundering and terrorist financing. The result of this exercise will be a descriptive assessment of the potential impact of the PSD2 and AMLD4 on those third party payment providers. Additionally, it will be assessed to what extent industry and regulatory guidelines – such as those of the European Central Bank (ECB), [13] the European Banking Authority (EBA) and those of the Financial Action Task Force (FATF)[14] – are taken into account. This will entail a normative assessment of where those guidelines should be followed more closely, where needed. Such assessment will establish the potential for sector-based self-regulation.

---

[11] *https://www.law.kuleuven.be/apps/icri/en/overview/showProject/282/*.

[12] The AMLD4 was adopted in May 2015. For the PSD2, a political agreement has been reached following trilogue discussions in June 2015. Also after their adoption, there will still be discussion and uncertainty regarding their implementation by the Member States.

[13] See: ECB (2013) "Recommendations for the security of Internet payments", *ecb.europa.*eu 16p. An accompanying assessment guide was released as: ECB (2014) "Assessment Guide for the Security of Internet Payments", *ecb.europa.eu*, 60p. Note that third party providers are addressed in a separate document: ECB (2014) "Final recommendations for the security of payment account access services following the public consultation", *ecb.europa.eu*, 25p. These recommendations are, however, mainly intended for transmission to the EBA and – in light of the ongoing review of the Payment Services Directive – are not intended to be taken as final.

[14] The Financial Action Task Force (FATF) is an inter-governmental body established by the Ministers of its Member jurisdictions. The objectives of the FATF are to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. Consequently, the FATF is a "policy-making body" which works to generate the necessary political will to bring about national legislative and regulatory reforms in these areas.

CRYPTOCURRENCIES - The second track (Section 6) focuses on the regulation of cryptocurrencies and their service providers. It will start with a concise, non-exhaustive description of the shortcomings of the current Payment Services Directive and the Second E-money Directive in regulating cryptocurrencies. The question whether cryptocurrencies could be included under the PSD2 and AMLD4 will then be analysed in more detail, followed by a normative assessment of the potential direction for the upcoming third revision of the E-money Directive. The goal of that exercise is to assess whether the original objectives of that directive still hold true in a fundamentally changed payments landscape, or whether revised objectives are needed. Next, the focus will be put on the service providers engaging in cryptocurrencies – specifically the cryptocurrency exchanges. Here, it will be analyzed whether they can be included under existing and upcoming AML and CFT regulation. The paper will take a closer look at recent developments in the US and Asian markets, such as the New York State Department of Financial Services' proposal to establish a license for virtual currency service providers, in order to critically assess the potential of licensing schemes in Europe in terms of AML and CFT.

CONCLUSION AND POLICY RECOMMENDATIONS - The last part of the paper (Section 7) will integrate the results of both tracks into final conclusions. It will formulate a number of policy recommendations allowing the extrapolation of this research to developing economies and in international cooperation. Such broader cooperation should be sought as the reach of third party payment providers and their risks of money laundering and terrorist financing are inherently global. Localized approaches must therefore be avoided.

5. Third Party Payment Service Providers under the EU's legal framework

RESEARCH OBJECTIVE - This section will analyse the legal position of third party payment providers under the EU's upcoming legal frameworks revising the existing Payment Services Directive and the Fourth Anti-Money Laundering Directive.[15] More specifically, the expected impact of the proposed PSD2 and AMLD4 on third party payment providers will be assessed, focusing on which actors will fall under the regulatory scope, to what extent and the consequences thereof. In addition, the potential risks associated with their activities will be identified and it will be assessed whether both legal frameworks adequately address these risks.

5.1. European Payment Services Directive

5.1.1. Proposal PSD2

SECOND PAYMENT SERVICES DIRECTIVE - The Payment Services Directive was adopted in 2007 and reviewed by the European Commission late 2012.[16] In July 2013, the European Commission presented its conclusions on this review and introduced two legislative proposals.[17] One of these proposals consists of introducing a regulation on interchange fees for card-based payment transactions.[18] The other one entails the replacement of the current Payment Services Directive by a new one ('PSD2').[19] In its Green Paper on card, internet and mobile payments of 2012, the European Commission found that payments were identified as one of the main barriers to the future growth of e-commerce.[20] While the Payment Services Directive did realize progress in this field, it was found that the EU payments market still remained too fragmented.[21] Moreover, the application of the directive was found to be inconsistent, leaving a legal vacuum for newly emerging service providers, and suffering from a lack of standardization and interoperability.[22] To solve such issues, it was decided to propose a new directive, rather than to amend the existing one. The new directive will have as its principal objective to further develop the EU electronic payment market in a technologically neutral manner by adapting the existing legal framework to emerging and innovative payment services.

---

[15] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, *OJ* L 141/73 of 5 June 2015 (hereinafter: Fourth Anti-Money Laundering Directive or AMLD4).

[16] Article 87 Payment Services Directive.

[17] European Commission (2013) "New rules on Payment Services for the benefit of consumers and retailers", *press release IP-13-730*.

[18] European Commission (2013) "Proposal for a regulation of the European Parliament and of the Council on interchange fees for card-based payment transactions", *COM/2013/0550 final.*

[19] European Commission (2013) "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*.

[20] European Commission (2012) "Green Paper Towards an integrated European market for card, internet and mobile payments", *COM/2011/0941 final*, 5.

[21] *Ibid.,* 6.

[22] European Commission (2013) "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* (Hereafter Proposal PSD2).

STATE OF PLAY - On 5 June 2015 the Council of the European Union published the final compromise text of the PSD2 and invited the Permanent Representatives Committee (COREPER) to approve the final text.[23] Before it can be formally adopted by the Council (which is anticipated in late 2015), the PSD2 will have to pass the plenary vote in the European Parliament (which is expected to take place in October). Once adopted, Member States will have two years to transpose the PSD2 into national law.

5.1.2. Key Changes of PSD2

NOTABLE CHANGES - Considering that the PSD2 is not yet finalised and technical discussions are still planned, some provisions remain subject to change. However, as major amendments are not expected, the subsequent paragraphs will offer a brief overview of the key changes. A table summarizing the key changes of the PSD2 will be provided at the end of this section.

SCOPE - The territorial scope of the PSD2 is somewhat enlarged with more reliance on the one-leg principle.[24] The negative scope[25] is mostly maintained, with the 'limited network' and 'value-added service' exceptions being reformulated.[26]

PAYMENT SERVICE PROVIDERS - Whilst the PSD2 continues to apply to six types of payment service providers, it does introduce two new forms of payment services provided by third party payment service providers (Hereafter TPP's), namely "*Payment Initiation Service Providers*" and "*Account information Service Providers*". TPP's are to be contrasted with "*Account Servicing Payment Service Providers*", who maintain the actual payment accounts. These TPP's will be required to be authorized as payment institutions. Consequently, the PSD2 introduces several new significant definitions:

- "(10) '*account servicing payment service provider' means a payment service provider providing and maintaining payment accounts for a payer*"

- "(11) '*payment initiation service provider' means a payment service provider pursuing business activities referred to in point 7 of Annex I*"

- "(32) '*payment initiation service' means a service to initiate a payment order at the request of the payment user with respect to a payment account held at another payment service provider*"

- "(33) *'account information service' means an online service to provide consolidated information on one or more payment accounts held by the payment service user with either another payment service provider or with more than one payment service provider".*

[23] Council of the European Union (2015), "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", *9336/15* (Hereafter final compromise text PSD2).
[24] One-leg out transactions are where one of the payment service providers is located outside the European Union or the European Economic Area (EEA). See articles 1-2 Proposal PSD2.
[25] The negative scope outlines the conditions under which the Directive is not applicable.
[26] Article 3 Proposal PSD2.

GENERAL RULES - The general rules for payment service providers still entail an information obligation, but the information to be provided for authorization has been expanded. The own funds calculation and the safeguards thereof have been maintained.[27] The authorization and registration procedure remains the same, with the addition of a register maintained by the European Banking Authority (EBA).[28] In terms of competent authorities, supervision and waivers, only the exercise of the right of establishment and freedom to provide services is expanded with tasks delegated to the EBA to issue guidelines and standards.[29] A notification duty has been added for service providers that want to be recognized as limited network.[30] The transparency and information requirements have been revised and now include explicit reference to information to be provided by third party payment providers.[31] The principles regarding the execution of payment orders remain mostly the same.[32] The main amendments relate to the inclusion of third party payment service providers and strong authentication under liability.[33] Also the chapter on data protection remains the same in the Proposal.[34]

RIGHTS AND OBLIGATIONS - Concerning the common provisions and authorization principles on the rights and obligations relating to payment services[35] a few more amendments have been made. For one, the scope of consent has been expanded.[36] Notably linked to the inclusion of third party payment providers are the provisions relating to access to and use of payment accounts, mainly relating to security and information requirements.[37] TPP's have also been inserted in other provisions.[38] Payer's liability for payments via distance communication where no strong customer authentication was required is reduced from EUR 150 to EUR 50 except in the case of fraud or gross negligence.[39] Provisions on liability allocation between third party payment service providers and other payment service providers have also been introduced. For direct debits, a principal right for refund has been included, which notably refers to the payment service provider to argue with the payee whether the conditions that would prevent a refund are met.[40]

SECURITY REQUIREMENTS - A new chapter relates to security requirements.[41] In contrast to the initial proposal the explicit references made to the proposed NIS directive[42] have been

[27] Articles 5-8 Proposal PSD2.
[28] Articles 10-20 Proposal PSD2.
[29] Articles 21-28 Proposal PSD2.
[30] Articles 29-30 Proposal PSD2.
[31] Articles 31-53 Proposal PSD2.
[32] Articles 69-83 Proposal PSD2.
[33] Article 80 Proposal PSD2.
[34] Article 84 Proposal PSD2.
[35] Articles 54-68 Proposal PSD2.
[36] Article 57 Proposal PSD2.
[37] Articles 58-59 Proposal PSD2.
[38] E.g. Articles 63-65 Proposal PSD2.
[39] Article 66 Proposal PSD2.
[40] Article 67 Proposal PSD2.
[41] Articles 85-87 Proposal PSD2.
[42] European Commission, Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, 2013/0027 (COD).

removed. Nonetheless, risk management and incident reporting requirements remain.[43] Strong authentication is needed for a diverse range of services, [44] unless they are exempted by the expected EBA guidelines. The complaint and redress procedure has been updated.[45] Competent authorities are designated and given the necessary powers to ensure and monitor effective compliance.[46] Moreover, payment service providers are to adopt measures for internal dispute resolution to settle complaints of payment service users.[47] Finally, the new directive aims at full harmonization[48] and transitional provisions are foreseen for existing payment service providers in anticipation of the entry into force of the Directive.[49]

5.1.3. Third Party Payment Service Providers

BACKGROUND - The notion of TPP's is one of the key developments since the adoption of the original Payment Services Directive. More and more, payment transactions are no longer exclusively conducted between a user and his bank, but also include an intermediate party that provides an interface between the merchant and the user's bank.[50] As these intermediaries are principally not collecting payments, they were excluded from the scope of the original directive. However, as they do act as access gateway to the user's payment information, their activities do bear important security, data protection and liability issues. This is the main reason why the European Commission proposed to bring these actors under the same framework, subjecting them to similar supervision, authorization, and security requirements as the classic payment service providers. While this reasoning seems to be widely endorsed, there are concerns on the precise implementation of such inclusion. For instance, it is feared that third party payment service providers would be enabled to access the personalized security credentials of users.[51] This would conflict, for instance, with the requirement that the user keep their personalized security features safe.

CORE ACTORS - With third party payment service providers now falling under the scope of the PSD2, three core actors need to be distinguished. As already mentioned, two new forms of payment service providers are introduced, namely, payment initiation service providers (PISP) and account information service providers (AISP). In addition, the PSD2 establishes a new term with account servicing payment service providers (ASPSP) which refers to the classic payment service providers, who provide and maintain payment accounts for a payment user.

[43] Articles 85-86 Proposal PSD2.
[44] Article 87 (1) Proposal PSD2 "*when the payer accesses his payment account online; initiates an electronic payment transaction; and/or 'carries out any action through a remote channel which may imply a risk of fraud or other abuses*".
[45] Articles 88-92 Proposal PSD2.
[46] Article 89 Proposal PSD2.
[47] Article 90 Proposal PSD2.
[48] Article 95 Proposal PSD2.
[49] Article 95 Proposal PSD2.
[50] Examples mentioned by the European Commission include iDeal and Sofort.
[51] European Banking Federation (2014) "Press Release: Banks: Payment package still needs work after EU Parliament vote", *EBF_007620*. Boudewijn, G. (2014) "PSD2: EPC Identifies Considerable Scope for Amendments of the Proposed New Set of Rules Related to the Activity of Third Party Payment Service Providers Offering Payment Initiation or Payment Account Information Services", *EPC Blog*, 25 March 2014.

TECHNOLOGICALLY NEUTRAL - Following the ECB's opinion of 5 February 2014 it is clear that the definitions concerning TPP's are drafted as simple and flexible as possible, to ensure that future emerging payment innovations will also be captured under the regulatory scope. In that regard any specific references to a particular technology has been removed.[52]

PAYMENT INITIATION SERVICES - A *payment initiation service* consists of the provision by a PISP of a software bridge between the website or other application of a merchant and the online banking platform of a payer's bank in order to initiate a payment transaction.[53] In other words it enables the payer to select a PISP as a payment option on a merchant's website, whereby the PISP acts as a medium between the customer and its online payment account. The added-value of payment initiation services lies in the immediate confirmation to the merchant that the requisite funds are available and that the payer has initiated the payment. This effectively encourages the merchant to ship the acquired products immediately as he is assured that he will receive the payment.[54] Moreover, payment users are provided with the ability to shop online without the need of a credit card.[55] It is however important to note that under the PSD2 a PISP cannot at any given time hold the payer's funds.[56] Its sole service is limited to executing a payment transaction on behalf of the payer. In the event that a PISP wishes to provide additional payment services, where the holding of a payer's funds is required, it should acquire the necessary authorization to do so.

IDEAL – SOFORT - To put this into perspective, we refer to iDEAL, a Dutch based company, who provides payment initiation services. iDEAL has agreements with several participating banks to offer customers the opportunity make payments using iDEAL. The payer has to select iDEAL as the preferred payment method on a merchant's website, where he then has to select which bank he wants to perform the transaction. Subsequently, the payer is redirected to the online banking module of his bank where he has to login as usual. The details of the payment transaction will already be filled out, so the payer only has to verify and approve the payment. Afterwards, an immediate confirmation from the bank is sent stating that the payment transaction was successful.[57] However, not all payment initiatives services adopt the same approach, SOFORT, a German based payment initiation service operates differently. SOFORT adopts a four step approach. First, a payer has to select the SOFORT payment method on the merchant's website, where it has to select the bank which will carry out the transaction. Next, the payer will be required to login to the API of SOFORT using their own personalized security credentials. SOFORT will then access the payer's account and initiate the payment. In a third step the payer will be required to confirm the

[52] European Central Bank (2014) "Opinion of 5 February 2014 on a 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", *OJ* C 224, 15.7.2014, 16-17.
[53] Recital 18 final compromise text PSD2.
[54] European Council (2015), "Press Release: Electronic payment services: Council confirms agreement with EP on updated rules", 4 June 2015.
[55] European Commission (2013) "MEMO: Payment Services Directive and Interchange fees Regulation: frequently asked questions", *MEMO-13-719.*
[56] Recital 18 final compromise text PSD2.
[57] For more information see https://www.ideal.nl/en/payer/what/

transaction using a non-reusable confirmation code. In a last step the payer will receive a summary of the SOFORT transaction or an order confirmation from the merchant.[58]

ACCOUNT INFORMATION SERVICES - *Account information services* are services whereby an AISP acts as an aggregator of data, where consolidated information on one or more of a payment service user's online payment accounts held by ASPSP's is provided. As such, the AISP provides the payment service user an overall view of his financial situation at a given moment. In practice the AISP will connect directly to the online platform of the user's ASPSP using the security credentials issued by the ASPSP to the user. The collected information from the online banking platform is then provided by the AISP on its website or application.[59]

MONEY DASHBOARD - Money Dashboard, a UK based service, is an example of an account information service provider.[60] It allows its users – after registration – to link their various internet-enabled bank and credit card accounts in one place. Customers can add new accounts by entering their personalised security credentials which will then link the account to Money Dashboard. In addition to providing an overview of financial accounts, Money Dashboard also provides customers with the opportunity to analyse past transactions breaking down spending habits and then provides prospective closing balances for the months ahead based on recent spending habits, allowing customers to take control of their budget.[61]

AUTHORISATION REQUIREMENTS - As TPP's are effectively brought under the regulatory scope of the PSD2 and do not fall within the exception fashioned for technical service providers, they will need to acquire proper authorisation in order to legitimately provide their services.[62] Nevertheless, the applicable authorisation requirements are somewhat more lenient compared to other payment service providers. Such leniency is reflected by the intent of the European Commission to bring more competition to the payment market by removing barriers to potential new innovative market entrants. The leading principle is that TPP's should not be subjected to overly burdensome regulatory obligations as that could effectively obstruct their entry onto the payment market. Hence, TPP's, in the event they exclusively offer payment initiation or account information services, are not subject to the 'own funds' requirements.[63] Moreover, AISP's are not subject to initial capital requirements whilst PISP's will need to hold at least EUR 50.000 at the time of authorisation.[64] The rationale for a more lenient approach concerning authorization requirements stems from the fact that TPP's never come into the possession of funds during payment transactions. In that regard, the PSD2 prescribes that AISP's, in light of the nature of the activities they perform, can enjoy a specific prudential regime, which waives certain authorization

[58] For more information see SOFORT Banking, How it works, https://www.sofort.com/eng-GB/buyer/sb/how-sofort-banking-works/
[59] Recital 18a final compromise text PSD2.
[60] Other examples include Yodlee and Mint.
[61] For more information see https://www.moneydashboard.com/getting-started
[62] Insofar the TPP is not already licensed as a credit institution or otherwise exempted from authorisation requirements.
[63] Recital 18b final compromise text PSD2.
[64] Article 6 final compromise text PSD2.

requirements altogether.[65] Despite the afforded leniency in authorization requirements, the PSD2 does however aim to bring all payment service providers, including TPP's, within the ambit of certain minimum legal and regulatory requirements. Thereby, more stringent obligations are applicable in the event of outsourcing or the use of agents. In addition, both TPP's will need to hold a professional indemnity insurance or a similar guarantee to cover their liabilities under the PSD2.[66] The required amount of indemnity assurance or a comparable guarantee will be further specified by the EBA, who will consider the risk profile of the undertaking and take the number of clients an AISP serves into account.[67]

INFORMATION AND TRANSPARENCY - TPP's will, just as other established payment institutions, need to comply with strict information and transparency regulatory requirements, in particular, vis-à-vis payment users and ASPSP's. Thus, in order to enhance consumer protection and safeguard payments security, PISP's are subject to stringent information requirements prior to the initiation of a payment order. For instance, it will have to communicate to the payer its identity and the extent of its services.[68] Similarly, after the initiation of a payment order, a PISP will be required to provide confirmation of the payment order, which should include a reference enabling the identification of the payment initiation.[69] Where applicable, a breakdown of the added charges payable to the PISP for its services has to be provided to the payer and the payee.

IDENTIFICATION OBLIGATION - Throughout the negotiations of the PSD2, concerns were raised on the fact that the initial proposal did not provide certainty that the ASPSP would be able to identify a TPP requesting access to a payment account. Given the fact that TPP's would in theory impersonate the payment user, ASPSP's would have no control or knowledge on who is in fact accessing the account.[70] According to the stakeholders this would weaken authentication measures which ultimately could lead to man-in-the-middle attacks.[71] As a result the PSD2 requires that TPP's need to identify themselves vis-à-vis the ASPSP for each payment initiation or communication session.[72]

Access to PAYMENT Accounts - Since TPP's do not provide nor maintain a payment account, they remain dependent on ASPSP's to be able to provide their services. Consequently, the PSD2 acknowledges the right for a payer to use a TPP to obtain payment services, by enabling access to and use of payment accounts. The concept mandates that ASPSP's are obliged to grant TPP's access to and use of payment accounts in the event payment users have explicitly given their consent.[73] However, it is not clarified whether the required consent is needed for each access request, nor does it specify how long the given consent

[65] Article 27a and article 5, (k) final compromise text PSD2.
[66] Article 5, 2 final compromise text PSD2.
[67] Article 5, 3 final compromise text PSD2.
[68] Article 38 final compromise text PSD2.
[69] Article 39 final compromise text PSD2.
[70] Wandhöffer, R. (2014) "Transaction Banking and the Impact of Regulatory Change, Basel III and other Challenges for the Global Economy", *Palgrave Macmillan*, 2014, p. 188-189.
[71] Kokert, J. and Held, M. (2014) "Payment Services Directive II: Risks and serious consequences for users and banks", *BaFin section for IT infrastructure of banks*, June 2014.
[72] Article 59-60 final compromise text PSD2.
[73] Article 58 final compromise text PSD2.

would last.[74] When ASPSP's offer online payment accounts they are thus required to provide secure facilities in order to enable TPP's to provide their services. However, such a requirement evidently implies operational difficulties, when considering the diversity of payment services and lack of standardized online banking interfaces.[75] The PSD2 has tasked the EBA to develop common and open standards to be implemented by all ASPSP's in order to ensure secure communications between the ASPSP's and TPP's.[76] In addition to acquiring the explicit consent by informing the payment user of the extent of the access, the PISP will need to comply with additional obligations which aim to enhance the security of these services. Aside from the obligation that PISP's must not hold the payer's funds at any given time, they have to ensure that the personalized security credentials are not accessible to other parties and that security credentials are transmitted through safe and secure channels.[77] Any additional information the PISP obtains through the payment initiation service can only be provided to the payee with the explicit consent of the payment service user.[78] In addition, whenever a PISP initiates a payment, it needs to identify itself as such to the relevant ASPSP. The PISP is moreover prohibited from storing any sensitive payment data or requesting additional information irrelevant to the payment transaction of the payment user. Furthermore, the PISP is expressly prohibited from using, accessing and storing any data for purposes other than initiating the payment transaction. The obligations placed on AISP's for access to and use of payment account information are parallel with those placed on PISP.[79] However, AISP's can only access information from designated payment accounts and associated payment transactions.[80]

NON-DISCRIMINATION - Besides providing the necessary facilities to ensure secure communications, ASPSP's are prohibited from applying any form of discrimination in their relations with TPP's. Such discrimination includes requiring the use of a particular business model, applying additional charges or giving them a lower priority.[81] Much to the dismay of industry stakeholders the PSD2 stipulates that ASPSP's cannot make access to and use of payment accounts dependent on any sort of contractual agreement.[82] Still, ASPSP's can for "*objectively justified and duly evidenced reasons*" related to unauthorized or fraudulent access or payment transactions refuse to grant TPP's access to payment accounts. In the event of such refusal, the ASPSP will need to inform the payment user of the reasons for such refusal.

