FINANCIAL ACTION TASK FORCE GROUPE D'ACTION FINANCIÈRE



FATF Report

Money Laundering Using New Payment Methods

October 2010



THE FINANCIAL ACTION TASK FORCE (FATF)

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering and terrorist financing. Recommendations issued by the FATF define criminal justice and regulatory measures that should be implemented to counter this problem. These Recommendations also include international co-operation and preventive measures to be taken by financial institutions and others such as casinos, real estate dealers, lawyers and accountants. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit the website:

WWW.FATF-GAFI.ORG

© 2010 FATF/OECD. All rights reserved.

No reproduction or translation of this publication may be made without prior written permission.
Applications for such permission, for all or part of this publication, should be made to
the FATF Secretariat, 2 rue André Pascal 75775 Paris Cedex 16, France
(fax +33 1 44 30 61 37 or e-mail: contact@fatf-gafi.org).

ACKNOWLEDGEMENTS

The FATF would like to thank Vodafone, Moneybookers and the Consultative Group to Assist the Poor (CGAP) for presentations provided to the project team during the 2009/2010 annual typologies experts' meeting in the Cayman Islands and MasterCard Europe for their presentation on prepaid cards at the project team's intersessional meeting in Amsterdam in 2010. In addition, comments received from the GSMA and Western Union, during the FATF private sector consultation, were also much appreciated.

TABLE OF CONTENTS

EXECUTIVE SUMMARY 7

CHAPTER 1: INTRODUCTION 9

CHAPTER 2: BACKGROUND 12

2.1 Recent Developments Related to Prepaid cards 14
2.2 Recent Developments Related to Internet Payment Services 16
2.3 Recent Developments Related to Mobile Payment Services 18

CHAPTER 3: RISK ASSESSMENT OF NPMS 20

3.1 Risk factors 24
3.2 Risk mitigants 32

CHAPTER 4: TYPOLOGIES AND CASE STUDIES 36

4.1 Typology 1: Third party funding (including straw men and nominees) 36
4.2 Typology 2: Exploitation of the non-face-to-face nature of NPM accounts 40
4.3 Typology 3: Complicit NPM providers or their employees 43
4.4 Cross-border transport of prepaid cards 46
4.5 Red Flags 47

CHAPTER 5: LEGAL ISSUES RELATED TO NPMS 49

5.1 Regulatory models applied to NPMs 49
5.2. Specific issues in regulation and supervision of NPM 53

CHAPTER 6: CONCLUSIONS AND ISSUES FOR FURTHER CONSIDERATION 66

APPENDIX A: SUPPLEMENTAL NPM QUESTIONNAIRE RESULTS AND ANALYSIS 72

APPENDIX B: EXCERPTS FROM THE 2006 REPORT ON NEW PAYMENT METHODS 96

APPENDIX C: RELATED PUBLICATIONS ON NPMS AND ML/TF RISK 103

APPENDIX D: THE EU LEGAL FRAMEWORK FOR NEW PAYMENT METHODS 107

APPENDIX E: GLOSSARY OF TERMS 111

EXECUTIVE SUMMARY

1. After the 2006 New Payment Method (NPM) report, the growing use of NPMs and an increased awareness of associated money laundering and terrorist financing risks have resulted in the detection of a number of money laundering cases over the last four years.

2. The project team analysed 33 case studies, which mainly involved prepaid cards or internet payment systems. Only three cases were submitted for mobile payment systems, but these involved only small amounts. Three main typologies related to the misuse of NPMs for money laundering and terrorist financing purposes were identified:

- Third party funding (including strawmen and nominees).
- Exploitation of the non-face-to-face nature of NPM accounts.
- Complicit NPM providers or their employees.

3. While the analysis of the case studies confirms that to a certain degree NPM are vulnerable to abuse for money laundering and terrorist financing purposes, the dimension of the threat is difficult to assess. The amounts of money laundered varied considerably from case to case. While some cases only involved amounts of a few hundred or thousand US dollars, more than half of the cases feature much larger amounts (four cases involved over 1 million US dollars mark, with the biggest involving an amount of USD 5.3 million).

4. The project team retained and updated the 2006 report´s approach to assessing money laundering and terrorist financing risk associated with NPMs and assesses the risk of each product or service individually rather than by NPM category.

5. Anonymity, high negotiability and utility of funds as well as global access to cash through ATMs are some of the major factors that can add to the attractiveness of NPMs for money launderers. Anonymity can be reached either "directly" by making use of truly anonymous products (*i.e.,* without any customer identification) or "indirectly" by abusing personalised products (*i.e.,* circumvention of verification measures by using fake or stolen identities, or using strawmen or nominees etc.).

6. The money laundering (ML) and terrorist financing (TF) risks posed by NPMs can be effectively mitigated by several countermeasures taken by NPM service providers. Obviously, anonymity as a risk factor could be mitigated by implementing robust identification and verification procedures. But even in the absence of such procedures, the risk posed by an anonymous product can be effectively mitigated by other measures such as imposing value limits (*i.e.,* limits on transaction amounts or frequency) or implementing strict monitoring systems. For this reason, all risk factors and risk mitigants should be taken into account when assessing the overall risk of a given individual NPM product or service.

7. Across jurisdictions, there is no uniform standard for the circumstances in which a product or service can be considered to be of "low risk". Many jurisdictions use thresholds for NPM transactions or caps for NPM accounts in order to define "low-risk scenarios"; but the thresholds and caps vary

significantly from jurisdiction to jurisdiction. Likewise, different views may be taken on the relevance of certain risk factors or of the effectiveness of certain risk mitigants, due to respective legal and cultural differences in jurisdictions.

8. Some jurisdictions allow firms to apply simplified CDD measures in cases of predefined low-risk scenarios. Again, there is no uniform standard across jurisdictions on the definition of "simplified CDD measures". Some jurisdictions even grant a full exemption from CDD measures in designated low-risk scenarios.

9. Not all NPM services are subject to regulation in all jurisdictions. While the issuance of prepaid cards is regulated and supervised in all jurisdictions that submitted a response to the project questionnaire, the provision of Internet payment and mobile payment services is subject to regulation and supervision in most, but not all jurisdictions (FATF Recommendation 23; Special Recommendation VI).

10. The project team also identified areas where the current FATF standards only insufficiently account for issues associated with NPMs:

- Where NPM services are provided jointly with third parties (*e.g.,* card program managers, digital currency providers, sellers, retailers, different forms of "agents"), these third parties are often outside the scope of AML/CFT legislation and therefore not subject to AML/CFT regulation and supervision. The concept of agents and outsourcing is only marginally addressed in the FATF 40 Recommendations and 9 Special Recommendations (in Recommendation 9 and Special Recommendation VI). More clarification or guidance from FATF on this issue would be welcome, especially as a few jurisdictions are considering a new approach on the regulation and supervision of agents.

- Many NPM providers distribute their products or services through the Internet, and establish the business relationship on a non-face-to-face basis, which, according to FATF Recommendation 8, is associated with "specific risks". The Recommendations do not specify whether "specific risks" equates to "high risk" in the sense of FATF Recommendation 5; if so, this would preclude many NPM providers from applying simplified CDD measures. While FATF experts have recently come to the conclusion that non-face-to-face business does not automatically qualify as a high risk scenario in the sense of Recommendation 5, it would be helpful if this could be confirmed and clarified within the standards.

11. It would be desirable if other Working groups within FATF decided to pick up the discussions described above to provide more clarity on the interpretation of the FATF Recommendations involved. Such work would not only be relevant and helpful for the issues of money laundering and terrorist financing, but also for the issue of financial inclusion.

12. NPMs (as well as other financial innovations) have been identified as powerful tools to further financial inclusion. Many of the challenges mentioned above (*e.g.,* discussion on simplified CDD in cases of low risk, full exemption from CDD, or the regulation and supervision of agents) are of high relevance for the entire discussion around financial inclusion, going beyond the issue of the vulnerability of NPMs to ML/TF purposes alone.

CHAPTER 1: INTRODUCTION

The 2006 report

13. In October 2006, the FATF published its first report on New Payment Methods (NPMs). The report was an initial look at the potential money laundering (ML) and terrorist financing (TF) implications of payment innovations that gave customers the opportunity to carry out payments directly through technical devices such as personal computers, mobile phones or data storage cards.[1] In many cases these payments could be carried out without the customer needing an individual bank account.

14. As these NPMs were a relatively new phenomenon at the time, only a few ML/TF case studies were available for the 2006 report. In addition, clear definitions of various NPM products and how they should be regulated were just beginning to be addressed by a limited number of jurisdictions. Therefore the report focused on raising awareness of these new products and the potential for their misuse for ML/TF purposes.

15. The 2006 report found that ML/TF risk was different for each NPM product and that assessing the ML/TF risk of NPM categories was therefore unhelpful. Instead, it developed a methodology to assess the risk associated with individual products.

16. The report concluded that it should be updated within a few years, or once there was greater clarity over the risks associated with these new payment tools. This report updates the 2006 report on NPMs and provides an overview of the most recent developments.

Objectives of the present report

17. Since the publication of the 2006 report, NPMs (prepaid cards, mobile payments and Internet payment services) have become more widely used and accepted as alternative methods to initiate payment transactions. Some have even begun to emerge as a viable alternative to the traditional financial system in a number of countries.

18. The rise in the number of transactions and the volume of funds moved through NPMs since 2006 has been accompanied by an increase in the number of detected cases where such payment systems were misused for ML/TF purposes. The NPM report in 2006 identified potential legitimate and illegitimate uses for the various NPMs but there was little evidence to support this. The current report will compare and contrast the "potential risks" described in the 2006 report to the "actual risks" based on new case studies and typologies. Not all potential risks identified in 2006 were backed up by case studies. This does not mean that those risks are no longer of concern, and jurisdictions should continue to be alert to the market´s development to prevent misuse and detect cases that went unnoticed before.

19. The report will also develop red flag indicators which might help a) NPM service providers to detect ML/TF activities in their own businesses and b) other financial institutions to detect ML/TF

[1] Including different storage media such as magnetic stripe cards or smart card electronic chips.

activities in their business with NPM service providers, in order to increase the number and quality of suspicious transaction reports (STRs).

20. Although more case studies are now available, issues surrounding appropriate legislation and regulations for NPMs are still a challenge for many jurisdictions. Consequently, the report also identifies the unique legal and regulatory challenges associated with NPMs and describes the different approaches national legislators and regulators have taken to address these. A comparison of regulatory approaches can help inform other jurisdictions' decisions regarding the regulation of NPM.

21. Finally, this report considers the extent to which the FATF 40+9 Recommendations continue to adequately address the ML/TF issues associated with NPMs.

Steps taken by the project team

22. The project team analysed publications about NPMs and ML/TF[2]. It also analysed the responses to questionnaires which covered the spread of domestic NPM service providers[3], the role of regulation in relation to NPMs and case studies detected in jurisdictions (the latter also including foreign service providers). Thirty-seven jurisdictions and the European Union Commission submitted a response.[4]

23. The majority of the respondents identified NPMs within their jurisdiction. Prepaid cards were the most common (34 of the countries have such providers), followed by Internet payment services (IPS) providers with 17 countries and mobile payment services with 16 countries offering each NPM respectively. Case studies were provided for the three NPMs: 18 cases involving prepaid cards, 14 cases involving Internet payment services and three cases involving mobile payment services.[5] A detailed summary is attached in Appendix A.

24. The project team also consulted with the private sector in several ways. During the 2009-2010 annual typologies experts´ meeting in the Cayman Islands, representatives from NPM service providers, including the Internet payment sector, the mobile payments sector and a representative from the Consultative Group to Assist the Poor (CGAP), provided presentations to the project team. At the project team´s intersessional meeting in Amsterdam in March 2010, a representative from a card technology provider in Europe gave a presentation on prepaid cards. A more wide-ranging private sector

---

2 See Appendix C for a list of publications used for this report.

3 Including a description of the biggest or most significant products and service providers.

4 The FATF and the NPM project team would like to thank all jurisdictions and organisations that have contributed to the completion of this report by providing experts to participate in the project team and by submitting responses to the project questionnaire, including (sorted alphabetically): Argentina, Armenia, Australia, Austria, Belarus, Belgium, Brazil, Bulgaria, Canada, Cayman Islands, Colombia, Denmark, Estonia, European Commission, France, Germany, Gibraltar, Italy, Japan, Jersey, Lebanon, Luxembourg, Macao, Mexico, Netherlands, Norway, Oman, Peru, Philippines, Poland, Portugal, Russia, Singapore, Slovak Republic, South Africa, St. Vincent & the Grenadines, Sweden, Switzerland, UK, Ukraine, USA, and the World Bank. The project team would also like to thank the secretariat of the Egmont Group for circulating the questionnaire among its members, thus increasing the outreach of the entire project.

5 Various reasons have been proposed for the low number of cases, including that transaction value and volume remains very small for mobile payments, or that these systems may not be attractive to money launderers, or that mobile providers and law enforcement have failed to detect criminality or that criminals, or indeed law enforcement are unfamiliar with the technology.

consultation was also conducted through the FATF electronic consultation platform where a draft of this report was presented for consultation.

Structure of the present report

25. This report is based on the FATF 2006 report. It attempts to avoid repetition as much as possible. The report therefore does not describe the general working mechanisms of NPMs.[6] Instead, it focuses on recent developments, updates the risk assessment and introduces new case studies.

26. The report is divided into 4 sections:

- Section 1 (chapters 1 and 2) introduces the project work as well as the key overarching issues. It also provides an overview of recent developments;
- Section 2 (chapters 3 and 4) addresses the risks and vulnerabilities of NPMs and presents case studies and typologies.
- Section 3 (chapter 5) addresses regulatory and supervisory issues, exploring the different national approaches to AML legislation as well as the prosecution of illicit NPM service providers.
- Section 4 (chapter 6) concludes the report and identifies issues for further consideration.

6 Relevant sections of the 2006 report (including definitions) are cited as excerpts in Appendix B.

CHAPTER 2: BACKGROUND

"New Payment Methods" and their development since 2006

27. In 2006, bank-issued payment cards and transactions via the internet or over the telephone were not really new. Depository financial institutions have offered remote access to customer accounts for decades. What was new about these technologies in 2006 was their use by banks outside of traditional individual deposit accounts and by non-banks, some of which did not fit traditional financial service provider categories and therefore sometimes fell outside the scope of regulation despite providing financial services such as the carrying out of payments or holding accounts. Indeed there are still several jurisdictions where NPM service providers are not subject to prudential and/or AML regulation.

28. The development of NPMs has created new opportunities for criminals to misuse such technologies for the purposes of ML and TF. This has, in turn, resulted in new typologies and created new challenges for law enforcement authorities.

The promotion of NPMs through jurisdictions and government agencies

29. NPMs have developed as a result of the legitimate need of the market for alternatives to traditional financial services. In some cases, this was driven by the demand for more convenient or safer ways to pay for online purchases; in other cases, their development was fostered by a desire to provide access to financial services for those who were excluded from traditional financial services (*e.g.,* individuals with poor credit ratings, minors, but also inhabitants of under-banked regions),[7] and the assumption that NPMs may have a positive effect on national budgets as well as overall national and global economic development.[8]

Box 1.

United States: Four million people who receive Social Security benefits lack bank accounts. To reduce reliance on paper checks, the United States began distributing these benefits using prepaid cards, which beneficiaries can use to purchase goods or get cash. Previously, beneficiaries cashed checks at non-banks and conducted transactions using cash or money orders.*

Pakistan: Fighting forced more than a million people from their homes in 2009. The Government of Pakistan

7 The World Bank, the Consultative Group to Assist the Poor (CGAP), the G-20 Access Through Innovation Sub Group and other organisations have also identified NPMs, mobile payment services in particular, as a possible tool for financial inclusion of the poor and/or the under-banked and launched initiatives to promote and support the implementation of NPMs in jurisdictions concerned.

8 This is due to efficiency gains in terms of transaction speed, finality of payments, security features of technology based payment methods and their lower costs compared to paper payment instruments. Another important characteristic of NPMs that explains policy-makers' support for their sound development is their accessibility: especially pre-paid cards and mobile payments grant easy access to the payment system by the whole population, including the unbanked. Given these potentialities, central banks in their capacity of payment system overseer have long since devoted specific attention to the development of NPMs. Ultimately, the Bank for International Settlements has launched an initiative to study the innovations in retail payments.

needed a way to deliver financial assistance to these displaced individuals quickly. Rather than distributing cash, the Government of Pakistan partnered with a bank to distribute prepaid cards with access to 25,000 Pak rupees (about USD 300). At the same time, a Pakistani bank and a payment card company installed wireless point-of-sale terminals at retailers where people could buy basic supplies. By using cards rather than cash, the Government of Pakistan provided immediate assistance to nearly 300,000 families through transparent distribution channels.**

* Direct Express Media (2008)
** Visa Corporate Site (2010)

30. As a result, some jurisdictions have adapted their regulatory framework to actively promote NPMs within their domestic market.

Box 2. The EU Commission openly encourages and promotes the development of NPMs and concluded in its Explanatory Memorandum to the original E-Money-Directive of 1998:*

—Electronic money has the potential to develop into an efficient and effective means of payment; it can play a significant role in the development and improvement of electronic commerce; and it can be an important tool in the completion of the single market and monetary union. The Commission is of the view that it is in the interests of both business and consumers alike that electronic money develops within a regulatory environment that instils trust and confidence in this new and developing payment instrument. At the same time it is vital that development is allowed to take place unimpaired by strict technological rules which will hamper innovation and restrict competition.

The Commission proposal (…) introduces the regulatory regime necessary to ensure the financial integrity of non-bank issuers without stifling developments in the domain of electronic money and will help to cultivate an environment in which the development of this new means of payment is promoted in the interests of business and consumers."

In a review of the original E-Money-Directive, the Commission kept up the aforementioned goals and intentions:**

—The general objective of the review of the EMD is to promote the emergence of a true single market for electronic money services in Europe. Contribute to the design and implementation of new, innovative and secure electronic money services. Provide market access to new players and real and effective competition between all market participants, thereby generating significant benefits to the wider European economy."

Accordingly, recital (4) of the amended E-Money-Directive*** reads:

—(4)With the objective of removing barriers to market entry and facilitating the taking up and pursuit of the business of electronic money issuance, the rules to which electronic money institutions are subject need to be reviewed so as to ensure a level playing field for all payment services providers."

* Commission of the European Countries (1998)
** Commission of the European Countries (2008)
*** Official Journal of the European Union (2009)

Other studies on NPMs and ML/TF risks and vulnerabilities

31. NPMs have attracted a significant amount of press coverage. They have also been the subject of an increasing number of public and private sector research initiatives. In addition, there are a number of recent or ongoing typologies projects of FATF and FSRBs that touch upon this subject.[9] This shows that the awareness of the opportunities and risks associated with NPMs has increased since the publication of the 2006 report.

32. These studies have often focussed on one category of NPMs only. This report is different as it will provide a broader comparative analysis of these issues and identify the commonalities shared by all types of NPMs. It will also identify the specific challenges within each category of NPMs.

[9] Recent or ongoing typologies projects include: FATF typologies report on *Money Laundering and Terrorist Financing vulnerabilities of commercial websites and Internet Payment Systems* (FATF (2008)); MONEYVAL workshop on Cybercrime (ongoing); EAG workshop on internet payments (ongoing).

2.1 Recent Developments Related to Prepaid cards

33. Prepaid cards can be split into two broad categories, open-loop cards and closed-loop cards.[10] This report focuses mainly on open-loop cards[11] because closed-loop cards only have a very limited negotiability. This does not mean that the ML/TF risk in closed-loop prepaid cards is very low: in fact, a few case studies involved closed-loop cards. However, in most of these case studies closed-loop cards were not used as a payment instrument, but as a mere intermediary store of value. This can be illustrated by the following two case examples:

Box 3. Stolen credit card information used to purchase closed-loop cards

In 2007, two defendants were prosecuted for purchasing closed-loop prepaid gift cards with stolen credit card account information. The defendants used the gift cards to purchase merchandise, which they then returned to the store in exchange for new gift cards, or they sold the merchandise for cash. Because the new prepaid cards were not linked to the stolen credit card account numbers, they were not affected when the theft of the credit card information was discovered. The defendants were convicted and ordered to pay USD 82 000 in restitution. One defendant was convicted of conspiracy and fraud and sentenced to 45 months imprisonment and three years supervised release. The other defendant was convicted of conspiracy and money laundering and sentenced to five months imprisonment and three years supervised release.

Source: United States.

Box 4. Suspected use of a closed-loop card company for money laundering and terrorist financing

Law enforcement information indicated that the owner of a prepaid phone card company was suspected of money laundering and having links to a terrorist organisation.

The owner conducted many large cash deposits into personal and business bank accounts and when questioned would indicate that prepaid phone cards were sold to retailers and convenience stores, and cash payments were received instead of cheques. This was apparently due to the fact that the owner was not confident that cheques would be honoured.

Some of the deposits were also conducted into accounts held by prepaid phone card suppliers.

Electronic funds transfers were also ordered by the owner to the benefit of individuals in Europe and the Middle East, sometimes through accounts which previously had not seen much activity. The owner was also the beneficiary of funds ordered by the same individuals.

Source: Canada.

34. During the June 2010 FATF plenary in Amsterdam, the plenary asked the project team to provide information regarding the nature and inherent risks of closed-loop prepaid cards.[12] However, beyond the two case examples above, the project team does not have sufficient data to assess the risk of such cards, as the questionnaire circulated at the beginning of the project explicitly excluded closed-loop cards from the scope of this project. Nevertheless several of the risk factors as well as the corresponding

10 For more details see the definition of prepaid cards as given in the FATF 2006 report (included as Appendix B to this report).

11 For the purposes of this report, the term prepaid cards includes the types of cards that were named "e-purses" in the FATF 2006 report.

12 The issue had come up after the mutual evaluation of Brazil; the assessment team had criticised Brazil for applying reduced CDD measures to such cards without having conducted a thorough risk assessment to determine the risk of such products first (FATF (2010)).

risk mitigants evaluated in this report that apply to open-loop cards may also apply to closed-loop cards (*e.g.,* regarding CDD measures or value limits).[13]

35. The overall volume of prepaid card transactions can only be estimated, as in most jurisdictions data on annual transaction volume for prepaid cards is not reported separately by the leading payment card networks, card-issuing banks, or non-bank issuers and service providers.[14] For the US, the total funds loaded onto prepaid cards in 2009 are estimated to have been USD 120.2 billion, according to research commissioned by MasterCard, Inc. and conducted by the Boston Consulting Group (BCG).[15]

36. While about 17% of U.S. consumers have a prepaid card,[16] outside the U.S. the percentage of consumers with a prepaid card tends to be lower and the market potential may be lower as well.[17]

37. Prepaid cards have been introduced in a number of countries, but in most countries the use of prepaid card appears to be less prevalent compared to the US. The BCG study mentioned above (see footnote 21) forecasts that the US will account for 53% of the global prepaid card market in 2017, and that UK and Italy will remain the largest markets for prepaid cards in Europe, with the UK accounting for 25% and Italy 20% of the entire European market by 2017.[18] The BCG study roughly supports a 2009 survey sponsored by the international payments processing firm First Data that found that Italy was the "most advanced prepaid market in Europe," while the UK market was described as "established," and the markets in Germany and Austria were described as "embryonic." [19] As a general trend it is safe to say that the usage and spread of prepaid cards has grown in recent years. According to the Basel Committee on Payment and Settlement Services (CPSS)[20] the number of issued "cards with an

---

13 Based on the discussion during the evaluation of Brazil and the indicators available, it may be worthwhile to analyse the money laundering and terrorist financing vulnerabilities of closed-loop prepaid cards in a separate typologies project.

14 MasterCard and Visa mix prepaid card transaction volume in with their debit card data. For the 12 months ending 30 June 2009, Visa reported 935 billion USD of consumer debit transactions for purchases of goods and services, with just over 84% of that volume taking place in the United States (United States Securities and Exchange Commission (2009a)). For MasterCard, in the year ending 31 December 2009, total debit card transaction volume was $814 billion, with 55% taking place in the United States (United States Securities and Exchange Commission (2009b)).

15 Payment News (2010)

16 Foster K., Meijer E., Schuh S., and Zabek A. (2010).

17 According to United Kingdom-based PSE Consulting: "US prepaid products rely on displacing check wage payments, and often the less well off are obliged to spend c.$50 - $60 per month on ‚check cashing', paying their utility bills or sending money home to their families. In Europe the greater prevalence of electronic salary payments and government benefits plus free ‚basic banking' products means the unbanked population is significantly smaller than in the US and consumers are unused to paying such high charges." (see: www.pseconsulting.com/pdf/articles/sep06/pse_repaid_press_release_110806.pdf)
This view is supported at least within the UK by the UK Payments Council, which in its new report, The Way We Pay 2010, finds that 89% of workers in the UK are paid by direct deposit to individual bank accounts with the remainder paid by check or cash. The report does not mentions prepaid cards. (Payments Council (2010)).

18 Master Card (2010)

19 First Data (2009)

20 Bank for International Settlements (2009)

e-money function"[21] has grown from 107.6 million in 2004 to 275.28 million in 2008 in selected CPSS countries.[22]

38. The project questionnaire asked jurisdictions for an estimate of prepaid cards issued by domestic payment service providers. Out of those jurisdictions that provided an estimate, the eight jurisdictions with the most cards issued are listed in the following table:

Jurisdiction	Cards issued (estimate)	Jurisdiction	Cards issued (estimate)
Japan	100 million	**Slovak Republic**	4 million
Singapore	15 million	**Mexico**	2.6 million
Italy	8 million	**Russia**	2 million
Norway	6 million	**France**	1.3 million

39. Since the first report was published in 2006, there have been no significant technical developments, most open-loop prepaid cards still rely on magnetic stripes. Where so-called "smart cards" are used featuring an electronic chip, this chip is usually used for processing additional customer information. Prepaid card systems that use the chip to store the funds on the card ("e-purses")[23] are usually still limited to domestic use and often have rather low value limits.

40. As described in the FATF 2006 report, prepaid cards can be an alternative to a variety of traditional banking products and services, such as debit or credit cards or traveller cheques. Many prepaid cards enable customers to make international payments, and some are increasingly offering features similar to conventional bank accounts: such card products may allow the customer not only to make payments, but also to receive payments from third parties. They may also allow cross-border remittances, *e.g.,* by issuing several "twin" or "partner" cards to one customer, which they can pass on to remittance receivers anywhere in the world. These "twin" or "partner" cards grant their holders access to the original card holders´ funds through the global ATM network.[24]

41. Some providers of Internet payment services and mobile payment services are known to provide their customers with an additional prepaid card to facilitate access to cash through the use of ATMs domestically and worldwide. This link was identified for mobile payments in the 2006 report, but has now been associated with IPS as well.

2.2 Recent Developments Related to Internet Payment Services

42. Internet payment services (IPS) can be provided by financial institutions and firms outside the financial services sector. They can rely on a bank account or operate independently from a bank account.

---

21 These are defined as "Reloadable multi-purpose prepaid cards which can be used at the sites of several service providers for a wide range of purposes and which have the potential to be used on a national or an international scale, but may sometimes be restricted to a certain area", Statistics on payment and settlement systems in selected countries – Figures for 2008 (December 2009), p. 312.

22 Statistics on payment and settlement systems in selected countries – Figures for 2008 (December 2009), table 10, p. 262. These figures include data from Belgium, France, Germany, Italy, Japan, Netherlands, Singapore and Switzerland; they do not include Canada, Hong Kong, Sweden, UK and the US ("nav"-data was not available).

23 See definition of e-purses in the FATF 2006 report on NPM, added to this report in Appendix B. For the purposes of this report, e-purses are included in the category "prepaid cards" (also see glossary s.v. "electronic purses").

24 See also: 5.2., *Identification of secondary card holders*, para. 196 ss.

43. Internet payment methods fall into one of three categories:

- Online banking, where credit institutions offer online access to traditional banking services based on an account held at the credit institution in the customer's name. Online banking is outside the scope of this document.

- **Prepaid Internet payment products**, where firms who may not be credit institutions allow customers to send or receive funds through a virtual, prepaid account, accessed via the Internet;

- **Digital currencies**, where customers typically purchase units of digital currencies or precious metals which can either be exchanged between account holders of the same service or exchanged against real currencies and withdrawn.

44. The market for prepaid Internet payment products has diversified and grown steadily since 2006 in parts of the world, possibly as a result of increased Internet usage and acceptance of Internet payments by online merchants. They are also increasingly being used to support person-to-person (p2p) transfers.

45. Recent years have seen the emergence of electronic currencies linked to **virtual worlds**, where users convert real currencies into virtual currencies in order to complete purchases within the virtual world environment. Within that same environment, p2p transfers are often conducted among users (*i.e.,* users sending virtual currencies to fellow users). These virtual currencies are not confined to a particular online game, as they can be traded in the real world and be converted into real currencies.

46. **Cash vouchers** have gained popularity in some markets. These vouchers can be bought anonymously at retailers, petrol stations etc. and are usually sold in units ranging from as low as 10 EUR up to 500 GBP (approx. 750 EUR).[25] Cash vouchers are originally designed for person-to-business (p2b) payments on the Internet, but can also be used for p2p transactions where they are accepted as a funding method by other NPM service providers (*e.g.,* prepaid card issuers or digital currency exchangers), or where they can be used for online gambling.

47. **Internet payment services are increasingly interconnected with different new and traditional payment services**. Funds can now be moved to or from a variety of payment methods, ranging from cash, money remittance businesses (*e.g.,* Western Union), NPMs, bank wire transfers, and credit cards. Furthermore, some IPS providers have started to issue prepaid cards to their customers, thus granting them access to **cash withdrawal through the worldwide ATM networks**.

48. As indicated previously, 15 of the jurisdictions responding to the questionnaire indicated that IPS providers were operating in their respective jurisdiction. Statistics regarding the number of such providers and active client accounts were not consistently provided. However for countries providing such statistics, the estimated number of providers varied between one and 23. As for the estimated number of active IPS accounts, it varied between 45 000 and over 80 million accounts.

---

[25] Cash vouchers share some characteristics with prepaid cards and are therefore considered to be prepaid cards by some, rather than IPS. As this report examines all NPMs, it is not necessary to make a final decision whether these should be considered prepaid cards or IPS.

2.3 Recent Developments Related to Mobile Payment Services

49. For the purposes of assessing risks and vulnerabilities it is essential to differentiate between "mobile payments" based on individual bank accounts or securities accounts for each customer (and recipient) held at a financial institution that is subject to adequate AML/CFT regulation and supervision, and those services offered separately from such accounts.[26] In this respect, it may be helpful to use the four categories of mobile payment systems described by the World Bank:[27] [28]

- Mobile financial information services: Users may view personal account data and general financial information, but there is no capability for any financial transaction and therefore may be considered low risk.

- Mobile bank and securities account services: Users may transact, in a similar fashion to internet banking. The service will be tied into individual bank or security accounts and is therefore (like internet banking) not considered a NPM in the strict sense of this report. Mobile bank and securities account services are likely to be regulated and supervised.

- **Mobile payment services**: Allows non-bank and non-securities account holders to make payments with mobile phones. However, payment service providers may be non-traditional financial institutions with widely varying controls and supervision measures.

- **Mobile money services**: Subscribers are able to store actual value on their mobile phone. They may use phone credits or airtime as tender for payment. Such systems offer versatility but may often fall out of regulation and prudential supervision altogether.

50. The scope of this report covers the last two categories only. However, some of the issues discussed in this report may apply for mobile bank and securities account services as well (*e.g.,* the issue of outsourcing business activities or using agents; or simplified due diligence measures; or non-face-to-face account opening).

51. Advances in mobile phone technology since the 2006 report should reasonably have been expected to facilitate a marked increase in the use of mobile payments systems. The expected proliferation of such systems was regarded as symptomatic of the trend for migration from paper to electronic payments common to all payment systems innovations.

52. Despite a predicted marked increase in the use and spread of mobile payments,[29] only a few providers have managed to run a successful and profitable business model[30] in the long term so far.[31]

---

26 These services may as well rely on the involvement of banks; however, in these business models the technical handling of payment transactions does not rely on individual bank accounts for each customer and recipient.

27 World Bank (2008)

28 Other terms and definitions may exist in the mobile payment service market such as "mobile wallets", "mobile money transfer" (indicating person to person payments) or "mobile payment" (indicating person to business, *i.e.,* retail or bill payment). In this report, these definitions are not used in this sense.

29 Estimates varied; it was suggested that 1.4 billion people will use cell phones to remit money domestically and across borders by 2015 (Michael Klein, World Bank (2008)). Other sources suggest that mobile phone transaction services will grow at 68% per year reaching almost USD 250 billion in 2012

53. As indicated previously, 15 of the jurisdictions responding to the questionnaire indicated that mobile payment service providers were operating in their respective jurisdiction. Statistics regarding the number of such providers and active client accounts were not consistently provided; not all responding jurisdictions made a clear distinction between mobile payments in the sense of this report and mobile banking. For countries providing such statistics, the estimated number of providers varied between one and 21 (including mobile banking models). As for the estimated number of active mobile payment service accounts, it varied between 26 000 and 15 million accounts.

54. Technological developments in mobile payment systems have included the fusing with other payment methods, including traditional payment methods as well as other NPMs:

- Some mobile payment service providers offer open-loop prepaid cards that are connected to the accounts of their customers; through this originally domestic providers may offer cross-border services, as this grants customers or third persons who were handed over the prepaid card access to the global ATM network.

- Some providers even allow for ATM withdrawals without the need for a card. Customers can initiate p2p transactions by passing on a certain code to third parties, who can enter the code into an ATM in order to receive the amount of money linked to that specific code.[32]

- Some providers cooperate with traditional money remittance services (*e.g.,* Western Union); the remittance service enables third parties that are not customers of the mobile payment service provider to send or receive to or from a customer, also across borders.

(Arthur D Little (2009)). These estimates do not only refer to mobile payments services in the sense of this report, but also include mobile banking services.

30 This observation only refers to mobile payments business models in the sense of this report, which does not include "bank based" models (*i.e.,* business cooperation models between banks and telecom companies where each customer needs to have an individual bank account).

31 There are several potential reasons for this, including the following: profit margins in mobile payments services are rather small; in order to make profits, a large number of customers and accepting merchants must be acquired; technological and security issues must be overcome to win the trust of customers. Prudential regulation as well as AML/CFT regulation has also been identified as a potential impediment for market success of NPMs in general, and mobile payment service providers in particular (see chapter 5 for more detail).

32 These non-card ATM withdrawals are currently restricted to domestic ATMs in the provider´s jurisdiction, and only to ATMs of the specific cooperating bank.

CHAPTER 3: RISK ASSESSMENT OF NPMS

NPMs: risk vs. opportunity

55. On the one hand NPMs, like all financial services and products, can be abused for ML/TF purposes. Most jurisdictions have therefore subjected NPM service providers to AML/CFT obligations and regulation.

56. On the other hand, where NPM providers are subject to AML/CTF obligations and appropriately supervised for AML/CTF purposes, NPMs can make payment transactions more transparent and help prevent corruption or other abuses. NPMs can shift customers from the unsupervised or even illegal sections of the payments market (*e.g., hawaladars*, underground banking services) into the formal sector. This means that where providers are subject to AML/CTF legislation and supervision, more transactions are monitored and suspicious transactions are identified and reported to a competent authority. Ultimately, this should result in better oversight of payment activities within a jurisdiction.

Box 5.
Example: Afghan police officers and US soldiers in Afghanistan

In May 2002, at the request of the Afghan Government, United Nations Assistance Mission for Afghanistan and the United Nations Development Program established the Law and Order Trust Fund for Afghanistan (LOTFA) to enable the Afghan police to return to work throughout the country with the first priority being the provision of police salaries. Working with the Afghan ministries of the Interior and Finance, and the United States Military Combined Security Transition Command Afghanistan, LOFTA opened more than 62 000 bank accounts for Afghan police officers and facilitated electronic funds transfers to make salary payments. In addition, the UN, Afghan, and U.S. authorities have been using M-paisa, launched in 2008 by the Roshan mobile company, in collaboration with First Micro Finance Bank, to make salary payments through mobile cell phones. Mobile payments were used in order to avoid police officers having to leave their posts to collect their salaries. Using electronic funds transfer rather than cash disbursement also helped to avoid corruption and bribery.*

Source: United States.

* United Nations Development Programme Afghanistan (2009)

57. Contrary to cash, NPMs can provide additional investigative leads for law enforcement agencies. This is because a transaction carried out through a NPM will always generate an electronic record, whereas cash does not. Even where CDD measures are not applied (*i.e.,* where the customer remains anonymous), the electronic record can, in some cases, still provide law enforcement with at least minimal data such as an IP address or the place where a payment was executed or funds withdrawn; this can potentially support the location or identification of a user suspected of money laundering or terrorist financing.[33] [34]

[33] For example, law enforcement might be able to obtain images of a suspect by analysing CCTV (video surveillance) data at point of sale or in locations where the product was used (ATMs, internet cafes etc.).

[34] Critics challenge the usefulness of the electronic traces rendered by anonymous services or products, pointing out that IP-addresses may be forged; or may be from public places such as "hot spots" or internet

58. This report refers to a number of cases where NPMs were used for money laundering purposes where cash or other traditional payment methods could instead have been chosen. It can therefore be assumed that some criminals consider NPMs to be a better option than cash for ML/TF purposes. This especially applies to cases where NPMs are a substitute for bulk cash to carry, or where the non-face to face nature of the business relationship facilitates the use of straw men or fake identities.[35]

NPMs and Terrorist Financing

59. Based on the case material submitted to the project team, this report focuses mainly on money laundering. Where terrorist financing issues are concerned, this will explicitly be noted in the text; otherwise most findings relating to money laundering apply to terrorist financing *mutatis mutandis*.

60. Out of the 33 case studies analysed in this report, only one has an obvious link to terrorist financing (see section 4: "Typologies", ***case 4***).

Common risks of NPMs

61. The 2006 report identified a number of characteristics shared by most NPMs. These include the absence of credit risk, speed of transactions and (often) non- face to face nature of the business relationship:

- Absence of credit risk

  Funds for use with NPMs are generally prepaid. This absence of credit risk means that service providers may have fewer incentives to obtain full and accurate information about the customer and the nature of the business relationship.

- Speed of transactions

  NPM transactions can be carried out and funds withdrawn or converted much quicker than through more traditional channels. This can complicate monitoring and potentially frustrate efforts to freeze the funds.

- Non-face to face business relationship

  Many (but not all) NPM providers' business model relies on non-face to face business relationships and transactions, which FATF Recommendation 8 identifies as presenting "specific"36 ML/TF risks due to increased impersonation fraud risk and the chance that customers may not be who they say they are.

---

cafes; in such cases, the information is of little use to law enforcement in jurisdictions where public and private video surveillance is less prevalent.

35 See *4.4.1, Cross-border transport of prepaid cards* and Chapter 4.2, *Case 20: Use of "ghost employees" to launder illicit funds through prepaid cards* for "cross-border transport of cards and "ghost employees" examples in the typologies sections.

36 If read in conjunction with the Interpretative note to Recommendation 5 (para. 7) and the Basel CDD paper (section 2.2.6, para. 48), "specific" risk appears to mean "higher" risk: "48. In accepting business from non-face-to-face-customers (…) there must be specific and adequate measures to mitigate the higher risk". See also para. 165 ss.

Assessing individual providers and products, not NPMs as such

62. One of the findings of the 2006 report was that ML/TF risks and vulnerabilities varied significantly among service providers and products, even within one and the same category of NPMs such as prepaid cards. This is due to the fact that the different products have different features that will affect their risk profile.

The Risk Matrix

63. The 2006 report developed a risk matrix which featured several risk factors to assess the risk associated with individual NPM products.[37] This matrix has been updated as follows:

- "Identification" has been renamed "CDD" and now encompasses identification, verification and monitoring.
- "Record keeping" has been added as an additional risk factor.
- "Value limits" and "usage limits" have been broken down into more detail; and
- "Segmentation of services" has been integrated into the risk matrix. Segmentation of services had already been identified as a challenge for regulators and law enforcement in the 2006 report, but had not been included in the risk matrix then.

64. Some of the risks (such as anonymity, methods of funding, value limits etc.) are the direct result of product design, while others result from the providers´ CDD measures (such as verification and monitoring procedures).

65. The risk factors listed in the following matrix should not be looked at in isolation but as a whole; a "high risk" rating in one risk factor does not necessarily mean an overall rating of "high risk" for the product. It is important to look at the whole picture not only including all risk factors, but also all risk mitigants implemented in order to effectively assess the risk associated with a particular NPM product.

Box 6.
Example: Risk factor "Usage limits / utility"

The risk matrix considers services that facilitate person-to-person (p2p) payments to be of a higher risk than services that facilitate person-to-business (p2b) payments only. This consideration is based on the fact that the p2p functionality enables a user to transfer funds to a much higher number of potential recipients, and without the need for an underlying purchase or any other "reason" for a transaction.

However, the p2p functionality of an NPM service does not automatically lead to an overall risk assessment of "high risk" for that service. Likewise, NPM services that are restricted to p2b payments cannot automatically be regarded as "low risk" services. Instead, the other risk factors listed in the risk matrix must be taken into account as well (*e.g.:* Are there identification/verification measures? Are there value limits? …)

Payment Methods Risk Factors				
Criteria		**Cash**	**NPM High risk**	**NPM Low risk**
CDD	Identification	anonymous	Anonymous	Customers are identified
	Verification	anonymous	Customer's identity (where obtained) is not verified on	Customer's identity is verified on the basis of reliable,

[37] Other publications on risk assessment have developed different approaches, using different risk factors, which are not adopted here. See for example World Bank Working paper (2008), p. 17 ss.

Payment Methods Risk Factors				
Criteria		**Cash**	**NPM High risk**	**NPM Low risk**
			the basis of reliable, independent source documents, data or information (*cf.* Recommendation 5)	independent source documents, data or information (*cf.* Recommendation 5)
	Monitoring	none	None	Ongoing Monitoring of business relationships
Record keeping		none	Electronic transaction records are generated, but not retained or not made accessible to LEA upon request	Electronic transaction records are retained and made accessible to LEA upon request
Value Limits	Max. amount stored on account / accounts per person	no limit	no limit	Amount limit (cf. para. 112 ss.)
	Max. amount per transaction (incl. loading / withdrawal transactions)	no limit	no limit	Amount limit (cf. para. 112 ss.)
	Max. transaction frequency	no limit	no limit	Transaction limit (cf. para. 112 ss.)
Methods of funding		n.a.	Anonymous funding sources (*e.g.,* cash, money orders, anonymous NPMs); also multiple sources of funds, *e.g.,* third parties	Funding through accounts held at a regulated financial or credit institution, or other identified sources which are subject to adequate AML/CTF obligations and oversight
Geographical limits		Some currencies are accepted more widely than others; currencies can be converted through intermediaries	Transfer of funds or withdrawal across national borders	Transfer of funds or withdrawal only domestically
Usage Limits	Negotiability (merchant acceptance)	Generally accepted	High number of accepting merchants / POS (*e.g.,* through usage of VISA or MasterCard standard)	Few accepting merchants / POS
	Utility	p2b, b2b, p2p, no online usage possible	p2b, b2b, p2p, online usage possible	p2b, b2b, online usage possible, but no p2p
	withdrawal)	n.a.	Anonymous and unlimited withdrawal (*e.g.,* cash through ATMs)	limited withdrawal options (*e.g.,* onto referenced accounts only); limited withdrawal amounts and frequency (*e.g.,* less than a certain fixed sum per calendar year)
Segmentation of services	Interaction of service providers	n.a.	Several independent service providers carrying out individual steps of the transaction without effective oversight and coordination	Whole transaction carried out by one service provider
	Outsourcing	n.a	Several singular steps are outsourced; outsourcing into other jurisdictions without appropriate safeguards; lack of oversight and clear lines of responsibility	All processes completed in-house to a high standard

66. Some types of NPMs are more affected by certain risk factors than others, but most risk factors apply to all types of NPMs to a certain degree. The following discussion of **risk factors (section 3.1)** will therefore be presented in a consolidated section for all NPMs together.

67. The ML/TF risks associated with NPMs can effectively be mitigated by firms' own AML/CTF policies and procedures and regulatory oversight. Like risk factors, the **risk mitigants** appear to be similar for all types of NPMs and are therefore presented in a consolidated **section 3.2.**

3.1 Risk factors

Customer Due Diligence

68. **Prepaid cards** can be designed to afford the customer absolute anonymity while maintaining a high degree of functionality. For example, some prepaid card issuers attract customers with anonymous prepaid cards with no or high loading and transaction limits.

Figure 1. Example of a prepaid card



Source: Internet screenshot July 2010

69. Prepaid cards can also easily be passed on to anonymous third parties who in some cases will be the beneficial owner. Where additional "twin cards" or "partner cards" are issued that are specifically designed and advertised for being passed on to third parties to allow remittances, these third parties/beneficial owners are often not identified. This emphasizes the significance of identifying at least the primary account holder /card holder.[38]

[38] There is always the potential for any payment card (including traditional debit or credit cards) to be shared with third parties who remain anonymous to the card issuing institution; but if the institution has adequately identified the primary card holder, law enforcement has a point of contact to associate with reports of suspicious transactions.

70. For many NPM providers, customer contact is often minimal as a result of business relationships being conducted on a non-face to face basis. As recognised by FATF Recommendation 8, this increases risks like identity fraud, impersonation fraud or the use of the product by third parties for illicit purposes. Absence of face to face contact is particularly common among **IPS providers** who generally conduct most of their business activities online. It may also be relevant for other types of NPMs (*e.g.,* online purchase of prepaid cards).

71. Most IPS providers ask for their customers´ names, but the levels of customer verification vary significantly, ranging from no verification at all (some providers only require a pseudonym) to sophisticated verification measures (see section 3.2 "risk mitigants").