STRONG CUSTOMER AUTHENTICATION - The PSD2 intends to safeguard a high level of electronic payment security. Therefore, payment service providers, including TPP's, are required to put security measures in place which ensure the confidentiality and integrity of payment transactions. Strong customer authentication measures are thus required when a payer i)

[74] Article 57 final compromise text PSD2.
[75] Salmony, M. (2014) "Access to accounts – why banks should embrace an open future 2014", *JPSS Journal of Payments Strategy & Systems*, Vol 8 No 2, May 2014, p. 157-171.
[76] Recital 51 and article 87a final compromise text PSD2.
[77] Except to the user and issuer of the personalised security credentials.
[78] Recital 51 final compromise text PSD2.
[79] Article 59 final compromise text PSD2.
[80] Article 59, 2d final compromise text PSD2.
[81] Recital 51 and articles 58-61 final compromise text PSD2. In particular in terms of timing, priority or charges compared with payment initiated directly by the payer.
[82] Article 58, 4a and 59, 3a final compromise text PSD2.

accesses his payment account online; ii) initiates an electronic payment transaction; and iii) carries out any action through a remote channel which exposes the payment user to risks of payment fraud or other abuses.[83] In the event of remote electronic payments, a strong customer authentication will additionally require the use of dynamic elements linking the transaction to the amount and the payee. The PSD2 defines strong customer authentication as "*an authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others and is designed in such a way as to protect the confidentiality of the authentication data*".[84] Strong customer authentication procedures also include personalized security credentials, which typically refer to the use of passwords and PIN numbers.[85] These credentials are employed to limit the risks of unauthorized access and other fraudulent related activities[86] and clearly reflect the strong customer authentication measures introduced in the SecuRe Pay recommendations published by the European Central Bank in May 2014.[87] The EBA is responsible to draft regulatory technical standards that further detail the requirements, *inter alia* requirements of strong customer authentication procedure and the exemptions thereof.[88]

PERSONALIZED SECURITY CREDENTIALS - Under PSD2, TPP's will be able to rely on the authentication procedures, including personalized security credentials, provided by the ASPSP. This, however, raises legitimate causes for concern. Undeniably, it is at odds with the obligations that rest on both the payment users, who are required to take all the necessary steps to ensure the safety and security of the issued personalized security credentials, and the ASPSP's, who similarly have to ensure that the personalized security credentials are not accessible to parties other than the payment service user.[89] Since payment service providers (save in the circumstance the payment user has committed fraud) that fail to comply with the strong authentication requirements are liable for any mishaps, a clear allocation of liability should be present. Throughout the negotiations of the PSD2, the industry continuously raised the ambiguity of this reliance.[90] Indeed, assenting payment users to disclose their security credentials to third parties is contradictory with the impetus of the PSD2, strengthening consumer protection vis-à-vis the possibilities of fraud and other security threats. The increased exposure of such credentials to third parties would evidently lower consumer protection and increase security risks.[91]

ALLOCATION OF LIABILITY - As already mentioned, a clear allocation of liability between the ASPSP and TPP's is necessary in the case of compliance with the requirements of strong authentication procedures. However, the revised allocation of liability does not sufficiently

[83] Article 87 final compromise text PSD2.
[84] Article 4, 22 final compromise text PSD2.
[85] Recital 18 final compromise text PSD2.
[86] Recital 51b final compromise text PSD2.
[87] European Central Bank (ECB), Final recommendations for the security of payment account access services following the public consultation, May 2014, pp. 25
[88] Article 87a final compromise text PSD2.
[89] Recital 51b final compromise text PSD2.
[90] VISA Europe (2014) "Our response to the European Commission's proposed revision of the Payment Services Directive", July 2014, p. 6.
[91] Boudewijn, G. (2015) "PSD2: Almost final – a state of play", *EPC Blog*, 18 June 2015.

provide an answer to the abovementioned ambiguity. Despite the provision that TPP's are deemed liable for the respective parts of the transactions that are under their control, the ASPSP remains the 'first-port-of-call' for payment service users. This implies that, even in the event of an unauthorized service caused by the PSP, the payment service user is entitled to demand compensation from its ASPSP. The ASPSP however, retains a right of recourse vis-à-vis the TPP, who will have to prove that the unauthorized, or the defective, payment for that matter did not occur through his fault. However, the PSD2 fails to clarify how this procedure would work in practice.[92] It is clear however, that the allocation of liability is not welcomed by the industry. Much to their dismay, ASPSP's remain responsible in the event a service with a TPP is unauthorized, defective or late. To make matters worse, the PSD2 explicitly prohibits the use of a contractual agreement between the ASPSP and a TPP, which could clarify the allocation of liability in specified circumstances. Consequently, the ASPSP's bear the burden of recovery and will need to take additional costs of possible legal action and insolvency of a TPP into account.[93]

DATA PROTECTION - Concerning data protection rules, the PSD2 permits the processing of personal data by payment service providers in order to safeguard the prevention, investigation and detection of payment fraud.[94] The processing of personal data should nonetheless be in accordance with Directive 95/46/EC.[95] Considering articles 58 and 59 which prohibit TPP's from storing sensitive payment data or using, accessing and storing any data for purposes other than their specified services, it is unclear in how far TPP's can comply with the data protection obligations set out in article 84.

RISK MITIGATION REQUIREMENTS - Finally, TPP's will need to take operational and security risk mitigation requirements into account. Article 85 stipulates that payment service providers need to establish a framework with appropriate mitigation measures and control mechanisms to manage the operational risks, including security risks, related to the payment services they provide. In addition, incident reporting requirements will equally become part of the repertoire for TPP's. As such they will be required, in the event of a major operational (including security) incident, to notify without undue delay the competent authorities. Moreover, if an incident can impact their customers they are required to provide them with necessary information, including mitigating measures to minimise the potential negative impact.[96]

[92] Recital 56 final compromise text PSD2.

[93] Boudewijn, G. (2014) "PSD2: EPC Identifies Considerable Scope for Amendments of the Proposed New Set of Rules Related to the Activity of Third Party Payment Service Providers Offering Payment Initiation or Payment Account Information Services", EPC Blog, 25 March 2014.

[94] Article 84 final compromise text PSD2.

[95] Directive 95/46/EC of the European Parliament and 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, *OJ* L 281 of 23 November 1995, 31-50. It is however important to note that the Data Protection Directive is currently undergoing a review, where the existing directive will be replaced by a Data Protection Regulation. See Proposal of 25 January 2012 for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final

[96] Article 86a final compromise text PSD2.

The following table summarizes the key changes of the PSD2 relating to TPP's:

Provision	Description
Definition **PISP** **AISP**	• *a service to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider* • *an online service to provide consolidated information on one or more payment accounts held by the payment service user with either another payment service provider or with more than one payment service provider*
PISP obligations	• Subject to licensing requirements • Cannot hold payment funds at any stage • Authenticate itself as a TPP to both the ASPSP, payer and payee in a secure way • Not store any sensitive payment data • Not use, access and store any data other than for the purposes of performing its service • Refrain from modifying the amount, recipient or any feature of the payment transaction.
AISP obligations	• Subject to licensing requirements • Services must be based on explicit consent • Authenticate itself as a TPP to both ASPSP and user in a secure way • Only access information of designated payment accounts and associated transactions • Prohibited from requesting sensitive payment data • Prohibited to use, access and store any data other than for the purposes of performing its services
ASPSP obligations	• Must allow TPP's access to online accounts • Provide facilities to ensure secure communications with TPP's • Provide transaction information to TPP's • Cannot discriminate TPP's in terms of priority, charges or timing of transaction except for objectively justified reasons • Can refuse access to online accounts for objectively justified and evidenced reasons relating to unauthorised use and/or fraud.
Security	• All TPP's are required to comply with authentication measures • TPP's must be able to rely on the authentication measures employed by the ASPSP • TPP's are obliged to adopt security measures to protect the confidentiality and integrity of personalised security credentials
Liability	• Payment user can obtain compensation from ASPSP in the event of unauthorised or incorrect execution of a payment transaction even if a PISP is involved • ASPSP has a right of recourse vis-à-vis the PISP

Table 1: Key changes PSD2

5.2. European Anti-Money Laundering Directive

5.2.1. AMLD4

STATE OF PLAY - On June 5, 2015, the fourth Anti-Money Laundering Directive (AMLD4)[97] and the Regulation on information accompanying transfers of funds (AMLR)[98], were published in the Official Journal of the European Union. The legislative package seeks to strengthen EU capabilities against anti-money laundering and counter-terrorist financing activities. The final text closely aligns with the proposed recommendations made by the Financial Action Task Force (FATF) in 2012,[99] which called for a more uniform set of rules and an increased focus on the risk-based approach. Whereas the Regulation is directly applicable from 26 June 2015, Member States have until 26 June 2017 to implement the Directive.

BACKGROUND - The European Commission indicated, in its application report of 2012, that in light of the evolving threat landscape concerning money laundering and terrorist financing, a periodic revision of the legal framework is required in order to be able to respond to newfound threats.[100] Whilst no fundamental shortcomings were identified under the existing AMLD3, the Commission nonetheless found that some minor modifications were necessary in order to bring the regulatory framework in line with the revised international standards of the FATF. Internal Market and Services Commissioner Michel Barnier stated that the EU is "*committed to rapidly incorporating the new international standards and to ensuring that the European system responds appropriately to evolving threats of money laundering and terrorist financing. The ingenuity of criminals to exploit gaps in the framework knows no bounds. Our aim is to propose clear and proportionate rules which both protect the Single Market and avoid overburdening market participants*."[101]

5.2.2. Third party payment providers

RISK-BASED APPROACH - In line with the FATF recommendations of 2012, the AMLD4 incorporates a more consolidated risk-based approach for more evidenced-based decision making. It is acknowledged that measures should be adjusted according to the level of risk presented in a given case. In its proposal for reform, the European Commission stated that the Directive would be less detailed regarding concrete measures to be taken where instead Member States, supervisory authorities and obliged entities[102] will be required to first assess the risks and then undertake appropriate mitigating measures.[103]

---

[97] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (AMLD4), OJ L 141/73.

[98] Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006, OJ L 141/1.

[99] Financial Action Task Force (2012), FATF Recommendations on International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, February 2012.

[100] European Commission (2013) "Frequently Asked Questions: Anti-Money Laundering", MEMO 13/64, 2013.

[101] European Commission (2012) "Press Release Anti-Money Laundering: creating a modern EU framework capable of responding to new threats", IP/12/357.

[102] The term 'obliged entity' replaces the existing 'designated persons' term used under the AMLD3 and refers to the institutions and other organisations to which the AMLD4 is applicable.

[103] European Commission, Proposal for a Directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, COM/2013/045 final, pp. 60.

SCOPE - Scope wise, the AMLD4 is principally aimed at credit and financial institutions as well as trust organisations, estate agents, gambling services and other persons trading in goods of payments to the extent that payments are made or received in cash amounting to EUR 10 000 or more. Payment service providers are not expressly mentioned under the applicable scope. However, Article 3 of the Directive specifies that financial institutions also encompass undertakings carrying out activities as listed in Annex I to Directive 2013/36/EU, including point 4 which refers to payment services as defined by the Payment Services Directive.[104] Considering that the PSD2 introduces the regulation of TPP's and defines them as payment service providers, it is evident that TPP's will be regarded as obliged entities and subject to the provisions of the AMLD4 once the PSD2 has been formally adopted.

RISK ASSESSMENTS - Pursuant to Article 8 of the AMLD4, Member States will have to ensure that obliged entities, which include TPP's, undertake necessary steps to identify and assess the risks of money laundering and terrorist financing, taking into account risk factors. The required steps will be dependent on the nature and size of the obliged entities and risk assessments will need to be documented and made available to the competent authorities of the respective Member States. However, competent authorities reserve the right to declare that individual risk assessments are not required where the intrinsic risks of a sector are clear and understood.[105] In addition, obliged entities will also have to implement internal policies and procedures to mitigate and manage the risks of money laundering and terrorist financing identified at EU level, by the Member State or through the own risk assessment. Again, Member States reserve the discretion to impose certain obligations only on some entities based on their size and nature, which entails that certain entities will have to appoint a compliance officer and an independent audit function to test the internal policies, where other entities won't.

CUSTOMER DUE DILIGENCE - Due diligence requirements have also been revised. The AMLD4 allows for different processes and measures to be taken according to the nature and severity of risks and clarifies under which circumstances simplified due diligence is appropriate. The European Commission felt it had to restrict the circumstances where a simplified customer due diligence was appropriate, as it was clear that many obliged entities often applied the 'specified customer' or 'specified product' exemption without sufficiently examining the appropriateness of applying such exemption.[106] Therefore, obliged entities are required to first determine the level of risk posed by a customer prior to the application of a simplified customer due diligence. The EBA is tasked with drafting guidelines which specify the risk factors to be taken into consideration and the measures to be taken in situations where simplified customer due diligence measures are deemed appropriate.[107] Whilst it is

[104] Directive (EU) 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC, OJ L 176/338.
[105] Article 8 AMLD4.
[106] The Commission stated: "*With regard to the current (Third) AMLD, the provisions on simplified due diligence were found to be overly permissive, with certain categories of client or transaction being given outright exemptions from due diligence requirements*." European Commission, Proposal for a Directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, COM/2013/045 final.
[107] Article 17 AMLD4.

conceivable that TPP's, as an obliged entity, will need to consider customer due diligence measures, it is necessary to bear in mind that burdening them with equally stringent provisions as other entities could be counterintuitive to the impetus of fostering innovation of new market players under the PSD2. Undeniably, the obligations of the AMLD4 could create new barriers to entry for TPP's by imposing requirements which surpass the business models in question. Requiring TPP's to conduct due diligence procedures would essentially impose a dual due diligence procedure on payment customers using TPP's, since ASPSP's have the same obligation. Such a requirement would be nothing more than a prohibitive burden. Nevertheless, the AMLD4 takes this situation into account and states that "*in order to avoid repeated customer identification procedures, leading to delays and inefficiency in business, it is appropriate, subject to suitable safeguards, to allow customers whose identification has been carried out elsewhere to be introduced to the obliged entities. Where an obliged entity relies on a third party, the ultimate responsibility for customer due diligence should remain with the obliged entity to which the customer is introduced*".[108] Regarding TPP's this would mean that ASPSP bear the burden of conducting due diligence on the account owner. In addition, PISP could also be exempted from due diligence procedures on the basis of article 12, 1(c) in the event its services are exclusively used to purchase goods or services. Also, ASPSP's have an additional requirement in the sense that obliged entities are required to verify that "*any person purporting to act on behalf of a customer is so authorised and identify and verify the identity of that person*".[109] Finally, the ALMD4 makes it possible for obliged entities to outsource their customer due diligence requirements to third parties, but the ultimate responsibilities remain on the obliged entity relying on the third party.[110]

CENTRAL BENEFICIAL OWNERSHIP REGISTRY - One of most anticipated provisions of the AMLD4, is perhaps the introduction of the central beneficial ownership register, which points to and provides information on the ultimate or beneficial owner of a given legal entity within their respective Member States.[111] Whilst Member States will be responsible to create such a registry, it is envisaged that these will all be interconnected. As such, obliged entities will be required to maintain information evidencing beneficial ownership. It was noted by the European Parliament that there is increasing international recognition of the need for transparency behind the ownership of legal persons and arrangements, as the use of shell companies with anonymous ownership structures are often thought to be facilitating tax evasion and other covert activity.[112] Relevant authorities and their financial intelligence units will have no restrictions in accessing the registry. Other entities such as credit and financial institutions banks and NGO's, can also be granted access to the register within the framework of due diligence requirements.[113] In addition, the register is also accessible to the public, such as investigative journalists, provided they can show a legitimate interest in the

[108] Recital 35 AMLD4.
[109] Article 13 AMLD4.
[110] Article 25-29 AMLD4.
[111] Article 30 AMLD4. A "beneficial" owner actually owns or controls a company and ultimately authorises transactions, whether such ownership is exercised directly or by a proxy. As such organisations will be required to hold information on the beneficial owners of an entity that owns 25% plus one share in a legal entity.
[112] European Parliament (2011) "Resolution of 15 September 2011 on the EU's efforts to combat corruption", B7-0481/2011, September 2011.
[113] Article 30 (5) AMLD4.

information.[114] Consequently these parties and organisations will be able to access general information such as the beneficial owner's name, month and year of birth, nationality, country of residence and details of ownership.[115] Any exemption to the access provided by member states will be possible only "on a case-by-case basis, in exceptional circumstances".[116] In addition, public access will also be available subject to an online registration by the individual applying for the information and subject to a nominal administrative fee.[117]

POLITICALLY EXPOSED PERSONS - The provisions on politically exposed persons (PEP) have also been brought in line with the FATF's recommendations.[118] The Directive extends the definition of PEPs to now also cover domestic PEPs and individuals entrusted with a prominent position in the organisation.[119] Family members of foreign PEPs will equally fall under the scope of PEPs and are defined as close associates. In addition, the Directive clarifies that enhanced due diligence should always be carried out when transactions involve PEPs. However, the provisions on PEPs are somewhat tempered by allowing obliged entities to make risk based decisions to limit the number of years an individual can be considered as a PEP.[120]

REPORTING OBLIGATIONS - TPP's will also need to take reporting obligations into account, where in the event they know, suspect or have reasonable grounds to assume that funds are the proceeds of criminal activity or are related to terrorist financing, they will have to notify the Financial Intelligence Unit of the concerned Member State.[121] Moreover, in the event of such suspicions, obliged entities are required to refrain themselves from carrying out the transactions.[122] Disclosures by the obliged entities to the competent authorities in the aforementioned cases shall not constitute a breach of any restriction on disclosure of information imposed by contractual agreements or regulatory provisions and shall not lead to the liability of the obliged entity. Nevertheless, the obliged entity is prohibited from informing the customer or otherwise involved persons that information concerning their transaction has been transmitted to the competent authorities or the fact that a money laundering or terrorist financing analysis may be carried out.[123]

---

[114] Legitimate interest is described by the European Parliament as suspected money laundering, terrorist financing and 'predicate' offences that may help to finance terrorism including tax crimes, corruption and fraud. Banks on their part, can prove legitimate interest in accessing the register in order to complete due diligence obligations on customers. Recital 14 AMLD4

[115] Article 30 (5) AMLD4.

[116] European Parliament (2015) "Press Release - Tougher rules on money laundering to fight tax evasion and terrorist financing", May 2015.

[117] Article 30 (5c) AMLD4

[118] Financial Action Task Force (2012), FATF Recommendations on International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, February 2012.

[119] Politically exposed persons are defined as individuals at a higher than usual risk of corruption due to the political positions they hold, such as heads of state, members of government, supreme court judges, and members of parliament, as well as their family members.

[120] Article 22 AMLD4

[121] Article 33 AMLD4.

[122] Article 35 AMLD4.

[123] Article 39 AMLD4.

DATA PROTECTION - Concerning data protection provisions, the European Commission called for "*the need to strike a balance between allowing robust systems and controls and preventative measures against money laundering and terrorist financing on the one hand, and protecting the rights of data subjects on the other is reflected in the proposal*."[124] As such, the processing of personal data can only be done for the purposes of prevention of anti-money laundering or counter terrorist financing and is subject to the safeguards of Directive 95/46/EC. In order to increase internal awareness of employees on security measures and data protection requirements, obliged entities will be required to organise training sessions aiding employees in the identification and recognition of money laundering and terrorist financing schemes.[125]

SANCTIONS - New and increased administrative sanctions have been added in case of serious, repeated or systematic breaches of requirements under the AMLD4. Considering the fact that competent authorities now dispose of a wide range of administrative sanctions, including publishing press statements concerning breaches of requirements, withdrawal of the authorisation of an obliged entity, imposing pecuniary fines and ordering an obliged entity to cease and desist specified conduct, the revised sanctions will now be applicable to all obliged entities. The AMLD4 provides for a maximum pecuniary fine of at least twice the amount of the benefit derived from the breach or at least EUR 1 million. The pecuniary sanctions for breaches involving credit or financial institutions are further increased and amount to at least EUR 5 million or 10% of the total annual turnover in the case of a legal person and a maximum pecuniary sanction of at least EUR 5 million in the case of a natural person.[126]

[124] European Commission (2013) "Proposal for a directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing", *COM/2013/045 final* and Recital 43 AMLD4.
[125] Article 46 AMLD4.
[126] Article 59 AMLD4.

The table below offers a brief summary of the key changes proposed by the AMLD4:

Provision	Description
Scope	• Scope is extended by lowering the threshold for cash payments from 15.000 EUR to 10.000 EUR. • Whilst TPP's are not explicitly mentioned as obliged entities, they do fall under the scope since they are regarded as payment service providers under article 3, point 4.
Risk-based approach	• Adopting of an evidence-based decision making approach. Obliged entities will have to carry out a risk assessment in order to identify and assess the risks they run related to money laundering and the financing of terrorism
Ultimate beneficial ownership register	• Member States are required to establish a central public register for ultimate beneficial owners. • Obliged entities will have to make available adequate, accurate and current information, including the name, date of birth, nationality and details of ownership • Register is accessible to the relevant authorities, obliged entities as well as the public provided they can demonstrate a legitimate interest.
Risk assessment	• Obliged entities will be required to identify and assess money laundering and terrorist financing risks taking into account various risk factors • Risk assessments need to be documented, up-to-date and made available to the relevant competent authorities • Obliged entities are to ensure that they have policies, controls and procedures in place to mitigate and manage effectively the risks of money laundering and terrorist financing • appointment of a Compliance Officer and of an Independent Audit Function (discretion to which obliged entities will have to appoint these remains with the Member States)
Simplified CDD	• Automatic application of simplified CDD in certain situations is no longer accepted. A preliminary risk assessment has to be performed in all cases.
Enhanced CDD	• Obliged entities are required to conduct enhanced CDD for a variety for reasons including for services such as, products or transactions that might favour anonymity, non-face-to-face business relationships or transactions, without certain safeguards such as electronic signatures, payment received from unknown or unassociated third parties or new products and new business practices
Dual due diligence	• TPP's will not have to conduct due diligence on customers who have already undergone the procedure by another obliged entity
Politically Exposed Person's (PEP)	• The regime of PEP has been extended to cover domestic PEPs and persons entrusted with a prominent function by an international organisation
Central point of contact	• Member States can require payment service providers to establish a central point of contact, in the event their headquarters is situated in another Member State to ensure on behalf of the appointing PSP compliance with AML/CTF rules
Sanctions	• Sanctions for non-compliance have increased significantly for both individuals and organisations. • Administrative sanctions include public reprimands, cease and desist notifications and removal from practice. Pecuniary sanctions are increased up to 10% of total annual turnover or at least 5 million EUR.
Harmonisation	• As the Directive is a minimum harmonisation Directive, the extent and the requirements that obliged entities must adhere may differ amongst Member States

Table 2: Key changes AMLD4

MINIMUM HARMONIZING DIRECTIVE - Evidently, TPP's will be subjected to the new anti-money laundering (AML) and counter-terrorist financing (CTF) provisions of the AMLD4. It remains, however, uncertain to what extent the requirements are applicable and appropriate. As the AMLD4 follows a minimum harmonisation approach much will depend on the actual implementation of the respective Member States.