72. The verification of the customers´ identity may be further hampered or impossible in jurisdictions that have no national identity card scheme, or other appropriate alternative forms of identification; this is a challenge often encountered by NPM providers operating in underbanked regions, especially **mobile payment services providers**. For this reason, the World Bank has recommended to jurisdictions intending to promote financial inclusion (*e.g.,* through mobile payment service providers) that if the jurisdiction´s "national identification infrastructure and other private databases lack coverage, integrity, or are not easily and cost-effectively accessible to financial institutions for verification purposes, the state should address these deficiencies".[39] Where customer data cannot be reliably verified, it may be appropriate to apply alternative risk mitigation measures (*e.g.,* imposing low value limits in order to qualify as a "low risk" product and be allowed to apply simplified CDD measures; see also below section 3.2, "value limits" as a risk mitigant (para. 112 ss.).

73. Where no identification or verification based on reliable and independent sources takes place, NPM providers run the risk of customers' holding multiple accounts simultaneously without the provider noticing.

Record keeping

74. According to FATF Recommendation 10, both identification data as well as transaction records should be maintained for at least five years. Transaction records must be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity. While neither Recommendation 10 nor the Interpretative Note to Recommendation 10 provides a definition of the term "transaction records", examples of necessary transaction records are provided by the FATF Methodology (10.1.1):

> *—Examples of the necessary components of transaction records include: customer´s (and beneficiary´s) name, address (or other identifying information normally recorded by the intermediary), the nature and date of the transaction, the type and amount of currency involved, and the type and identifying number of any account involved in the transaction."*

75. These examples do not explicitly list the IP addresses of customers initiating a payment transaction through a personal computer. Only in a few cases have jurisdictions, regulators or industry have issued guidance that it can be advisable to do so.[40]

---

39 World Bank (2009a), Annex 1 (A 1.1), p. 173 ss.; these World Bank recommendations are based on and quoted from: Bester, H., D. Chanberlain, L. de Koker, C. Hougaard, R. Short, A. Smith and R. Walker (2008), p. xi,; p. 39, 40.

40 For example, the *UK JMLSG Guidance (2007)* Part II Sector 3, explains how IP addresses can form part of a customer´s identity.

76. Law enforcement agencies have reported investigative cases where providers had not kept record of IP addresses at all, or not sufficiently, or had already deleted them before law enforcement agencies could access them. The increased ML/TF risk with providers that have no robust record keeping policy regarding all relevant transaction data lies in the fact that weak record keeping impedes criminal prosecution.

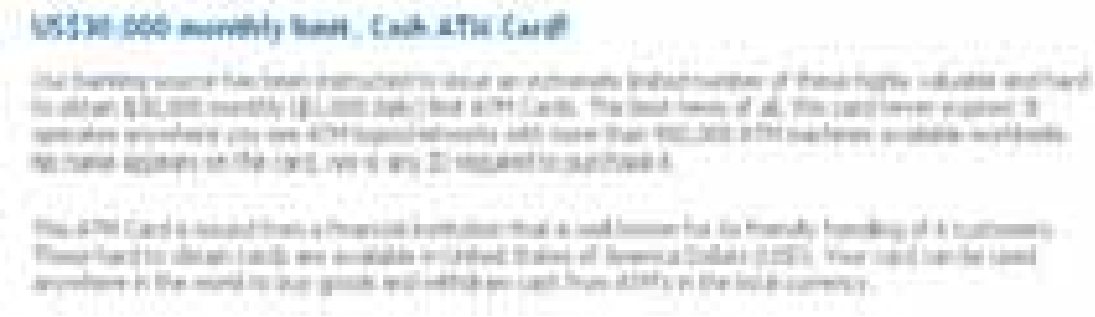
Value limits

77. The term "value limits" refers to limitations on the maximum amount that can be held in a NPM account or product; or limitations on the maximum amount per single payment transaction; or limitations on the frequency or cumulative value of permitted transactions per day/week /month/ year; or a combination of the aforementioned limitations. Also the number of accounts or cards allowed per customer can be considered a type of value limit.

78. Where value and transaction limits are not imposed, the availability of funds is limited only by the amount loaded onto the account. This increases the product's appeal to would-be money launderers and consequently the ML/TF risk the product is exposed to.

79. The higher the value and/or frequency of transactions, the greater the money laundering and terrorist financing risk. Similarly, high, or no, account limits increase the risk as well.

80. Most **Mobile payment service providers** impose rather low (*i.e.,* strict) value limits on their products, whereas a wide variety of approaches can be found for **Internet payments services and prepaid cards providers.** For example, prepaid cards may be designed as a non-reloadable card with a rather low account cap (such as USD 100); on the other hand, there are reloadable cards with no or rather high account caps such as USD 30 000 per month.



Source: Internet screenshot July 2010 *

* As mentioned above, some offers of anonymous prepaid cards are fraud. The project team did not investigate whether the product advertised by this screenshot is fraudulent or not.

81. Providers of products with high or no value limits are often based in jurisdictions where NPM providers are not or insufficiently regulated and supervised for AML/CTF purposes, but sell their product internationally (through agents or over the Internet). However, such providers of anonymous prepaid cards with high or no limits have also been found to operate in jurisdictions whose regulatory regimes and supervision are generally considered robust.[41] Such anonymous cards are often not promoted by the issuing institution itself, but by intermediaries some of which have specialised in founding and selling companies abroad, preferably in tax havens, thus providing a complete "privacy

[41] In 2007, the German *Bundeskriminalamt* (BKA) conducted a special investigation on payment cards; during that investigation, the BKA detected six cases of anonymous prepaid cards sold via the internet; the issuing banks were located in Europe and Central America.

package" to their customers. Some of those anonymous prepaid cards however have been discovered to be fraudulent.

82. Value limits may be linked to the product´s CDD requirements (*i.e.,* strict limits where the level of CDD measures is low, and higher or no limits where the level of CDD measures is high; see also below section 3.2 "risk mitigants", value limits).

Methods of funding

83. NPMs can be funded in different ways - including anonymously through sources such as cash, money orders or funds transfers from other anonymous NPM products. Anonymous funding methods may result in no or insufficient paper trails regarding the funding transaction and the origin of the funds.

84. Cash funding is especially popular with NPM providers that sell pre-funded products through distribution agents (*e.g.,* prepaid cards and cash vouchers sold by retailers, or mobile prepaid funds sold by phone shops.)[42] Cash funding through distribution agents can increase ML/TF risk, especially where the distributing staff have no CDD obligations and/or no sufficient training in AML/CFT compliance.

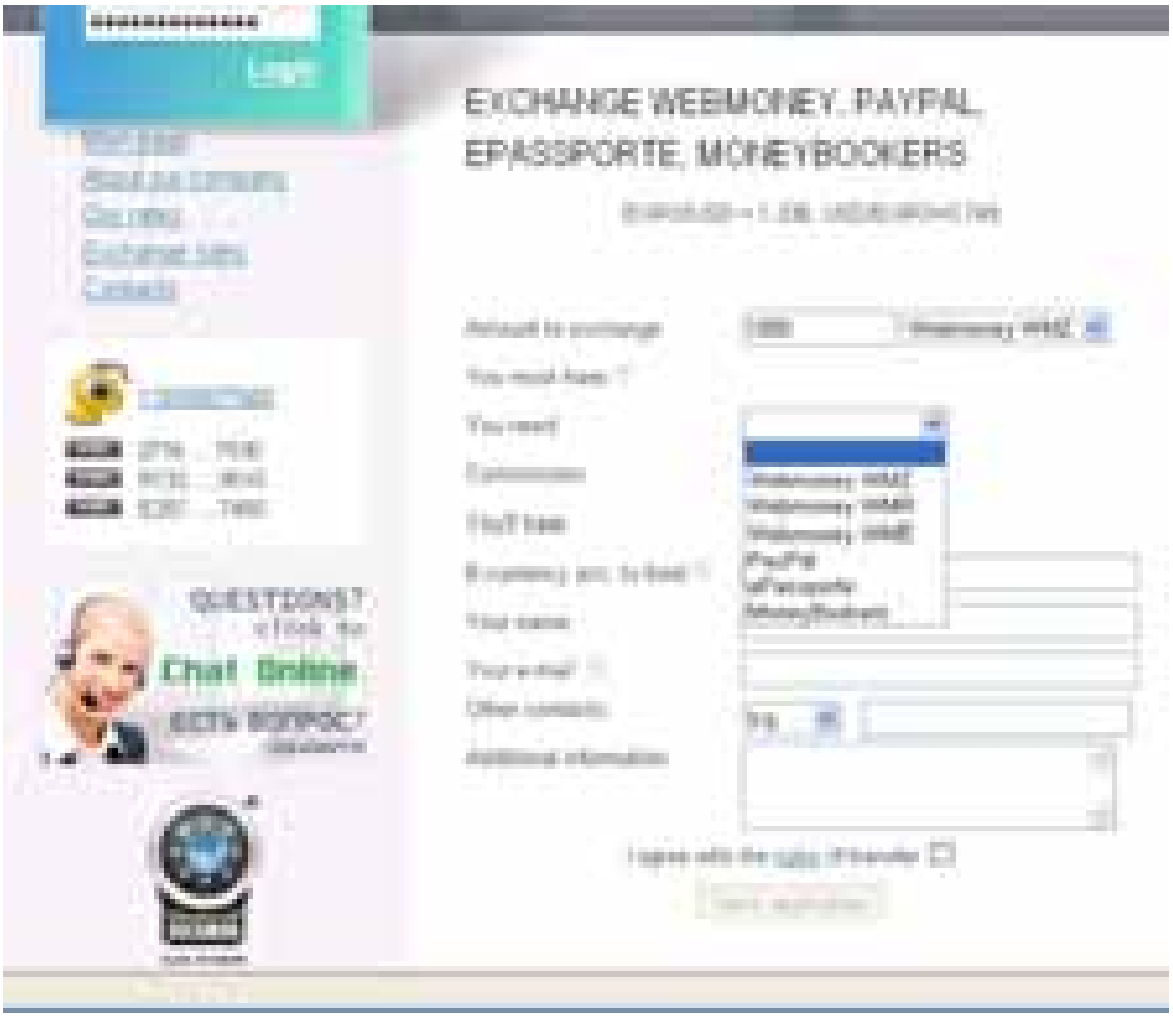
85. Other than funding through anonymous sources, the ML/TF risk will increase where the funds can stem from different sources, including third parties. For example, where there is a co-operation with money remittance businesses, these may be used to not only fund the customer's own personal account, but also to fund the account of third persons.

86. As most IPS and mobile payment services are account-based, another possibility of "indirect funding" arises when the service provider allows for person-to-person (p2p) transactions within the system. In such cases the provider's funding restrictions may be circumvented by funding an account in cash through a digital currency exchanger (or other third parties), who will then transfer the funds into the customer´s account.

---

42 In under-banked regions where few customers have bank accounts, and where the NPM service (often mobile payment services) is supposed to substitute for the lack of bank accounts, there may be few alternatives to cash funding.

Figure 2. Example of online exchange of currency



Source: Internet screenshot May 2010.

87. As different NPM providers have different funding and withdrawal methods, exchangers enable customers to circumvent these procedures by simply converting the funds into a more suitable provider's currency.

Geographical limits

88. The wider the geographical reach of a NPM product, the higher the ML/TF risk will be. Cross-border functionality renders a service more attractive to launderers; it also enables payment service providers to conduct their business from jurisdictions where they may not be subject to adequate AML regulation and supervision, and where they may be outside the reach of foreign law enforcement investigations.

89. While many payment service providers who offer cross-border services may cooperate well with their domestic supervisors and law enforcement agencies, some providers may refuse to provide information to foreign agencies or may face legal obstacles for doing so. Formal legal assistance requests can be very time-consuming and often have only little chance of success. As a result, some agencies may refrain from requesting legal assistance and close the investigation instead. This

phenomenon is exacerbated if the service is provided by several providers interactively who are located in several different jurisdictions (see "segmentation of services", para. 96 ss.).

90. Open-loop prepaid cards can be used to quickly move cash around the world by using the ATM network to withdraw funds, with no face-to-face transaction required. The global network providers (VISA, MasterCard) can limit the use of prepaid cards to certain jurisdictions or regions, but most open-loop prepaid card business models are designed to function globally. Although the ATM network was not designed to be used as a person-to-person money transmission system, it is now also being marketed as one.

Figure 3. Example of internet transfer



Source: Internet screenshot August 2010.

91. Internet payment services providers can be headquartered or licensed in a jurisdiction different from where the customer is located, and because IPS can use a variety of funds transfer methods, payments can potentially be initiated and received from anywhere in the world. Most IPS providers offer their services globally, thus facilitating cross-border transactions.

92. Most mobile payment service providers were originally designed for domestic transactions only. An increasing number of providers offer the possibility to effect cross-border payments between specific countries, opening so-called payment corridors (*e.g.,* from the UK to Kenya, or Philippines to Malaysia). While there have been attempts to implement multinational business models for mobile payments, currently there still is no truly global mobile payment service provider yet.

93. However, some mobile payment service providers have extended their outreach by connecting with the global ATM network (by providing their customers with prepaid cards) or by cooperating with

global money remittance businesses. Through this, an originally domestic service provider can effectively carry out cross-border transactions into and out of its original jurisdiction.

Usage limits

94. The usage limits for NPM products can differ by product and by service provider. NPM products with limited functionality are exposed to fewer AML/CFT risks than those that allow customers to use the product more widely.

95. Open-loop prepaid cards, especially when they are based on a well established and widespread technical standard (VISA, MasterCard) generally have the least usage limits, as they can rely on an existing extensive infrastructure for payment transactions, including the global ATM network and a very high number of accepting merchants / point-of-sale (POS).

- Negotiability(merchant acceptance)

  Visa and MasterCard branded prepaid cards are accepted by domestic and foreign merchants that are part of VISA or MasterCard's payment networks. As the standards used for prepaid card payments typically are largely identical[43] with those of regular debit or credit card payments, such prepaid cards are accepted as a means of payment almost everywhere where a credit card would be accepted for payment (as long as the prepaid funds are sufficient for the intended payment), including online shops.

  When using IPS and mobile payment services providers, payment transactions can often only be carried out between customers of the same IPS provider. Payments services that are widely accepted will be more attractive to money launderers than those that allow funds to be spent with a limited range of merchants only.

  In some markets, mobile payments services are used exclusively for micropayments (*e.g.,* mass transport tickets, vending machines, and ringtones); the number of accepting merchants is limited. In other markets where mobile payment services may be used as a substitute for bank accounts and wire transfers, the negotiability is often much higher, resulting in greater risk.

- Utility

  In order to carry out a classic prepaid card payment, the receiver/payee needs to have the necessary technical equipment (card reader, online access to system). Therefore, most card payment receivers are businesses (p2b-payments). However, where prepaid cards are designed to receive payments / funds from external sources, or where the cards or specific partner cards can be passed on to third parties or used to fund other NPM accounts, p2p payments are also facilitated.

  Most IPS and mobile payment services feature p2p-payments, but some are designed to facilitate p2b payments for underlying shopping transactions only (*e.g.,* cash vouchers), which generally decreases the ML/TF risk. However, where "merchants"[44] accepting such payments

---

43 There are controls that countries or institutions can apply that prevent cards from being used for certain purchases; or in ATM machines; or that limit the transaction value etc. Because of this, the functionality of prepaid cards can vary and does not necessarily equal that of credit cards.

44 Which is a wider term and encompasses more than the classic online shop.

are being used for financial services provision (*e.g.,* money transmission service accepting these payment methods as a funding method) or criminal purposes (*e.g.,* illicit online gambling providers accepting this payment method), the ML/TF risk remains high.

- Funds withdrawal

  Cash can be withdrawn from many open-loop prepaid cards via the ATM networks. In addition, in several jurisdictions merchant points of sale may be easily used to withdraw cash by overpaying purchased merchandise and receiving the overpaid amount in cash ("cash back").[45] Easy cash access and high negotiability, coupled with the fact that prepaid cards[46] are much easier to transport than bulk cash (an ISO standard financial transaction card can be considerably more compact than currency[47]), may make prepaid cards a convenient substitute for cash in bulk cash smuggling ML schemes,[48] assuming a high account limit and/ or no verification of customer identification.

  Most IPS and mobile payment services providers restrict the possibility of redeeming money in the same way they restrict the funding methods. For example, redemption of funds may be restricted to a transfer of funds into an account held in the customer's name at a credit or financial institution.

  Where cash is used as a method of funding, it is usually also possible to withdraw cash from the mobile payment account, *i.e.,* through agents. This not only increases the ML/TF risk, but may also create additional challenges for the mobile payment service provider. For example, there have been reports about fraudulent agents, or problems with the cash supply for requested withdrawals.

  Providers may facilitate cash payouts through cooperation with money remittance businesses or brick-and-mortar exchangers that will trade electronic funds for cash. Some IPS and mobile payment providers also offer to load the funds onto a prepaid card, thus granting their customers access to cash withdrawal through the worldwide ATM network. One mobile payment provider (in cooperation with a domestically operating bank) even enables access to the cooperating bank´s ATMs without the customer needing to have a bank account or a prepaid card: upon request, the customer is provided with a one-time authorisation code which he (or a third party) can enter into the ATM, together with the customers phone number and the amount he wishes to withdraw.[49]

Segmentation of services

96. NPMs can be more exposed to risks where several parties are involved in performing the payment service jointly, such as card issuers, program managers, exchangers, distributors and other

---

45 This "cash back" method of withdrawing funds has originally been developed for and is commonly applied with regular credit or debit cards.

46 The card often acts as an access device to withdraw the funds and initiate payments.

47 The volume of an ISO standard "financial transaction card" is 3 525.8 cubic millimetres. The volume of a 20 EUR note is 1 435.6 cubic millimetres. The volume of a 20 USD bill is 1 129 cubic millimetres. Thus, a payment card with access to just 100 EUR or 100 USD is already considerably more compact than five 20 EUR notes or five 20 USD bills.

48 See *4.4.1. Cross-border transport prepaid cards.*

49 *Cf.* Finextra (2010).

types of intermediaries or agents. The number of these parties generates potential risks of segmentation and loss of information. This may be exacerbated if important services are outsourced to potentially unregulated third parties without clear lines of accountability and oversight, or which are located abroad. Payment schemes with a high degree of segmentation may raise issues for supervisors in terms of competences, international cooperation, powers and means to supervise and to safeguard them effectively.

97. Providers often use **agents** not only for cash acceptance and cash withdrawals, but also to establish new customer relationships. In most jurisdictions agents who are not credit or financial institutions are not themselves subject to AML/CFT obligations. The legal and regulatory responsibilities for complying with relevant AMLCFT legislation or regulation remain with the NPM provider. This means that the NPM provider will be liable for any failure by the agent to meet the provider´s AML/CFT obligations on its behalf ("agent's risk").[50] The provider therefore has to be satisfied that the agent carries out their function effectively. Given the vast number of agents that some providers have to rely on (*e.g.,* hundreds of branches of a big retailer), this may be difficult – even more so where agents are based in a foreign jurisdiction, or potentially, where the agent makes use of further agents ("sub-agents").[51]

98. Where a provider cooperates with money remittance businesses, these are generally used to accept cash for funding and/or pay out cash for withdrawals. This can to some extent add an additional level of AML/CFT compliance, as in most jurisdictions money service remitters are subject to AML/CFT regulation and supervision themselves. However, the regulatory requirements may be different: for the money service businesses, the customer´s transaction usually being a one-off transaction, whereas for the NPM provider the transaction is part of an ongoing customer relationship. Furthermore, the risk may increase if the cooperating money remittance business is located in a jurisdiction that does not enforce equivalent AML/CFT standards.

99. A special phenomenon of segmentation of services is associated with a certain type of IPS, so-called digital currency providers (DCP), which use "exchangers" as an integral part of the payment transaction chain. DCP do not directly issue their "digital currency" to their customers / account holders, and as a consequence do not receive an equivalent incoming flow of money from their customers. Instead, customers have to purchase their digital currency from exchangers, who will then transfer the purchased amount of digital currency into the customers DCP account. Some exchangers are subsidiaries of DCP, but many are legally independent businesses or natural persons. Exchangers may be brick-and-mortar businesses (*i.e.,* exchanging cash and other traditional payment methods for digital currency and vice versa) or pure online businesses (exchanging electronically transferred money for digital currencies, or exchanging digital currencies for other digital currencies or IPS funds).

3.2 Risk mitigants

100. Like any financial product, the AML/CTF risk associated with NPMs is high in the absence of appropriate safeguards. However, there are effective risk mitigants that can significantly reduce the identified risks.

---

50 The term "agents risk" comes from the FATF paper "*Risk Based Approach: Guidance for Money Service Businesses*", FATF (2009a), pages 32 ss.

51 While this phenomenon of sub-agents has not yet been observed with NPM service providers, it has become apparent in the latest typologies report on money service businesses.

101. The following risk mitigants should not be looked at separately but as a whole; some of them are intertwined or affect more than just one specific risk factor. It is important to look at the whole picture including all risk factors and all risk mitigants in order to effectively assess the risk associated with a particular NPM product.

Identification and verification measures

102. Identification and verification measures allow firms to understand who their customer and, where relevant, the beneficial owner is. This is important in that this information forms the basis for ongoing monitoring of the business relationship. It also allows firms to verify that the customer is who they claim to be, identify whether a customer is associated with multiple accounts (or cards; or cash vouchers), and create a paper trail for law enforcement.

103. For products and services that rely on the internet, the internet protocol address (IP-address) should be part of the identification data collected and retained by the provider. The IP-address can help minimise the potential for a customer to access multiple accounts, even if those are anonymous.

104. Some jurisdictions exempt providers from applying customer due diligence measures where the ML/TF risk is considered very low. Sometimes, these exemptions are conditional on the imposition of low value and transaction thresholds. Some jurisdictions also allow NPM providers to benefit from a one-off transaction exemption from CDD. In those situations, it is important that institutions have systems in place to detect if a customer holds multiple cards or accounts, which can be an indicator for a customer circumventing the CDD procedures by structuring the funds into several "low risk" products.

105. Where verification takes place on a non-face to face basis, it is important that firms employ anti-impersonation fraud checks to be satisfied that their customer is who they claim to be. Anti-impersonation checks include, but are not limited to: correspondence with the customer at their verified home address; requiring the first payment to be carried out through an account in the customer's name with a regulated credit institution from a FATF-equivalent jurisdiction; and requiring copy documents to be certified by an appropriate person.[52] Accompanying anti-fraud checks, such as using dynamic codes which change with each single transaction or access to an IPS, or checking of biometric data (such as fingerprint and voice recognition systems),[53] can add to the AML policies of a provider and help prevent a single customer from opening multiple accounts unnoticed.

106. Where a payment service provider uses third parties to establish customer contact and to accept and pay out cash (*e.g.,* retailers or money remittance businesses), firms can mitigate risk by ensuring that these are appropriately trained and qualified in AML/CFT compliance, preferably subject to regulation and supervision themselves in a jurisdiction with equivalent AML/CFT regulatory standards.

107. Where NPMs can be used for p2p remittances, providers can mitigate risk by ensuring that the recipient of the payment does not remain anonymous and that safeguards are put in place, which are similar to those expected from firms executing wire transfers.

---

[52] Basel Committee on Banking Supervision (2001), section 2.2.6; Joint Money Laundering Steering Group Guidance (2010), Part I Chapter V;

[53] *Cf.* World Bank (2009b)

Monitoring

108. NPMs are based on computer technology and therefore provide good prerequisites for effective monitoring and reporting procedures. Transactions carried out through NPM services always leave electronic footprints which can be monitored and analysed, even where NPMs benefit from exemptions from customer due diligence (*i.e.,* the customer remains anonymous). This means that providers can block accounts where they detect abnormal transaction patterns or otherwise become suspicious that their product might be abused for ML/TF purposes.

109. Monitoring systems can be a very effective tool to mitigate an NPM product's financial crime risk.

To be effective, such systems must at a minimum allow the provider to identify:

- Discrepancies, for example between submitted customer information and the IP address.
- Unusual or suspicious transactions.
- Cases where the same account is used by multiple users.
- Cases where the same user opens multiple accounts.
- Cases where several products are funded by the same source.

110. Where products benefit from customer due diligence exemptions, systems should detect where a customer approaches a limit (on one product/transaction or cumulatively) beyond which full customer due diligence has to be applied.

111. Effective monitoring systems are also the basis for effective reporting of obligated NPM providers.

Value limits

112. Account balance and transaction limits as well as restrictions in the frequency of transactions may prevent criminals from having continuous access to large amounts of money for illicit purposes. Applying a risk-based approach, value limits can be tailored to reflect the needs and risks attached to each market segment and NPM product. For example, there may be effectively no transaction limits when the service is linked to a fully identified and verified bank or credit card account, but a reduced transaction limit or service where there is a reduced ID requirement.

113. Where NPM providers are subject to AML/CFT regulation and supervision, in application of a risk-based approach their products often do not require the full application of customer verification measures ("simplified CDD" or "reduced CDD"), ranging from reduced normal CDD to total exemptions from the CDD requirements. [54] Value limits are often a decisive factor whether a product can be considered to be of "low risk" and therefore apply for simplified CDD or not.

114. Value and transaction limits can be a very powerful risk mitigant as they render a product less attractive to money launderers, especially when coupled with effective monitoring systems and procedures that prevent multiple purchases of low-value cards or multiple low-value accounts for a

[54] See *5.2, Exemptions from AML obligations*.

single customer. For example, the restrictive value limits implemented by most mobile payment service providers are thought to be one of the main reasons that so few ML case studies involving mobile payments have been detected so far.

115. One of the challenges for applying value limits is to define an appropriate threshold which can be considered low risk. Different jurisdictions and service providers have come to different conclusions as to what thresholds they consider to be "low risk".[55] Furthermore, low transaction amounts that may deter Money launderers might still be attractive for the purpose of terrorist financing, which is generally thought to involve much smaller amounts than ML.

Methods of funding

116. The ML risk associated with anonymous funding methods can be mitigated by restricting funding methods to sources where providers can rely on another institution´s CDD measures, such as previously identified bank accounts, credit or debit cards or other personalised payment methods.[56] While excluding cash or other anonymous sources as a funding method significantly reduces risk, it may not be feasible in such markets where NPM service providers are the only access to the financial system for a good part of the under-banked population (*e.g.,* mobile payment services in jurisdictions with weak banking infrastructure).

117. Issuers with restricted funding methods should be in a position to detect indirect funding through third parties (*e.g.,* exchangers) by attentive monitoring. They can further reduce ML/TF risk by not only restricting the funding method, but also restricting the number of parties allowed to fund the product (*e.g.,* regarding cards: the cardholder alone, or the employer in the case of payroll cards), thus limiting the possibility of third party funding.

---

55 See 5.2, *The definition of low risk cases*, para. 161.

56 This does not constitute reliance as per FATF Recommendation 9, and is unlikely, by itself, to satisfy Recommendation 5´s requirement for using a reliable and independent source to verify a customer´s ID.

CHAPTER 4: TYPOLOGIES AND CASE STUDIES

118. In 2006 when the FATF New Payment Methods report was released, the potential for the misuse of NPMs was already apparent. However, at that time there was little evidence to support this. Since then, both the availability and adoption of NPMs have grown significantly as has evidence of misuse (especially with prepaid cards and IPS), as demonstrated by the following case studies. It should be noted that most case studies concern money laundering and there are only a few isolated cases with suspected links to terrorist financing, even though NPMs have been identified as being vulnerable to terrorist financing.[57]

119. The case studies demonstrate the following typologies: *1)* Third party funding (including strawmen and nominees); *2)* Exploitation of the non-face-to-face nature of many NPM accounts; and *3)* Complicit NPM providers or their employees. The typologies are presented in an order based on whether or not all NPMs, or two of them or at least one NPM has been used in such a way.

120. The project team came to the conclusion that it was not appropriate to present a fourth typology on "anonymity". While many case studies involved taking advantage of the possibility of remaining anonymous, only three cases (***cases 8,10 and 31***) involved NPM products that provided "direct" anonymity, *i.e.,* the product did not require ID/VER at all. Numerous other cases that involved products that may provide "indirect" anonymity, are dispersed over the other three typologies identified (*e.g.,* strawmen, stolen or fake customer data or online data manipulation). "Anonymity" as such may be a general and overarching issue with NPMs, but it is too vague to construct a separate typology.

4.1 Typology 1: Third party funding (including straw men and nominees)

121. NPM accounts can be funded anonymously where the specific business model permits.

122. Prepaid cards can be funded by cash, bank transfers, and person-to-person (p2p) transfers. Customers of most IPS providers can also conduct p2p transfers. These funding methods may allow complicit third parties to fund the prepaid cards or the IPS accounts willingly (*e.g.,* by paying for the sale of illicit merchandise or for gambling, refer to ***cases 1-3, 6***),[58] or may be used by fraudsters to get funds from unwilling victims of their illegal activities. In such cases the distinction between the predicate offence and the subsequent placement phase of money laundering may be difficult. Nine case studies illustrate how prepaid cards and IPS accounts can be funded through third parties for the purpose of money laundering.

123. Similar to IPS providers and prepaid cards, mobile payment services allow third-party funding which can be exploited by criminals. In three cases, criminals used the p2p payment feature of a mobile payment service provider to fund their accounts. In all cases, the third parties were defrauded or tricked

---

57 UN Counter-Terrorism Implementation Task Force (2009), p. 14; also confer World Bank (2009b).

58 EUROJUST has also indicated that NPM are often used to buy or sell child obscenity/child pornography images online to avoid attention from public authorities. Presently the EFC (European Financial Coalition against the Commercial Sexual Exploitation of Children Online) is in contact with a certain number of such NPM providers.

into sending money to the criminals, making the use of the mobile payment service provider also part of the predicate offence. It should be noted that the amounts involved in these cases were small.

124. There is also evidence that even robust identification and verification requirements can be circumvented by the use of third parties such as straw men or financial agents/financial mules.

a. Prepaid Cards:

Case 1: Laundering of proceeds gained through illegal online steroid sales

In 2007, there were three cases with a total of seven defendants who were charged with selling athletic performance enhancing drugs, such as human growth hormone and anabolic steroids, illegally online and laundering the proceeds. All three cases involved loading the defendants' prepaid cards as an optional payment method for completing the online sale of the illegal substances. In one case, the defendant earned USD 60 000 in 11 months from his online steroid business. In another case, the defendant laundered about USD 125 000 in 21 months using prepaid cards. All three cases were resolved with guilty pleas. Defendants received prison sentences.

Source: United States.

Case 2: Laundering of illegal gambling proceeds through prepaid cards

In 2007, a number of defendants were charged with facilitating illegal gambling. The organisation involved onshore agents in the United States who recruited gamblers, collected losses, and distributed winnings, and an offshore organisation that operated an Internet site that processed bets and set odds.

Among the methods used to transfer the illicit gambling proceeds between the onshore agents and offshore organisers was to open and load U.S. prepaid card accounts and then send the card information (card number, expiration date and card verification value) to the website operators. The cards themselves were not sent out of the country. Instead, the offshore organisers would use the card accounts to make online or phone-based purchases. The online gambling operation earned about USD 100 000 a month.

Six defendants pleaded guilty to illegal gambling and were sentenced to three years probation. One defendant pleaded guilty to illegal gambling and money laundering and was sentenced to three years probation and six months home confinement. One defendant pleaded guilty to conspiracy and was sentenced to four years probation. One defendant pleaded guilty to bulk cash smuggling and was sentenced to four months imprisonment and three years probation.

Source: United States.

Case 3: Payment for drugs using prepaid cards

In 2009, a number of defendants were charged with running a drug trafficking ring in a federal prison and receiving payment outside the prison through prepaid cards. Gang members outside the prison allegedly established prepaid card accounts in the name of the defendants, who allegedly instructed their customers — their fellow prisoners — to pay for the drugs by having family members outside the prison deposit payments into the defendants' prepaid card accounts. The defendants have not yet gone to trial.

Source: United States.

Case 4: Possible use of prepaid cards for terrorist financing purposes

In a particular case, a father and his son, suspected to be operating as money remitters, held numerous prepaid cards which were charged daily from all over Italy. Shortly after, the sums were withdrawn so as the cards accounts' balances were almost always near to zero. A portion of the sums withdrawn from the prepaid cards was transferred to a bank account held by the father; funds were also credited to the same bank account from Pakistanis. The funds on the account were further used to order credit transfers. Both persons were found to be involved in the terrorist attacks which occurred in Mumbai in 2008.

Source: Italy.

Case 5: Prepaid cards used to launder drug proceeds

Following the dissemination of Suspicious Transaction Reports (SUSTRs) received by AUSTRAC to a law enforcement agency, an AUSTRAC alert was raised on a suspect and his associate. The information related to a student who on a number of occasions loaded structured amounts of AUD 9 900 to avoid reporting thresholds onto prepaid debit cards in his own name and that of his associate (i.e., conducting third-party loading transactions). The suspect had previously come to the notice of law enforcement agencies in relation to a cocaine seizure which he was alleged to have organised. Following further research and intelligence gathering a joint operation commenced involving multiple law enforcement agencies.

A further 15 SUSTRs were recorded on the AUSTRAC database, showing both the suspect and his associate conducting deposits of structured amounts onto prepaid debit cards. AUSTRAC information detected a further series of financial transactions linked to both targets. An assessment of AUSTRAC information was disseminated to the law enforcement agencies and assisted the investigation, resulting in the arrest of both targets. The associate departed Australia for South America and returned to Australia from another South American destination 12 days later with approximately 5.8 kilograms of cocaine in his baggage. He later admitted that he had previously brought drugs into Australia on two occasions for a payment of AUD 28 000 each time. He was arrested and charged with importing and possessing a prohibited import. The suspect was also charged with conspiracy to bring into Australia approximately 5.8 kilograms of cocaine, structuring and money laundering of almost AUD 400 000. He was found guilty and sentenced to seven years imprisonment.

Source: Australia.

b. Internet Payment Services:

Case 6: Use of IPS to move illicit proceeds gained through the sale of forbidden racist propaganda

In at least two proceedings regarding the illegal distribution of right wing propaganda music CDs, an IPS provider played a decisive role.

The service was used to effect the transfer of funds (purchase prices) to natural persons in Germany and abroad, involving buyers, retailers and most likely also wholesale dealers and producers (as can be concluded from the high amounts of some transactions) of racist propaganda material.

Distributing such material constitutes a criminal offence under German criminal law.

Source: Germany.

Case 7: Use of an IPS to move illicit proceeds gained through the sale of stolen goods on a commercial website

In 2004, an individual was charged with possession of stolen goods and benefiting from proceeds of crime. Over a three year period, the individual stole goods, bought stolen goods, and then sold them on a commercial website. The proceeds passed through an IPS account attached to his commercial website user accounts. The individual sold over 9 000 items including DVDs, computer hardware and software, and Nintendo Gameboys, for a total of over USD 459 000. Local law enforcement found CAD 188 000 in savings bonds that had been purchased with a portion of the proceeds. The individual was sentenced to two years in jail and fined CAD 83 000.

Source: Canada.

Case 8: Use of cash vouchers to collect extortion money

An unknown criminal sent an extortionate letter to a food discounter in Germany and demanded EUR 250 000 in cash vouchers issued by an IPS provider situated in the UK. The IPS provider ensured that the cash vouchers were supplied in the form requested. The provider was able to monitor the voucher numbers in the computer system and reported the point of sale where one of the vouchers was used to the police. The money was not paid out because the criminal was already arrested in an Internet cafe after observation by the police in Germany.

Source: Germany

Case 9: Suspected laundering of illicit proceeds gained through the possible online sale of counterfeit goods

An individual, working in France for a foreign company, had an account with an IPS provider and a bank account in France. The foreign company suspected to be involved in the scheme also held a bank account in France.

The account of the individual was credited for 138 operations and an amount of EUR 357 245. Among those, 44 operations were credited via the IPS provider – for more than EUR 300 000. Those latest operations seemed to come from sales made on a commercial website. Shortly after, nearly all of the money was transferred to the foreign company account in France.

The individual was suspected to be a strawman possibly used by the company to open an IPS account since companies cannot open accounts with IPS providers in France. Besides, the individual was known by the French customs for being involved in counterfeiting. This individual was found to have sold 18 650 articles over a period of five years.

Source: France.

Case 10: Laundering of illicit proceeds through cash vouchers

In 2010, several cases of the following pattern were reported to the German FIU. The average amount of the laundered proceeds of crime ranged from EUR 4 500-6 000. Transaction numbers were initially "phished" by Trojans from a bank account held in Germany. The "phishing transfer" was made to a bank account held by the financial agent.

The financial agent withdrew the money – deducting his commission – in cash. He subsequently purchased cash vouchers (max. EUR 500 per voucher) of an IPS provider at various issuing offices, like petrol stations, newspaper kiosks. The purchase was anonymous without identification of the buyer. The financial agent (*i.e.,* third party) sent the voucher number or a scanned copy of the voucher by e-mail to the person giving instructions. The PIN code was used on the Internet for payment of goods and services and for gambling websites on the Internet.

The law enforcement authorities were unable to trace the transaction channels.

It should be noted that, in such a case, several vouchers for smaller amounts –also if purchased at different locations- can be used jointly and combined. A conversion to other digital currencies by using various exchangers acting on the Internet is also possible.

Source: Germany.

Case 11: Use of digital currency account to facilitate Internet fraud and money laundering

A young person, acting as a nominee, opened a digital currency account to enable him to receive the proceeds of Internet banking thefts from an offshore associate. He then attempted to redeem the value of the digital currency account by requesting the digital currency exchanger to provide him with postal money orders. In an effort to conceal his identity he informed the cash dealer that he had lost his passport and requested that the exchanger call a money service business and inform them that a person matching his description would present himself to collect the money orders at a particular time. It is believed that he was not going to send money offshore but would keep the proceeds for himself. He has been arrested and prosecuted.

Source: Australia.

Case 12: IPS providers and nominees used to purchase illegal substances and launder proceeds from their sales

A law enforcement investigation targeting smugglers of steroids, growth hormones and other illegal performance enhancing drugs identified a number of targets involved in importation and distribution, operating throughout Australia. The traffickers within Australia were found to be sending funds overseas totalling several hundred thousand dollars to purchase the illicit substances. Additionally, they were found to be receiving several thousand dollars each week in revenue from the sale of the illicit substances.

The traffickers used legitimately issued identities, obtained in false names, to open multiple post office boxes to receive the drugs. Internet chat rooms and forums were used for networking and for online ordering. Individuals used IPS providers and money remittance services in Australia to make payments which were mainly under AUD 1 000.

Overseas suppliers were aware of prohibited imports into Australia and intentionally provided false descriptions of the goods to circumvent controls. The traffickers enlisted friends and spouses to make payments on their behalf and chose different branches from which to make payments. They would also regularly change names and purposely misspell names and addresses. The full addresses of the overseas beneficiaries were never reported, only the region.

Law enforcement executed over 140 warrants across Australia throughout this operation.

Source: Australia.

c. Mobile Payment Services:

Case 13: Suspected use of mobile payments to move funds related to fraud

A victim was fooled into believing that the spouse was involved in an accident and the victim was asked to send money using a mobile payment provider to pay doctor‘s or hospital‘s bill.

Source: Philippines.

Case 14: Suspected use of mobile payments to move funds associated to telemarketing fraud

SMS messages were sent to victims claiming that they had won an electronic raffle. To claim their prize, they were asked to send money using a mobile payment provider to pay for taxes related to prizes.

Source: Philippines.

Case 15: Selling stolen phone credits through mobile P2P payments

In April 2010, an individual was sentenced in Cayman Islands for using stolen credit card information to illegally obtain phone credits which he then sold through the mobile P2P payment services. Although the amount of money was small, the individual was charged for money laundering activity under the Proceeds of Crime Law of Cayman Islands.

Source: Cayman Islands Attorney General´s Office.

4.2 Typology 2: Exploitation of the non-face-to-face nature of NPM accounts

125. Many NPMs rely on a business model where face to face customer contact is minimal or nonexistent. This can facilitate abuse by criminals for money laundering purposes.

126. In a number of cases NPM products were used to launder illicit proceeds gained from fraud following identity theft or from stealing money from bank accounts or credit/debit cards using computer hacking or phishing methods. Since the bank accounts or credit and debit cards were held in the names of legitimate customers, the criminals were able to use them as reference accounts for the funding of prepaid cards or IPS accounts. In such instances, the NPM providers could not detect that the transactions were actually not initiated by their legitimate customer, or detect any other suspicious activity.

127. In other cases, stolen or fake identities were used to create NPM accounts which were also used as transit accounts in the laundering of illegal proceeds, or to commit both criminal activities (*e.g.,* fraud) and money laundering at the same time.

128. The prepaid card or IPS account appeared to be mainly used as transit accounts in most cases. Once the illicit funds had been transferred to those accounts, criminals or their associates withdrew them at ATMs or spent the funds for purchases of goods (often on the Internet).

129. Although in many of the case studies presented below, the IPS or prepaid card provider could not have detected suspicious activity, some shortcomings in some providers´ identification and verification processes and monitoring systems is likely to have contributed to the illegal activity going undetected for some time. For example, in Case 27, although individual bank transfers appeared legitimate, the use of four reference bank accounts in different cities for the same IPS account should have raised suspicion with the IPS provider.

a. Prepaid Cards:

Case 16: Laundering of proceeds stolen from individuals' bank accounts

In 2007, six defendants were prosecuted for using stolen information to transfer money illegally from bank accounts to accounts controlled by the defendants, including prepaid cards. The defendants used a freely available software program to scan the Internet for vulnerable personal and commercial computers holding financial account information. The defendants then initiated fraudulent transactions to transfer funds from the victims' accounts to accounts created in the names of front companies. A portion of the illicit proceeds in the front company accounts was used to load prepaid cards which the defendants used to make purchases. The defendants were accused of laundering about USD 166 000 in eight months. The six defendants each pleaded guilty to conspiracy charges and were sentenced to from 3 to 36 months in prison.

Source: United States.

Case 17: Laundering of proceeds stolen from a company's payroll accounts

Two defendants were charged in 2009 with illegally accessing business computer systems via the Internet and fraudulently transferring funds from the victims' bank accounts to prepaid cards. The defendants allegedly used stolen account logins and passwords to access victims' online personnel management accounts, which, among other things, allowed users to establish direct deposit of employee wages. The defendants allegedly directed employee wage payments to the hackers' prepaid card accounts. Over a period of 11 months, the defendants allegedly transferred USD 19 967.43 in illegally obtained funds. The defendants have not yet been tried.

Source: United States.

Case 18: Laundering of phishing activity proceeds through prepaid cards

In this case, prepaid cards are used as transit accounts where criminals sent funds from bank accounts after identity theft of the accounts' holders. The phisher pretended to be the bank account holder and sent funds to the prepaid card that was issued in the name of a strawman. After the funds were transferred to the card, a corresponding amount of cash was withdrawn at ATMs.

Additional typology: Use of strawman.

Source: Italy.

Case 19: Laundering of counterfeiting and fraud proceeds through open-loop prepaid cards

Within a few months, the accounts of Mr. POL and company BE were credited by international transfers for some 500 000 EUR from a Swiss company acting as an agent and trader in securities. These funds were used to load prepaid cards. In most cases, these cards were loaded with EUR 5 000 (maximum limit). Mr. POL claimed to have loaded these prepaid cards because he had given them to his staff for professional expenses. As soon as the money was loaded on the cards, the card holder quickly withdrew the money by repeatedly withdrawing cash from ATM machines.

Mr. POL was the subject of a judicial investigation regarding counterfeiting and fraud. Given the police information on Mr. POL, the funds from Switzerland may have been of illegal origin and linked to the fraud and counterfeiting for which Mr. POL was known. This hypothesis was confirmed by the ingenious scheme (international transfers, prepaid cards and cash withdrawals) used to repatriate funds to Belgium.

Source: Belgium.

Case 20: Use of "ghost employees" to launder illicit funds through prepaid cards

In 2009, a defendant was charged with embezzling from his employer and laundering the stolen funds through prepaid payroll cards. The defendant, a manager with a janitorial service, interviewed job applicants for the purpose of stealing their personal information which he used to create fake employment positions which came with prepaid payroll cards. The defendant kept the payroll cards, using them to withdraw money from ATMs and purchase goods. In three years, the defendant laundered about USD 200 000. The defendant has not yet been tried.

Source: United States.

Case 21: Credit card fraud and money laundering

In 2006, two defendants were prosecuted for using 61 stolen credit card account numbers to fund —virtual prepaid cards," which provide an account number, expiration date, and card verification value, but no physical card for consumer non-face-to-face transactions. The defendants then used these —virtual cards" to overpay their tuition at a university in the United States. The university issued a check for USD 31 045, the amount of the over-payment, thus helping the defendants to launder their illicit proceeds. One defendant pleaded guilty to wire fraud and was sentenced to 38 months imprisonment and five years supervised release. The other defendant was convicted of making a false statement in a loan application, money laundering, mail fraud, aggravated identity theft and possession of unauthorised access devices. He was sentenced to 61 months imprisonment and five years supervised release.

Source: United States.

Case 22: Laundering of proceeds gained through ID theft

In 2006, a defendant who managed a prepaid card program was prosecuted for using his prepaid card program to launder illicit proceeds for identity thieves. The identity thieves created 21 card accounts with stolen identity information, and loaded the cards with approximately USD 1 million stolen from victims' bank accounts. The bank account information had been stolen from user accounts of one IPS provider. The identity thieves withdrew funds from the prepaid card accounts at ATMs in Russia. The defendant pleaded guilty to money laundering charges and was sentenced to 120 months imprisonment.

Additional typology: Complicit NPM provider or program manager.

Source: United States.

Case 23: Fraud and money laundering

In 2007, three defendants were prosecuted for illegally accessing a payment processor and initiating fraudulent transactions resulting in approximately USD 700 000 being credited to 80 prepaid cards. The defendants allegedly operated from a hotel room using a laptop computer, a payment card encoder, and the phone line to access a commercial payment processor, misrepresenting themselves as businesses entering refund transactions, and using the card encoder to transfer the value of the fraudulent refunds to their prepaid cards. The defendants withdrew approximately USD 200 000 a day of the value loaded onto the prepaid cards at nearby ATMs and by purchasing Postal money orders. The principal defendant was convicted, but has appealed the conviction. Two other defendants plead guilty.