5.3. Industry & Regulatory Guidelines

A. ECB recommendations and EBA guidelines

EUROPEAN FORUM FOR THE SECURITY OF RETAIL PAYMENTS - At the same time the European Commission was finalizing its draft proposal for the reform of the Payment Services Directive, several other regulatory initiatives, all aiming at ensuring the security of online payments, were undertaken. These regulatory initiatives are a result of the increased level of cooperation between the European Central Bank (ECB) and the European Banking Authority (EBA). In the context of the growing relevance of security in retail payment issues a European Forum for the Security of Retail Payments (SecuRe Pay) was created. Established in 2011, the SecuRe Pay forum is the result of a voluntary cooperative initiative set up by the European Central Bank and comprises of relevant authorities from the European Economic Area (EEA) with the aim of facilitating the understanding of issues related to the security of electronic retail payment services.[127] It mainly focusses on the safety of electronic retail payment services, systems and schemes. This includes the whole processing chain of electronic retail payment services, irrespective of the payment channel used. Since its conception, the SecuRe Pay forum has published a number of recommendations, including on the security of internet payments and mobile payments[128] and for the security of payment access account services. In addition, the European Banking Authority issued its final guidelines regarding the security of internet payments, which converted the recommendations made by the SecuRe Pay forum in 2013 into guidelines. These guidelines correspond to the requirements set out by the Payment Services Directive and are to be updated with the formal adoption of the PSD2.

B. ECB recommendation for the security of internet payments

COMPLY OR EXPLAIN - Following a public consultation round in 2012, the final recommendations for the security of internet payments developed by the SecuRe Pay forum was published by the ECB in January 2013. The recommendations reflect the experiences of Member States overseers and supervisors and take into account the observation of increased levels of fraud of internet payments. The principal aim of the recommendations is to contribute to fighting payment fraud as well as enhancing consumer trust in internet payments. The recommendations adopt a 'comply or explain' approach entailing that addressees will have to comply with both the recommendations and key considerations or provide their

[127] European Central Bank, Mandate of the European Forum on the Security of Retail Payments, October 2014, pp. 3.
[128] European Central Bank (ECB), Recommendations for the Security of Mobile Payments – Draft document for Public Consultation, 2013, pp. 26.

reasoning for non-compliance. The recommendations prescribe that the addressees should implement the requirements by 1 February 2015.[129]

SCOPE - The recommendations begin by defining the scope and commends that all payment service providers as defined by article 1 of the PSD are subject to the minimum security requirements. Payment integrators offering payment initiation services are considered payment service providers under the recommendations and thus also fall under the scope. The impetus of the recommendations is to define common minimum requirements for the following internet payment services: i) card payments (including virtual card payments and registration of card payment data for use in wallet solutions; ii) credit transfers; iii) direct debit electronic mandates; and iv) transfer of electronic money.[130] In addition, a range of services are explicitly excluded from the scope of the final recommendations and include amongst others: credit transfers where a third party accesses the customer's payment account; mobile payments other than Internet browser-based payments; and payments where the instruction is given by post, telephone order, voice mail or using SMS-based technology. Given the fact that the recommendations are in line with the Payment Services Directive, third party payment providers do not fall under the scope of the recommendations.[131]

RECOMMENDATIONS - The report outlines 14 recommendations as well as key considerations and best practices which addressees of the recommendations are encouraged to adopt. The recommendations are formulated as generically as possible to accommodate continual business and technological innovation, and do not attempt to set specific security or technical solutions. These recommendations are divided up into 3 overarching categories: i) the general control and security environment; ii) specific control and security measures for internet payments and iii) customer awareness, education and communication.

GENERAL CONTROL AND SECURITY ENVIRONMENT - The general control and security environment requires that payment service providers need to implement and periodically review a formal security policy for all internet payment services. Such a policy should define security objectives, assign roles and responsibilities and include risk management capabilities. Risk assessment should be carried out and documented prior to and during the provision of internet payment services. Specific attention will need to be given to the security of sensitive payment data. Payment service providers should also establish a consistent and integrated approach towards the monitoring and handling of security incidents, including security-related customer complaints and establish incident reporting procedures in the event of major payment security incidents. In addition, risk control and mitigation measures are required. In that regard, payment service providers are required to implement security measures in order to mitigate identified risks, incorporating multiple layers of security defence ('defence in depth'), where the failure of one line of defence is covered by the next line of defence. Appropriate security solutions to protect networks, websites, servers and communication links against abuse or attacks are required. Finally, payment service

[129] European Central Bank (ECB), Recommendations for the Security of Internet Payments, January 2013, pp. 16.
[130] *Ibid.*, 2.
[131] *Ibid.*, 2.

providers shall be equipped with the technology to trace all transactions and payment data.[132]

SPECIFIC CONTROL AND SECURITY MEASURES - Under specific control and security measures, payment service providers will need to adequately be able to identify customers in line with the European anti-money laundering legislation and confirm their willingness to make internet payments before being granted access to payment services. Prior information should also be provided to the customer concerning the requirements for performing secured internet payment transactions and its inherent risks. Customers should also be contractually informed that the PSP may block a specific transaction or the payment instrument on the basis of security concerns. The initiation of internet payments including the access to sensitive payment data should at all times be protected by strong customer authentication measures, which according to the recommendations is key to the prevention of internet payment fraud. The recommendations specify that a two-factor authentication, whereby at least one element should be non-reusable and non-replicable should be used. Furthermore, the recommendations require effective and secure procedures for the delivery of personalised security credentials, payment-related software and all personalised payment-related devices. In addition, payment service providers need to limit the number of log-in and authentication attempts as well as the validity of one-time passwords, employ a fraud detection system to enable the prevention, detection and identification of fraudulent transactions. Lastly, sensitive payment data, including all data used to identify and authenticate customers, need to be appropriately secured against theft and unauthorised access when stored, processed or transmitted. In that regard end-to-end encryption is required for all internet payments.[133]

CUSTOMER AWARENESS, EDUCATION AND COMMUNICATION - The final category of recommendations concern customer awareness, education and communication. In first instance payment providers are required to offer guidance and assistance to their customers on how to securely manage their internet payment transactions. In doing so, at least one secure channel should be made available to directly communicate with the customers. Moreover, customers should be informed about updates in security procedures, and be provided with assistance for all questions, complaints and requests for support regarding internet payments. In addition, limits (e.g. maximum amounts) for internet payment services should be implemented. Finally, payment services are required to confirm the payment initiation and provide customers with information allowing them to validate the integrity of their payment transaction. In the event a payment service provider informs customers on the availability of electronic statements through an alternative channel (e.g. SMS or e-mail) sensitive payment data should not be included in such communications or otherwise be masked.[134]

ASSESSMENT GUIDE - In addition to the recommendations, the SecuRe Pay Forum published an assessment guide to provide the supervisory and oversight authorities with a harmonized

[132] *Ibid.*, 5-6.
[133] *Ibid.*, 8-13.
[134] *Ibid.*, 13-14.

interpretation of the recommendations so as to ensure that compliance assessment is conducted consistently and efficiently throughout EEA.[135]

C. EBA guidelines on the security of internet payments

STATE OF PLAY - On 19 December 2014 the European Banking Authority (EBA), published its final guidelines on the security of internet payments. These final guidelines are based on the recommendations for the security of internet payments published by the SecuRe Pay forum described above. The conversion of the SecuRe Pay recommendations into guidelines aims to provide a solid legal basis for the consistent implementation of the security requirements across the EU. [136]

PUBLIC CONSULTATION ROUND - In light of the ongoing discussions of the PSD2, the EBA issued a public consultation round in October 2014 seeking input from stakeholders on how the potentially higher security standards required by the PSD2 should be catered for by the EBA.[137] Ultimately the EBA concluded that in light of the continually high levels of fraud observed on internet payments a delay in the implementation of the guidelines until the transposition of the PSD2 would be detrimental to the confidence of market participants in payment systems.

TWO-STEP APPROACH - As such the EBA opted for a two-step approach, whereby the final guidelines incorporate the SecuRe Pay recommendations and enter into force on 1 August 2015. The implementation of more stringent security requirements set out in the PSD2 will then be implemented at a later stage defined by the PSD2.

COMPLY OR EXPLAIN - Pursuant to article 16(3) of the EBA Regulation No 1093/2010 the competent authorities and payment institutions must make every effort to comply with the guidelines.[138] According to article 16(3) of the EBA Regulation the guidelines adopt a 'comply or explain' approach, whereby competent authorities must either confirm that they will comply with the requirements of the guidelines or provide reasoning for their non-compliance.

EBA MANDATE UNDER THE PSD2 - On 22 May 2015, the EBA issued a press release stating that it was preparing itself to develop the requirements necessary to ensure secure, easy and efficient payment services across the EU as mandated by the PSD2. In order to do so, the EBA will once again issue a public consultation round with the relevant stakeholders to receive input as early as possible within the regulatory development process. The PSD2 mandates for the EBA are expected to include requirements to improve operational and security requirements for payment services. The EBA will develop this work in close cooperation with the European Central Bank (ECB), through the Forum for the Security of

[135] European Central Bank (ECB), Assessment Guide for the Security of Internet Payments, 2014, pp. 66.
[136] European Banking Authority (EBA), Final Guidelines on the security of internet payments, EBA/GL/2014/12, 2014, pp. 42.
[137] *Ibid.*, 3.
[138] Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a Supervisory Authority (European Banking Authority), amending decision No 716/2009/EC and repealing Commission Decision 2009/78/EC, OJ L 331, pp. 12–47.

Retail Payments (SecuRe Pay).[139] The mandate for the EBA under the PSD2 include the requirements to improve both operational and security requirements for payment services. However, as the security requirements under PSD2 are not expected to come into force until 2018/9, the final Guidelines issued by the EBA in December 2014 will apply until such time.

BRIDGING THE GAP - Pending the formal adoption of the PSD2, the recommendations of the ECB and the final guidelines of the EBA are definitely a step in the right direction as they clearly emphasize the need for an increased focus on customer security and privacy through pro-active communication and notification requirements. As the final guidelines primarily build on the PSD, TPP's currently do not fall under the scope of the final guidelines. Evidently, this will change with formal adoption of the PSD2, which bring TPP's under the regulatory scope. Whilst compliance with the EBA guidelines will be a challenge for most payment service providers, especially when considering the narrow timeframe, the guidelines nonetheless bridge the gap between the current security requirements and the proposed increased security obligations under the PSD2, allowing for a smoother transition in the long run.

NATIONAL COMPLIANCE - However, as the EBA guidelines adopts a 'comply or explain' approach, competent national authorities have to notify whether they will comply or otherwise give reasoning for non-compliance. As of yet, the United Kingdom, Slovakia and Estonia have all declared that they will not comply with the issued guidelines of the EBA.[140] In a statement issued on 2 April 2015, the UK's financial Conduct Authority (FCA) stated that "*Implementation of the Guidelines will require some providers to make significant changes to their systems and controls and significant additional changes are likely to be necessary following implementation of PSD2. We indicated to the UK market in March 2014 that we would be requiring compliance with the SecuRe Pay Recommendations in line with PSD2 transposition, and we remain of the view that it is reasonable, in all the circumstances, for FCA to incorporate the detail of the Guidelines (or equivalent guidelines issued under PSD2) into our supervisory framework in line with this timetable. Our intention is that this will be done in a way that is equally binding on all types of payment service provider.*"[141]

REGULATORY SEGMENTATION - In contrast to the objectives of the guidelines which aim for a consistent implementation across the EU, the 'comply or explain' approach leads to a regulatory segmentation where some jurisdictions follow and apply the security requirements of the EBA and others do not. This in turn contradicts the concept of full harmonization as prescribed by the PSD2.

<u>D. ECB recommendations for the security of payment account access services</u>

[139] European Banking Authority (EBA), Press Release outlining its upcoming initiatives for the regulation of retail payments, 21 May, 2015.

[140] The EBA has published a compliance table which details, which national competent authorities intend to comply with the EBA final guidelines. See European Banking Authority (EBA), Compliance Table – Guideline Based on information supplied by them, the following competent authorities comply or intend to comply with: EBA Guidelines EBA/GL/2014/12 on the security of internet payments, published on 19th December 2014., EBA/GL/2014/12 Appendix 1.

[141] Financial Conduct Authority (FCA), Statement on the response to the EBA Guidelines on the Security of Internet Payments, 2015.

SECURITY OF PAYMENT ACCOUNT ACCESS SERVICES - Considering the fact that the SecuRe Pay recommendations on the security of internet payments excluded TPP's from its scope, a complementary recommendation concerning the security of payment account access providers was published in May 2014.[142] Initially, the report was drafted exclusively for the transmission to the EBA, whereby the ECB only published a public note outlining the outcome of the public consultation round which took place in November 2013.[143] The decision not to make the recommendations public was based on the ongoing discussions on the revision of the Payment Services Directive and the lack of supervisory competences on providers of payment account access services. In addition, the ECB also referred to the proposed mandate for the EBA to develop guidelines on security measures under the PSD2. Nonetheless, due to a public access request the ECB published the text in May 2014. Whilst the report was made public, addressees are not expected to comply with the prescribed requirements at this moment.

PUBLIC CONSULTATION - The outcome of the public consultation round reflects the same concerns that were raised under the revision of the Payment Services Directive. The main issues relate to the need for contracts, a clear allocation of liability and the sharing of personalized security credentials. These issues were all considered and addressed by the SecuRe Pay forum in the recommendations. Following the public consultation round, five conclusions were drawn from the input of the various stakeholders: 1° TPPs should be licensed and supervised, 2° TPPs should ensure that customers are appropriately authenticated by relying on strong customer authentication, 3° TPPs' access to information on payment accounts should be limited to the minimum they need for their activity, 4° TPPs and ASPSPs should ensure mutual authentication when communicating in the context of providing payment account access services and 5° the non-sharing of the personal user credentials with the TPP would address the security concerns by some of the current interactions between TPPs and ASPSPs.[144] Besides the fact that TPP's should be licensed and supervised, both the TPP and the ASPSP have to ensure mutual authentication in their communications. Also, TPP's should ensure that customers are authenticated through strong customer authentication, but should not rely on personalized security credentials issued by ASPSP's as these should not be shared. Finally, access to information of payment accounts should at all times be limited to the minimum required for the provision of their service. Ultimately, the recommendations seek to enhance the protection provided to the account owner by promoting the security of payment account access services. Analogous to the report on the security internet payments, the recommendations for the security of payment account access services are drafted as generically as possible so as to allow a flexible approach which accommodates future innovations.

SCOPE - The recommendations are applicable to all TPP's irrespective of the device that is used by the payment user.[145] The report however does exclude certain services from its

[142] European Central Bank (ECB), Final recommendations for the security of payment account access services following the public consultation, May 2014, pp. 25.
[143] European Central Bank (ECB), public note on the security of payment account access services, March 2014, pp. 5.
[144] European Central Bank (ECB), public note on the security of payment account access services, March 2014, pp. 3.
[145] In addition, ASPSP's will need to take certain security requirements into account as the initial recommendation on internet security do not consider the relations between ASPSP's and TPP's.

scope, primarily those which have been covered by previous recommendations such as mobile payments which are not payment account access services,[146] digital and mobile wallet services unless when being used by TPP's and similar services provided by an ASPSP to its customers without the involvement of a TPP. It is important to note that ASPSP's will have to consider the recommendations made in this report as well as those prescribed by the recommendations on the security of internet payments.

STRUCTURE - The structure of the recommendations on TPP's is parallel with the recommendations on the security of internet payments, resulting in the issuance of final recommendations which are further outlined by key considerations. The report sets out several conditions which the addressees are encouraged to adopt. Similar to other payment service providers, TPP's should protect the security of the payment user's account and related data by adopting strong security and control measures which ensure a high level of security. Next, sufficient transparency is required, which should allow account owners and payees to make informed decisions both prior and during the use of the services of a TPP. In order to allocate liability, TPP's should ensure they can trace their transactions which require authentication measures in all communications between the involved entities (including the ASPSP, merchant and/or payee). Such authentication facilitates the identification of which entity was responsible for which part of a given transaction in case of defects, security or fraud incidents. In the event of such incidents the recommendation requires that there is sufficient communication between the involved entities. Concerning strong authentication measures, the recommendations state that security credentials should not be shared between a TPP and the ASPSP, which reflects the ECB opinion on the draft proposal of the PSD.[147] Also the duration of which a TPP has access to a payment account should be limited so as to minimize the risk of data misuse. In addition, TPP's will be required when providing services to e-merchants that these comply with the necessary security requirements through the use of contractual provisions.[148] Comparable to the SecuRe Pay recommendations for the security of internet payments, the report contains similar risk assessment, incident monitoring and reporting, risk control and mitigation and traceability requirements for TPP's and ASPSP's. In addition, the recommendations state that TPP's should provide customers with advice and guidance on how to securely use their services.

SECURITY RISKS - The report further recognizes the specific characteristics of TPP's and their involvement in the payment chain as prone to security risks similar to those of other payment services. As such, the report emphasizes the need for a level-playing field whereby TPP's should ensure the same level of security of their payment services as existing payment solutions, implying that TPP's should also adopt strong customer authentication measures. As already mentioned, the recommendations do not support the idea of sharing personalized security credentials, instead suggesting two alternative solutions. The TPP

[146] European Central Bank (ECB), Recommendations for the security on mobile payments – Draft document for public consultation, November 2013.

[147] European Central Bank (ECB), Opinion of the European Central Bank of 5 February 2014 on a 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, CON/2014/9.

[148] In addition, TPP's should adequately identify e-merchants by subjecting them to due diligence processes prior to granting them access to their services. See Key Consideration 6.2 of the final recommendations for the security of payment account access services.

could either issue its own security credentials[149] or securely redirect the customer to the ASPSP for authentication. The rationale for such an approach lies in the acknowledgment that customers using TPP's would be susceptible to increased risks should security credentials be shared across an additional interface. In that regard, the report suggests the development of common European standards, which should outline the redirection procedure as well as the ASPSP's interface that allows the customer to authorize the payment. Considering the fact that TPP's remain dependent on the 'goodwill' of ASPSP's, the common standards should also specify the expectations of the 24/7 availability of the interface for authentication procedures provided by ASPSP's.

TECHNICAL STANDARDS - Whilst the report does not make any attempts at offering technical solutions, it does suggest that the EBA, in close cooperation with the ECB, could develop these standards as it is already tasked with the development of similar technical standards under the PSD2. This was also the initial objective of the recommendations, whereby the EBA could use the recommendations as input for its own guidelines based on the newfound regulatory obligations.

5.4. Interim Analysis

AMLD4 - Since the AMLD4 follows a minimum harmonization approach, the extent and consequences of requirements and obligations will depend on the transposition of the individual Member States into their national law. As a result, it is not possible to assess the impact of the AMLD4 on TPP's at this stage. For that reason, only the findings of the PSD2 will be discussed in this section.

PSD2 - Overall, the PSD2 has been welcomed by most stakeholders.[150] The initial objectives set out by the European Commission, developing an integrated European payment market that fosters competition, innovation and security, by taking into account new emerging payment services are well reflected in the regulatory framework. The most fundamental change of the PSD2 is the extension of its scope which now covers third party payment providers. Under the framework of the PSD2, TPP's will be subject to stringent regulatory standards similar to those placed on traditional payment service providers under the PSD. As analyzed above, it is clear that TPP's will need to acquire proper authorization and comply with security and consumer protection requirements. As initially set out by the European Commission, this will effectively instigate a level-playing field amongst payment service providers.[151] Moreover, TPP's must accept liability for unauthorized or defective transactions, for the parts under their control. In addition, TPP's will need to comply with information and transparency requirements vis-à-vis the payer, payee and ASPSP's.

[149] European Central Bank (ECB), Final recommendations for the security of payment account access services following the public consultation, May 2014, p. 12.

[150] It has to be noted however, that the European Banking Federation was critical of the PSD2 stating that "*A fragile balance has been sought between sometimes conflicting objectives such as innovation, user security, market integration, data protection and competition. The final agreement broadly reflects political ambitions to see a bigger role played by non-bank service providers*." European Banking Federation (2015) "EBF Statement on EU Payment services Agreement", May 2015.

[151] Salmony, M. (2014) "Access to accounts – why banks should embrace an open future 2014", *JPSS Journal of Payments Strategy & Systems*, Vol 8 No 2, May 2014, p.157-171.

REMAINING UNCERTAINTIES - Despite subjecting TPP's to high regulatory standards, certain key areas remain problematic and unresolved. In particular, the current provisions on authentication including the use of security credentials, liability allocations in case of unauthorized or defective payment services and the transition period cause legitimate grounds for concern.

SECURITY & STRONG CUSTOMER AUTHENTICATION - Perhaps the main cause for concern is whether the PSD2 sufficiently addresses the security issues that originate with the inclusion of TPP's under the regulatory scope. Considering that one of the main drivers of the PSD2 was to ensure the safety and security of payment services, enhancing customer protection should be a focal point of the PSD2. Nevertheless, the current provisions on strong customer authentication measures including personalized security credentials which seek to increase the security of electronic payments elevate concerns and require clarifications. As the PSD2 grants TPP's access to and use of payment accounts, provided they have acquired consent of the payment user, TPP's will be able to either initiate a payment transaction on behalf of their customer or aggregate payment information. These types of services fall under article 87 of the PSD2 which prescribes the necessity of applying strong customer authentication measures and ensures that payment service providers adopt security measures which protect the confidentiality and integrity of the payment user's personalized security credentials. However, article 87 (1d) continues and states that TPP's should be able to rely on the customer authentication issued by the ASPSP. The actual extent of this provision remains unclear; does this mean that the payment service users should share their security credentials with TPP's? Recital 51b of the final compromise text states that "*The obligation to keep personalised credentials safe is of the utmost importance to protect the funds of the payment service user and to limit the risks related to fraud and unauthorised access to the payment account. However, terms and conditions or other obligation imposed by payment service providers on the payment service users in relation to keeping personalised security credentials safe should not be drafted in a way that prevents payment service users from taking advantage of services offered by other payment service providers, including payment initiation services and account information services. Furthermore, the abovementioned terms and conditions should not contain any provisions that would make it more difficult in any way to use the payment services of other payment service providers authorised or registered under this Directive"*. Considering the fact that both the payment user is required to undertake necessary steps to ensure the safety of their security credentials and ASPSP's are obligated to ensure that personalized security credentials are not accessible to third parties, it remains uncertain whether sharing the security credentials is considered safe and secure. Throughout the negotiations industry stakeholders have repeatedly voiced their concerns and requested guidance on this matter. According to them, allowing the use of personal security credentials issued by ASPSP's to TPP's is impermissible as, on the one hand, exposing the credentials through more communication channels, increases security risks, and on the other hand, it conveys the wrong message to customers on how to safely conduct payment services in an online environment.[152] The European Consumer Organisation reiterated this view stating that TPP's receiving personal security features

[152] Boudewijn, G. (2015) "PSD2: Almost final – a state of play", EPC Blog, June 2015 and European Banking Federation (2015) "EBF Statement on EU payment services agreement", May 2015.

threatens consumer protection and far exceeds the objective of adequate authentication.[153] Indeed, as the text currently stands, consumers are invited to share their security credentials with third parties. Even more concerning is that consumers will have to actively research whether that TPP is properly licensed, rather than being a third-party acting with criminal intent. Needless to say, such a practice increases consumer exposure to a raft of security risks including identity theft and payment fraud, phishing, man-in-the middle attacks and money laundering schemes.