Source: United States.

Case 24: Fraud and money laundering

In 2009, three defendants were charged with stealing USD 5 million by hacking into a prepaid card company's database, stealing card information and manipulating account balances and transaction limits. The defendants allegedly used the card information to create duplicate prepaid cards and used them to withdraw money from ATMs throughout the world. In one month the defendants withdrew USD 750 000. Two defendants pleaded guilty to conspiracy, money laundering, bank fraud and counterfeit access device product but have not yet been sentenced. A third defendant pleaded guilty to conspiracy and access device fraud charges but has not yet been sentenced.

Source: United States.

b. Internet Payment Services

Case 25: Laundering of illicit proceeds through a digital currency provider

In 2009, the suspect illegally accessed individuals' Internet banking accounts and instructed the computer system to remit about JPY 740 000 (USD 8 300) to a digital currency exchanger to get e-currency units. Then, the suspect sold off a portion of the e-currency units to another digital currency exchanger to get real money. Finally the suspect made the digital currency exchanger deposit the money into some bank accounts that were acquired illegally and controlled by him.

Source: Japan.

Case 26: Fraud scheme and money laundering conducted through Internet payment services

An individual devised a scheme to defraud users seeking to purchase textbooks on a commercial website. The individual created approximately 384 phony bank accounts which were opened at a bank in Jurisdiction Z, for non-existent employees who he indicated to the bank, would sell college textbooks. The individual then used the bank account information to open approximately 568 seller accounts with the commercial website using P2P online payment services (i.e., an IPS provider).

The defrauder advertised the college textbooks for sale on all of the phony commercial website seller accounts he had created. Buyers, believing they were purchasing books from the commercial website sent over USD 5.3 million in payment to the seller accounts, using the IPS provider.

The defrauder subsequently transmitted the illicit proceeds from the IPS provider seller accounts to several Singapore-based bank accounts.

The law enforcement agency from Jurisdiction Z contacted Singapore's law enforcement agency, who then responded quickly to seize the tainted funds. With the close cooperation between the law enforcement agencies, the seized funds were successfully repatriated to the victims. The defrauder was also charged for wire fraud in Jurisdiction Z.

Source: Singapore.

Case 27: Funds stolen from bank accounts laundered through IPS accounts

A computer criminal stole the victim´s personal data for online banking (including customer and account data) then opened a fraudulent account with an IPS provider under the name of the victim. The personal data provided in the opening of the account (phone number, home address, date of birth etc.) were fake. The email addresses given were issued by so-called —free providers" that do not conduct any identification or verification of their customers themselves.

The criminal named a reference bank account for funding the fraudulent IPS account. This reference account was the victim's.

Then the criminal effected a fraudulent transaction from the victim´s reference bank account to the fraudulent IPS provider account. As the funds came from the referenced bank account, the transaction appeared legitimate to the IPS monitoring system. The received funds were transferred to other accounts held with the IPS. The law enforcement authorities were neither able to trace the money flows nor find out the criminals´ identity.

The criminal repeated this scheme with several victims, but always using the same IPS account. Thus, he changed the reference bank account for this IPS account four times in two months; the four named reference bank accounts were held with different banks in different cities.

Source: Germany.

4.3 Typology 3: Complicit NPM providers or their employees

130. A number of submitted cases feature prepaid card and IPS providers or their employees, which are controlled by criminals and wilfully or recklessly assisting money laundering and terrorist financing activities. In such cases, market entry restrictions such as fit and proper tests have failed or are not applicable to the respective entity under that jurisdiction.

131. In some instances (case studies #28, #30 and #31), both IPS and prepaid card providers were suspected to be complicit and colluding in facilitating the laundering of illicit proceeds.

a. Prepaid Cards

Case 28: Suspected use of open-loop cards & online payment systems to launder drug proceeds

This case was generated following the receipt of information from a foreign FIU which indicated that a number of individuals were charged for laundering millions of drug proceeds through a company providing open-loop prepaid cards in Country A. The funds were suspected to be loaded on prepaid cards and moved, for example, from Country A to South America, that is, back to the drug traffickers. Other criminal activities were also suspected to be the source of the illicit funds.

Two of the individuals, associated to the prepaid card company, were found to have addresses in both Country A and Canada, and had opened bank accounts and established at least one company in Canada.

The prepaid card company was located in Country A, but held many accounts in that country and in Canada. The bank accounts in Country A and in Canada were used to receive funds from various individuals and entities located in a number of different countries in Central America, Europe, Caribbean, Africa, Asia, South Asia as well as in Country A and Canada.

It was further revealed that two Canadian Internet Payment System providers (IPS) sent funds to the same prepaid card company in Country A. Based on available information, it appeared that both IPS offered a prepaid card service to their clients, which was provided by the prepaid card company in Country A.

One of the Canadian IPS was the subject of another case in which it was suspected of facilitating the laundering of Ponzi scheme proceeds.

Suspicious transactions included third-party cash deposits and international electronic funds transfers (EFTs). Most of the funds received in the Canadian accounts were transferred back to the accounts held in Country A by the prepaid card company and two other associated companies also located in Country A.

Additional typology: Third party funding

Source: Canada.

Case 29: Embezzlement activities and money laundering

In 2007, a defendant was prosecuted for embezzling more than USD 375 000 from his employer, a national chain convenience store, by fraudulently loading the proceeds onto prepaid cards. The defendant allegedly processed routine transactions that involved adding value to prepaid card accounts which appeared to be held by actual customers, but did not take in funds to cover the transactions. Although these transactions were processed by the prepaid card company, the defendant allegedly ensured that the transactions were not being recorded internally to avoid the detection of his embezzlement.

Source: United States.

b. Internet Payment Services

Case 30: Suspected use of IPS (including digital precious metals) and open-loop prepaid cards to launder proceeds of fraud schemes

This case was initiated following the receipt of information from law enforcement and a foreign financial intelligence unit (FIU) which indicated that a Canadian IPS provider, its subsidiary in the United States and other associated entities were suspected of laundering illicit proceeds derived from pyramid schemes (Ponzi schemes) and telemarketing fraud schemes.

It was revealed that the Canadian IPS also had subsidiaries in a European and an Asian country. In addition, it was found that at least five digital currency exchangers (located in Canada, the United States and a Northern European country), two digital precious metals providers (United States), three open-loop prepaid cards providers (in Canada and the United States) were knowingly or unknowingly used in this complex money laundering scheme. One of the prepaid card providers was found to have offered its product for the use of a virtual world´s gamers who could fund their virtual world accounts and withdraw their virtual currencies into real currencies directly at ATMs.

Generally, funds sent from foreign countries to Canadian bank accounts held by the Canadian IPS and prepaid cards providers were either used to load prepaid cards or to settle accounts* with other IPS or prepaid card providers located in other countries. In some instances, suspicious funds entered the financial system in Canada and appeared to be then layered through other countries, sometimes coming back to Canada.

Suspicious transactions included large deposits of cash and bank drafts often followed by international electronic funds transfers (EFTs) and the layering of illicit funds through EFTs sent between various bank accounts.

Source: Canada.

* In most instances, the reporting of these transactions were provided by financial institutions and involved the transfer of funds between the pooled bank accounts held by the IPS and prepaid card providers. Information about clients of the IPS and prepaid card providers were not available.

Case 31: Laundering of illicit funds through digital currency and prepaid cards

Within the scope of an investigation, an international group of offenders transferred illegally- obtained money through a financial service provider to Eastern European countries, where it was withdrawn by members of the group and converted to electronic currency through digital currency exchangers.

The digital currency was then transferred to accounts held by offenders with a financial service provider handling electronic currency in the countries involved. In co-operation with a bank located in an offshore region this financial service provider issued MasterCard "Cirrus-cards" (prepaid cards), which were acquired anonymously and loaded with electronic currency. The cards could be used worldwide in payment transactions at points-of-sale (POS) and cash dispensers which accept "Cirrus".

In this way, the flow of illegally obtained money was effectively concealed, and the offenders were able to access the secure illicit money promptly and anonymously.

Source: Germany.

Case 32: Laundering of illegal online gambling through an IPS

In 2007, an Internet payment business based in the Isle of Man and publicly traded on the Alternative Investment Market (—AIM") of the London Stock Exchange — admitted to criminal wrongdoing and agreed to forfeit USD 136 million in criminal proceeds as part of an agreement to defer prosecution.

The IPS business participated in a conspiracy to promote illegal (according to U.S. legislation) Internet gambling businesses and to operate an unlicensed money transmitting business.

Source: United States.

Case 33: Money laundering through a digital precious metals provider

In 2008, an Internet-based digital currency business, and its three principal directors and owners, pleaded guilty to criminal charges relating to money laundering and the operation of an illegal money transmitting business.

Several characteristics of the digital currency business operation made it attractive to users engaged in criminal activity, such as not requiring users to provide their true identity, or any specific identity. The digital currency business operation continued to allow accounts to be opened without verification of user identity, despite knowing that the business was being used for criminal activity, including child exploitation, investment scams, credit card fraud, money laundering and identity theft. In addition, the digital currency business assigned employees with no prior relevant experience to monitor hundreds of thousands of accounts for criminal activity. They also participated in designing a system that expressly encouraged users whose criminal activity had been discovered to transfer their criminal proceeds among other accounts of said digital currency business. Unlike other IPS providers, the digital currency business operation did not include any statement in its user agreement prohibiting the use of its services for criminal activity.

Source: United States.

4.4 Cross-border transport of prepaid cards

132. The 2006 FATF report featured another perceived risk / typology for the abuse of prepaid cards, namely the replacement of illicit cross-border movement of cash with the cross-border transport of prepaid cards. The best example to illustrate this does not involve open-loop prepaid cards, but traditional bank-issued debit cards. In 2007 in the United States, two defendants were charged with money laundering in connection with the transfer of drug profits to Colombia via the ATM network. The defendants allegedly instructed family members, friends and others to establish 380 bank accounts in six states. The defendant then made deposits between USD 500 and USD 1 500, allegedly depositing more than USD 100 000 in 112 bank accounts in a single day. For each account, the account holder obtained two ATM cards. The defendants kept one ATM card and mailed the other to Colombia where the funds were withdrawn via ATMs.

133. There are similar cases involving the cross-border movement of closed-loop payment cards as well as a few instances involving the cross-border movement of open-loop prepaid cards. For example:

- Prepaid cards were sent from the US to Canada with no balance, and a limit of USD 1 000. Although the cards were sent to Canada they were redeemable only in the United States. These cards were suspected to have been fraudulently purchased with cloned credit cards.

- In another instance, prepaid cards were sent from South America to Canada. These cards were sent to one individual, but were in the name of a number of other individuals. The issuer of the cards had surfaced in another investigation in the past. The individual to whom the cards were sent had also surfaced in the past and been of interest to European and American law enforcement authorities. As a result of the investigation, the cards were cancelled as the bank did not wish to tarnish its reputation.

- In Australia, the holder of a prepaid card was found to have regularly loaded value by paying cash just below the AUD 10 000 reportable threshold. A second card linked to the same account was sent overseas where the funds were withdrawn through ATMs. The process was repeated, with more than AUD 100 000 laundered through the scheme.

- An Australian investigation identified an individual as the holder of 12 legitimately issued driver's licences under fictional identities, as well as one licence issued under his real identity. In addition, the individual was identified as being in possession of numerous false identity documents and foreign passports. When the individual was detained by law enforcement officers he was found to be carrying approximately AUD 140 000 in cash generated by criminal activities and 46 prepaid cards. A search warrant at a storage unit rented in his name located further prepaid cards and gift cards. It was alleged the money was being taken to India for the purposes of money laundering. It appears that the individual purchased these cards, which are available over the counter at post offices and service stations in values of AUD 50 and AUD 100. Markings on some of the cards indicated they were valued at AUD 500, which suggested that they were purchased online.

134. While the first two aforementioned examples raise concerns about potential misuse of prepaid cards for money laundering purposes, they could not clearly be linked to money laundering or terrorist financing. However, the last two examples have been linked to money laundering and the fourth one also demonstrates how anonymous prepaid cards can be used in such criminal schemes.

135. Two of the case studies submitted (***cases 22 and 28***) also imply that cross-border movement of prepaid cards was involved, as the funds were withdrawn from the card in a jurisdiction different from

where they had been loaded. However, there are no additional details that would confirm that assumption (*e.g.,* detecting or confiscation of cards due to cross-border controls).

136. Based on the above, it appears that since 2006, a limited number of cases involving cross-border transport of prepaid cards have started to emerge. However, given the small number of examples available to date, the project team believed that it may be premature to combine these cases under one typology on its own. The lack of examples can be explained by the fact that prepaid cards are neither considered currency nor bearer negotiable instruments in the sense of FATF Special Recommendation IX in most jurisdictions. Accordingly there is no obligation to make a declaration when crossing borders. It is also very difficult for customs officers to easily differentiate prepaid cards from regular credit cards given that both share very similar physical attributes.

4.5 Red Flags

137. The analysis of the case studies identified red flags which are relevant to all NPM products and services. In addition, a small number of red flags appear to be associated predominantly with suspected complicit prepaid card providers. A few case studies are referred to as examples of the red flags and do not constitute the complete list of cases associated with each of the red flags.

138. Red flags will be indicators of suspicious activity where a product's actual use deviates from its intended use or does not make economic sense. For example, cash withdrawals in foreign jurisdictions will be expected where the product is a prepaid traveller card, but unusual where the product is marketed to minors. Red flags should therefore not be applied unthinkingly, but tailored to the product's characteristics.

All NPMs:

- Discrepancies between the information submitted by the customer and information detected by monitoring systems (***case 19***).
- Individuals who hold an unusual volume of NPM accounts with the same provider (***cases 21 and 23***).
- A large and diverse source of funds (*i.e.,* bank transfers, credit card and cash funding from different locations) used to fund the same NPM account(s) (***cases 6, 7, 16 and 17***).
- Multiple reference bank accounts from banks located in various cities used to fund the same NPM account (***case 27***).
- Loading or funding of account always done by third parties (***cases 1 and 3***).
- Numerous cash loading, just under the reporting threshold of USD 10 000 (*i.e.,* structured loading of prepaid cards), of the same prepaid card(s), conducted by the same individual(s) on a number of occasions (***case 5***)
- Multiple third party funding activities of a NPM account, followed by the immediate transfer of funds to unrelated bank account(s) (***cases 9 and 26***).
- Multiple loading or funding of the same accounts, followed by ATM withdrawals shortly afterwards, over a short period of time (***cases 18 and 19***).

- Multiple withdrawals conducted at different ATMs (sometimes located in various countries different from jurisdiction where NPM account was funded) (***cases 4 and 24***).

- NPM account only used for withdrawals, and not for POS or online purchases (***cases 18 and 19***).

- Atypical use of the payment product (including unexpected and frequent cross-border access or transactions) (***cases 2 and 24***).

Specific to suspected complicit prepaid card providers:

- Large number of bank accounts held by the same prepaid card company (sometimes in different countries) apparently used as flow-through accounts (may be indicative of layering activity) (***case 28***).

- Prepaid card company located in one country but holding accounts in other countries (unexplained business rationale which could be suspicious) (***case 28***).

- Back and forth movement of funds between bank accounts held by different prepaid cards companies located in different countries (may be indicative of layering activity as it does not fit the business model) (***case 30***).

- The volume and frequency of cash transactions (sometimes structured below reporting threshold) conducted by the owner of a prepaid card company do not make economic sense (***case 30***).

CHAPTER 5: LEGAL ISSUES RELATED TO NPMS

139. This chapter addresses how the provision of NPMs is regulated in different jurisdictions.[59] **Section 5.1** introduces different regulatory approaches that are currently being applied to NPMs. **Section 5.2** deals with specific challenges for regulators, law enforcement and supervisors.

5.1 Regulatory models applied to NPMs

140. The FATF Recommendations require all entities or persons conducting certain activities to be subject to AML/CTF obligations and oversight. These include entities or persons transferring money or value, or issuing and managing means of payment.[60] Most NPM providers are therefore financial institutions and should be regulated and supervised in line with Recommendation 23 or Special Recommendation VI.

141. In NPM business models with a strong segmentation of services, *i.e.,* with several entities carrying out the financial activity jointly, it can be difficult to judge whether the respective contribution of one single entity in the chain is sufficient to designate it as a financial institution (and consequently subject it to regulation and supervision). Examples for this are the business models of digital currency providers,[61] but also the use of agents.[62] In both examples, different views are taken on whether these activities should be regulated and supervised or not.

142. Analysis of the questionnaire responses for this project showed that there are three different approaches to regulating New Payment Methods. In some jurisdictions NPM providers are not subject to AML/CFT regulation at all, or only certain types of NPMs are regulated. In others, the regulatory regime developed for more traditional financial institutions (such as banks or Money Service Businesses) also applies to NPM providers, or they are subject to new regulatory regimes specific to NPM providers.

5.1.1 Not subject to regulation

143. In some jurisdictions certain NPMs are not subject to regulation. In others, the degree of regulation differs depending on the type of NPM.

---

59 The World Bank is preparing work on regulation of "innovative retail payment products", which includes the NPM services featured in this report. To this end, a questionnaire has been launched in July 2010. The World Bank survey builds upon the *Survey on Electronic Money and Internet and Mobile Payments*, published in 2004 by the Committee on Payment and Settlement Systems (CPSS) of the Bank for International Settlements, Basel.

60 FATF Glossary – "financial institution".

61 This is discussed in more detail below, see para. 170 ss.

62 This is discussed in more detail below, see para. 175 ss.

144. Issuers of **prepaid cards** are subject to both prudential and AML regulation in every jurisdiction that responded to the project questionnaire and that has domestic issuers of such cards.[63]

145. However, where there is a segmentation of services through the use of third parties that do not fit into the traditional definitions of financial institutions, these are usually not subject to regulation (*e.g.,* card program managers, retailers etc.). Third parties include agents and outsourcing arrangements. This issue is discussed in more detail below (See chapter 5.2 (*The use of agents / Outsourcing CDD measures*), para. 175 ss.).

146. As regards **Internet payment services**, 15 jurisdictions have reported Internet payment service providers seated in their jurisdiction. Of these, four jurisdictions did not require providers to obtain a licence or register for the provision such services.[64] As a result, there are no legal AML/CFT obligations for such providers in these jurisdictions. One of these unregulated providers (a digital currency provider) holds about 11 million customer accounts, serving customers from all over the world. While other unregulated providers may also operate globally, they do not reach the same size.

147. Third parties associated with Internet payment services are usually needed for funding the IPS account or withdrawing funds from it. They can be regulated or unregulated entities. Regulated entities are themselves subject to AML obligations and include traditional money remittance businesses (*e.g.,* Western Union), prepaid card issuers or banks.

148. Unregulated third parties are not normally within scope of AML legislation and include digital currency exchangers, which are a vital component of digital currency providers´ business models as they sell digital currencies for regular money or other e-currencies.

149. The provision of **mobile payment services** is regulated in most of the 15 jurisdictions that have identified domestic providers of such services.[65] However, in some jurisdictions the service is provided by unregulated entities (such as telecommunications companies) which have no legal AML/CFT obligations.

In its Working paper no. 146,[66] the World Bank has recommended that mobile payment services providers should be subject to regulation:

"1. The FATF may wish to consider treating telephone companies that facilitate transactions as financial institution (...).

2. After this, assessors should consider mobile financial services when applying the FATF methodology to country AML and CFT compliance (...)."

150. Mobile payment service providers often use agents for the distribution of their services, opening new customer accounts, as well as receiving and paying out cash from or to customers. Such agents typically are numerous and are themselves not subject to immediate regulation.

---

63 See Appendix A, *Prepaid Cards*, Table B.

64 See Appendix A, *Internet Payment services*, Table B.

65 See Appendix A, *Mobile payment services*, Table B.

66 World Bank (2008), p. 53.

5.1.2 Subject to existing regulation for traditional financial services

151. Some jurisdictions apply the same regulatory regime to NPM service providers as they apply to traditional financial institutions. As a consequence, in these jurisdictions, the provision of NPM services is restricted to banks or other traditional financial institutions.

152. For all jurisdictions that have submitted a response to the questionnaire, **open-loop prepaid cards** may only be issued by regulated financial institutions due to regulatory requirements. It is also the policy of card technology providers (*e.g.,* VISA, MasterCard) to only cooperate with such regulated entities.[67]

153. Although not enough details were provided by jurisdictions when responding to the questionnaire to provide exact numbers, it appears that in relation to **Internet payment services** some jurisdictions subject IPS providers to the same legal and regulatory requirements as traditional financial institutions, while others restrict IPS provision to banks or classify IPS providers as money services businesses or remittance providers.[68]

154. Finally, some jurisdictions restrict **mobile payment services** to banks or co-operation between banks and telecommunication companies. Such "bank-based models" usually result in each customer having an individual bank account which they can access through the mobile phone, rendering such services a type of mobile banking rather than mobile payment in the sense of this report.

155. Even though such mobile banking schemes fall outside the scope of this project, they do have to cope with some of the same issues and risks as mobile payment services (especially as regards such risks resulting from non-face-to-face business and the use of agents, or the application of simplified CDD measures), as can be seen from the following examples.

Box 7
Example: Mexico

As part of the efforts to promote financial inclusion, Mexico´s financial authorities have implemented a Mobile Banking model, making use of the existing telecommunications network to provide elemental banking services to the population, also in rural and remote areas.

The Mexican authorities distinguish between two types of Mobile banking:

In the classic mobile banking model, mobile phone users can link their mobile phone to an existing bank account (debit or credit card).

In the newly introduced mobile payment* model, phone users may open (bank) accounts at a telecommunications provider´s who acts as a banking agent. These so-called –low transactional accounts" are limited to basic banking services (deposits, withdrawals and incoming/outgoing payments), and transactions are limited to approx. 700 USD per month, resulting in lower CDD requirements.**

* The term –mobile payment" used by the Mexican authorities is not identical with the term –mobile payment" used in this report; see glossary.

** See 5.2, *The definition of low risk cases*, para. 161 for more details.

---

67 These are mostly credit institutions, but may also be other types of regulated institutions, *e.g.,* electronic money institutions in the EU (see 5.1.3, *Subject to specifically designed regulation*).

68 See Appendix A, Table B and C for Internet Payment services.

Box 8
Example: South Africa

In South Africa, a bank entered into a partnership with a mobile phone service provider to provide a banking service where accounts could be opened and activated via the phone without personal contact with the bank or a representative of the bank. The South African Reserve Bank has issued a Guidance note to determine the minimum set of criteria that must be met in the identification and verification process for such account openings.[69]

5.1.3 Subject to specifically designed regulation

156. Some jurisdictions have implemented a dedicated regulatory regime for providers of NPMs. For example, the EU´s "Electronic Money Directive" introduced "electronic money institutions", a new category of financial institutions. These are subject to the same AML obligations as traditional financial institutions, but the prudential requirements differ in recognition of restrictions imposed on e-money institutions´ activity.