ECB OPINION - In its legal opinion on the European Commission's proposal for the PSD2, the ECB stated that for reasons of security and customer protection, the access of payment accounts to third parties requires a robust focus on strong customer authentication procedures which would appropriately identify the payment customer. Otherwise, given the fact that TPP's would in theory impersonate the payment user, ASPSP's would have no control or knowledge on who is in fact accessing the account which in turn would give rise to substantial risks of identity theft. In contrast to the current text of the PSD2 the ECB did not opt for the reliance by TPP's on authentication measures issued by the ASPSP. It stated that "*TPPs could ensure this through either redirecting the payer in a secure manner to their account servicing payment service provider or issuing their own personalised security features. Both options should form part of a standardised European interface for payment account access. This interface should be based on an open European standard and allow any TPP to access payment accounts at any PSP throughout the Union.*[154]"

EBA MANDATE UNDER THE PSD2 - The EBA will have the opportunity to provide some much needed clarifications on the extent of the provision as article 87 of the PSD2 has tasked them with the development of regulatory standards which will specify i) the requirements of the strong customer authentication procedures; ii) the possible exemptions of the application of such measures; iii) the requirements that security measures have to comply with in order to protect the confidentiality and the integrity of the payment service users' personalized security credentials; and iv) the requirements for common and secure open standards of communication for the purpose of identification, authentication, notification, and information, as well as for the implementation of security measures, between account servicing payment service providers, payment initiation service providers, account information service providers, payers, payees and other payment service providers.[155]

ALLOCATION OF LIABILITY - The allocation of liability under the PSD2 also requires clarifications. As ASPSP's are required to provide access to and use of payment accounts to TPP's, it is critical that there is a clear allocation of liability. In theory, the PSD2 states that each payment service provider is liable for their respective parts in the payment service. In that regard the onus lies with the relevant TPP to prove that it was not at fault. Nevertheless, the ASPSP remains the first point of contact for a payment user in case of unauthorized

[153] The European Consumer Organisation (2013) "Proposal for a revised Payment Service Directive – BEUC position", 2013, p. 4.
[154] European Central Bank (ECB), Opinion of the European Central Bank of 5 February 2014 on a 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, CON/2014/9, p. 5.
[155] Article 87a Proposal PSD2.

transactions or access. Such an approach was also defended by the ECB who stated that "*From a customer protection perspective, it is natural that a payer would turn to the account servicing payment service provider for a refund, since their relationship with the TPP may only take place on a one-off basis, e.g. for payment initiation. The account servicing payment service provider could then claim compensation from the TPP, unless the TPP can prove that it was not responsible for the error*."[156] Such reasoning however does not sit well with the ASPSP's, who legitimately ask the question why they are deemed liable for a relationship of which they have no control over.[157] The ASPSP does enjoy a right to recourse, but the extent of it remains unclear, as the provision does not clarify the operative process. This effectively entails that ASPSP's bear much of the liability burden, especially when considering the fact that new emerging TPP's will often not have sufficient funds to compensate the damage. The German Federal Financial Supervisory Authority (BaFin) underlined this concern when it pointed at the modest initial capital requirements of TPP's asserting that "*It is questionable whether this liability base is sufficient given that internet fraud is on the increase and hackers are becoming more and more professional. It is likely that account servicing PSPs will be exposed to greater legal and operational risk".*[158]

NO BASIS FOR CONTRACTUAL AGREEMENTS - To further complicate matters, article 82(2) of the PSD2 prescribes that any additional financial compensation can be determined in accordance with agreements between the ASPSP's and other payment service institutions. Traditional banks voiced their concerns early on in the discussions on the PSD2 and called for the obligation for TPP's to enter into contractual relations with the relevant ASPSP's, so liability allocation could be further specified.[159] However, the final compromise text prescribes that TPPs shall not be required to enter into contractual relationships with ASPSP's in the context of payment initiation or account information services. Since TPP's are dependent on ASPSP's providing them the necessary information in order to be able to provide their services, requiring contractual agreements could have adverse effects for competition in the market. Nevertheless, this leaves ASPSP's with the question how and if they can be compensated for additional costs incurred after having compensated a payment service user on behalf of a TPP. According to industry stakeholders the PSD2 creates a legal vacuum, whereby ASPSP's do not possess a legal basis for their legitimate claims to recover costs of the TPP.[160]

[156] European Central Bank (ECB), Opinion of the European Central Bank of 5 February 2014 on a 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, CON/2014/9, p. 30.

[157] Santamaría, J. (2014) "PSD2: EPC Calls on EU Lawmakers to Maintain the Firewall Protecting Consumers Making Internet Payments. This Means: No Sharing of Any Personalised Security Credentials with Third Parties - Update on legislative process leading to the adoption of the revised Payment Services Directive", EPC, 12 June 2014.

[158] Kokert, J. and Held, M. (2014) "Payment Services Directive II: Risks and serious consequences for users and banks", BaFin section for IT infrastructure of banks, June 2014.

[159] European Banking Federation, EBF position paper on Payment Account Service: Innovation and Security should go hand in hand, 2013, p. 3.

[160] Seibel, H. (2014) "PSD2: Analysis of Selected Aspects of Recent European Parliament Report Raises More Questions for Clarification - A review of the European Parliament´s Report on PSD2 with regard to the payer´s refund right in case of direct debits and some of the implications of the involvement of third party payment service providers", EPC Newsletter, 29 April 2014.

TRANSITION PERIOD - Finally, there remain some concerns about the transition period before the provisions and requirements set out in the PSD2 are applicable. Concerning TPP's the PSD2 foresees a grandfather rule. After the publication of the final compromise text, the Netherlands issued a declaration on the text. It expressed its concerns on the transitional period applicable on TPP's. It stated that "*The Payment Services Directive 2 seems to allow Payments Initiation Service Providers in this period to offer services under an European Passport while the technical standards of EBA ensuring the security of these payments are not yet in force*". Accordingly, incidents occurring during the transition period, could be detrimental to consumer trust in electronic payments due to the absence of adequate security standards.[161]

5.5. Comparative Analysis on TPP's in the US and Asia

BACKGROUND - As outlined in the previous section, rapid technological evolutions in the payment market along with the emergence of new and alternative payment solutions, in particular TPP's, has led to the revision of the EU Payment Services Directive. One of the main underlying causes for this revision was the preservation of consumer trust in the safety and reliability of newfound payment methods. By subjecting new innovative payment services to regulatory scrutiny, security, liability and data protection concerns are largely alleviated. However, the emergence of TPP's is not limited to the EU. The exponential growth of e-commerce along with the substantial increase in online transactions in recent years has had a significant impact on a global scale. In this section a brief comparative analysis will be conducted of the developments of TPP's outside of the EU, mainly focussing on the Asian and US market.

5.5.1. Asia

THIRD-PARTY PAYMENT SERVICES - The growth of e-commerce and of online transactions has been equally significant in the Asian market, giving rise to various new payment solutions and increased competition from non-financial institutions offering third-party payment services. Within the Asian market, examples of such non-financial institutions are Alipay[162] and Tenpay[163] in China and Globe in the Philippines.[164] In terms of TPP development China is arguably the most established market, with recent reports suggesting that there are currently 269 licensed TPP's active in the Chinese market.[165]

ADMINISTRATIVE MEASURES ON PAYMENT SERVICE OF NON-FINANCIAL INSTITUTION - Already in 2010 the People's Bank of China (PBOC) acknowledged the need for regulatory reform in order to preserve oversight of the expanding payment market by adopting the Administrative Measures on Payment Service of Non-financial Institution ('Measures').[166] These Measures

[161] Declaration of the Netherlands, on the final compromise text of the Proposal for a Directive of the European Parliament and of the Council 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, 9337/15, 8 June 2015.

[162] *global.alipay.com/ospay/home.htm*.

[163] *global.tenpay.com/about_us/overview.shtml*.

[164] *globe.com.ph/paybill*.

[165] Borst, N. (2015) "Non-Banks and Retail Payments: Innovations in China and the United States", Asia Focus, January 2015.

[166] People's Bank of China, Measures for the Administration of Payment Services of Non-financial Institutions, effective 1 September 2010.

principally support innovative TPP's but recognise the need to regulate these services accordingly. The Measures aim to enhance the development of the payment service market by regulating services provided by non-financial institutions in order to prevent payment risks and protect the rights and interests of all concerned parties.[167] According to the Measures, payment services provided by non-financial institutions refer to "*monetary capital transfer services provided by non-financial institutions as the middlemen between payers and payees*"[168] and include payments through networks,[169] the issuance and acceptance of prepaid cards and bankcard acquiring. In order for a non-financial institution to engage in payment services, a Payment Service License from the PBOC, as well as an approved business license – which specifies the particular services a provider will offer – will need to be obtained. To be eligible for the Payment Service License, the Measures prescribe several requirements including the establishment of the organisation in China,[170] minimum registered capital and the establishment of an anti-money laundering compliance system.[171] Moreover, TPP's are required to perform customer screening and record keeping for all their customers.

PAYMENT SERVICE LICENSE - Since the introduction of the Measures and the Payment Service License, the PBOC has granted a license to 270 non-financial institutions by March 2015. However, in August 2015 the PBOC effectively revoked a payment license of an organisation, after it was found to have misused its customers' money, forging documents and operating beyond its scope, bringing the total back to 269 licensed TPP's.[172] Recent reports have suggested that of those 269 organisations only 112 organisations received a license to engage in internet payment services. [173] Despite the various providers the online payment market in China is strongly concentrated as is illustrated by the market dominance that the top 2 TPP's, including Alipay and Tenpay account for over 90% of the market share. [174]

[167] Article 1 Measures for the Administration of Payment Services of Non-financial Institutions
[168] Article 2 Measures for the Administration of Payment Services of Non-financial Institutions
[169] Payments through networks are defined as: "*the transfer of monetary funds between payers and payees via public or private networks, including currency exchange, internet payment, mobile phone payment, fixed phone payment, digital TV payment.*"
[170] The Measures do not address the licensing of foreign-invested enterprises but it does state that the PBOC will issue separate legislation that will address the scope of services which may be provided by foreign-invested Payment Institutions. However, since the issuance of the Measures in 2010, legislation governing the licensing of foreign-invested enterprises have not been dispensed. Nevertheless, two foreign-invested enterprises Edenred China and Sodexo Pass China have been granted licenses to provide prepaid card services in China.
[171] Article 8 Measures for the Administration of Payment Services of Non-financial Institutions
[172] Spring. J., (2015) "China central bank shuts down payment firm for fraud", Reuters, 28 August 2015.
[173] The Paypers. (2015) "PBOC to issue new third-party payment licenses", The Paypers, 24 July 2015.
[174] Want China Times. (2015) "PBOC likely to issue new third-party payment licenses: market observers", Want China Times, 23 July 2015.

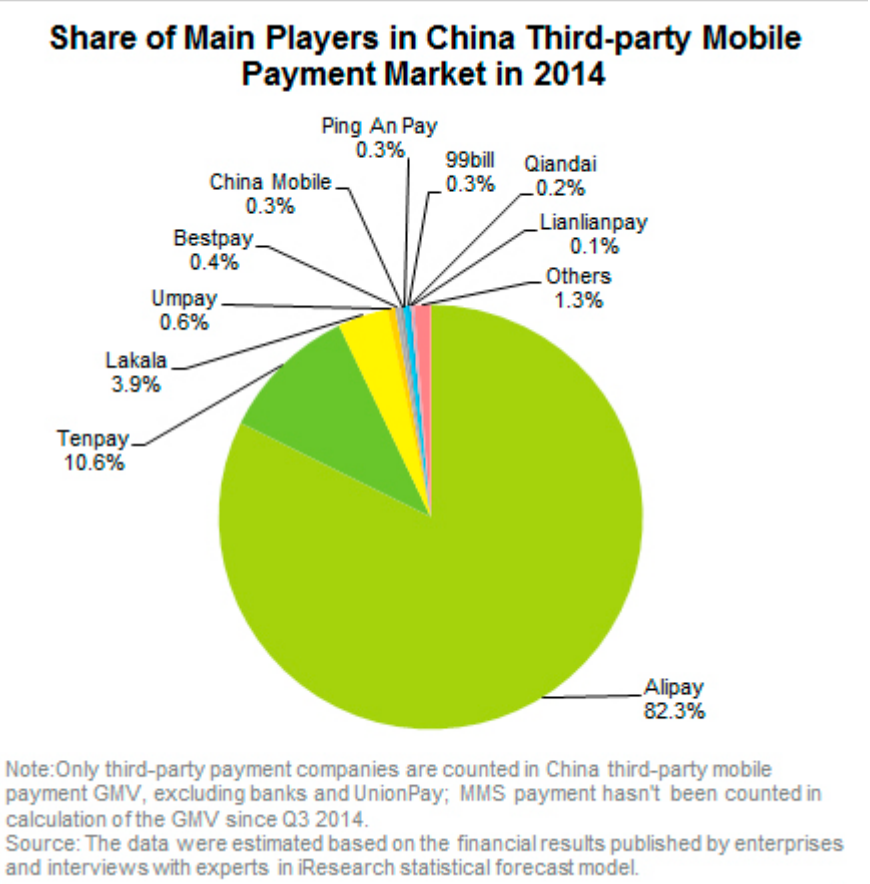

Figure 1: China Third-Party Mobile Payment Market Share[175]

GROWING TENSIONS WITH TRADITIONAL FINANCIAL INSTITUTIONS - Competition with traditional financial institutions is equally fierce, where tensions between the emerging TPP's and UnionPay, the national bank card network has often led to outright conflicts. With the sudden rise of TPP's, UnionPay has not only had to tolerate more competition but also had to deal with the fact that TPP's are increasingly sidestepping on UnionPay's bank card payment system to lower transaction fees.[176] These tensions reached a stalemate in 2013, when UnionPay contacted financial institutions that had signed agreements with TPP's, demanding that all online transactions had to be integrated into the UnionPay network.[177]

REGULATORY REVIEW - The granting of numerous payment service licenses to non-financial institutions nonetheless, clearly reflects the supporting stance of the PBOC of the development of TPP's. However, the PBOC recently underlined its acknowledgment of potential security and liability issues that these new payment providers can represent. On 31 July 2015, the PBOC issued the *Administrative Measures for Internet Payment Services of Non-Banking Payment Institutions* ("Draft Measures') which endured a public consultation round until the 28 August 2015. The draft measures seek to implement additional

[175] iResearch China. (2015) "China Third-party Mobile Payment GMV Quadruples", iReseach China, 13 March 2015.
[176] Borst, N. (2015) "Non-Banks and Retail Payments: Innovations in China and the United States", Asia Focus, January 2015.
[177] Weinland, D. (2014) "Central Bank Sends Mixed Signals on Online Payments", South China Morning Post, 21 July 2014.

restrictions on TPP's with the aim of establishing more safeguards against payment fraud and money laundering activities. As already mentioned the PBOC revoked the first payment services license of a TPP after it was found to have misused customers' money, forging documents and operated beyond its scope. The incident reflects the risks inherent to opening up payment services to non-financial institutions and underlines the PBOC focus on tightening the regulations applicable to TPP's.[178] Key provisions contained in the draft measures include, specific technical requirements in relation to customer identity verification,[179] an annual limit and daily cap for online payments,[180] restrictions on funds remitted between bank accounts[181] and a ban on the provision of certain financial services.[182] Prior to the public consultation the draft measures were received sceptically, with stakeholders concerned that the draft measures would obstruct new market entrants due to the significant costs involved in operating multiple verification measures whilst the transactions caps would negatively impact the revenue-streams for online payment providers, ultimately stifling technological innovation in the market. The draft measures do allow for some leeway, stating that TPP's which offer adequate security measures for payment instructions such as digital certification or the use of electronic signatures can agree on a higher daily cap in dialogue with the customer. Otherwise the daily cap will be limited to RMB 5,000 for payment instructions verified through 2 or more means not including a digital certificate or electronic signature or RMB 1,000 if payment instructions are verified through fewer than 2 means. Due to the widespread concerns of these measures,[183] the PBOC issued a second statement assuring that the impact on individual spending cap would be minimal as consumers who want exceed the cap would be transferred to the platforms of the financial institutions.[184] This statement raised concerns that the PBOC is protecting the interest of the traditional financial institutions who are coming under increased pressure due to the competition of these TPP's. However, the main rationale of

[178] Shaotong, L. (2015) "New Regulation on Third-party Payments Stirs Controversy ", CRJ English, 4 August 2015. China Daily. (2015), "PBOC proposes cap on third-party online payments", China Daily, 3 August 2015.

[179] The opening of a payment account for customers will require the payment institution to register and verify the identity through 3 external channels (e.g. credit reporting agencies, tax office,..). In addition, the draft measures also makes a distinction between two payment accounts, namely, a 'comprehensive account' and a 'consumption account', which account can be opened is dependent on the degree of identity verification of the customer. Considering the fact that a 'comprehensive account' can only be set up in the event the customer verification process is conducted face-to-face or through no fewer than 5 external channels, it offers more in terms of possible services, as it can be used for transactions, remittances and purchases of investment or financial products, as well as offering a higher annual online payment limit. A 'consumption account' will only be able to offer transaction and remittance services. Cheong, H.L. (2015), "Potential Game Changers: Stringent new controls on the internet payment industry", DLA Piper, 8 September 2015.

[180] The PBOC plans to limit the amount an individual can pay online to RMB 5,000 (7000 EUR) per day, unless the customers identity is verified through security tokens and electronic signatures.

[181] Restrictions are imposed on remittances between a customers' payment account and bank accounts. In result, customers are only permitted to transfer funds from their own personal savings or current account into their own payment account, and vice versa.

[182] The draft measures clearly state that TPP's are not financial institutions and as such are prohibited from providing financial services in any form. According to the draft measures financial services include cash deposits and withdrawals, money lending, funding, wealth management, guarantee services and currency exchange. As a result, TPP's will be prohibited to hold funds for peer-to-peer (P2P) lenders

[183] Soo, Z. (2015) "Outrage as China mulls limiting online payments to US$800 a day, except through state-owned banks", South China Morning Post, 3 August 2015.

[184] Shaotong, L. (2015) "New Regulation on Third-party Payments Stirs Controversy ", CRJ English, 4 August 2015.

the PBOC's approach lies in answering to potential liability issues, as large transactions through TPP's are beyond the protection of bank deposit insurance and will leave consumers vulnerable to possible risks.[185] Such a stance is indeed backed up by the exemptions on the restrictions. If TPP's can ensure a secure platform through digital certification and signature qualification checks, they will be largely unaffected by these new restrictions.[186]

MONEY LAUNDERING MEASURES - In addition to the Measures, TPP's will have to take into account the Anti-Money Laundering Law of 2007.[187] The Law prescribes anti-money laundering principles applicable to both financial and non-financial institutions which include the implementation of supervisory measures,[188] the establishment of client identification processes and report on suspicious transactions.[189] In addition, these Anti-Money Laundering Measures require payment institutions to establish an anti-money laundering department responsible for both money laundering and counter terrorism financing, in addition to setting up internal control mechanisms to improve the detection of suspicious activities by filing these systems with the local branch of the PBOC.[190]

TAIWAN - Other countries in the Asian market are similarly reforming their regulatory landscape taking the emergence of TPP's into account. Taiwan, for instance, recently passed the Electronic Payments Processing Institutions Act which permits non-financial institutions to offer third-party payment services, including open collection and payment, deposits, and remittances.[191] The principal aim of the act is to solidify the development of electronic payment institutions and provide consumers with secure and convenient fund transfer services. According to the Act, the services to be provided by TPP's, include the initiation and receipt of the actual transaction amount on behalf of their customers, provide virtual accounts on which funds can be stored electronically and transferring payments between electronic payment accounts. The Act defines an Electronic Payment Institution as an organisation that operates an Internet electronic payment platform and serves as an intermediary where the users can register and open an account for recording money transfers and deposits of money value. In addition, organisations who also transmit payment instructions and payment receipts between the payer and the payee online through electronic devices fall under the scope.[192] The Act however, does prescribe a minimum capital requirement,[193] whilst the maximum value of funds stored and transferred per transaction is limited to NT$50,000.[194] In contrast to China, the Act does address foreign-invested enterprises and states that these are required to obtain licenses from Taiwan's authorities before providing online payment services.[195] According to recent reports Taiwan

[185] China Daily. (2015), "PBOC proposes cap on third-party online payments", China Daily, 3 August 2015.
[186] Fan, W. (2015) "China considers limiting third-party online payments", ECNS, 2 August 2015.
[187] People's Bank of China order No. 1 Rules for Anti-Money Laundering by Financial Institutions.
[188] Article 3 Anti-Money Laundering Law.
[189] Article 17-22 Anti-Money Laundering Law.
[190] Article 15 Anti-Money Laundering Law.
[191] Act Governing Electronic Payment Institutions effective 3 May 2015.
[192] Tseng, J. (2015), "Taiwan Act Governing Electronic Payment Institutions", K&L Gates, 26 May 2015.
[193] Section 7 of the Act.
[194] Section 15 of the Act and Cheng, M. (2014) "Taiwan Finance Committee Streamlines Development of Mobile Payments Services", Payment Week, 30 December 2014.
[195] Lan, K. (2015) "Taiwan Turns On The Engine of E-Commerce By Passed Third-Party Payment Regulations", Ctimes, 18 January 2015.

will issue the first batch of third-party payment licenses to organisations applying for permission to offer their services in Taiwan.[196] Regarding anti-money laundering measures, TPP's currently do not fall under the scope of '*financial institutions*' under Article 5 of the Money Laundering Prevention Act of Taiwan,[197] meaning that TPP's are not subjected to customer identification and record keeping requirements. Recently however, the Ministry of Economic Affairs of Taiwan was instructed to propose amendments to the Money Laundering Prevention Act to include TPP's.[198]

JAPAN - Japan has not specifically addressed TPP's, but the Payment Services Act of 2010 prescribes provisions for non-financial institutions wishing to offer funds transfer actions.[199] The Act is less restrictive than the Banking Act of 1981 and places fewer restrictions on non-financial institutions, as it does not explicitly restrict the types of funds transfer services providers may offer.[200] According to the Act, non-financial institutions can engage in fund transfer services in Japan provided they are registered as "fund transfer business operators".[201] These operators are also required to take anti-money laundering measures into account pursuant to Act on Prevention of Transfer of Criminal Proceeds of Japan.[202]

CONCLUSION - Clearly, the emergence of TPP's within the Asian market have instigated regulatory initiatives all aiming to address security concerns whilst preserving consumer confidence and trust in these new payment providers. In general, TPP's are required to obtain a license from the relevant national authorities ensuring that they meet minimum operational standards. Nevertheless, as the market share of TPP's in online payments continues to increase, governments are seeking to further revise their regulatory landscape, adopting more stringent approaching due to the ever-increasing concerns of security, consumer protection and money-laundering issues.