Box 9
The EU concept of "electronic money"

According to Article 2 no. 2 of the revised EU Electronic Money Directive(EMD)* the term electronic money (or "e-money") is defined as follows:

"'electronic money' means 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;..:"

This definition has been carefully chosen to ensure technological neutrality and to encompass business models where the value is stored either individually on a customer´s device (such as a card or a mobile phone) or collectively on a central server. As a consequence, the term electronic money covers all types of NPMs discussed in this report.

The issuance of e-money is reserved to banks and "electronic money institutions", a new type of financial institution created by the EMD. Both types of financial institutions are subject to prudential and AML/CFT supervision. Compared to banks, the scope of activities in which electronic money institutions may engage is limited to a) issuing electronic money; b) the full range of payment services as defined in the EU Payment Services Directive**; c) provision of credit facilities linked to the payment services provided; and d) other business activities other than issuance of electronic money. However, e-money institutions cannot accept deposits. This constraint in activities is counterbalanced by an alleviation of prudential requirements for electronic money institutions. This is intended to facilitate market entry to newcomers.

The EMD, in conjunction with the 3rd Money Laundering Directive, leaves it to each member state´s discretion to allow simplified Customer Due Diligence for low risk products that do not exceed certain thresholds. The vast majority of member states has made use of this option to allow simplified Customer Due Diligence.***

* Official Journal of the European Union (2009)
** Official Journal of the European Union (2007)
*** For more details on the EMD and its interconnectivity with the Payment Services Directive, see Appendix D.

157. The United States is currently considering the introduction of a new subtype of money services business called "provider of prepaid access".[70] Unlike the EU legislation described above, this legislative initiative does not intend to facilitate market entry to new competitors in the market for payment services, but to close what has been identified as a gap in regulation.

69 South African Reserve Bank (2008)

70 See *Box 11 – United States* on FinCen´s *Notice of Proposed Rulemaking*.

5.2. Specific issues in regulation and supervision of NPM

158. Where NPM service providers are regulated, supervisors, law enforcement agencies and legislators are faced with a number of legal and practical challenges. Some guidance already exists in relation to some of these issues, but others have yet to be addressed.

The issues highlighted in the following are:

- Simplified Customer Due Diligence
  - The definition of low risk cases
  - Exemptions from AML obligations: Low risk financial activities and institutions -vs.- Low risk customers/products
  - Non-face-to-face business models: level of required CDD measures
- Digital currency providers: the use of exchangers
- The use of agents / outsourcing CDD measures
- "Hybrid" service providers
- Suspicious transaction reporting in cross-border scenarios
- Law enforcement and supervisory action against foreign providers
- Identification of secondary card holders

159. This list is not comprehensive or exhaustive; it focuses on issues related to the prevention and prosecution of Money Laundering and Terrorist Financing, regulation and other aspects of the FATF 40 + 9 Recommendations.[71]

Simplified Customer Due Diligence

160. Several jurisdictions allow financial institutions to apply simplified or reduced Customer Due Diligence measures in cases of low risk. There is however no uniformity of approach or a shared understanding with regards to (1) when a product can be considered low risk and (2) to what degree CDD measures can be reduced.

The definition of low risk cases

161. Several jurisdictions have identified in their legislation certain low risk scenarios in which simplified due diligence can be applied. With regard to NPMs, most jurisdictions rely mainly on value limits and transaction thresholds to define low risk scenarios, while others look at more risk factors including *e.g.,* the cross-border functionality of a product, the funding mechanisms and the usage limits of a product (see for example the South African approach in the text box below). According to the approach promoted by this report, a risk assessment should consider as many risk factors (as listed in the

[71] Other challenges may include the creation of fair competition and a level playing field, consumer protection aspects etc.

risk matrix above)[72] as possible in order to be more reliable and meaningful. The FATF standards currently do not provide guidance on or definitions of low-risk scenarios or related monetary thresholds specifically for NPM. Some private sector representatives have indicated that such guidance would be welcome.

162. Where jurisdictions use value limits to designate low risk situations, they differ significantly among jurisdictions, ranging from USD 5100 per year (Switzerland),[73] or USD 700 per month (Mexico)[74] to USD 1 000 per day (USA).[75]

Box 10
European Union:

The vast majority of member states has made use of the option to allow simplified Customer Due Diligence according to Article 11 par. 5d of the 3rd Money Laundering Directive* as amended by the second e-money Directive**, which states that member states may allow their institutions to apply simplified CDD measures with regard to electronic money

—where, if it is not possible to recharge, the maximum amount stored electronically in the device is no more than EUR 250, or where, if it is possible to recharge, a limit of EUR 2 500 is imposed on the total amount transacted in a calendar year, except when an amount of EUR 1 000 or more is redeemed in that same calendar year upon the electronic money holder's request in accordance with Article 11 of Directive 2009/110/EC. As regards national payment transactions, Member States or their competent authorities may increase the amount of EUR 250 referred to in this point to a ceiling of EUR 500.—

* Official Journal of the European Union (2005)
** Official Journal of the European Union (2009)

Box 11
United States

According to a US Notice of Proposed Rulemaking*, certain low value prepaid programs shall not be subject to the new regulation:

—Providing prepaid access to funds subject to limits that include a maximum value (...)where such maximum value is clearly visible on the prepaid access product:

(i) Not to exceed USD 1 000 maximum value that can be initially loaded at the time of purchase of the prepaid access;

(ii) Not to exceed USD 1 000 maximum aggregate value (such as through multiple transfers of value to a single prepaid access product) that can be associated with the prepaid access at any given time; and

(iii) Not to exceed USD 1 000 maximum value that can be withdrawn from the prepaid access device on a single day.

The reason for exempting such prepaid programs is that it is believed —that the potential for misuse is slight". **

* Federal Register (2010)
** Federal Register (2010), p. 40.

72 See above para. 63 ss.

73 Amount converted into USD for reasons of comparability; the actual threshold is CHF 5 000.

74 Amount converted into USD for reasons of comparability; the actual threshold is 2 000 UDIs ("inflation-indexed units").

75 Some of the following value limits refer to other products than NPMs, *e.g.,* bank accounts. However, they were included here to give a better overview over different approaches to handling low risk.

Box 12
South Africa:

In May 2010 South Africa has enacted an exemption for low risk prepaid products which exempts financial institutions issuing prepaid products from certain CDD obligations if the following criteria are met:

—(a) the value of every individual transaction initiated through the use of the prepaid payment instrument cannot exceed ZAR 200;

(b) the available balance cannot exceed ZAR 1 500 at any time;

(c) the monthly turn-over of value loaded onto the prepaid instrument cannot exceed ZAR 3 000;

(d) can only be used to purchase goods or services in the Republic;

(e) the reloading of value to the prepaid instrument to enable use or further use of the prepaid instrument can only be done by means of an online system requiring the client to enter a personal identification number;

(f) the use of the prepaid instrument cannot enable the remittance of funds, the withdrawal of cash or the receipt of cash as part of a transaction for the payment of goods or services or in any other form whatsoever." *

* South African Government Gazette (2010)

Box 13
Mexico:

In order to promote the financial inclusion of in particular the low income population, Mexico introduced a simplified regime of low risk products with simplified KYC and CDD requirements for specific transactions, products and financial services. These low risk products include the following two subtypes of bank accounts that are different from traditional bank accounts:

—Low Transactional accounts" are restricted to natural persons whose monthly deposits transactions are below 2 000 Units of Investment —UDI (approx. USD 700). Simplified rules apply for KYC, account opening and Monitoring and Reporting.*

—Low Risk Accounts" are available for natural and legal persons whose accumulated transactions, including deposits and withdrawals, on a monthly basis do not exceed 40 000 UDIs (approx. USD 14 000). Simplified rules similar to those for —low transactional accounts" apply to these accounts, but more customer data needs to be collected when opening such an account.**

* The file requires to be integrated only with the client basic data (name, address and birth date) and it is not required to maintain a copy of the documentation. However, there is the obligation for the applicant to actually display a formal ID when initially opening this type of account.

** The file requires to be integrated with the client´s whole list data requirements, and it is not required to maintain a copy of the documentation. However, there is the obligation for the applicant to actually display a formal ID when initially opening this type of account.

5.2 Exemptions from AML obligations: Low risk financial activities and institutions -vs.- Low risk customers/products

163. The current FATF standards provide some flexibility that allow jurisdictions to allocate resources in the most efficient way to address the most pressing ML/TF risks. To deal with low ML/TF risks, the standards provide two options that must be clearly differentiated: (1) partial or full exemption from AML regulation and supervision for low risk activities and institutions; and (2) simplified or reduced CDD for low risk customers or products.

1. According to the glossary of the FATF Methodology (see definition of the term "financial institution"), there are two theoretical possibilities for partial or full exemption from regulation and supervision:

    a. Jurisdictions are permitted to exempt from or limit the application of the standards for **certain financial activities** on the basis of a proven low risk, and only in strictly limited and justified circumstances. Such an exemption would apply to the respective financial activity as such and automatically affect all institutions carrying out such an activity. As regards NPM, the project team is not aware of any jurisdictions that have

declared the provision of NPM as such exempt (fully or partially), based on a proven low risk.

Box 14
Example: Australia

Under the Australian AML/CTF Act, issuing a stored value card, or increasing its value, only constitutes a designated service if the value stored on the card is greater than:

- AUD 1 000, if whole or part of the monetary value stored on the card may be withdrawn in cash; or
- AUD 5 000, if no part of the monetary value stored on the card may be withdrawn in cash.

Where stored value cards are issued under amounts of AUD 1 000, the services associated with them are not designated services for the purposes of the AML/CTF Act and consequently not subject to any of the AML/CTF obligations imposed by that Act.

b. In addition, when a financial activity is carried out by a person or entity **on an occasional or very limited basis** (having regard to quantitative and absolute criteria) such that there is little risk of money laundering or terrorist financing activity occurring, a jurisdiction may decide that the application of anti-money laundering measures is not necessary (either fully or partially) for that particular person or entity. This provision aims at non-financial institutions that occasionally carry out financial activities on the side (*e.g.,* hotels that occasionally exchange small amounts of currency for their guests).

2. Where a certain financial activity is not exempted from AML regulation and supervision, Recommendation 5 requires that financial institutions should undertake customer due diligence measures. The extent of such measures may be determined on a risk-sensitive basis, allowing for the application of **reduced or simplified CDD measures** in cases of low risk.

Box 15
Example: EU

According to EU legislation, the issuing of electronic money is a regulated financial activity, regardless of any value limits or thresholds that may apply to a certain product. Accordingly, issuers of electronic money are subject to the member states´ national AML/CFT laws.

The 3rd EU Money Laundering Directive grants member states the opportunity to allow their financial institutions to apply simplified CDD measures in designated cases of low risk. For the issuing of electronic money, concrete low risk scenarios are defined by Art. 11 para 5 lit. d of the Directive (see above para. 161 for more detail).

164. Although the term "simplified CDD measures" has not been defined (neither by the FATF standards nor by most of the national regulatory regimes or guidance), an exemption from CDD measures can only be granted in the cases described above under option 1), not in the cases of option 2). As a result, where firms carry out a designated financial activity and therefore are subject to AML/CFT obligations, exemptions from the CDD requirement are considered a breach of FATF Recommendation 5[76]. Accordingly, over the last five years more than ten jurisdictions have been criticised in their mutual evaluation reports for granting exemptions from CDD measures in low risk cases.[77]

165. In spite of this, several jurisdictions argue that in the absence of a definition of "simplified or reduced CDD" in the FATF standards an exemption can be considered as a case of simplified or reduced

---

[76] The FATF has also confirmed this understanding of Recommendation 5 in several publications on the Risk Based Approach (*cf. Guidance on the Risk-Based Approach to combating Money Laundering* and *Terrorist Financing: High Level Principles and Procedures*, June 2007, para. 1.24 and 1.26 (p. 6); also *cf. Risk Based Approach: Guidance for Money Service Businesses*, July 2009, para 48 (p. 14)).

[77] These exemptions did not necessarily relate to the provision of NPM services.

CDD measures, and that therefore the wording of Recommendation 5 does not necessarily exclude exemptions in low risk cases. For example, according to EC legislation, EU member states are allowed to exempt issuers of electronic money from applying any CDD measures in designated low risk cases,[78][79] and many member states have made use of this option. As a result, several NPM products issued in the EU are effectively anonymous.[80]

Non-face-to-face business models: level of required CDD measures

166. Non-face-to-face business is currently addressed by FATF Recommendation 8, which recommends that *"financial institutions should have policies and procedures in place to address any* ***specific risks*** *associated with non-face-to-face business relationships or transactions."* While the wording of Recommendation 8 does not explicitly speak of "high risk", the Interpretative Note to Recommendation 5 (para. 7) makes a reference to the Basel CDD paper (section 2.2.6) for specific guidance, which says:

> *"48. In accepting business from non face-to-face customers (...) there must be specific and adequate measures to mitigate the* ***higher risk****."*

Within the work being currently done by the FATF in the perspective of the 4th round of mutual evaluations, there is a clear recognition that non-face-to-face business relationships or transactions represent **a higher ML/TF risk**.

167. Recommendation 5 suggests that "*for* ***higher risk categories****, financial institutions should perform* ***enhanced due diligence***". Furthermore, the Interpretative Note to Recommendation 5 (para. 13) adds:

> "Simplified CDD measures are not acceptable **whenever** there is suspicion of money laundering or terrorist financing or **specific higher risk scenarios apply**."

The FATF standards do however not clarify whether "specific risk" in the sense of Recommendation 8 equates to "higher risk scenario" in the sense of Recommendation 5. If this interpretation were correct, NPM products relying on non-face to face transactions should not be eligible for simplified CDD.

168. To base a product or service´s risk rating on one risk factor alone (here: non face to face) would not take into account the principles of risk assessment developed in the 2006 NPM report (and retained by the project team in this report). According to these principles of risk assessment for NPMs, all risk factors featured in the risk matrix presented in para. 65 of this report should be taken into account when assessing the risk of an individual NPM service or product. Non-face-to-face business relationships and transactions do increase the risk rating of an NPM service or product, but other product features (*e.g.,* solid identification and verification procedures; or strict value limits) can considerably mitigate the risk, and even lead to the product or service being assessed as "lower risk" after all. Accordingly, such business models would not categorically have to apply enhanced CDD measures, but might even qualify for the application of simplified CDD measures in certain circumstances of low risk.

---

78 For more detail see Appendix D, section 3:*The Third Anti-Money-Laundering Directive (2005/60/EC)*.

79 The European commission has defined technical criteria that will classify certain scenarios as "low risk" in Art. 11 and 40 of Directive 2005/60/EC in conjunction with Art. 3 of Directive 2006/70/EC.

80 Mainly cash vouchers and some prepaid cards (open-loop and closed loop), whereas IPS providers usually ask at least for the customer's name (which may remain unverified though).

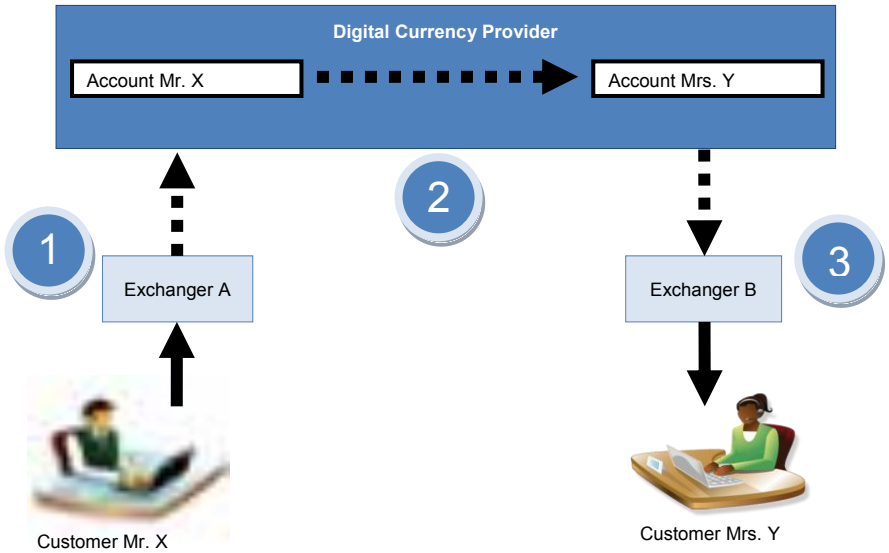
169. The project team has been informed that this issue is currently being discussed within FATF. It was indicated that the qualification of non-face-to-face business models as "higher risk" by the FATF standards might not automatically lead to a qualification as a higher risk scenario in the sense of Recommendation 5. It would be helpful if this conclusion was reflected in the standards (*e.g.,* in an Interpretative Note to Recommendation 5 or Recommendation 8).

Digital currency providers: the use of exchangers

170. The segmentation of services in digital currency business models makes it difficult to determine who the provider of the payment service is and thus subject to regulation.

171. The following diagram illustrates the segmentation of services in a digital currency provider business model, in which the actual payment is broken down into three separate steps, each carried out by a different entity:

Figure 4. Digital Currency Provider



Step 1: Funding of the customer account
Customer Mr. X pays an amount of real money to Exchanger A, who holds a certain amount of the digital currency. In exchange for the money received, the exchanger transfers an equivalent amount from his digital currency account to customer Mr. X´s digital currency account.

Step 2: Transfer of Digital currency
Customer Mr. X instructs the Digital Currency Provider to transfer a certain amount of digital currency to the Digital Currency account of Customer Mrs. Y.

Step 3: Withdrawal of funds
Customer Mrs. Y transfers a certain amount of digital currency from her own Digital currency account to the Digital Currency account of Exchanger B. In exchange for the digital currency received, the exchanger transfers an equivalent amount of real money to Customer Mrs. Y.

Source: NPM project team

172. In some jurisdictions, none of these steps would be considered a regulated activity in their own right:

- The exchangers exchange real money for digital currency, or even digital currency for another type of digital currency from different providers. They transfer value, but only between accounts of one and the same principal; they do not transfer money to third persons.
- The Digital currency provider transfers value from one person to another; however, he neither receives real money from the payer, nor does he pay out real money to the payees.

173. Other jurisdictions consider these activities to be regulated, and as a consequence consider all entities involved to be subject to supervision.

Box 16
US: MSB´s

The prosecution of an offshore Internet payment service marketing online to U.S. citizens prompted the application of existing law regarding money transmitters to any online payment service facilitating money transmission. The money transmitter definition in the U.S. states, in part:

"Any person, whether or not licensed or required to be licensed, who engages as a business in accepting currency, or funds denominated in currency, and transmits the currency or funds, or the value of the currency or funds, by any means…"

In addition to successfully applying this definition, and the associated registration, recordkeeping, and reporting obligations, to online payment services, including digital currency providers, U.S. prosecutors have applied it successfully to offshore service providers sending and receiving funds to U.S. customers.

Box 17
Germany: Involvement in unlawful business / Teilakttheorie ("theory of partial acts")

According to the German Banking Act, supervisory authorities may issue a cease-and-desist-order not only against entities conducting unlawful business themselves, but also against undertakings which are involved in the preparation, the conclusion or the settlement of such business.

Similarly, a provider is considered a "de facto branch" of a financial institution if it carries out relevant steps ("partial acts") of a financial service for that institution. As a consequence, the "de facto branch" needs to be licensed unless the financial institution it works for is licensed either in Germany or another member state of the European Economic Area.

Based on the aforementioned principles, the German authorities have initiated an administrative proceeding against an unlicensed, Germany-based digital currency exchanger that traded in digital currency issued by a provider seated in South-East Asia. The administrative proceeding is still ongoing.

174. The problem of regulating and supervising Digital currency providers and their related entities such as exchangers is exacerbated by the fact that their services often require no physical presence in a jurisdiction, but can be carried out from anywhere via the Internet. The entities involved are therefore able to choose a jurisdiction where they are not subject to regulation as their seat and provide their services from there.

The use of agents / Outsourcing CDD measures[81]

175. CDD and other AML measures are usually carried out by officers or employees of the regulated financial institution itself. However, in many NPM business models these tasks are in practice performed by third parties, including agents, intermediaries, or are outsourced. While these can be

81 For the purposes of this report, the terms "agent" and "outsource" shall be used synonymously.

different legal concepts entailing different legal obligations and requirements, for the purpose of this report these concepts shall be used interchangeably.

The FATF 40+9 Recommendations address the issue of agents and outsourcing in two different contexts, namely in Recommendation 9 and Special Recommendation VI.

176. Recommendation 9 only marginally touches on this subject. It refers exclusively to third party reliance and introduction; it does not cover agents and outsourcing agreements, nor does it provide a definition of outsourcing or agency. However, a footnote in the Methodology text accompanying Recommendation 9 is actually the only place within the standards that explicitly explains the current FATF approach towards agents and outsourcing: "*the outsource or agent is to be regarded as synonymous with the financial institution i.e., the processes and documentation are those of the financial institution itself.*"[82]

177. The only Recommendation explicitly mentioning agents is Special Recommendation VI, which recommends that "*each country should take measures to ensure that persons or legal entities, including agents, that provide a service for the transmission of money or value, including transmission through an informal money or value transfer system or network, should be licensed or registered and subject to all the FATF Recommendations that apply to banks and non-bank financial institutions.*" The interpretative note to Special Recommendation VI defines an agent as "*any person who provides money or value transfer service under the direction of or by contract with a legally registered or licensed remitter (for example, licensees, franchisees, concessionaires).*"

178. The general interpretation of Special Recommendation VI is that it does not require agents to be subjected to AML obligations and supervision in their own right either. While the wording of Special Recommendation VI may leave room for other interpretations, this can be concluded from the definition of "agent" in the glossary of the methodology (which implies that the agent is subdued to the regulated principal) and the Interpretative Note to Special Recommendation VI, which in paragraph 8 finds it sufficient that the principal business maintains "*a current list of agents which must be made available to the designated competent authority"*

179. According to these principles in the current FATF standards, in most jurisdictions agents and outsources of financial institutions are not normally subject to AML legislation or regulation themselves, thus having no legal AML/CFT obligations of their own.[83] Instead, the principal (or outsourcer), being a regulated institution, will remain solely responsible for meeting the AML/CFT obligations for its activity, including actions (and omissions) of its agents or outsources. Shortcomings of the agent are attributed to the principal (*i.e.,* financial institution), which may be sanctioned for any breach of its own AML/CFT obligations, conducted by its agent.

180. As regards Money Services Businesses, FATF has issued some guidance on the handling of agents, providing some useful input on the notions of "know your agent", agent monitoring and agent training. While this guidance does not explicitly refer to NPM service providers, these concepts appear to be applicable those as well.

---

82 Footnote 16 of the FATF Methodology for assessing compliance with the FATF 40 Recommendations and the FATF 9 Special Recommendations.

83 Agents are often subject to contractual AML/CFT responsibilities that are imposed on them by the agency contract with their principal. However, there is no direct legal liability of the agents and no possibility for authorities to sanction agents if they breach their contractual AML/CFT obligations. There are usually no legal requirements for the principal to impose contractual AML/CFT responsibilities on their agents.

181. Some jurisdictions, including the U.S. and Germany, have recently reassessed their approach and have come to the conclusion that there is a gap in regulation. As a consequence, they propose to impose legal AML/CFT obligations on agents. The term "agent" in this sense may cover many different activities, including for example card program managers or sellers of prepaid funds.

a) Card program managers

182. In some business models, the prepaid card program is effectively run by card program managers. The card program manager may have ownership and control of the business model and take any important business decisions, while the issuing bank only provides access to the technical card platforms. As a result, a card program manager´s role in an NPM business model may be greater than that of a traditional outsource or agent.[84] Still, like a regular agent, the card program manager usually is not supervised and outside the scope of AML legislation, while the issuing financial institution remains legally responsible for meeting its legal and regulatory obligations.

183. This separation of business responsibility and regulatory liability situation is exacerbated if the card program manager and the issuing bank are located in different jurisdictions. If, for example, the card program manager is based in a jurisdiction with a robust regulatory regime (to which the card program manager is not subject though), this strict regime could be circumvented by cooperating with an issuing bank that is based in a jurisdiction with lower AML/CFT standards or less effective supervision.

184. A related issue is market entry. As most card program managers are not currently subject to regulation and supervision, they are also not subject to market entry requirements like fit-and-proper tests carried out by the supervisory authorities. It is therefore often down to the issuing institution themselves to identify whether its agent/program manager´s intentions are legitimate. Case studies evidence that some institutions have failed to discover the illegitimate intentions of their program managers, or have even knowingly and collusively entered into a co-operation with illegitimate program managers (see above section 4 "Typologies", *cases 22 and 28*).

185. As a result, some jurisdictions are currently considering subjecting card program managers and other third parties subject to legal AML/CFT obligations. No such regime has been finalised yet. The most advanced initiative is a US notice of proposed rulemaking (NPRM) by FinCEN, which was published for public consultation on June 28, 2010.[85]

Box 18

According to the NPRM, FinCEN proposes to implement a new subtype of Money Service Business (MSB) called "provider of prepaid access". The provider of prepaid access is described by FinCEN as follows:

"In general, this term will apply to any person that serves in the capacity of oversight and control for a prepaid program. The determination of the applicability of this term to any given player in the program's transaction chain will be a matter of facts and circumstances; we do not "assign" this term to any particular role. We recognize that there may be situations in which no single party alone exercises exclusive control. However, we do believe that there will always be a party in the transaction chain with the predominant degree of decision-making ability; that person plays the lead role among all the others, and is in the best position to serve as a conduit for information for regulatory and law enforcement purposes. We wish to state clearly and emphatically that identifying the provider of prepaid access is not simply an arbitrary decision by the program participants. As with other MSBs, the role of the provider of prepaid access is determined through the facts and circumstances surrounding the activity; no single act

84 The definition of "agents" for the purpose of Special Recommendation VI in the glossary of the FATF methodology states that agents work "*under the direction of or by contract with a legally registered or licensed remitter*" This implies that the agent usually is considered to be subordinated to the principal, *i.e.,* the financial institution.

85 Federal Register (2010)

or duty alone will be determinative. While not exhaustive, we consider the following activities to be strong indicators of what entity acts in a principal role:

• The party in whose name the prepaid program is marketed to the purchasing public. For example, whose press release trumpets the launch of a new product? Whose name is used in print, on-line advertisements, and on the face of the card/device itself? In legal parlance, the individual or entity who „holds himself out" as the lead player will be a very important determining characteristic.

• The party who a „reasonable person" would identify as the principal entity in a transaction chain—the principal decision-maker.

• The party to whom the issuing bank looks as its principal representative in protecting its network relationship and its brand integrity.

• The party who determines distribution methods and sales strategies.

• The party whose expertise in the prepaid environment is recognised by the others, particularly by the issuing bank, as instrumental in bringing together the most appropriate parties for the delivery of a successful program.

We intend for these enumerated characteristics to illustrate that there is no one single determinant; the provider of prepaid access need not do, or refrain from doing, any single activity. The totality of the facts and circumstances will identify the provider of prepaid access."

As a type of MSB, providers of prepaid access would have to be registered with FinCEN. According to the NPRM, they should be obligated to establish and maintain AML programs (incl. staff training), to collect identification data and transaction records and retain them for five years, and to file CTRs and SARs. FinCEN also proposes to impose the same obligations on the ~~s~~sellers" of prepaid access; these however should not be considered MSBs and accordingly would not have to register with FinCEN.

The new obligations of providers and sellers of prepaid access shall not affect the legal liability of any involved banks or financial institutions: their AML obligations remain unchanged.

b) Sellers of prepaid funds

186. Several NPM providers use a network of partners (*e.g.,* retailers, pharmacies etc.) to sell their product to the customers. In some jurisdictions, there are moves to treat these as agents acting on behalf of the NPM provider, while in others they are treated as plain merchants rather than agents.

Box 19

United States

In the Notice of proposed rulemaking (NPRM) described above,* FinCEN proposes to impose direct AML/CFT obligations not only on the issuing bank and the ~~p~~providers of prepaid access", but also on the seller of prepaid products:

~~"~~We are also mindful that, among all the typical parties, a very important role is that of the seller. The seller alone has face-to-face dealings with the purchaser and is privy to information unavailable elsewhere in the transaction chain. For that reason, we believe the seller to be secondarily important among all the entities involved in the program. (…) The seller is uniquely situated to see the first step in the establishment of a prepaid relationship, and to interact directly with the purchaser who may, or may not, be the ultimate end-user of the card. The requirements of this party to maintain records over a five-year time period and to report suspicious activity, also serve the law enforcement´s needs.

(…)

The seller of prepaid access is the party with the most face-to-face purchaser contact and thus becomes a valuable resource for capturing information at the point of sale, unlike any other party in the transaction chain. Typically, the seller is a general purpose retailer, engaged in a full spectrum product line through a business entity such as a pharmacy, convenience store, supermarket, discount store or any of a number of others. Precisely because this party deals face-to-face with the purchaser, and has the ability to capture unique information in the course of completing the transaction, we believe the seller should fall within the regulation´s direct reach.

Because the seller´s role is complimentary with, but not equal to, the authority and primacy of the provider of prepaid access, we choose not to require registration with FinCEN. The seller, we believe, is generally acting as an agent on behalf of the provider and this treatment is consistent with other agents under the MSB rules.

However, the seller´s agency does not excuse compliance with the other responsibilities assigned under this

proposed rule: (1) the maintenance of an effective AML program, (2) SAR reporting, and (3) recordkeeping of customer identifying information and transactional data."

* Federal Register (2010)

187. Similarly, in Australia besides issuing prepaid cards the activity of "increasing the monetary value" (*i.e.,* loading or reloading funds onto cards) of certain stored value cards[86] is considered a designated service which makes providers of such services a reporting entity under the Australian AML/CTF Act and incurs a range of important obligations. These include the requirement to have an AML/CTF program, customer identification and ongoing customer due diligence, record keeping and reporting obligations.

188. Other jurisdictions do not share the point of view described above, *i.e.,* that the current approach to agents would constitute a gap in regulation, and do not support the idea of subjecting agents to AML obligations in their own right. As an alternative, it has been suggested to reinforce or clarify the requirements on the outsourcing / agency agreements of financial institutions, especially as regards AML/CFT obligations. Many jurisdictions have legislation in place on requirements for outsourcing contracts; however, this is currently not mirrored in the FATF 40+9 Recommendations.

"Hybrid" service providers

189. Some non-financial business companies have started to take up providing NPM services (*e.g.,* telecommunications companies providing mobile payment services). These "hybrid" payment service providers may challenge existing regulatory regimes because due to their financial activities, in many jurisdictions they would either be excluded from the market (as such activities are limited to credit institutions only);[87] or they would be subject to regulation regarding all their lines of business, not only their financial activities. Furthermore, if the hybrid provider is a big company, due to its size it would be impossible to make use of regulatory waivers in many jurisdictions.

190. These hindrances may force interested hybrid providers to either provide their financial services through a separate legal entity focussed on financial services, or may deter some potential candidates from entering into the market of NPM altogether.

Box 20
Example European Union

The new EU regime for the issuance of e-money as revised by the second E-Money Directive (EMD) aims at facilitating market access to newcomers, namely telecommunication companies or large-scale retailers who want to engage in the market of e-money. Following the Payment Services Directive, the exclusivity principle will no longer apply to electronic money institutions, who are now entitled to engage in any business activity besides issuing electronic money (Art. 6 para 1 lit. e) EMD).

For the calculation of an electronic money institution´s own funds or safeguarding requirements, only the funds relating to the e-money business are taken into account, excluding the funds relating to other lines of business activity ("ringfencing").

Suspicious transaction reporting in cross-border scenarios

191. The provision of cross-border services, which is typical for many NPM business models (especially most IPS providers) raises issues as regards filing suspicious transaction reports and the effectiveness of law enforcement. In most jurisdictions, NPM providers are only obligated to report

86 Australian Attorney-General's Department (2006)

87 See 5.1.2, *Subject to existing regulation for traditional financial services*.

suspicious transactions to their home FIU, even if the persons involved in the suspicious transaction (customer / sender / receiver) are based in a different country. That country´s FIU will depend on an effective international cooperation and information sharing with the NPM provider´s home FIU. Where such cooperation is lacking, the effectiveness of the STR reporting regime and law enforcement of suspicious cases may be seriously impeded.

192. Where agents are used to provide cross-border services, the situation is similar. Agents are usually not subject to the STR regime in most jurisdictions. If they report suspicious transactions, it will most likely be towards their principals (*i.e.,* the NPM service provider) on a contractual basis. As described above, the NPM provider would then file an STR to its home FIU, but not necessarily to the FIU of the country where the agent is based.

Box 21
European Union

Within the EU Committee on Money Laundering and Terrorist Financing (CPMLFT), it is currently being discussed to which Financial Intelligence Unit reporting should be done in cross-border situations, as well as issues of attribution of competence among AML supervisors where a payment institution under the Payment Services Directive has a recourse to an agent to sell services in another Member State than the one where it is established.

While this discussion arose with regard to agents of money remittance services, the outcome of the discussion will have an immediate impact on NPM providers for whom the same provisions regarding agents apply.

Law enforcement and supervisory action against foreign providers

193. Where NPM providers provide their services across borders online only (*i.e.,* without any physical presence in the jurisdiction of the customer), foreign authorities will have limited possibilities to take action, but will normally have to rely on their counterparts in the jurisdiction where the provider is based.

194. However, some national authorities have successfully taken action against foreign providers by making use of the tools of their national criminal law and their national administrative law.

195. For example, United States authorities have used the provisions of US criminal law to impose sanctions on foreign providers located in the Isle of Man (see above **case 31**) and in the Caribbean (see above **case 33**). These national sanctions could be applied as the defendants (*i.e.,* the directors and owners of the foreign providers) either resided in the US or travelled into the US.

196. German authorities have issued administrative cease-and-desist orders against IPS service providers located in South-East Asia and Central America. According to German supervisory law, such measures can be taken only if business is conducted in Germany. However, authorities have considered activities that were provided from abroad, to take place “in Germany” when certain conditions were met. As regards the provision of financial activities through the internet, the activity will be considered to be conducted in Germany if the content of the website is designed to target the German market. Indicators for this include (list not exhaustive): domain of the website (“.de”), website in German language, customer information that is specific to Germany or the German financial sector, references to the German legal framework, and appointment of German contact persons.

Identification of secondary card holders

197. Several prepaid card providers issue cards that are specifically designed to facilitate cross-border remittances. In such business models, a main card is issued to the customer / cardholder; in addition, the customer will dispose of one or several additional cards (also “partner cards”; “remittance cards”) which they can pass on to third persons; these are the intended recipients of the remittance

transactions. The remittance is then carried out in two steps: first the cardholder loads the remittance amount on the prepaid card; secondly, the recipients may withdraw the amount at any ATM worldwide with the help of their secondary cards.

198. In a number of these business models, only the main cardholder is identified. The holders of the additional cards often remain unknown to the card issuer.

199. In the 2009 Mutual Evaluation Report for New Zealand, one such business model and the related supervisory practice have been described in much detail:

Box 22
New Zealand Mutual Evaluation 2009

According to the Mutual Evaluation Report at the time the assessment was conducted, where there were three or more –afacility holders" (=account or card holders) financial institutions in New Zealand were generally –onlyrequired to perform CDD on the principal facility holders (*i.e.,* those whom the financial institution reasonably regards, for the time being, as principally responsible for the administration of the facility", while all other facility holders who remained **unidentified** were also able to conduct transactions via the facility held at the financial institution. This was criticised by the assessment team and affected the rating for Recommendation 5. *

However, as regards the **verification** of such secondary cardholders, the assessment team apparently had no objections to the application of simplified CDD:

—49. Simplified CDD is allowed when the facility provided is a remittance card facility. In such cases, there is no requirement to verify the identity of the second card holder (2008 Interpretation Regulations). These types of remittance card facilities are only offered by one bank in New Zealand. The authorities advise that the remittance card regulation exemption was designed to mitigate the AML/CFT risks that could attach to remittance products, and places a number of conditions and constraints on the eligibility for exemption. These conditions and constraints include: *i)* a maximum total annual remittance, and maximum balance on the card of NZD 9 999.99; *ii)* eligible cards can only be used on international bank Automated Teller Machine (ATM) and *Electronic Funds Transfer at Point of Sale* (EFTPOS) networks; *iii)* full FTRA verification and record keeping requirements apply to the primary card holder (account opener); *iv)* identification and record keeping requirements apply to the one other permitted card holder (who cannot be resident in New Zealand); and **v)** the issuing institution is required to carry out ongoing due diligence and transaction monitoring on the facilities. The authorities concluded that the above limitations mitigate the AML risk to an acceptable degree for the product to be offered in New Zealand on the basis that full CDD is applied to the primary card holder and simplified CDD is applied to the second card holder. This conclusion was based on a review co-ordinated by the Reserve Bank and involving officials including the Ministry of Justice, the Ministry of Pacific Island Affairs and the FIU. The review considered material from the NZ Police, APG and FATF, including typologies and evidence of misuse of stored value card and travel card-type products. Discussions were also held with several banks about product options and AML/CFT risk management options, and sample data was collected about remittance volumes and average size. A Public Discussion document and subsequent Cabinet paper were produced justifying the limitations in the regulation to mitigate the AML/CFT risk to reasonable levels consistent with the expected form and approach of the new AML/CFT Bill and New Zealand s longer term compliance with the FATF Recommendations.—

* FATF (2009b), p. 84, 93.

200. While generally all holders (*i.e.,* primary and secondary holders) of an account or a card should be identified, there is room for discussion whether this is still necessary if the specific card model can be qualified as "low risk" and therefore simplified CDD measures might be applied. While a full exemption from CDD measures regarding the (primary) customer has been criticised as not in line with Recommendation 5,[88] it is unclear whether this should also apply to an exemption of secondary card holders (assuming that the primary card holder has been appropriately identified and verified). This will be dependent on the degree of control the secondary card holder has over the product, and whether he needs to be qualified as a customer of the NPM provider, or might be considered the customer´s beneficial owner, or some kind of beneficiary.

88 See 5.2, *Exemptions from AML obligations.*

CHAPTER 6: CONCLUSIONS AND ISSUES FOR FURTHER CONSIDERATION

201. Market adoption of NPMs has increased since the 2006 report, and is likely to increase even more in the future. More and more NPMs offer the opportunity to transfer funds globally. As a result, evidence of the misuse of NPMs for purposes of ML and –to some extent- TF have also increased.

202. New types of NPMs are likely to emerge in the future. Because of the convergence and combination of NPMs it will be more complex for supervisors and legislators to assess if such payment systems are vulnerable to ML/TF abuse. The continued development of NPMs therefore requires an appropriate, flexible and „future proof' FATF framework.

203. In addition to the risk assessment (section 3) and the development of typologies (section 4), this report examines whether the FATF 40+9 Recommendations continue to provide an adequate framework to address recent technological and regulatory developments in the field of NPMs.

204. The project team has come to the conclusion that the FATF Forty Recommendations and Nine Special Recommendations provide a broadly adequate framework to address the vulnerabilities associated with new payment methods, although there is a need for the FATF to explore some issues in the international standards that require further development or clarification. The project team is aware of the fact that FATF has already launched a thorough review of its standards and that some issues raised in this paper are being addressed in this context.

205. The project team has concluded that it would be desirable for FATF to provide more clarity on some issues that arise in relation to NPMs. It is understood that some of those issues are already being addressed in the context of the preparation of the fourth evaluation round.

206. When discussing the questions listed below, the responsible working groups should take into account not only aspects related to the prevention of ML and TF, but also the positive and beneficial effects of NPMs (*e.g.,* financial inclusion, shifting transactions from the informal to the formal sector, promotion of competition and economic growth in national markets) as well as legitimate market demand and private sector concerns in order to find an appropriate balance.

207. In all cases the cost/benefit ratio should be taken into account when making policy decisions on NPMs. Decision makers should carefully consider *e.g.*:

- Whether the AML/CFT benefit justifies the potential extra costs and efforts that may arise for institutions as well as for supervisors, FIUs or other agencies.

- Whether there is a risk that specific measures might lead to significant disadvantages for NPM customers (*e.g.,* regarding cost or "convenience" of the NPM service) and whether these potential disadvantages might tempt some customers to make their payment transactions through unregulated payment service providers instead.

208. Policy decisions should strive to find the right balance between an efficient and comprehensive AML/CFT regime and legitimate market demand and private sector concerns.

Questions relating to simplified CDD:

1. Should Recommendation 5 provide for an exemption from CDD measures in cases of "low risk"? (Recommendation 5)

209. Recommendation 5 recommends that "*financial institutions should not keep anonymous accounts or accounts in obviously fictitious names.*"

210. Furthermore, Recommendation 5 recommends that "*financial institutions* ***should apply each of the CDD measures*** *(as listed in Recommendation 5) but may* ***determine the extent of such measures on a risk sensitive basis*** *depending on the type of customer, business relationship or transaction. The measures that are taken should be consistent with any guidelines issued by competent authorities. For higher risk categories, financial institutions should perform enhanced due diligence. In certain circumstances,* ***where there are low risks, countries may decide that financial institutions can apply reduced or simplified measures***."

211. The standards do not provide a definition of "reduced or simplified CDD measures", and they do not explicitly exclude exemptions from this term either. A number of jurisdictions currently grant institutions a full exemption from CDD measures in designated low risk cases. While this has been criticised to be not in line with Recommendation 5 in some mutual evaluations, there are also others (including a number of jurisdictions, organisations such as the World Bank and private sector representatives) that take the view that Recommendation 5 does (or should) provide the possibility to grant exemptions from CDD measures in low risk cases.

212. In the context of the review of the standards, the FATF will be proposing some changes to the standards that aim at addressing these concerns. The following aspects should be taken into account:

213. Exemption from verification:

- The overall risks of a product or service can also be mitigated by other means such as applying account and transaction limits. Imposing very restrictive limits on the transactions or other functionalities may have an even more deterring effect to would-be launderers than the prospect of being verified. Furthermore, intensive monitoring can help mitigate the ML risk of products as well.

- In some jurisdictions, verification of the customer´s identity may be difficult to accomplish, especially where ID documentation or other reliable documentation is not available for a great part of the population.

- Verification can also prove to be a financial burden for institutions or customers (*e.g.,* where customers must travel a long distance to the bank or vice versa to be verified), deterring customers and institutions alike, and potentially endangering the economic success of individual NPM providers.

- Case studies indicate that criminals were able to launder money even where verification had taken place, *e.g.,* by using stolen or fake identities, or strawmen.

214. Exemption from identification:

- Unlike verification, identification does not seem to cause a lot of cost or effort; the NPM provider simply needs to ask the customer's name.

- In the case of additional cardholders, can it be acceptable to exempt institutions from the identification of the additional cardholders (*e.g.,* if the primary cardholder is thoroughly identified and verified, and other measures and systems such as monitoring are in place)?

2. Is the application of simplified CDD acceptable for non-face-to-face business models? (Recommendations 5 and 8)

215. FATF should provide clarity whether non-face-to-face business models automatically qualify as "high risk scenarios" in the sense of Recommendation 5. While FATF experts have recently discussed this, there is no official statement yet that "specific risk" should not automatically equate with "higher risk" in the sense of Recommendation 5. It would be helpful if FATF could provide greater clarity on this by amending the standards, taking into account the following aspects:

- The approach to risk assessment chosen in this report (and the 2006 report) suggests that all risk factors and all mitigants should be taken into account in order to find an overall risk rating of an individual product or service. It would be against this approach to assess a product as high risk just because it features one particular risk factor (*i.e.,* non face to face), without looking at the all the other risk factors and mitigants.

- Several NPM providers currently apply simplified CDD to non face to face business models and would be seriously affected if this practice was declared inacceptable. Private sector representatives have indicated that this might jeopardize the commercial viability of some NPM services.

Questions relating to the treatment of agents:

3. Should agents of NPM providers be subject to regulation and own AML/CFT obligations? (Recommendation 23, Special Recommendation VI)

216. Depending on the type of activities carried out by agents, they can play a very important role in the execution and completion of a payment transaction. Compared to more traditional financial services, the use of agents to carry out functions related to AML/CFT appears to be more common among NPM providers. Such agents may be required as an intermediary or an interface between traditional financial services and more "virtual" payment services. Using agents may also be an effective and inexpensive alternative to opening branches for NPM service providers, especially when providing NPM services abroad.

217. The FATF 40 + 9 Recommendations do not require agents to be subjected to AML/CFT obligations in their own right. While some jurisdictions have recently suggested that this might constitute a gap in regulation, others consider the current approach appropriate and sufficient.

218. FATF should consider whether the standards should more explicitly address issues relating to the effective oversight of agents carrying out key operational functions, either through direct supervision or through indirect supervision carried out by the principal

219. When making this consideration, the following aspects should be taken into account:

- FATF should consider providing guidance to NPM providers on how to design the contractual relationship with their agents and to enable supervisors to control whether the institution fulfils its AML/CFT obligations through its agents. While some guidance has already been introduced for Money Service Businesses (*e.g.,* the concepts of "know your agent", agent

monitoring and agent training),[89] it remains unclear whether FATF considers this guidance applicable for other financial institutions (such as NPM providers) as well.

- Where agents are subjected to AML obligations, this should not result in a reduction of the principals´ own AML obligations.

- Suspicious transaction reporting: agents are often the only persons having actual face-to-face contact to the customer. Valuable information for suspicious transaction reporting (*e.g.,* suspicious customer behaviour) may therefore only be available to the agent. Such information may be lost or delayed if the agent has no reporting obligations or needs to report to the principal only.

- A reporting obligation for agents should not result in a reduction or waiver of the institution´s own obligation to file suspicious transaction reports. The financial institution may have additional information on the customer and his transactions that is not available to the agent, and may therefore be able to detect suspicious transactions that would not be noticed by an agent.