5.5.2. United States

BACKGROUND - The United States has always been widely recognised as an innovator in terms of payment solutions. Third-parties have played a crucial role in the development of US payment systems mostly providing complementary tasks for financial institutions. However, organisations are increasingly offering competitive services to traditional financial institutions providing for alternative payment methods. Payment customers are gradually being provided with payment services that bypass the traditional payment chain. PayPal for instance allows users to link their bank account with their PayPal account for verification purposes.[203] Customers can then choose to either complete transactions through their credit and/or debit card or deposit money on their PayPal balance to complete transactions in an alternative manner. In recent years, numerous non-bank payment service providers have

[196] Chen, T. (2015) "Third-party payment licenses to be issued next month", Taipei Times, 28 July 2015.
[197] The Money Laundering Control Act, effective 23 April 1997.
[198] Executive Yuan. (2013), "Legal basis for third-party payment services affirmed", Executive Yuan, 7 August 2013.
[199] Payment Services Act No. 59 effective April 1 2010.
[200] Suda, H. & Itokawa, T. (2010), "Non-bank entities engage in fund transfer services", International Financial Law Review, 1 September 2010.
[201] The Act defines funds transfer services as: "exchange transactions (limited to those specified by Cabinet Order as small sum transactions) carried out by persons other than Banks". Article 2(2) Payment Services Act.
[202] Act No. 22 of 2007 on Prevention of Transfer of Criminal Proceeds of Japan.
[203] *paypal.com/webapps/mpp/about-paypal-products.*

emerged in the US, including Google, Amazon and Square.[204] The services provided by these providers are diverse and range from alternative payment services to bank card processing services.[205]

MONEY TRANSMITTERS - Payment innovations have been backed up by a fairly supportive regulatory framework. Nevertheless, the regulatory landscape in the US is less unified as TPP's are primarily regulated as money transmitters on a state-by-state basis. For instance, according to the Florida Statute a money transmitter requires a license which "*authorizes the holder to transmit currency, monetary value, or payment instruments, either by wire, facsimile, electronic transfer, courier, the Internet, or through bill payment services or other businesses that facilitate such transfer, within this country or to or from locations outside this country*".[206] Evidently, each state has adopted its own specific requirements but most states require a surety bond in order to ensure money transmitters do not misuse customer funds.[207] It is however, important to note that not all TPP's are considered as money transmitters. Services such as payment gateways[208] are TPP's but are not involved in the actual processing or the transmitting of payment services. Instead these offer a secure API which facilitate communication between payment service providers.[209]

MONEY SERVICES BUSINESS - On a Federal level, all money transmitters fall under the scope of '*money services business*' regardless of the size of transactions.[210] Organisations falling under the scope of money services business are required to register with the Financial Crimes Enforcement Network (FinCEN) under the Bank Secrecy Act.[211] This entails that TPP's will need to comply with registration, reporting, recordkeeping and anti-money laundering measures contained in the Bank Secrecy Act. This strong focus on potential security risks is illustrated by a FinCEN Advisory relating to risks associated with third-Party Payment Processors with the primary aim of strengthening efforts to protect the payment market from money-laundering and terrorist financing activities.[212] Consequently, this entails that TPP's will need to comply with registration, reporting, recordkeeping and anti-money laundering measures contained in the Bank Secrecy Act.[213] The Act requires financial institutions to keep records of payment transactions exceeding US$10,000 and to report suspicious activity that might signify money laundering, tax evasion, or other criminal activities.[214]

---

[204] *cash.me*.
[205] Borst, N. (2015) "Non-Banks and Retail Payments: Innovations in China and the United States", Asia Focus, January 2015.
[206] Section 560.209 of the Florida Statutes
[207] E.g. Section 1315.07 of the Ohio Revised Code, the Revised Code of Washington Section 19.230.030 and Title 6, Chapter 12, Article 1 of the laws of State of Arizona
[208] Examples include Google Checkout, Wirecard and Moneybookers.
[209] These organisations will typically need to either be an Independent Sales Organization (ISO) or a Member Service Provider in order to be able to offer payment gateway services.
[210] 31 CFR Chapter X § 1010.100.
[211] 31 CFR Chapter X § 1022.380.
[212] Financial Crimes Enforcement Network (2012) "Advisory Risk Associated with Third-Party Payment Processors", FIN-2012-A010, 22 October 2012. See also Federal Deposit Insurance Corporation, (2012) "Financial Institution Letters: Payment Processor Relationships", FIL-3-2012, Revised July 2014.
[213] 31 CFR Chapter X § 1022.210.
[214] 31 CFR Chapter X §1022.320

MONEY LAUNDERING AND TERRORIST FINANCING - As TPP's fall under the scope of money services businesses they can, pursuant to Section 314(b) of the USA Patriot Act of 2001, after giving notice to FinCEN, voluntarily exchange information with other money services businesses for the purpose of identifying and reporting possible money laundering or terrorist financing, under protection of the legal safe harbor.[215] In addition, the Patriot Act prescribes minimum standards for financial institutions in relation to the verification of the identification of a customer when opening an account.[216]

FRAGMENTED LEGAL FRAMEWORK - Whilst the regulatory framework for TPP's is somewhat fragmented due to both specific State Law and Federal Law being applicable, it nonetheless supports the further development of these innovative services by not placing overly burdensome provisions on new innovative market entrants. Nevertheless, TPP's looking to engage in national financial activities in the US, will not only need to comply with the Federal legal framework; they will also need to take into account the diverse legal patchwork of applicable State law provisions. TPP's will typically be required to obtain a money transmitter license in the State they are offering their services. Such an obligation aims to preserve consumer confidence in new and alternative payment solutions. On a Federal level, security, money-laundering and terrorist financing concerns are alleviated by placing obligations on all money services businesses.

The following table summarizes the similarities and discrepancies between legal framework in the US and Asia and that of the EU:

Provision	EU	US	China
Regulation of TPP's	Yes	TPP's do fall under the regulatory scope as money transmitters or money services businesses	Yes
TPP definition	A clear distinction is made between PISP's and AISP's	n/a	Payment Services of non-financial institutions
License required	Yes	Yes, money remitters require State licensing	Yes
Capital requirements	Yes, both initial capital and additional funds requirement	Dependent on State requirements	Yes, 100 million RMB in registered capital (or 30 million RMB for local services)
AML rules	Yes	Yes, through a separate Act*	Yes
*The Bank Secrecy Act and the Patriot Act			

Table 3: EU, US and China comparison

[215] Financial Crimes Enforcement Network (FinCEN), Advisory Guidance to Money Services Businesses on Obtaining and Maintaining Banking Services, 26 April 2005.
[216] Section 326 USA Patriot Act.

6. Cryptocurrencies and service providers

EU, US AND ASIA - In this section, the legal status of cryptocurrencies and their service providers will be analyzed. First, the focus will be put on the current EU legal framework in this matter – as set by the Payment Services Directive and the Second E-money Directive – and the shortcomings thereof.[217] In the same step, the focus will also be put on the position of cryptocurrencies under the current legislative proposal of PSD2 and the recently adopted AMLD4. Also a tentative look at the upcoming proposal for a Third E-money Directive (EMD3) will be made. Second, in a comparative analysis of developments in the US and Asia, the potential for regulation of service providers through licensing schemes will be analyzed.

6.1. Virtual currencies under the EU's legal framework

6.1.1. PSD

PAYMENT SERVICE PROVIDERS - The main scope of the Payment Services Directive are payment service providers.[218] When a particular service provider aims to offer what constitutes a payment service under the scope of the directive – and its applicable national implementations by the EU Member States – this service provider will – as a payment service provider – therefore become subject to specific regulation.

AUTHORIZATION - More in particular, these payment service providers need to be authorized, and are subjected to capital and own funds requirements, as well as to provisions regarding their liability, recordkeeping duties, and transparency and information duties.[219]

WAIVERS - As this legal framework was feared to impose unnecessary burdens on new market players, the PSD does also contain provisions aimed at limiting or waiving a number of requirements for small market players, such as the authorization procedure[220], and includes derogations for low value payments – also referred to as micropayments.[221]

APPLICATION TO CRYPTOCURRENCY SERVICE PROVIDERS - From its scope of application, it can be derived that the Payment Services Directive aims to regulate only the service providers themselves and not the issuers of the funds used in such payments. As a result, the directive cannot regulate the emission of cryptocurrency.[222] Also the application of the directive to cryptocurrency service providers seems to be difficult. The formulation of payment services[223] to which the directive applies does not leave much room for the inclusion of cryptocurrency services. As a core principle, the payment services covered by the directive revolve around the notion of 'funds', which is defined as "*banknotes and coins, scriptural money and electronic money as defined in Article 1(3)(b) of Directive 2000/46/EC*".[224] Here, it can indeed be held that privately issued currencies also fall under the scope of this

[217] For this matter, conclusions are drawn from earlier work: Vandezande, N. (2014) "Between Bitcoins and mobile payments: will the European Commission's new proposal provide more legal certainty?", *International Journal of Law and Information Technology, 22*(3), 295-310.
[218] Article 1 Payment Services Directive specifies six categories of payment service providers.
[219] Articles 4 – 9, 16 – 25 and 30 – 50 Payment Services Directive.
[220] Article 26 Payment Services Directive.
[221] Article 53 Payment Services Directive.
[222] ECB (2012) "Virtual Currency Schemes", *ecb.europa.eu*, 43.
[223] As defined in the annex to the Payment Services Directive.
[224] Article 4(15) Payment Services Directive.

definition[225], regardless of their denomination. However, where such currencies are not denominated in euro or a currency of an EU Member State outside of the Eurozone – as is the case for cryptocurrencies – titles III and IV of the directive do not apply.[226] Therefore, it would theoretically be possible for certain cryptocurrency service providers to fall under the scope of the Payment Services Directive, be it that only the requirements following from title II of the directive would apply.

SCOPE EXCEPTIONS - However, the Payment Services Directive has a rather broad range of scope exceptions, listed under article 3. Three of these exceptions are of particular importance for cryptocurrency service providers.

ADDED VALUE EXCEPTION - The first of these scope exceptions is the added value exception. The Payment Services Directive considers payment services as, amongst others, payment transactions executed and consented to by telecommunication, digital or IT devices to the provider of such device or network and acting as an intermediary between the user and the supplier of the goods and services.[227] For those purposes, the position of the payment service provider as an intermediary is important, as a more elaborate role could be considered to fall under a scope limitation.[228] If a payment service provider were therefore to add value to his role by offering a broader range of services, it could thus exceed the role of a mere intermediary.[229] An active curator of an online store platform – such as Apple's App Store and Google Play – could therefore be considered to go beyond the position of mere intermediary and thus be exempted from the scope of application of the Payment Services Directive. A similar argument can be made for cryptocurrencies. Where a service provider would offer a range of services going beyond what an intermediary would offer, it could be exempt from the scope of the directive.

LIMITED NETWORKS EXCEPTION - The second scope limitation is the limited networks exception, which holds that the directive does not apply to services used for the acquisition of goods or services '*within a limited network of service providers or for a limited range of goods or services*'.[230] Also here, closed and curated online store platforms – also referred to as 'walled gardens' – could be considered as limiting the range of services offered, as well as the range of service providers offering their services. As the application of this scope limitation has proven problematic in practice, arguments could be made either way.[231] For cryptocurrencies, it could be argued that their wide potential does not allow them to be exempted from the application of the directive on the grounds of operating within a 'limited network' and serving for a 'limited range' of goods and services. Conversely, it could also be

[225] *ec.europa.eu/internal_market/payments/docs/framework/transposition/faq_en.pdf*, question 164.
[226] As follows from article 2(2) of the directive.
[227] Annex to the Payment Services Directive.
[228] Article 3 (l) Payment Services Directive; DLA Piper (2009) "EU study on the Legal analysis of a Single Market for the Information Society - New rules for a new age?", *ec.europa.eu*, 12-13.
[229] DLA Piper (2009) "EU study on the Legal analysis of a Single Market for the Information Society - New rules for a new age?", *ec.europa.eu*, 12-13. See also recital 6 to the Payment Services Directive, providing that it is appropriate for the '*legal framework to apply to cases where the operator acts only as an intermediary who simply arranges for payment to be made to a third-party supplier*' (emphasis added).
[230] Article 3 (k) Payment Services Directive.
[231] DLA Piper (2009) "EU study on the Legal analysis of a Single Market for the Information Society - New rules for a new age?", *ec.europa.eu*, 18.

argued that many cryptocurrencies have not reached this wide potential and are only accepted within a particular group or community, and that therefore the exception could still apply.[232]

MONEY EXCHANGE SERVICES - Finally, it must be noted that the Payment Services Directive does not include money exchange services under its scope of application, if the funds are not held on a payment account.[233] As many cryptocurrency services are aimed at providing precisely exchange services, this would also put those service providers outside of the scope of the directive.

APPLICATION TO CRYPTOCURRENCIES IMPLAUSIBLE - The result of these broad scope exceptions is that the application of the Payment Services Directive to cryptocurrencies seems implausible at best. While a broad interpretation of the notion of 'funds' could open the door for cryptocurrencies, the scope exceptions almost certainly rule out the application of the directive to this technological development.

6.1.2. EMD2

E-MONEY ISSUERS - The Second E-money Directive targets the issuers of electronic money, or e-money. The directive uses a very narrow definition of this concept, which thus limits its scope of application significantly. Limited use prepaid instruments, such as store and membership cards, are for instance already explicitly excluded from its scope.[234] Moreover, the Second E-money Directive shares a number of scope limitations with the Payment Services Directive.

SIMILARITIES TO PSD - Overall, the Second E-money Directive follows the same path as the Payment Services Directive, a result of legislative convergence in this field. More in particular, the Second E-money Directive contains provisions regarding mergers and takeovers[235], initial capital and own funds[236], safeguards[237], complaint and redress procedures[238], etc. As was the case for the Payment Services Directive, smaller market players can be exempted.[239]

DEFINITION OF E-MONEY - The Second E-money Directive has an important scope limitation in its narrow view of what constitutes e-money. The directive defines this notion as "*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*".[240] There is another element, which in the Second E-money Directive is no longer included in this definition, namely the

[232] Jacobs, E. (2011) "Bitcoin: A Bit Too Far?", *Journal of Internet Banking and Commerce* 16.
[233] Article 3(f) Payment Services Directive.
[234] Recital 5 Second E-money Directive.
[235] Article 3 Second E-money Directive.
[236] Article 4 – 5 Second E-money Directive.
[237] Article 6 – 7 Second E-money Directive.
[238] Article 13 Second E-money Directive.
[239] Article 9 Second E-money Directive.
[240] Article 2 (2) Second E-money Directive.

redeemability requirement.[241] This requirement holds that e-money must be redeemable at par value, meaning that a link is preserved between the value of e-money and physical money. [242]

ORIGIN OF DEFINITION - The requirement of e-money being issued on receipt of funds was not present in the original discussions regarding e-purses and e-money at the European Monetary Institute in the 1990's, nor in the European Commission's original proposal for the First E-money Directive. This element was only introduced in one of the later stages of the legislative process leading up to the First E-money Directive, namely in the Council of the European Union's common position. More in particular, the Council introduced the element of "*issued on receipt of funds of an amount not less in value than the monetary value issued*" into the definition of e-money, stating that "*the bearer must always pay in full for the electronic money received"* and that it will "*thus not be possible to issue electronic money for a higher amount than that paid in exchange*".[243] With this reasoning, the Council seems to have wanted to ease the ECB's concern for the over-issuing of e-money, or inflationary schemes.[244] However, this concern was already addressed by the inclusion of a redeemability requirement. The introduction of the issuance requirement can therefore be considered as somewhat superfluous, as the redeemability requirement already deals with the ECB's concerns regarding the potential dangers of unrestricted e-money creation.[245] Moreover, its inclusion in the definition of e-money can be argued to even have adverse results, as it does not prohibit over-issuing of e-money, but simply excludes such schemes from the scope of the directive.[246] In doing so, the schemes feared most by the ECB were not subjected to regulation, but simply placed outside the legal framework.

IMPLEMENTATION OF DEFINITION - It is also to be noted that several Member States had issues implementing this particular element of the e-money definition.[247] As a result, this element was in the Second E-money Directive changed to "*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*".[248]

---

[241] Article 11 Second E-money Directive.

[242] European Central Bank (2012) "Virtual Currency Schemes", *ecb.europa.eu*, 16. For instance, if a user purchases e-money valued at EUR 10, he will later be able to redeem that e-money for EUR 10. In other words, value fluctuations – such as those found in cryptocurrencies such as bitcoin – should not affect e-money.

[243] Council of the European Union (1999) "Common Position (EC) No 8/2000 adopted by the Council on 29 November 1999 with a view to adopting a Directive 2000/…/EC of the European Parliament and of the Council of … on the taking-up, pursuit of and prudential supervision of the business of electronic money institutions", *OJ* C 26 of 28 January 2000, 7.

[244] As expressed, for instance, in ECB (1998) "Report on electronic money", *ecb.europa.eu*, 13-14.

[245] While one author has argued that this element is integral to the definition of e-money – and proposed to go even further by fully including the redeemability requirement into the definition as well – this reasoning fails to take into account the criticism voiced by other authors, as well as the problems encountered by the Member States during the implementation of this element. Athanassiou, P., Mas-Guix, N. (2008) "Electronic money institutions", ECB Legal Working Paper Series nr.7, *ssrn.com/abstract_id=1000855*, 20-22.

[246] Lelieveldt, S. (2001) "Why is the Electronic Money-Directive Significant?", *EPSO Newsletter*, 7, May 2001; Vereecken, M. (2001) "A Harmonised EU Legal Framework for Electronic Money", *EPSO Newsletter*, 7, May 2001; Kohlbach, M. (2004) "Making Sense of Electronic Money", *The Journal of Information, Law and Technology (JILT)*, nr. 1, 7-8; DLA Piper (2009) "EU study on the Legal analysis of a Single Market for the Information Society - New rules for a new age?", *ec.europa.eu*, 8.

[247] The Evaluation Partnership ltd. (2006) "Evaluation of the E-money Directive (2000/46/EC) – final report", *ec.europa.eu*, 48.

[248] Article 2(2) Second E-money Directive.

The latter part of this element brings the Second E-money Directive in line with the Payment Services Directive. A payment transaction according to the Payment Services Directive is an "*act, initiated by the payer or by the payee, of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee*".[249] This definition is very broad and neutral and aims to cover a whole range of possible transactions whereby a monetary value is transferred between two parties, regardless of the existence of an obligation hereto between them.

NOT APPLICABLE TO CRYPTOCURRENCIES - From the requirement that e-money is to be issued on receipt of funds it follows that an e-money issuer cannot decide to create new e-money units at will.[250] This means that e-money under the Second E-money Directive must inherently be considered as a prepaid good.[251] It is this element that poses difficulties regarding cryptocurrencies, which are by nature issued following the algorithm underlying the cryptocurrency and are thus not subjected to the will of a central issuer. Such would therefore exempt cryptocurrencies from the scope of application of the Second E-money Directive.[252]

SCOPE EXCEPTIONS - Moreover, the scope exceptions of the Payment Services Directive discussed before also apply to the Second E-money Directive. The result of this would be that even if cryptocurrencies could be argued to be e-money – *quod non* – the broad range of scope exceptions could still allow cryptocurrency service providers to escape the scope of application of this legal framework.

MONEY MATRIX - The ECB itself summarizes the whole range of types of money in the following matrix, from which it becomes clear how it sees virtual currencies as an unregulated field:

	Physical	**Digital**
Unregulated	Certain types of local currencies	Virtual currencies
Regulated	Banknotes and coins	E-money, Commercial bank money (deposits)

Table 4: Money matrix[253]

6.1.3. PSD2

SCOPE EXCEPTIONS - The European Commission's proposal for a Second Payment Services Directive still includes a broad range of scope exceptions, with the main innovation being the inclusion of third party payment providers discussed under section 5 of this paper.[254] The

[249] Article 4(5) Payment Services Directive.
[250] Weber, R., Darbellay, A. (2010) "Legal issues in mobile banking", *Journal of Banking Regulation* 11, 135.
[251] *Id.*
[252] Stokes, R. (2012) "Virtual money laundering: the case of Bitcoin and the Linden dollar", *Information & Communications Technology Law* 21, 227-228.
[253] European Central Bank (2012) "Virtual Currency Schemes", *ecb.europa.eu*, 11.
[254] Articles 1 – 3 Proposal PSD2.

definitions relevant to this topic have changed little, meaning that certain cryptocurrency service providers could still be argued to fall under the scope of the directive, in as far as they provide payment services and are not covered by one of the scope exceptions. The added value, limited network, and exchange services exceptions have been retained, albeit that the former two have been slightly reformulated as they were found to leave "*room for conflicting interpretation and abuse*".[255]

ADDED VALUE EXCEPTION - First, the added value exception in the proposal states that the payment transaction must be conducted by a "*provider of electronic communication networks or services*" to a subscriber to those networks or services for the purchase or consumption of the received content, regardless of what device is used, or performed from or via an electronic device and charged to the related bill within the framework of a charitable activity or for the purchase of tickets. This means that the provision of digital content must be seen as an ancillary service to the electronic communications services provided by the network or service provider. Moreover, the European Commission has proposed a clear value limit, limiting the scope of the exception to single transactions of maximum EUR 50 and cumulative transactions of maximum EUR 300 per billing month. The clarification that this exception should only apply to providers of electronic communications services would mean that this exception would be unlikely to still apply to the providers of cryptocurrency services.[256]

LIMITED NETWORK EXCEPTION - For the limited network exception, the proposal refers to examples such as "*store cards, fuel cards, membership cards, public transport cards, meal vouchers or vouchers for specific services*", as also found in the Second E-money Directive.[257] Moreover, the proposal adds phrases such as 'specific instruments' and 'used in a limited way'. While these could be understood as an effort to demarcate and narrow down the exception's scope, such vague and undefined terminology leaves the same potential for broad and divergent interpretations as the original wording did. It can therefore be expected that this exception – if adopted in its current form – will still result in divergent application practices between Member States. It could also still be argued to apply to cryptocurrency service providers, for as far as their acceptance remains limited.

NO PSD-EMD MERGER - While originally the PSD and the EMD2 should have been subjected to a review at the same time, the European Commission has decided to postpone the review of the EMD2. This effectively rules out a merger between both legal frameworks, which had been anticipated given the strong reliance of the EMD2 on the PSD.

6.1.4. AMLD4

RECENT DEVELOPMENTS - The EU has since long supported a legal framework regulating anti-money laundering and anti-terrorist financing principles. Currently, the main legal instrument in this framework is the earlier mentioned Third Anti-Money Laundering

[255] Payment Committee (2012) "Summary Record of the Sixth meeting of the Payments Committee of 21 March 2012", *ec.europa.eu*, PC/005/12, 3.
[256] Unless such service provider would indeed be a provider of electronic communication networks or services.
[257] Recital 12 Proposal PSD2.

Directive (AMLD3). Early 2013, the European Commission proposed a revision to this framework by means of a new directive.[258]

CRYPTOCURRENCIES NOT INCLUDED - The original Proposal AMLD4 does not mention cryptocurrencies, or virtual currencies at large. Also the opinions issued by the European Central Bank, the European Economic and Social Committee, and the European Data Protection Supervisor do not make any reference to this issue.[259] Only in the Committee report tabled before the European Parliament's first plenary reading an amendment has been inserted referring to anonymous e-money products.[260] This amendment can, however, not be understood as covering cryptocurrencies, since these forms of virtual currencies are – as discussed before – no e-money under the EU's definition of this notion.

EBA CALL TO ACTION - In the meantime, the EBA had adopted an opinion on virtual currencies[261] in which a strong call was made to bring virtual currencies – including cryptocurrencies – under an existing legal framework. More in particular, the EBA called for virtual currencies to be included under the scope of the EU's Anti-Money Laundering Directive.[262] While the EBA favors a more comprehensive action in the long-term, this proposal could provide a short-term solution to "*'shield' regulated financial services from V*[irtual]*C*[urrency] *schemes*".[263] The European Commission reacted positively to this call for action, hinting that the possibility to include virtual currencies under the Proposal AMLD4 would be discussed at the trialogues.[264]

FRENCH PROPOSAL FOR INCLUSION OF CRYPTOCURRENCIES - In those discussions, held in February 2015, France[265] made a statement in support of strengthening the legal framework against terrorist financing. In this statement, the need to assess the risks posed by virtual currencies

[258] Proposal AMLD4. The legislative process leading up to the AMLD4 was discussed earlier in this paper in section **Error! Reference source not found.**.

[259] European Central Bank (2013) "Opinion of 17 May 2013 on a proposal for a directive on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing and on a proposal for a regulation on information accompanying transfers of funds", *CON/2013/32*; European Economic and Social Committee (2013) "Opinion of 23 May 2013 on the Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds COM(2013) 44 final – 2013/0024 (COD) and the Proposal for a Directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing COM(2013) 45 final – 2013/0025 (COD)", *ECO/344*; European Data Protection Supervisor (2013) "Executive summary of the Opinion on a proposal for a Directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, and a proposal for a Regulation of the European Parliament and of the Council on information on the payer accompanying transfers of funds", *OJ* C 32 of 4 February 2014, 9-12.

[260] European Parliament (2014) "Committee on Economic and Monetary Affairs and Committee on Civil Liberties, Justice and Home Affairs: Report on the proposal for a directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (COM(2013)0045) – C7-0032/2013 – 2013/0025(COD))", *A7-0150/2014*, amendment 10.

[261] European Banking Authority (2014) "Opinion on 'virtual currencies'", *EBA/Op/2014/08*.

[262] *Ibid.*, 6.

[263] *Id.*

[264] Payment Systems Market Expert Group (2014) "Minutes of the meeting of 22 October 2014, Brussels", *PSMEG 008/14*, 2-3.

[265] In response to the January 2015 terrorist attack on the magazine *Charlie Hebdo*.

is mentioned.[266] However, the Council's position adopted in April 2015 makes no explicit mention of virtual currencies and only includes the European Parliament's amendment on anonymous e-money instruments.[267] The Council's text does include a new recital 19, referring to new technologies and holding that "*competent authorities and obliged entities should be proactive in combating new and innovative ways of money laundering*".

FURTHER PROCEDURE - The European Parliament's Committee on Economic and Monetary Affairs and the Committee on Civil Liberties, Justice and Home Affairs have already issued a draft report in which they support the Council's position and recommend the plenary meeting to adopt that text without further amendment.[268] Also the European Commission has expressed its agreement with the Council's position, thus resulting in the adoption of the final text in May 2015.[269]

NO EXPLICIT INCLUSION OF CRYPTOCURRENCIES - From these documents, it is clear that it was not the European Commission's original intention to include cryptocurrencies under the scope of its Proposal AMLD4. The final text does not explicitly take up this matter either, leaving only a broad reference in a recital that could be construed as referring to such technological developments. Also the reference to anonymous e-money instruments cannot be understood as referring to cryptocurrencies.

---

[266] Council of the European Union (2015) "Proposal for a Directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (first reading) - Adoption (a) of the Council's position (b) of the statement of the Council's reasons - Statements", *7768/15 ADD 1*, 2-3.

[267] Council of the European Union (2015) "Position of the Council at first reading with a view to the adoption of a Directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC - Adopted by the Council on 20 April 2015", *5933/4/15 REV 4*.

[268] European Parliament (2015) "Committee on Economic and Monetary Affairs and Committee on Civil Liberties, Justice and Home Affairs: Draft Recommendation for second reading on the Council position at first reading with a view to the adoption of a directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (05933/3/2015 – C8-0109/2015 – 2013/0025(COD))", *PE554.948*.

[269] European Commission (2015) "Communication pursuant to Article 294(6) of the Treaty on the Functioning of the European Union concerning the position of the Council on the adoption of a Directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing", *COM(2015) 188 final*. The text was official adopted by the European Parliament in its plenary meeting of 20 May 2015: European Parliament (2015) "Legislative Resolution of 20 May 2015 on the Council position at first reading with a view to the adoption of a directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (05933/4/2015 – C8-0109/2015 – 2013/0025(COD))", *A8-0153/2015*. The text was published 5 June 2015: Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, *OJ* L 141 of 5 June 2015, 73-117.

YET ALSO NO EXPLICIT EXCLUSION - This, however, does not necessarily exclude cryptocurrencies from the AMLD4's scope altogether. The UK, for instance, has already proposed steps to include virtual currency service providers – especially exchange services – under its national AML and CFT frameworks.[270] Moreover, it has been suggested that virtual currency service providers could fall under the scope of the AMLD4's 'obliged entities'.[271] The precise degree with which cryptocurrencies can be included under the AMLD4's scope given the lack of a direct formulation in this regard can therefore be expected to become the subject of further discussion during the directive's implementation stage.[272] As is often the case for a directive, the final word on this matter will follow from the interpretations used by the Member States when transposing the text into their national legal order.

6.1.5 Quo vadis EMD3?

REVISION OF EMD2 - Article 17 of the EMD2 holds that the European Commission was to present a report on the implementation and impact of this directive by 1 November 2012. As noted, this was intended to coincide with the review of the PSD, suggesting a possible merger between both legal frameworks. However, due to the late implementation of the EMD2 by the Member States, such report has, as of the time of writing, not been presented yet.[273] The result of this – with the PSD2 being close to adoption – is that the European Commission will likely first propose amendments to the EMD2 or adopt a new directive, with the prospect of merging this revised framework with that set by the PSD2 later on.

WIDE SCOPE EXCEPTIONS - When considering the possibility of a Third E-money Directive (EMD3), a number of observations regarding the EMD2 can be made. While the EMD2 did correct some of the problems experienced with the original EMD[274], its scope exceptions are still too

---

[270] HM Treasury (2015) "Digital currencies: response to the call for information", *gov.uk/government/uploads/system/uploads/attachment_data/file/414040/digital_currencies_response_to_call_for_information_final_changes.pdf*, 19.

[271] Payments Council (2014) "HM Treasury – Digital currencies: call for information – Payments Council and BBA response", *paymentscouncil.org.uk/files/payments_council/response_to_consultations/2014/bba_submission_on_hmt_digital_currencies_consultation.pdf*, 3.

[272] While the European Commission did acknowledge that virtual currency exchange platforms were not included in the AMLD4, it does propose "*to look again into virtual currencies*". Payment Systems Market Expert Group (2015) "Minutes of the meeting of 28 April 2015", *PSMEG/005/15*, 3.

[273] The European Commission has ordered a study on the impact of the EMD2. The results of this study were presented before the Payment Systems Market Expert Group on 28 April 2015, but the final report is yet to be released.

[274] Such as the definition of e-money, which stated that e-money must be *"issued on receipt of funds of an amount not less in value than the monetary value issued".* This criterion was not adopted in full or at all by all Member States. The Evaluation Partnership ltd. (2006) "Evaluation of the E-money Directive (2000/46/EC) – final report", *ec.europa.eu*, 48. Another issue concerned mobile operators: as the prepaid credit they issue can be used for other purposes than making phone calls – such as buying ringtones or paying parking tickets – the practice of issuing such prepaid credit essentially made mobile operators e-money issuers. Mobile operators, of course, did not agree with being subjected to this legal framework. European Commission (2005) "Application of the E-money Directive to mobile operators - Summary of replies to the Consultation paper of DG Internal Market", *ec.europa.eu*, 2. The result of this controversy was that the European Commission issued a guidance document, in which it pleads for a differentiated treatment of mobile operators. European Commission (2005) "Application of the E-money Directive to mobile operators – Guidance Note from the Commission Services", *ec.europa.eu*, 4.

wide and have caused differences in treatment between Member States.[275] The result of this is that e-money issuers are found to be concentrated in those Member States that employ a favorable interpretation.[276]

EVOLUTION AWAY FROM PREPAID CARDS - Moreover, a more fundamental observation regarding the EMD's objectives can be made. Originally, it were multipurpose prepaid cards that sparked the discussions that would lead up to the first EMD.[277] By now, however, connected point-of-sale (POS) terminals that accept debit and credit cards have become ubiquitous in stores all over the world, transaction costs have been lowered, and transaction processing time has been shortened significantly. The result is that these multipurpose prepaid cards have outlived their general usefulness, and their most prominent examples are being discontinued.[278] Luckily, the European legislator already foresaw an extension of the scope of this directive. Rather than focusing solely on the notion of electronic purses, as such multipurpose prepaid cards are often called, the focus was specifically put on the broader notion of e-money. This is to be understood as also including network-based non-physical money, although the precise scope of this notion has not always been very clear.[279] Over the years, it has become evident that this has allowed pre-funded online payment schemes – such as PayPal – to become the foremost example of e-money.[280]

THEN WHAT IS E-MONEY? - The application of the e-money legal framework to service providers such as PayPal or Google Wallet has, however, never been very straightforward. Services such as these essentially allow their users to transfer money from their regular bank accounts to accounts held at the service provider, in order to allow for easy further transfers to other account holders.[281] Here, some authors have argued that such account-based transfers do not fall under the scope of what was intended for the EU's legal framework on

[275] Janowski, P. (2015) "Study on the impact of Directive 2009/110/EC on the taking up, pursuit and prudential supervision of the business of electronic money institutions", *circabc.europa.eu/sd/a/16b51176-38ec-40f8-9dce-1d46e1c35ad9/4%20-%20Presentation%20EMD%20-%20April%2028th%20Meeting.ppt*, slide 8.
[276] *Ibid.*, slide 14.
[277] Such as Proton in Belgium, Chipknip in the Netherlands, and Geldkarte in Germany.
[278] Proton was terminated in 2014, as was Chipknip. Geldkarte is currently being phased out and will be discontinued in 2018.
[279] H. van der Wielen (1997) "Electronic Money: a European Perspective", presented at the Seminar on Electronic Money, hosted by the Bank of England, London 4 February 1997, *www.simonl.org/docs/readeremdnb.pdf*, 16. In the same presentation, reference is made to "*electronic cash (on cards or networks)*", further evidencing that e-money could be used as the broader term, applying to both card-based and network-based systems. In its proposal for an Electronic Money Directive, the European Commission proposes a "*technology-neutral legal framework that harmonises the prudential supervision of electronic money institutions to the extent necessary for ensuring their sound and prudent operation and their financial integrity in particular*". European Commission (1998) "Proposal for a European Parliament and Council Directive on the taking up, the pursuit and the prudential supervision of the business of electronic money institutions (COM(1998) 461)", *OJ* C 317 of 15 October 1998, 7. Despite this clear desire to use broad terminology, a number of elements – such as the technical references in the EMD's e-money definition and the focus on low-value transactions – did maintain the impression that e-money mostly revolves around multipurpose prepaid cards.
[280] The Evaluation Partnership ltd. (2006) "Evaluation of the E-money Directive (2000/46/EC) – final report", *ec.europa.eu*, 30.
[281] For instance, when a PayPal account is linked to a debit card, money is transferred from the bank account to which the debit card acts as access instrument to the PayPal account. The user can use this PayPal balance to conduct subsequent transfers to other PayPal accountholders.

e-money.[282] Nevertheless, PayPal did successfully register as an e-money issuer in the UK.[283] A few years later, however, it decided to register as a bank in Luxembourg.[284] Google Wallet, which provides services similar to those of PayPal, is currently registered in the UK as an e-money issuer.[285] The UK's Financial Services Authority – the predecessor of the current Financial Conduct Authority – has drawn the line between deposits and e-money as follows: "*a deposit involves the creation of a debtor-creditor relationship under which the person who accepts the deposit stores value for eventual return. E-money, in contrast, involves the purchase of a means of payment*."[286] The European Commission, however, does not seem to share this reasoning that e-money instruments are mainly means of payment as it created a separate legal framework precisely for payment services.[287] Moreover, the members of the Payment Systems Market Expert Group have already remarked that the differences between payment services and e-money services are disappearing, explicitly mentioning the example of PayPal.[288]

CONSEQUENCES FOR VIRTUAL CURRENCIES - The uncertainty of what precisely constitutes e-money has a direct impact on virtual currencies. For instance, many types of virtual currencies are not prepaid instruments, thus disqualifying them as e-money.[289] The result of this is that at the present moment those virtual currencies can by definition be considered as payment instruments that do not fall under the scope of the EMD's legal framework.[290] Also in the virtual currencies that do utilize prepaid value – such as store gift cards – the applicability of the e-money definition is uncertain.[291] Moreover, the scope exceptions applicable to the

[282] González, A.G. (2004) "PayPal: The legal status of C2C payment systems", *Computer Law & Security Review*, Vol. 20, 297-298. González further argues that PayPal does essentially engage in deposit-taking activities as defined under EU law, despite its terms of use stating otherwise. Fullenkamp and Nsouli argue that PayPal uses a digitalized version of public government-issued money, as traditional e-banking services provided by credit institutions do. Their argument is that e-money in the true sense should use a privately issued currency. Fullenkamp, C., Nsouli, S.M. (2004) "Six Puzzles in Electronic Money and Banking", *IMF Working Paper WP/04/19*, 8-9.

[283] Under the UK Financial Services Authority's firm reference number 226056.

[284] More in particular, PayPal is a partnership limited by shares under Luxembourg law authorized to operate as a bank under article 2 of the Law of 5 April 1993 on the financial sector, supervised by the "Commission de surveillance du secteur financier" (CSSF).

[285] Under the UK Financial Conduct Authority's firm reference number 900008.

[286] Financial Services Authority (2011) "Implementation of the second Electronic Money Directive: supplement to HM Treasury's consultation – Feedback on CP10/25 and part of CP10/24, and final rules", *Policy Statement PS11/2*, 73.

[287] González, A.G. (2004) "PayPal: The legal status of C2C payment systems", *Computer Law & Security Review*, Vol. 20, 297-298. The author also references a direct statement from the European Commission that services such as PayPal are closer to credit transfers, thus indicating that they would fit better under the scope of the PSD than under the EMD. European Commission (2003) "Communication concerning a New Legal Framework for Payments in the Internal Market", *COM(2003) 718 final*, 23.

[288] Payment Systems Market Expert Group (2012) "Minutes of the meeting of 27 March 2012, Brussels", *ec.europa.eu*, 4.

[289] Cryptocurrencies, for one, are issued per their underlying algorithm, not on receipt of funds. Other forms of virtual currencies – such as the now discontinued Microsoft Points and Facebook Credits – can be obtained through store-bought cards carrying a code that relates to a certain balance of that virtual currency. These balances are therefore issued before the funds from users buying those cards are received.

[290] This is the reasoning followed by the European Central Bank, which explicitly considers all virtual currencies as the unregulated opposite of regulated e-money: European Central Bank (2012) "Virtual Currency Schemes", *ecb.europa.eu*, 11.

[291] In part also due to the redeemability requirement.

legal framework on e-money could still place these virtual currencies outside of the scope of that legal framework.[292]

NEW OBJECTIVES FOR AN EMD3 - Which conclusions can then be drawn from this with regard to a potential EMD3? *First*, it is clear that the original objectives for the EU's legal framework on e-money are becoming increasingly irrelevant. On the one hand, multipurpose prepaid cards are largely being phased out. On the other hand, the general feeling toward network-based e-money is that such services are so closely related to payment services that it may be questioned whether this duality between the frameworks set by the PSD and the EMD can still be upheld. *Second*, from the early results of consultations on the impact of the EMD2, it becomes clear that this directive has only provided marginal improvement over the original EMD in clarifying what constitutes e-money. At the present moment, there is an ever increasing number of novel payment methods and instrument that is excluded from the EMD2's narrow scope. This group, virtual currencies, is already becoming larger than what constitutes e-money and will likely continue to grow in the coming years. If there would be a future for an EMD3, it would therefore be unwise to bar these virtual currencies from its scope.

6.1.6. EU Member States

NATIONAL APPROACHES - While at the level of the EU the topic of virtual currencies is slowly gaining more attention, several EU Member States have already adopted a national approach on the matter. At the present moment, no EU Member State has taken active steps to block virtual currencies, nor has created a specific legal framework on virtual currencies. As a result, most of these national approaches focus on how to embed this development in their current legal frameworks.

TAXATION OF VIRTUAL CURRENCY TRANSACTIONS - Most of the discussion regarding virtual currencies within EU Member States is focused on the tax treatment of virtual currency transactions. The most important example hereof is a case currently pending before the Court of Justice of the European Union of the Swedish Tax Authority.[293] In this case, the Court is asked whether "*the exchange of virtual currency for traditional currency and vice versa* […] *constitute the supply of a service effected for consideration,* [and, if so, whether these] *exchange transactions are tax exempt*".[294] In the opinion of Advocate General Juliane Kokott, the EU's legal framework on VAT can be applied to virtual currencies, even though they are not legal tender.[295] An exchange service, exchanging virtual currency for legal tender and the other way around, can then be exempted from VAT.[296] This opinion is in line with thinking in several Member States. The Netherlands, for instance, has already noted to be considering a

[292] For instance, store gift cards can generally only be redeemed at the issuing store, thus allowing for the application of the limited networks exception.
[293] CJEU, Skatteverket *v* David Hedqvist, C-264/14.
[294] *Id.*
[295] CJEU, Skatteverket *v* David Hedqvist, C-264/14, opinion of Advocate General J. Kokott of 16 July 2015, §18.
[296] CJEU, Skatteverket *v* David Hedqvist, C-264/14, opinion of Advocate General J. Kokott of 16 July 2015, §45. Interesting is that the Advocate General points out a linguistic error in the German version of the VAT Directive, requiring the use of legal tender, which is not present in other versions.

similar direction.[297] Also Belgium[298], Finland[299], Denmark[300], and Spain[301] have taken this position.

NEGATIVE VIEWS - Not all Member States agree with this view. Estonia, for instance, holds the view that virtual currency transactions are subject to VAT.[302] Also France still holds a negative view on virtual currencies.[303] Germany concurs with the Estonian view.[304] The German Federal Financial Supervisory Authority (BaFin) has considered virtual currencies as financial instruments, as being units of account similar to foreign currencies but without the status of legal tender.[305] As such, certain services concerning the use and trading of cryptocurrencies would become subject to regulatory oversight. This position was confirmed by the German Minister of Finance.[306]

FURTHER DEVELOPMENT IN THE UK - Apart from agreeing with the position of VAT exemption[307], the UK currently seems to be the only Member State so far planning to develop a specific legal framework on virtual currencies. In 2014, HM Treasury launched a program looking into the question of virtual currency regulation.[308] The results of a public consultation round were published in March 2015.[309] Interesting here is the response of the UK Home Office, which proposes to limit the creation of virtual currencies to the government, thus giving the government full control over virtual currencies.[310]

NO SPECIFIC OPINION YET - Last, there are a number of Member States that have not yet specifically addressed the issue of virtual currency regulation. These include Croatia, Cyprus, Greece, and Ireland.[311]

POSITIVE SIGNS AND POTENTIAL FOR HARMONIZATION - The more recent wave of Member States adopting a more neutral approach toward virtual currencies can be considered as a

[297] Van Wirdum, A. (2014) "Dutch Official: Bitcoin Transactions Probably Not Liable for VAT", *coindesk.com,* 25 November 2014.
[298] Rizzo, P. (2014) "Belgian Tax Body: Bitcoin Trades Not Subject to VAT", *coindesk.com,* 22 September 2014.
[299] Stanley-Smith, J. (2014) "Finland recognizes Bitcoin services as VAT exempt", *International Tax Review*, 14 November 2014.
[300] Sharkey, T. (2014) "Denmark Declares Bitcoin Trades are Tax-Free", *coindesk.com,* 25 March 2014.
[301] Bello Perez, Y. (2015) "Spanish Bitcoin Community Celebrates Bitcoin's VAT Exemption", *coindesk.com*, 23 April 2015.
[302] Hajdarbegovic, N. (2014) "Estonia: VAT Should Apply to Full Value of Bitcoin Trades", *coindesk.com*, 11 December 2014.
[303] Banque de France (2013) "Les dangers liés au développement des monnaies virtuelles: l'exemple du bitcoin", *banque-france.fr*.
[304] Cuthbertson, A. (2015) "Cryptocurrency round-up: UK and Germany divided over bitcoin and Bit-Reserve breaks fund-raising record", *IBTimes*, 9 January 2015.
[305] Münzer, J. (2013) "Bitcoins: Aufsichtliche Bewertung und Risiken für Nutzer", *www.bafin.de*, 19 December 2013.
[306] Deutscher Bundestag, Schriftliche Fragen, *17/14530*, 41.
[307] Cuthbertson, A. (2015) "Cryptocurrency round-up: UK and Germany divided over bitcoin and Bit-Reserve breaks fund-raising record", *IBTimes*, 9 January 2015.
[308] *gov.uk/government/speeches/chancellor-on-developing-fintech.*
[309] HM Treasury (2015) "Digital currencies: response to the call for information", *gov.uk*.
[310] Home Office (2015) "Digital Currencies: call for information", *scribd.com/doc/269477425/Home-Office-Digital-Currency-Response-CoinDesk*.
[311] Library of Congress (2014) "Regulation of Bitcoin in Selected Jurisdictions", *loc.gov.*

significant step forward from the situation during the late 2013 – early 2014 Bitcoin hype. At that time, somewhat more negative signals were submitted in response to the perceived dangers and implications of virtual currencies. Moreover, the outcome of the aforementioned CJEU case will impose an important level of harmonization in treatment of virtual currencies, at least from the perspective of taxation. This will provide Member States with a starting point from which EU-level regulation of this matter can be discussed.

6.2. Comparative analysis on virtual currency service providers in the US and Asia

CONFLUENCE BETWEEN E-MONEY AND PAYMENT SERVICES - As noted under the previous section, the differences between e-money services and payment services are becoming increasingly slimmer. The result of this is that it may be questioned whether there is not more of a need to directly regulate the service providers, rather than taking a detour via the concept of e-money.[312] A similar remark can be made for the providers of virtual currency services. In this section, a comparative analysis will be made of regulatory initiatives regarding virtual currency service providers outside of the EU, with the main focus being on the US and the Asian market. These markets have demonstrated more advanced initiatives toward virtual currencies than what can be found in the fragmented approach followed by EU Member States.

6.2.1. United States

FEDERAL APPROACH BY FINCEN - In early 2013, the US Financial Crimes Enforcement Network (FinCEN), a bureau of the United States Department of the Treasury, published a guidance document in which it considers virtual currencies as media of exchange that can operate like a currency, but that do not possess the attributes of real currency, such as being legal tender.[313] Despite virtual currencies not being considered real currency, FinCEN does consider virtual currency exchangers – those that exchange virtual currency for real currency, funds, or other virtual currency – and administrators – those that issue or redeem virtual currency – as money services businesses (MSB) when they (1) accept and transmit convertible virtual currencies, or (2) buy or sell convertible virtual currencies for any reason.[314] Users who only obtain convertible virtual currency and use it to purchase real or virtual goods or services are not considered a MSB.[315] This classification of virtual currency service providers as being subject to regulation was made possible due to FinCEN's earlier efforts, in 2011, to update a number of definitions in order to provide the "*needed flexibility to accommodate innovation in the payment systems space under our preexisting regulatory framework*".[316] The core element of importance to virtual currencies is that money transmission can include the transmission of "*other value that substitutes for currency*", rather than limiting this to the transmission of legal tender.[317] The result of this is that virtual currency exchangers and administrators must register as a MSB, and adhere to

[312] As noted by the Payment Systems Market Expert Group, see footnote 288.
[313] FinCEN (2013) "Guidance Document - Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies", *FIN-2013-G001*, 1.
[314] *Ibid.*, 3. The reasoning used here is that the "*definition of a money transmitter does not differentiate between real currencies and convertible virtual currencies*".
[315] As their activities do not fall under the scope of the definition of "money transmission services".
[316] US Senate Committee on Homeland Security and Governmental Affairs (2013) "Beyond Silk Road: Potential Risks, Threats and Promises of Virtual Currencies – Testimony of Jennifer Shasky Calvery", *hsgac.senate.gov*, 8.
[317] 31 CFR 1010.100(ff)(5)(i)(A).

recordkeeping and AML control measures.[318] In the meantime, FinCEN has adopted a number of rulings on the matter, thus further explaining the scope of this evolution.[319]

ENFORCEMENT BY FINCEN - FinCEN has also been active in enforcing this matter. After the release of the guidance document, the US Department of Homeland Security seized accounts belonging to a US-based subsidiary of then-largest bitcoin-exchange Mt.Gox on the basis of this company not being registered as MSB.[320] FinCEN also took action against Liberty Reserve, basing its action on the USA PATRIOT Act.[321] Recently, FinCEN pursued action against Ripple, a payment system and currency exchange supporting various legal tender currencies, virtual currencies, as well as its own native currency XRP. The Ripple system is operated by Ripple Labs, which wholly owns a subsidiary – XRP II – that engages in selling the XRP virtual currency. Thus, under FinCEN's rules, XRP II engages in money transmission, requiring it to register as a MSB. While XRP II did eventually register as MSB in 2013, it was later found to not have implemented an AML program nor having conducted reporting duties. As a result, XRP II was fined USD 700.000.[322]

STATE DEVELOPMENTS - Also at State level, legislative action has been taken or is underway. The State of New York is the first State considering specific regulation of virtual currency service providers. In 2013, the State Department of Financial Services launched an inquiry regarding virtual currencies.[323] In this inquiry, the Department lauds virtual currencies for bringing technological innovation to commerce platforms, while also pointing out the risks presented by these developments under their current regulatory grey area.[324] It therefore aims to investigate whether virtual currency service providers should be considered as money transmitters, as regulated and licensed under State law, or whether an entirely new framework should be considered.[325] Later, a public hearing on the matter was announced.[326]

---

[318] *Ibid.*, 9; FinCEN (2013) "Guidance Document - Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies", *FIN-2013-G001*, 3-5.

[319] For instance, it was ruled that a virtual currency trading platform is covered by the scope of MSB (FIN-2014-R011), yet not to a rental system for cryptocurrency mining hardware (FIN-2014-R007). Also cryptocurrency users that perform mining activities for private use are not considered a MSB, nor does their occasional conversion of cryptocurrency into real currency make them a money transmitter (FIN-2014-R001). Moreover, a company purchasing and selling convertible virtual currency as an investment exclusively for the company's benefit is not a money transmitter (FIN-2014-R002).

[320] Mt.Gox did later receive a MSB license. Buterin, V. (2013) "MtGox Gets FinCEN MSB License", *Bitcoin Magazine*, 29 June 2013.

[321] More in particular, the action was based on section 311, finding Liberty Reserve's transactions of primary money laundering concern. US Department of the Treasury (2013) "Treasury Identifies Virtual Currency Provider Liberty Reserve as a Financial Institution of Primary Money Laundering Concern under USA Patriot Act Section 311", *Press release,* 28 May 2013. One of the people involved in the scheme was given the maximum sentence for conspiring to operate an unlicensed money transmitting business. US Department of Justice (2014) "Chief Technology Officer of Liberty Reserve Sentenced to Five Years in Prison", *Press release 14-1393*, 12 December 2014.

[322] FinCEN (2015) "FinCEN Fines Ripple Labs Inc. in First Civil Enforcement Action Against a Virtual Currency Exchanger", *Press release*, 5 May 2015.

[323] New York State Department of Financial Services (2013) "Notice of Inquiry on Virtual Currencies", *Press memo* 12 August 2013.

[324] *Ibid.*, 1.

[325] *Ibid.*, 1-2.

[326] New York State Department of Financial Services (2013) "Notice of Intent to Hold Hearing on Virtual Currencies, Including Potential NYDFS Issuance of a 'BitLicense'", *Press memo* 14 November 2013.

Shortly after those hearings, it was remarked that the inclusion of virtual currencies under the existing regulatory framework would not suffice to cover all of the specific characteristics of virtual currencies, and that therefore a new legal framework would be proposed.[327] This was followed by a public order holding that the Department would consider applications for the establishment of virtual currency exchanges.[328] In July 2014, a first proposal for a legal framework was published, together with a public comment period.[329] In December 2014, an updated framework incorporating feedback from those public comments was presented, together with a new public comment period.[330] In May 2015, the first virtual currency service providers was granted a State license[331], with the final regulatory framework following shortly thereafter.[332] The State of California already passed an act to repeal a section of its Corporations Code that limited corporations to putting into circulation only "*the lawful money of the United States*".[333] Now, following the initiative of New York, the State is considering a similar licensing model for virtual currency businesses.[334] The State of Texas, on the other hand, does not consider virtual currency exchange or transmission as currency exchange or money transmission under the Texas Financial Code.[335] Due to its broad use of the term 'payment instrument', the State of Florida also requires virtual currency services to register as money service business.[336] A proposed amendment to the North Carolina Money Transmitters Act regulates the sale and receipt for transmission of virtual currencies and maintaining control over virtual currency on behalf of others.[337] The State of Connecticut enacted rules requiring money transmitters seeking a

[327] Lawsky, B.M. (2014) "Remarks on the Regulation of Virtual Currencies", presented at the *New America Foundation*, Washington, DC, 11 February 2014.

[328] New York State Department of Financial Services (2014) "Order pursuant to New York Banking Law§§ 2-b, 24, 32, 102-a, and 4001-b and Financial Services Law§§ 301(c) and 302(a)", *dfs.ny.gov*, 11 March 2014.

[329] New York State Department of Financial Services (2014) "Regulation of the Conduct of Virtual Currency Businesses", *NYS Register*, 23 July 2014, 14-16; New York State Department of Financial Services (2014) "NY DFS releases proposed BitLicense regulatory framework for virtual currency firms", *Press release* 17 July 2014.

[330] New York State Department of Financial Services (2014) "Superintendent Lawsky remarks on revised BitLicense framework for virtual currency regulation and trends in payments technology", *Press release* 18 December 2014. The actual revised text was released in February 2015. Fogg, J.K. (2015) "NYDFS Changes to Proposed BitLicense Regulations", *Virtual Currency Report*, 9 February 2015.

[331] Be it as a trust company, not a company under the intended BitLicense.

[332] New York State Department of Financial Services (2015) "NYDFS grants first charter to a New York virtual currency company", *Press release* 7 May 2015; New York State Department of Financial Services (2015) "NYDFS Announces Final Bitlicense Framework for Regulating Digital Currency Firms", *Speech by Benjamin M. Lawsky, Superintendent of Financial Services* 3 June 2015; Regulation of the Conduct of Virtual Currency Businesses, *New York State Register* 24 June 2015, nr. DFS-29-14-00015-A, 7-9 (hereinafter: Regulation).

[333] An act to repeal Section 107 of the Corporations Code, relating to business associations, *Cal. Assemb. B. 129* (2013-2014), Chapter 74 (Cal. Stat. 2014).

[334] Bill regarding an Act to repeal Section 107 of the Corporations Code, and to add Section 2178 to, and to add Division 11 (commencing with Section 26000) to, the Financial Code, relating to currency, *Cal. Assemb. B. 1326* (2015-2016), as amended in Senate on 6 July 2015 (hereinafter: Proposal Bill).

[335] Texas Department of Banking (2014) "Regulatory Treatment of Virtual Currencies Under the Texas Money Services Act", *Supervisory Memorandum 1037*, 2-3. However, it does view the exchange of cryptocurrency for sovereign currency through a third party exchange – as is the case for most cryptocurrency exchanges – as money transmission.

[336] Ewbank, L.T., Reyes, C.L., Hansen, J.D. (2014) "Two Florida Users of Localbitcoins.com Arrested for Money Laundering and Unlicensed Money Transmission", *Virtual Currency Report*, 11 February 2014.

[337] A Bill to be entitled an Act to enact the North Carolina Money Transmitters Act as requested by the Office of the North Carolina Commissioner of Banks (NC Money Transmitters Act.-AB), *N.C. Assemb. B. H289* (2015-2016).

license to conduct their business to state whether that business would include the transmission of monetary value in the form of virtual currency.[338]

NY STATE BITLICENSE - The State of New York's proposed BitLicense would require virtual currency businesses or their agents to obtain a license to conduct their activities.[339] Exemptions are possible for those chartered under New York Banking Law and approved by the superintendent, and merchants and consumers that use virtual currency solely for the purchase or sale of goods or services or for investment purposes.[340] Virtual currencies are considered as "*any type of digital unit that is used as a medium of exchange or a form of digitally stored value*", regardless of whether that unit is managed centralized or decentralized, or created by computing effort.[341] This definition does not extend to so-called closed-loop currencies – virtual currencies that can only be used within a gaming platform and cannot be converted into legal tender – virtual currencies used in customer affinity or rewards programs, or digital units used on Prepaid Cards.[342] Virtual currency business are those that (1) transmit virtual currency or receive them for transmission – except when such transmission is conducted for non-financial purposes and does not involve the transfer of more than a nominal amount of Virtual Currency, (2) store, hold or maintain custody or control of virtual currency on behalf of others, (3) buy or sell virtual currency as a customer business, (4) perform exchange services as a customer business, or (5) control, administer, or issue a virtual currency.[343] Moreover, it is held that the development and dissemination of software does not constitute virtual currency business activities. The license can be applied for at the superintendent and needs to include amongst others information about the business, its affiliates, and its directors and principal shareholders, an independently prepared background report, fingerprints, a financial statement, tax information, and insurance policies.[344] When not all requirements are satisfied, a conditional license may be awarded.[345] Licensees must appoint a compliance officer to oversee their compliance with these rules.[346] The superintendent may determine the amount and form of capital that must be maintained by the licensee in order to safeguard its financial integrity.[347] To protect customer assets, licensees must maintain a surety bond or trust account in US dollars, and virtual currency held on behalf of others must be maintained in full, unless instructed otherwise by those on whose behalf the virtual currency was held.[348] New products, services or activities or material changes to existing ones must be reported.[349] When control over a licensee's activities changes – also including mergers or acquisitions – such event is subject to prior approval by the superintendent.[350] All virtual currency business activities must be

[338] An Act concerning mortgage correspondent lenders, the Small Loan Act, virtual currencies and security freezes on consumer credit reports, *Conn. Pub. Act 15-53*.
[339] Section 200.3 Regulation.
[340] *Id.*
[341] Section 200.2(p) Regulation.
[342] *Id.*
[343] Section 200.2(q) Regulation.
[344] Section 200.4(a) Regulation. This application is subject to a USD 5.000 application fee: Section 200.5 Regulation. A license can be suspended or revoked after a hearing: Section 200.6(c)-(d) Regulation.
[345] Section 200.4(c) Regulation.
[346] Section 200.7 Regulation.
[347] Section 200.8 Regulation.
[348] Section 200.9 Regulation.
[349] Section 200.10 Regulation.
[350] Section 200.11 Regulation.

recorded and preserved for at least seven years in order to allow for the determination of compliance.[351] Such records must include, amongst others, transaction amounts and dates, the names and account numbers of parties involved in those transactions, bank statements, records of meetings of the board of directors, and records regarding compliance with applicable state and federal anti-money laundering laws, rules, and regulations.[352] The superintendent will examine those records at least once every two years in order to determine the financial soundness of the business, management policies, and compliance.[353] Moreover, licensees must submit quarterly financial statements regarding their financial condition, financial projections, and compliance.[354] Additionally, yearly audited financial statements have to be submitted, including statements regarding management's responsibilities in preparing those statements, an assessment of the licensee's compliance, and certification of the statements by an officer or director of the licensee.[355] To further ensure customer protection and compliance, licensees are required to maintain an AML program, based on a risk assessment for the legal, compliance, financial, and reputational risks associated with their activities.[356] Such program must provide for internal procedures to maintain compliance, as well as independent testing thereof, and provide for record-keeping, and reporting on transactions and suspicious activities.[357] Also the adoption of a cybersecurity program is required, as well as the appointment of a chief information security officer, to ensure the availability of their services, and to protect their data from tampering.[358] As an emergency measure, a business continuity and disaster recovery (BCDR) plan must be drafted.[359] All advertising and marketing material must identify the licensee's status as licensed virtual currency business.[360] Licensees must communicate to their customers about the risks involved with virtual currencies, as well as of the applicable terms and conditions.[361] Last, an accessible complaint mechanism must be provided.[362]

CALIFORNIA STATE PROPOSAL - The proposed California State Bill amends the California Financial Code to hold that virtual currency businesses must be properly licensed, and must comply with capital requirements and reporting duties. Moreover, the Commissioner of Business Oversight would be able to investigate virtual currency businesses, and to revoke licenses and impose penalties where needed. The definition of virtual currencies employed here corresponds in part to that of the State of New York's proposal, referring to any type of digital unit that is used as a medium of exchange or a form of digitally stored value, and excluding virtual currencies used on gaming platforms, or as part of customer affinity or rewards programs if they cannot be redeemed for fiat currency.[363] Virtual currency

[351] Section 200.12 Regulation.
[352] *Id.*
[353] Section 200.13(a) Regulation.
[354] Section 200.14(a) Regulation.
[355] Section 200.15(b) Regulation.
[356] *Id.*
[357] Note that this also includes know-you-customer (KYC) and due diligence obligations, and explicitly forbids virtual currency transactions that would obfuscate or conceal the identity of an individual customer or counterparty: Section 200.15(g) Regulation.
[358] Section 200.16 Regulation.
[359] Section 200.17 Regulation.
[360] Section 200.18 Regulation.
[361] Section 200.19 Regulation.
[362] Section 200.20 Regulation.
[363] Section 26000(b) Proposal Bill.

businesses are those that maintain full custody or control of virtual currency on behalf of others.[364] While principally these businesses must be licensed, the Bill provides a number of exemptions: US departments and agencies at federal, State or local level; money transmission via the United States Postal Service; commercial banks insured via the Federal Deposit Insurance Corporation; licensed money transmitters; merchants or consumers using virtual currencies solely for the purchase or sale of goods or services; transactions where "*the recipient of virtual currency is an agent of the payee pursuant to a preexisting written contract and delivery of the virtual currency to the agent satisfies the payor's obligation to the payee*"; virtual currency network software developers, distributors or servicers; those contributing software, connectivity or computing power to virtual currency networks; and those providing data storage or cyber security services for licensed virtual currency businesses.[365] As in New York, the application is subject to a USD 5.000 application fee and must contain predefined information on the applicant and the virtual currency business, including financial information and ownership information.[366] Each licensee must maintain a certain amount of capital, calculated taking in account – amongst others – its assets, liquidity, risk exposure, liabilities, volume of virtual currency activities, activities in other States, and financial protection through trust accounts and bonds.[367] The commissioner can examine virtual currency businesses to verify their compliance.[368] Licensees are required to file reports in the case of bankruptcy, receivership, when revoking or suspending their license, in case of cancellation of their bond or trust accounts, or when charged or convicted for a felony.[369] A license can be surrendered voluntarily[370], and the commissioner can make decisions, issue opinions or provide guidance on the requirements.[371] To protect the general welfare of the public, the commissioner may exercise all powers regarding virtual currency businesses enclosed in the Bill, or order those businesses to comply.[372] Licenses can be suspended or revoked, for instance when the virtual currency business does not comply with the provisions of the Bill or the commissioner's examination thereof, in case of fraud, when unsafe practices or practices that go against the public interest are conducted, or in the case of insolvency or bankruptcy.[373] The commissioner's acts are subject to review[374], and the licensee may request a hearing when his license has been revoked or suspended.[375] The commissioner can also impose civil penalties.[376] Licensees must file independently prepared audit reports and public accountant certifications for each fiscal year, as well as quarterly

[364] Section 26000(c) Proposal Bill.
[365] Section 26004 Proposal Bill.
[366] Section 26006 Proposal Bill. Particular for the California Bill is that it is more specific in including fees for license renewals, branch offices, an hourly fee for applicant or licensee examinations, and a fee for those acquiring control over a licensee.
[367] Section 26008 Proposal Bill.
[368] Section 26009 Proposal Bill. Such examination can be held jointly with other State or federal regulators: Section 26010 Proposal Bill.
[369] Section 26011 Proposal Bill. Records must be kept for three years: Section 26012 Proposal Bill.
[370] Section 26013 Proposal Bill.
[371] Section 25014 Proposal Bill. This includes informal guidance to prospective applicants: Section 26015 Proposal Bill.
[372] Section 26016 Proposal Bill.
[373] Section 26017 Proposal Bill.
[374] Section 26018 Proposal Bill.
[375] Section 26019 Proposal Bill.
[376] Section 26020 Proposal Bill. Other enforcement options granted to the commissioner are also maintained: Section 26022 Proposal Bill.

financial reports, unless exempted therefrom by the commissioner.[377] Virtual currency businesses must provide clear information regarding the potential risks of virtual currencies to their customers.[378] Upon completion of virtual currency transactions, receipt containing specific information must be issued.[379] As in New York, the Commissioner may provide exemptions.[380] Licensed money transmitters can convert their license.[381] Provisional licenses can be issued to small businesses of less than USD 1 million in outstanding obligations.[382] While the State of California's Bill shows a number of clear similarities to the State of New York's proposed regulation, there is also a notable difference in that the Bill does not include broad AML, cybersecurity or BCDR requirements.[383]

SIMILARITIES TO EU LAW - Both proposals demonstrate a number of similarities to the EU's legal framework on payment services. In all of these frameworks, there is a specific service provider – the virtual currency business in the US frameworks and the payment service provider in the EU – that must be authorized to conduct its business. To gain such authorization – or license – the service providers must apply to a local regulator, taking into account a number of information requirements. On both sides of the Atlantic, strict capital requirements are imposed on these service providers. Moreover, specific measures must be adopted to safeguard customer assets, and the use of agents is regulated. Last, the service providers are subjected to recordkeeping and information duties.

DIFFERENCES FROM EU LAW - The main difference between the approach followed in the EU and the US regarding virtual currencies is that in the US FinCEN has taken steps to include virtual currencies under the definition of money transmitter, thus allowing that certain virtual currency businesses could become subjected to the regulation of money service businesses. While under the EU's legal framework regarding payment services a small argument could be made for the inclusion of certain virtual currencies[384], such inclusion would be limited at best. If the EU were to undertake a concerted effort at regulating virtual currency service providers, it would therefore have to open up its existing framework, or device a new framework altogether.

[377] Section 26023 Proposal Bill. An additional fee may be levied for the commissioner's expenses in administering this duty: Section 26024 Proposal Bill.
[378] Section 26025 Proposal Bill.
[379] Section 26026 Proposal Bill.
[380] Section 26029 Proposal Bill.
[381] Section 26031 Proposal Bill.
[382] Section 26032 Proposal Bill.
[383] Note that exemptions for mining operations and software development, while not present in the original proposal, where added during the State Assembly discussions.
[384] See section 6.1.1.

The following table summarizes the similarities and discrepancies between the two US legislative proposals and the current EU legal framework:

	NY	Cal.	EU
Regulation of VC service providers	Yes	Yes	No
VC definition	Any type of digital unit that is used as a medium of exchange or a form of digitally stored value	Any type of digital unit that is used as a medium of exchange or a form of digitally stored value	None
Exclusions	Closed loop currencies, customer affinity and rewards programs, prepaid cards, software development and dissemination	Gaming platforms, customer affinity and rewards programs, VC that cannot be redeemed for fiat currency, software and VC network development	n/a
License required	Yes	Yes	Authorization required if operating as payment institution
Capital requirements	To be determined by superintendent	To be determined by the commissioner	Determined by PSD*
Recordkeeping requirements	Yes	Yes	Yes*
AML rules	Yes	No	Yes, through separate directive*
Cyber security rules	Yes	No	Limited security principles*
*: if the service provider is covered by the PSD			

Table 5: US-EU comparison

6.2.2. Asia

PAYMENT SYSTEMS DEVELOPMENT IN ASIA - Over the years, the Asian market has often proven to be the center of innovation in payment systems. Already in 1996, the Seoul Transportation Card was issued, a contactless prepaid card used on Seoul's bus transportation network.[385] A year later, a similar initiative was launched in Hong Kong.[386] Hong Kong's Octopus Card, however, would soon outgrow its original status as a transportation card and can now be used as a payment method in all kinds of retail outlets, parking lots, self-service kiosks and leisure facilities, and has also been adopted as a means of access control, for instance in private buildings.[387] More than 13 million transactions are processed every day, for a value over HK$ 150 million.[388] The Octopus Card makes use of Sony's FeliCa technology, which has been

[385] *mifare.net/en/showcases/showcase-seoul*.
[386] *octopus.com.hk/about-us/milestones/en/index.html#_yr1997*.
[387] *octopus.com.hk/get-your-octopus/where-can-i-use-it/en/index.html*.
[388] *octopus.com.hk/octopus-for-businesses/benefits-for-your-business/en/index.html*.

adopted in various places across Asia. One example is Singapore's EZ-Link card, which apart from functioning as a transportation card is also expanding its retail payments capabilities.[389] An example within Japan is the Kantō region's Suica card.[390] A new version of FeliCa has been implemented in mobile phones to form *osaifu keitai*, Japan's standard in mobile wallets.[391]

CHINA - While the recent developments in cryptocurrencies mainly find their origins in the US, an important segment of this market is shifting toward Asia. Mt.Gox, the once largest bitcoin exchange, conducted its main business in Japan. As of the time of writing, some of the largest bitcoin exchanges are located in China.[392] Despite the rising importance of the Asian market for cryptocurrencies and virtual currencies at large, regulatory response has been less positive. Late 2013, the People's Bank of China, together with the Ministry of Industry and Information Technology, the Chinese Banking Regulatory Commission, the Chinese Insurance Regulatory Commission, and the Chinese Security Regulatory Commission issued a notice in which the risks regarding cryptocurrencies are explained.[393] As a core principle, cryptocurrencies are not recognized as real currencies, and financial and payment institutions are therefore limited in their actions regarding cryptocurrencies.[394] More in particular, they cannot offer cryptocurrency as a product or service, use them toward the government or in insurance services, offer direct or indirect cryptocurrency services to their customers, accept them as payment instrument, operate cryptocurrency exchanges, use cryptocurrencies in financial products, or set up cryptocurrency investment trusts or funds.[395] The result of this notice is that the Chinese government has decided to sever the ties between cryptocurrencies and the established financial system. It has, however, by no means outlawed the use of cryptocurrencies by users, or even the establishment of cryptocurrency businesses. For this, it must be reminded that the notice only provides guidance – with the prospect of future regulation – and no regulation itself.[396] Moreover, the notice is only aimed toward regulated financial and payment institutions, not toward users or merchants. Thus far, the notice does not seem to have diminished the importance of the Chinese market for cryptocurrencies. Also, the Special Administrative Region of Hong Kong has taken a liberal approach toward cryptocurrencies, holding that as they are no real currency and only a virtual commodity, they do not fall under the scope of the Hong Kong Monetary Authority's scrutiny.[397]

DIVERGENT ASIAN VIEWS - Many other Asian countries have remained more ambiguous in their position on virtual currencies. One example is India, where the Reserve Bank issued a

[389] Note that to facilitate payments beyond the transportation network, the EZ-Link Card implemented a new standard. *ezlink.com.sg/use-your-ez-link-card/where-to-use*.
[390] *jreast.co.jp/e/pass/suica.html#category03*.
[391] *nttdocomo.co.jp/english/service/convenience/index.html#p01*.
[392] Including BTC China, OKCoin, LakeBTC, and Huobi.
[393] Yin Fa [2013] No. 289; Song, K., Xu, T., Kaiser, N. (2014) "Bitcoin in China: a legal perspective", *Eiger Law*, 2.
[394] Song, K., Xu, T., Kaiser, N. (2014) "Bitcoin in China: a legal perspective", *Eiger Law*, 3.
[395] *Id.*
[396] Wang, J. (2013) "China's Statement on Bitcoin is Open to Interpretation", *CoinDesk*, 16 December 2013.
[397] Lee, S. (2014) "Robocoin's Bitcoin Teller Machine Won't Need Hong Kong Approval", *Bloomberg*, 6 January 2014.

warning regarding the use of cryptocurrencies[398], leaving several bitcoin operators to shut down their services in India amidst the legal uncertainty.[399] Bank Indonesia issued a similar statement holding that cryptocurrencies and other virtual currencies are no legal payment instrument.[400] Similarly, Bank Negara Malaysia has stated that bitcoin is no legal tender and that it does not intend to regulate its operations.[401] Also the Philippines maintains the legal uncertainty.[402] The Monetary Authority of Singapore, on the contrary, has announced that it will adopt measures to regulate virtual currency intermediaries regarding AML and CFT.[403]

JAPAN - Japan has taken a stance that at first sight may seem somewhat similar to that of China, holding that cryptocurrencies are no legal tender or bond – thus prohibiting financial institutions from dealing in them – but leaving the general public free to use them.[404] However, the Japanese government went further in considering virtual currencies as commodities and has also supported the establishment of a self-regulating body, the Japan Authority of Digital Assets (JADA).[405] JADA recommends operators of digital assets to register, provide information to their customers, adopt strong security and AML measures, and to comply with KYC principles.[406]

AUSTRALIA AND RUSSIA - In the wider Asian region, Australia's Taxation Office has considered transactions in virtual currencies as barter transactions for taxation purposes.[407] The Central Bank of the Russian Federation has referenced the general prohibition to release and distribute monetary substitutes in the Russian territory.[408] The Russian Ministry of Finance went even further, proposing legislation that would impose fines on cryptocurrency transactions.[409]

COMPARISON TO EU AND US - The approach toward virtual currencies found in Asian countries can be deemed rather different from what is found in the US. Whereas in the US regulators are undertaking efforts in bringing virtual currencies within the scope of the current legal frameworks, including those regarding AML and CFT, most Asian countries continue to explicitly put virtual currencies outside the scope of the law. This approach not only perpetuates legal uncertainty for users that conduct virtual currency transactions for legitimate purposes, it may also complicate regulatory oversight over the use of virtual currencies for illegitimate purposes. As such, the Asian approach displays more similarities to

[398] Reserve Bank of India (2013) "RBI cautions users of Virtual Currencies against Risks", *Press Release 2013-2014/1261*.
[399] PTI (2013) "Bitcoin operators shut shop in India amid RBI warning", *Indian Times*, 27 December 2013.
[400] Bank Indonesia (2014) "Statement Related To Bitcoin and Other Virtual Currency", *16/6/DKom*.
[401] Bank Negara Malaysia (2014) "Statement on Bitcoin", *Notice 2 January 2014.*
[402] Bangko Sentral ng Pilipinas (2014) "Warning Advisory on Virtual Currencies", *Media release 3 June 2014.*
[403] Monetary Authority of Singapore (2014) "MAS to Regulate Virtual Currency Intermediaries for Money Laundering and Terrorist Financing Risks", *Media release 13 March 2014.*
[404] Cruz, K. (2014) "Bitcoin Regulation in Japan", *Bitcoin Magazine*, 23 October 2014.
[405] *Jada-web.jp.*
[406] JADA (2014) "Summary of Guidelines for JADA, Japan Authority of Digital Assets", *jada-web.jp/wp-content/uploads/2015/01/SummaryofGuidelinesforJADA_v1-0_20141023.pdf*.
[407] Australian Taxation Office (2014) "ATO delivers guidance on Bitcoin", *QC 42159*.
[408] Bank of Russia (2014) "On the use in transactions "virtual currency", in particular, Bitcoin", *Press release* 27 January 2014.
[409] Roudik, P. (2014) "Russia: Fines for Bitcoin Transactions Will Be Introduced", *loc.gov/lawweb/servlet/lloc_news?disp3_l205404151_text*.

the approach followed thus far in the EU, where the divergent opinions of Member States have not yet yielded a more concerted action toward AML and CFT measures for virtual currencies.

7. Conclusions

REGULATORY SCRUTINY FOR TPP'S UNDER PSD2 - It is clear that the EU recognizes the need for a regulatory revision to keep up with the dynamic nature of the payment services market. Significant changes due to the proliferation of new payment solutions and the advent of new security threats has shifted the focus towards the promotion of a more integrated and efficient European payments market by creating a level playing field for payment services providers instilling more competition, whilst also demanding strong consumer protection. In that regard a revision of the Payment Services Directive was deemed necessary to regulate a new type of entity, namely, third party payment service providers. The PSD2 effectively places TPP's under regulatory scrutiny subjecting them to a number of obligations and requirements including: authorization, transparency and information and data protection.

SOME UNCERTAINTY REGARDING TPP'S REMAINS - Whilst the PSD2 is definitely a step in the right direction, certain aspects pertaining to the specific characteristics of TPP's remain unclear. In particular, the provisions concerning the allocation of liability and the requirements of strong authentication measures raise legitimate questions. The ambiguity is not aided by diverging obligations of the PSD2 and recommendations made by the SecuRe Pay forum on the security of payment account access services. Where the PSD2 allows for TPP's to rely on the authentication measures issued by ASPSP's, the recommendations, in line with the ECB's opinion on the draft proposal, state that issued security credentials should not be shared between ASPSP's and TPP's. It is essential that if the European Commission wishes to capitalize its initial objectives that the provisions, requirements and technical standards are clear, consistent and secure. Whilst nothing is definitive at this moment, as the PSD2 still needs to be formally adopted, much will depend on the EBA who has been tasked with the development of technical standards of security measures under the PSD2.

TPP'S ALSO COVERED UNDER AMLD4 - As the PSD2 defines TPP's as payment service providers, they are also subjected to the anti-money laundering and counter terrorist financing measures under the AMLD4. The EU rightfully recognizes the security risks pertaining to the use of TPP's. As such TPP's will be required to perform risk assessments and conduct due diligence procedures on their customers, in particular on e-merchants. However, as the AMLD4 does not envisage maximum harmonization, there is a realistic possibility that a consistent approach across the EU is not on the cards. Member States retain the possibility to take the nature and size of obliged entities into account when contemplating whether an obliged entity will be required to implement certain security requirements. Ultimately, this could lead to a patchwork of applicable requirements across the Member States which in turn would be detrimental to both the EU-wide coordination as well as international coordination efforts on anti-money laundering and counter terrorist financing.

CHINA - Outside the EU, non-financial institutions offering a diverse range of financial services are also emerging. Within the Asian market, China is the frontrunner both in terms of operational development and legislative framework. Already in 2010, TPP's were subjected to licensing requirements prior to being able to engage in payment services. Whilst this approach is laudable, regulatory initiatives do somewhat restrict the openness of the market. One of the requirements for TPP's to obtain a Payment Service License is the provision that a TPP needs to have been established in China. As a result only two foreign TPP's have until now been granted with such a license. Similar to Europe, security concerns

relating to the use of TPP's have increased, leading to additional regulatory initiatives, where both China and Taiwan are for instance proposing limits on payment amounts via a TPP.

US - The regulatory landscape in the US is somewhat different to Europe and Asia as relevant provisions for non-financial institutions, and TPP's, are dispersed across State and Federal Law. TPP's who are considered as money transmitters will have to obtain a State license in each of the States it wishes to engage in payment services. In addition, TPP's will have to abide by Federal Law which prescribes numerous anti-money laundering, counter-terrorist financing and reporting obligations.

NO GLOBAL CONSENSUS ON TPP'S - Considering the relative novelty of TPP's, there is currently no global unified approach regarding regulatory initiatives concerning TPP's. The main issue is perhaps defining the scope of regulatory scrutiny. Whilst the EU has defined TPP's by distinguishing PISP's and AISP's, neither the US nor the Asian market has attempted to characterize TPP's in such a fashion. Whether the approach of the EU is a step in the right direction remains to be seen. Considering rapid technological advancements and the resulting innovative payment solutions, there is a risk that the defining TPP's too strictly could outdate the regulatory framework too quickly. Nevertheless, there is some consistency to be found in the regulatory initiatives as a growing number of countries are subjecting non-financial institutions, such as TPP's, to licensing requirements in order to keep regulatory oversight. As TPP's continue to emerge it is also clear that security concerns grow; China and the EU are prime examples of issuing specific regulatory provisions concerning these providers.

NEED FOR COORDINATION TO ENSURE CONSISTENCY - The various regulatory initiatives focusing on enhancing payment security in the online environment is a positive evolution which should be encouraged. Nevertheless, it is essential that these initiatives are coordinated to ensure a consistent approach. As analyzed above, payment service providers and in particular TPP's will be subjected to more stringent security requirements, ensuring a smooth overlap between competing compliance requirements is essential in order to be able to promote a secure, competitive and innovation-driven payment services market.

WORK AHEAD FOR VIRTUAL CURRENCY UNDER EU LAW - In terms of virtual currencies, the main conclusion that can be drawn with regard to their regulation under EU law is that there is still quite some work ahead. *First*, no convincing argument can be made for the inclusion of virtual currencies under the current legal frameworks set by the PSD or EMD2. *Second*, recent legislative procedures – such as those for the AMLD4 and PSD2 – have not paid sufficient attention to this development, thus leaving virtual currencies largely untouched. While the AMLD4 could be construed to extend to virtual currencies, the precise degree to which this will succeed in deterring their abuse for money laundering or terrorist financing purposes remains to be seen. *Third*, future legislation – such as a potential EMD3 – remains a development to be watched closely. However, in order for a potential new legislative framework regarding e-money to extent to virtual currencies, a more fundamental reconfiguration of the very notion of e-money is needed. With multipurpose prepaid cards having lost the field and network-based money services coming closer and closer to being payment services, the original purposes of the e-money framework are quickly losing their

relevance. A reorientation toward virtual currencies could then bring new life to this notion, and extend the legal framework to include recent developments such as cryptocurrencies.

RISING VIRTUAL CURRENCY REGULATION IN THE US - Another approach can be found in the US, where financial regulators have already undertaken efforts at bringing certain virtual currency service providers – mainly the virtual currency exchanges – under the existing legal frameworks regarding money services businesses. Started at the Federal level, these legislative efforts are now finding their way to the State-level, where the States of New York and California have already introduced proposals toward regulation. This would effectively require virtual currency service providers to be licensed, and impose requirements regarding their own capital, as well as regarding AML and CFT. As part of these schemes, sanctions for non-compliance could be imposed.

SIMILARITIES AS BASIS FOR INTERNATIONAL COOPERATION - The regulatory approach followed in the US shows a number of clear similarities to the EU's own legal framework on payment services. It could therefore be envisioned that an overhaul of the e-money framework would eventually lead to a similar legal regime for virtual currencies as what is currently proposed in the US. This approach could also hold potential for other countries that are still struggling to grasp this matter, as can be seen in the Asian markets. Moreover, given the inherent international scope of virtual currencies, a more unified stance on this matter would serve to support international cooperation. Stronger international cooperation can be held to be imperative in order to successfully impose and enforce AML and CFT rules for virtual currencies.

8. Policy Recommendations

The previous section listed the conclusions that can be drawn from the research conducted within the framework of this study. In this section, a number of concise policy recommendations will be distilled from that research. The aim is to provide parties from both the public and private sector with key take-away points.

8.1. Public sector recommendations

Recommendation 1: Address remaining ambiguities

Currently, the EU is modernising the regulatory framework of the payment market by revising the Payment Services Directive. The revision represents a major restructuring of the EU payment market by bringing third party payment service providers (TPP's) under the scope of the PSD, ultimately recognising the market demand for these new service providers. Whilst the focus on promoting competition and fostering innovation in the form of payment initiation service providers (PISP's) and account information service providers (AISP's) is laudable, it cannot be achieved at the expense of consumer protection or general security of payment instruments. Since TPP's are dependent on traditional payment institutions to be able to provide their services, there is a divided accountability for both providers in terms of liability and security. However, as the PSD2 currently stands it fuels legal uncertainty in both areas, potentially leading to an inconsistent and fragmented approach, which in the end is detrimental to customer protection efforts. The ambiguity is not aided by diverging obligations of the PSD2 and recommendations made by the SecuRe Pay forum on the security of payment account access services. It is evident that well-delineated provisions are necessary to preserve customer confidence in payment instruments. **In that regard it is critical that the European Banking Authority (EBA) - who has been mandated to issue guidelines on a number of key issues – addresses the remaining ambiguities and provide some much needed clarity.**

Recommendation 2: Harmonise EU legal framework

Besides the PSD2, there are several other initiatives focussing on increasing the security of online payments. The AMLD4 aims to strengthen the integrity and stability of the financial system by revising anti-money laundering and counter-terrorist financing requirements. **It is imperative that European Institutions and Member States adequately coordinate their regulatory initiatives in order to avoid potential legal conflicts.** The PSD2 and the AMLD4 currently seem at odds with one another. Whilst the PSD2 adopts a more lenient approach to TPP's by not subjecting them to overly burdensome regulatory requirements, the AMLD4 imposes on those same TPP's more stringent AML/CTF requirements which appear to be counter-intuitive. In addition, in contrast to the ambition of the PSD2 which aims to establish an EU-wide integrated payment market, the AMLD4 is a minimum harmonising Directive, meaning that payment service providers will have to take a patchwork of fragmented national AML/CTF requirements into account. **Therefore Member States must develop their legal initiatives in close cooperation with one another in order to ensure consistency and reduce the risks of legal uncertainty.**

Recommendation 3: Coordinate global regulatory initiatives

Currently, there is no global consistency regarding the regulatory framework concerning TPP's. Whereas the EU and the majority of the Asian market adopt a specific approach

explicitly regulating TPP's and subjecting them to specific requirements, the US regulates TPP's indirectly by placing them under standard regulations for non-financial service providers. Considering the fact that TPP's are active in online payments, **international lawmakers should strive for a consistent approach - coordinating how TPP's are internationally defined and regulated - as it would prove to be beneficial** for these emerging payment service providers by allowing them to engage in cross-border activities.

Recommendation 4: Avoid a nationalist approach to virtual currencies

At the present moment, there is still a wide variety of opinions on virtual currencies to be found between EU Member States. While there have been calls to regulate this matter at the level of the EU, coming from the EBA and the European Commission, no legislative action is currently underway. The decision in a pending CJEU case could provide a starting point for further initiative. Also in Asia, there are significant differences in how countries view this development. It is, however, clear that this globalized matter should not be regulated at the level of one nation individually. **Therefore, European Institutions must develop regulation in this field with a clear outlook on establishing cooperation between Member States, as between the EU and the international community.** Especially in developing economies seeking alignment with the broader community can prove vital to effective regulation.

Recommendation 5: Adopt a rational outlook on virtual currencies

Early public sector views on virtual currencies – and cryptocurrencies in particular – have not been very positive. Some reports have overestimated the potential impact – both positive and negative – of this matter. A positive approach toward regulation can be found in the US, where the State of New York initiated a lengthy and active dialogue with a broad field of stakeholders while drafting its legal framework. While it is the duty of financial regulators and lawmakers to uphold the law, protect consumers and to limit illegal activities, **regulators should recognize that virtual currencies – as well as other so-called FinTech innovations – are a nascent development that should not be crushed by overzealous regulation.** Moreover, it may be recognized that it is not always possible to apply existing regulation to radically different technology.

8.2. Private sector recommendations

Recommendation 6: Look beyond the disruptive forces

It is evident that innovative technologies and new business models are disrupting the status-quo in the payment market. The PSD2 has perhaps taken the (r)evolutions a step further by granting TPP's access to online payment accounts, forcing traditional payment institutions to facilitate access through their API's. Whilst it is true that traditional payment services will have to endure additional costs to facilitate the business model of TPP's by being required to allow third party access, they should not exclusively focus on the disruptive force. Instead, they should be aware of the changes and recognise the opportunities of the technological advancements for their own digital agenda. In that sense, **traditional financial institutions should see the PSD2 as an incentive to adapt their current strategy in order to benefit from technological innovations themselves.** Traditional financial institutions could for instance look to set up new partnerships and increase collaboration with TPP's, monetize their API's or even look to set up their own form of TPP.

Recommendation 7: Need for compliance

With the emergence of TPP's, the increase of online payment fraud and the recognised importance of preserving customer confidence in payment instruments, the regulatory initiatives are increasingly focused on security. Given this increased emphasis of the importance of security measures, **payment service providers should review their current processes in order to ensure they are compliant with future obligations**. One of the aspects still subject to further clarification concerns the technical interfaces and security standards between TPP's and ASPSP's. It remains to be seen to what extent the EBA will detail the required specifications through the Regulatory Technical Standards, but **service providers should nonetheless assess their security measures of their API's when dealing with TPP's**.

Recommendation 8: Do not dismiss virtual currencies wholesale

Some financial actors have dismissed the idea of looking into how they could cooperate with virtual currencies within their services solely on the basis that the volume of transactions of Bitcoin at its peak popularity was nowhere in the same field as those processed by major global credit card companies. While it is true that no virtual currency has yet become a major monetary unit, there are many other purposes to be achieved. Here, a comparison can be drawn to the development of mobile payment services by telecommunications operators in **Africa** – such as M-Pesa in Kenya and Tanzania. **Financial actors should recognize virtual currencies as important tools to many developing nations' unbanked population.** Also applications for micro-lending to foster entrepreneurship are being considered.

Recommendation 9: Mind the Block Chain

Perhaps the most interesting thing to come forward from the development of cryptocurrencies is the **block chain technology**. At the moment, this technology is already being applied in a host of applications such as notary-like transaction ledgers and self-executing smart contracts. Also within the financial sector, a number of applications are being developed. Both NASDAQ and NYSE are exploring the development of private exchange markets based on the block chain technology, as well as the use thereof in ownership ledgers. Also private companies are entering the market, with Overstock's CEO recently launching a block chain based securities trading platform. **Financial actors should pay attention to further developments in this technology in order to fully benefit from upcoming market trends.**