- Furthermore, FATF could consider which authority the principal and/or agent should be reporting to if agents located in a different jurisdiction than their principal are subjected to reporting obligations: the FIU in the principal´s ("home") jurisdiction; or the FIU in the agent´s ("host") jurisdiction; or double reporting to both jurisdictions?[90]

- Staff training: where agents are subjected to AML/CFT obligations, they should also be required to appropriately train their staff. This training may also be provided by the principal.

- Cost of compliance: where new AML obligations are imposed on agents, this may lead to additional costs and efforts, rendering the service less attractive for agents and/or customers. However, in business models where agents currently already are subject to contractual AML obligations towards their principal, it is unclear whether subjecting them to legal (rather than contractual) AML obligations should effectively result in a relevant increase of costs and efforts.

- Subjecting agents to direct legal AML/CFT obligations may potentially serve as a strong disincentive to act as an agent, potentially making it difficult for NPM providers to find agents and thereby reducing the number of access points to regulated and supervised NPM service providers.

- Efficiency of oversight: if agents are regulated and subjected to AML/CFT obligations, there will be a significant increase in the number of entities to be supervised by the financial supervisors. There are doubts whether this can be accomplished effectively in all cases.

---

89 FATF (2009)

90 For example, Jersey has issued guidance that agents should report to both FIUs.

4. How should the term "agent" be defined (Recommendation 9, Special Recommendation VI)?

220. Regarding the term "agent", the first difficulty is to find a valid delineation to the terms "outsourcing" and "reliance" or "third party introduction" (as addressed by Recommendation 9). The project team understands that this issue is currently being addressed within FATF.

221. Secondly, FATF does not define the types of activities that can be considered as creating an agency relationship. For example, exchangers used in digital currency business models may argue that they are independent businesses trading in electronic currency. Sellers of prepaid funds (*e.g.,* retailers selling prepaid cards or cash vouchers) might argue that they are just merchants, acting outside the financial sector.

Other issues:

5. Should the scope of Special Recommendation IX be expanded to include "electronic money" or "stored value", especially prepaid cards? (Special Recommendation IX)

222. Special Recommendation IX recommends that "countries should have measures in place to detect the physical cross-border transportation of **currency and bearer negotiable instruments**, including a declaration system or other disclosure obligation."

223. The 2006 report identified the cross-border movement of prepaid cards as a potential ML risk. The project team still considers this a significant potential risk, even though only few case studies have been submitted to prove that criminals have made use of that potential typology in the past.

224. In order to control and counter the cross-border movement of stored value, it would be helpful for customs authorities if they could make use of the tools that have been implemented for the cross-border movement of cash and bearer negotiable instruments according to Special Recommendation IX, such as a declaration or disclosure system and the possibility to confiscate funds. However, in most jurisdictions, these tools (that have their origin in Special Recommendation IX) are only applicable to currency and bearer negotiable instruments, which means that prepaid cards do not have to be declared when crossing borders.[91]

225. Most jurisdictions do not classify prepaid cards, or other means of "stored value" or "electronic money", as cash or bearer negotiable instruments in the sense of Special Recommendation IX. In order to be able to subject these cards to cross-border controls, it would therefore be necessary to widen the scope of Special Recommendation IX (and resulting from that national custom laws) to include such cards as well (alternatively, the text of Special Recommendation IX might remain unchanged, but the definition of either "cash" or "electronic money" might be widened to include stored value or electronic money). When considering expanding the scope of Special Recommendation IX, the following aspects should be taken into account:

- There are currently different opinions whether Prepaid cards should fall under the scope of Special Recommendation IX. While some jurisdictions stress the point that such cards

---

[91] Only few jurisdictions apply these rules to prepaid cards. For example, section 12a of the German Customs Administrative Act (*Zollverwaltungsgesetz*) applies cross-border controls to "cash and equivalent means of payment" including a.o. "cheques, bills of exchange, precious metals and stones and electronic money" (section 1, para 3a *Zollverwaltungsgesetz*).

resemble cash in many ways, others find them to be a type of debit or credit card, which were intentionally kept outside the scope of Special Recommendation IX.

  - Prepaid cards resemble cash in that they are anonymous, represent a certain currency value and can be widely used for the purchase of goods or services. The cards are paid in advance (no credit system) and can be transported across borders.

  - On the other hand, prepaid cards are also similar to the use of debit or credit cards, which undoubtedly do not fall under the scope of Special Recommendation IX. The value of prepaid cards is usually not stored on the card itself, but on a server, with the card being only an access device to the funds.

- It should be examined further whether the reasons that excluded credit and debit cards from the scope of Special Recommendation IX are valid for prepaid cards as well.

- Effectiveness: Currently, there are still technical difficulties with the verification of prepaid cards. It is unclear how custom officials would determine the actual value that is stored on a card. Would card readers have to be installed, and would these work for all technical standards from different card providers? However, technical challenges may be overcome once a legal foundation has been laid for cross-border controls for prepaid cards.

- Where prepaid cards can be transported across borders with no or only minimal funds on it, and then be funded (or "activated") after they have arrived at their destination, this can also effect the efficiency of a cross-border declaration regime for such cards.

6. Should Recommendation 10 include IP addresses for transactions initiated through a personal computer?

226. There is currently no explicit requirement under Recommendation 10 to retain the IP addresses of personal computers through which a payment transaction is initiated. While most NPM providers would most likely do so in their own interest, there are reports from law enforcement about providers who do not retain the IP addresses of their customers, or delete them too soon (*i.e.,* before the 5-year period suggested by Recommendation 10). The FATF should take note of this issue and consider adding the IP address to the list of examples of "necessary records on transactions" in crit. 10.1 of the Methodology.

7. Updating this study

227. Taking into account the continuous development in the sector of NPMs, regarding the technical development as well as the corresponding reaction of legislators and responsible authorities, the project team suggests that this study be updated after an appropriate period of time. Depending on future developments in certain sectors, and on future case studies detected, it may be reasonable to alternatively publish separate typologies reports on single categories of NPMs (*e.g.,* typology report on prepaid cards).

APPENDIX A: SUPPLEMENTAL NPM QUESTIONNAIRE RESULTS AND ANALYSIS

This section gives an overview of the responses by a total of 37 jurisdictions plus the European Union Commission to the questionnaire issued by the project team. The majority of the respondents identified NPMs in their jurisdiction with prepaid cards being most popular (34 of the countries have such providers), then followed by IPS providers with 17 countries and mobile payment services with 16 countries.

The summary of the information provided by each jurisdiction is provided in the following tables and is presented by NPM category, that is, prepaid cards, Internet payment services and mobile payment services.

- Table A: Short description of the NPM and market (when provided)
- Table B: Information on regulatory provisions and any additional information
- Table C: AML/CFT provisions can derive from regulations in place or from business practice
- Table D: Reports of AML/CFT cases or if any illegal operators have been found

Prepaid Cards

Prepaid cards is the largest NPM category with thirty-four countries (more than double the number (14) of countries identified in 2006) reporting its presence in their jurisdiction. All prepaid cards are issued by financial and credit institutions. However, the prepaid card programs are often managed by third parties that are not, in some instances, directly covered by the AML/CFT regime. Information regarding the market size is rarely available and when provided varies extensively, that is 300 to over 100 million card holders.

Thirty-three out of 37 jurisdictions reported some form of licensing and registration requirements, as well as supervision and AML/CFT provisions for prepaid card issuers and program managers. One country reported no licensing or registration requirements but indicated that such providers were supervised. Some countries such as United States and Mexico are currently in the process of making changes to their legislation and regulations to ensure a better AML/CFT coverage of such organisations.

Twelve countries indicated that it was possible to acquire prepaid cards anonymously in cases where the maximum account balance was limited. For other countries, it is not possible to do so.

A total of 18 case studies included in this report were provided by seven different countries. Seven additional countries referred cases for which not enough details were provided or it was impossible to provide them because of legislative limitations. All countries reported that no illegal operator was known to operate in their jurisdiction.

A. Description of Prepaid Cards

Countries	Short description of NPM	Examples of limits
Argentina	Prepaid cards are offered by about 7 providers; some cards issued are associated to a bank account, and for the other prepaid product the customer must be a client of the bank to obtain the card. Normal CDD measures must be applied (overall estimate of 929 000 cards and 7 providers)	
Australia	Prepaid cards are offered but no statistics regarding the number of providers and users were provided	Only the prepaid cards issued with a value limit of AUD 1 000 or more are covered by the Australian AML/CTF Act.
Belarus	Prepaid cards are offered by at least two providers and are issued by banks, and therefore fall under the same regulations as banks	
Belgium	About 106 providers mainly issued by banks	
Brazil	Prepaid cards issued by banks jointly with VISA and Mastercard but no further information provided	
Bulgaria	Two providers with about 5 000 cards – regulations are in accordance with EU Directives	
Canada	Six providers with nine products – all issued by banks jointly with credit card providers; cards loaded by online bill payment function from a bank account, cash at MSB agent location or authorised retailer location or financial institution, direct deposit in some instances, card to card transfers through SMS on cell phones; multiple cards can be linked to one account in at least one instance	Varies depending on card type but with maximum balance up to CAD 10 000; daily withdrawal limit up to CAD 2 000; daily purchases up to CAD 2 000; maximum per load up to CAD 10 000
Cayman Islands	One provider (money services business) with about 140 cards – no additional information was provided	
Colombia	2 providers with over 410,000 accounts; cards are issued by financial institutions and are Visa or Mastercard branded; they are used for low value payments; one the available cards is rechargeable	
Denmark	Prepaid cards issued by banks in conjunction with VISA and Mastercard but little information provided as to the features of the products.	
Estonia	No providers in jurisdiction and prepaid cards not used as payment instrument in Estonia – however, one prepaid card company registered in a foreign country and issuing cards in another country were found to be active in Estonia and other countries – that prepaid card company no longer active in Estonia	

Countries	Short description of NPM	Examples of limits
European Union	13 prepaid card issuers operating with e-money license. Of the 3 biggest prepaid products offered, 2 non-reloadable have a maximum limit of 150 EUR and one is a Mastercard reloadable prepaid; estimated 164 million cards at end of 2008	When maximum limit of 150 EUR for non-reloadable and 2 500 EUR for reloadable cards – no CDD necessary
France	All credit institutions can issue open-loop prepaid cards (about 1.3 million issued in 2008); most common type of prepaid card funded by bank transfers or credit cards held by parents; Among many other products, one virtual card is loaded with credit card or through SMS on cell phone; one other card is used for international money transfers and managed from the Internet or a mobile phone by SMS and is funded by credit card or mobile phone... latter can only be purchased in France but will be soon available to other European customers	First type is reloadable up to 600 EUR but initial load amounts no more than 100 EUR; for virtual card, transactions must be under 150 EUR; international money transfer card can be used for maximum 6 000 EUR per year for both receiving and sending (total)
Germany	About 100 providers and 300 000 to 500 000 cards – most of the cards issued by banks, often in association with retail companies, and can be used at ATMs and POS; also have some prepaid cards that are solely virtual, *i.e.,* only used online and no physical card provided to client	
Gibraltar	Two providers with 70 000 cards (one is only marketed in the UK and the other one is marketed in EU and EEA); due diligence limited to registered cards only	
Italy	180 providers with over 8 million cards for use at ATMs and credit card payment systems - various types including ones issued by post offices in Italy which can receive payments by one major IPS provider and can be funded by cash, transfer of funds from other card holder; another one issued by a bank can be funded by cash at bank branches, at ATMs belonging to same bank as issuer of the card, through Internet and mobile banking	Post office prepaid card is reloadable for a maximum of 3 000 EUR; another card can have a maximum load of 10 000 EUR; another one reloadable up to 5 000 EUR
Japan	8 major e-purses companies with over 105 million accounts; also referred to as prepaid certificates; funded and redeemed through bank transfers and credit cards; available at convenience stores, vending machines and department stores etc.	
Lebanon	Issued by banks and financial institutions and Visa or Mastercard branded with over 39 000 accounts; mostly purchased and used by individuals for Internet purchases	On average, total balance of USD 300
Luxembourg	2 providers – one provider estimated at 200 000 reloadable cards; another card is provided through EPT (postal services) which must be linked to a personal account at EPT	
Macao	Only one prepaid product and no further information provided with estimated 304 accounts – only credit card institutions can issue prepaid cards	
Mexico	6 credit institutions (4 in process) with overall number of over 2.6 million which provide anonymous and personalised cards	

Countries	Short description of NPM	Examples of limits
Netherlands	3 providers (2 offering only non-reloadable cards and one reloadable card used for payroll); issuers of prepaid cards are licensed as a credit institution or as an electronic money institution	Non-reloadable cards are from 5 to 50 EUR; Payroll prepaid card has a total maximum balance of 10 000 EUR and a daily maximum of 5 000 EUR
Norway	Prepaid card issued by all commercial and savings bank. And VISA mentioned as a prepaid but no further information provided (140 banks issued about 6 million)	
Peru	No providers seated in jurisdiction and no regulations currently exist but are under consideration	
Philippines	24 banks (including branches of foreign banks) have issued prepaid/cash cards; providers are considered electronic money issuers (EMIs) which are required to determine individual and consolidated balances of their e-money instruments; a total of over P350 million outstanding balance as of December 2009 and February 2010 in one instance and over 500 000 card holders for one provider (info not provided by other two providers) – see questionnaire response for more info on legislative framework	Aggregate monthly load limit of P100 per e-money (or card) holder – deemed very low
Portugal	5 providers and about 75 500 accounts; one is used by corporations which provide them to employees;	one reloadable card only used in Portugal has a maximum balance of 15 000 EUR, a maximum payment of 5 000 EUR or 20 transactions per day
Republic of Armenia	Six banks have issued over 1650 cards; only banks can issue prepaid cards	
Republic of Poland	4 types of prepaid cards all issued by banks licensed under Polish law and have either the VISA or Maestro logo. No further information provided in terms of limits, funding and withdrawal.	
Russia	18 providers with over 2 million cards; one of provider distributes the card on website, post office and couriers and it can be funded through mobile payments; some of the cards are virtual	
Singapore	The banks are fully liable for the stored value collected (more than 20 providers and over 15 million open-loop prepaid cards in circulation); one provider uses contactless technology primarily in transport sector and small retail (close to 10 million cards); another provider uses smart card technology retail purchases (close to 6.5 million cards)	
Slovak Republic	12 providers (banks) have issued almost 4 million cards; agents can serve as intermediaries and are covered under the Payment Services Directive (2007/64/EC)	
South Africa	Four different card types all issued by one bank and branded by Visa; over 100 000 cards	

Countries	Short description of NPM	Examples of limits
St. Vincent & the Grenadines	Two providers have issued over 16 000 cards; prepaid debit cards are only issued by local banks and there no intermediaries	
Sultanate of Oman	All prepaid are bank issued of which 2 are Visa International linked. No further information provided on products. (4 providers with close to 120 000 accounts)	
Sweden	Swedish credit institutions and Swedish financial institutions are allowed to issue prepaid debit cards.	
Ukraine	Not much info provided – just stats regarding STRs and possible cases involving prepaid cards	
United Kingdom	FSA regulates e-money issuers. Not all issuers are also providers of prepaid cards	
United States	Federal Reserve estimated that there were USD 13,3 billion worth of open-loop prepaid card purchase transactions in the US in 2006 (compared to $2,4 trillion for credit cards) – many different prepaid cards are available and can be funded using wire transfers or with cash at agents locations; some programs are managed by third parties who are responsible to identify customers and provide all transaction data to the issuing bank and notify the bank of suspicious transactions; some issuing banks manage their own programs; a new regulation currently under consideration, would require among other things that certain non-bank businesses managing prepaid card programs register with the US federal government	

B. Access to Activity

Countries	Registration/Licensing (Y/N)	Supervision (Y/N)	Additional Information
Argentina	Y	Y	
Australia	N	Y	
Belarus	Y	Y	
Belgium	Y	Y	
Brazil	Y	Y	
Bulgaria	Y	Y	

Countries	Registration/Licensing (Y/N)	Supervision (Y/N)	Additional Information
Canada	Y	Y	Prepaid cards are not explicitly covered under Canada's AML/CTF regime but most issuers and distributors are covered
Cayman Islands	Y	Y	
Colombia	Y	Y	
Denmark	Y	Y	
Estonia	n/a	n/a	
European Union	Y	Y	
France	Y	Y	
Germany	Y	Y	Institutions issuing e-money must verify identity of customer and record it (although not needed to do it by means of reliable documents) for all types of cards – even when non-reloadable and under 150 EUR or reloadable and under 2 500 EUR within one year
Gibraltar	Y	Y	
Italy	Y	Y	
Japan	Y	Y	
Lebanon	Y	Y	
Luxembourg	Y	Y	
Macao	Y	Y	
Mexico	Y	Y	
Netherlands	Y	Y	
Norway	Y	Y	
Peru	n/a	n/a	
Philippines	Y	Y	
Portugal	Y	Y	
Republic of Armenia	Y	Y	
Republic of Poland	Y	Y	

Countries	Registration/Licensing (Y/N)	Supervision (Y/N)	Additional Information
Russia	Y	Y	
Singapore	Y	Y	
Slovak Republic	Y	Y	
South Africa	Y	Y	
St. Vincent & the Grenadines	Y	Y	
Sultanate of Oman	Y	Y	
Sweden	Y	Y	
Ukraine	no info	no info	
United Kingdom	Y	Y	
United States	Y for issuing banks; currently N for non-bank issuers and 3rd party program managers	Y	

C. AML/CFT Provisions

Countries	Customer Due Diligence (Y/N)	Record-keeping (Y/N)	Suspicious transaction Reporting (in 2009)	Other AML Policies & Procedures (Y/N)
Argentina	Y	Y	14	Y
Australia	Y	Y	Yes but no exact number available	Y
Belarus	Y	Y	1 348 (June 1, 2009 to May 31, 2010)	n/a
Belgium	Y	Y	16	Y
Brazil	Y	Y	951	n/a
Bulgaria	Y	Y	none	Y
Canada	Y for issuing banks; currently N for 3rd party program managers if not an	Y for issuing banks; currently N 3rd party program managers if not an	10 re open-loop & 80 re closed-loop	Y

Countries	Customer Due Diligence (Y/N)	Record-keeping (Y/N)	Suspicious transaction Reporting (in 2009)	Other AML Policies & Procedures (Y/N)
	MSB	MSB		
Cayman Islands	Y	Y	320 in 2008/09	n/a
Colombia	Y	Y	96 re open-loop 22 re closed-loop	Y
Denmark	Y	Y	none	Y
Estonia	n/a	n/a	n/a	n/a
European Union	Y	Y	none	Y
France	Y	Y	none	Y
Germany	Y	Y	25	Y
Gibraltar	Y	Y	42	Y
Italy	Y	Y	122	Y
Japan	N	Y	none	N
Lebanon	Y	Y	none	Y
Luxembourg	Y	Y	none	Y
Macao	Y	Y	40	Y
Mexico	Y	Y	5	Y
Netherlands	Y	Y	none	Y
Norway	Y	Y	Not able to distinguish	Y
Peru	n/a	n/a	n/a	n/a
Philippines	Y	Y	301 in 2009	Y
Portugal	Y	Y	none	Y
Republic of Armenia	Y	Y	8	Y
Republic of Poland	Y	Y	none	Y

Countries	Customer Due Diligence (Y/N)	Record-keeping (Y/N)	Suspicious transaction Reporting (in 2009)	Other AML Policies & Procedures (Y/N)
Russia	Y	Y	none	N
Singapore	Y	Y	85	Y
Slovak Republic	Y	Y	none	Y
South Africa	Y	Y	48 since July 2009	Y
St. Vincent & the Grenadines	Y	Y	none	Y
Sultanate of Oman	Y	Y	details with Royal Oman Police	Y
Sweden	Y	Y	none	Y
Ukraine	no info	no info	2107	no info
United Kingdom	Y	Y	105	Y
United States	Y for issuing banks; currently N for non-bank issuers and 3rd party program managers	Y for issuing banks; currently N for non-bank issuers and 3rd party program managers	Y for issuing banks; currently N for non-bank issuers and 3rd party program managers; 836 reported in 2008 by banks, MSBs and securities firms	Y

D. AML/CFT Cases – Illegal operators

Countries	Legally possible to use service anonymously (Y/N)	Law Enforcement Cases (Y/N)	Illegal Operators
Argentina	n/a	N	n/a
Australia	Y	Y	N
Belarus	N	N	unknown
Belgium	N	Y	N
Brazil	n/a	N	N
Bulgaria	Y	N	N
Canada	N	Y	N

Countries	Legally possible to use service anonymously (Y/N)	Law Enforcement Cases (Y/N)	Illegal Operators
Cayman Islands	N	N	unknown
Colombia	Y	Y	none
Denmark	Y	N	Cannot be disclosed
Estonia	N	One international case already provided by other country	n/a
European Union	Y	N	n/a
France	N	N	none
Germany	N	Y	none
Gibraltar	Y	N	N
Italy	Y	4 recurring schemes	N
Japan	Y	N	N
Lebanon	N	N	N
Luxembourg	N	N	N
Macao	N	2 cases which appear to involve bank debit cards (not sure if they are prepaid) or credit cards	N
Mexico	Y	No examples provided but indicated 3 formal complaints and 10 intelligence reports	N
Netherlands	Y	N	One provider offered or wanted to offer service without a license
Norway	N	N	N
Peru	n/a	n/a	n/a
Philippines	N	Y	N
Portugal	N	N	N
Republic of Armenia	Y for cards with maximum load of 1 300 USD	N	N
Republic of Poland	N	N	N

Countries	Legally possible to use service anonymously (Y/N)	Law Enforcement Cases (Y/N)	Illegal Operators
Russia	Y for cards less than 500 USD	N	N
Singapore	Y for cards with load limit of 1 000 USD or less	N	N
Slovak Republic	N	N	No info provided
South Africa	N	No details provided but mentioned that cases usually involve 419 scams (telemarketing fraud) and ACB credit fraud	N
St. Vincent & the Grenadines	N	N	N
Sultanate of Oman	N	No details provided but referred to phishing and skimming cases – details with Royal Oman Police	N
Sweden	N	N	N
Ukraine	no info	2 schemes and 2 cases provided but not very clear	no info
United Kingdom	N	2 generic examples – not real cases	N
United States	Y (Mastercard and Visa limit anonymous cards to 500 USD and 750 USD respectively)	Y	N

Internet Payment Services

The number (17) of countries reporting the presence of IPS providers remains almost the same as the one reported (15) in 2006. These refer to services which include online payments to merchants, to individuals (p2p) which are account-based. They can be funded by bank transfers, credit card, prepaid card, other IPS accounts and digital currency providers. Three additional countries only reported the presence of online banking services which are directly linked to bank accounts and not covered in this report.

Nineteen out of 37 jurisdictions reported some form of licensing and registration requirements, as well as supervision and AML/CFT provisions for IPS providers. One country reported no licensing or registration requirements but indicated that such providers were supervised. Only four countries indicated that it was possible to open IPS accounts anonymously under certain conditions such as when transactions are conducted under a low threshold.

A total of 14 case studies included in this report were provided by seven different countries. Five additional countries referred cases for which not enough details were provided or it was impossible to provide them because of legislative limitations. All countries for the exception of two countries reported that no illegal operator was known to operate in their jurisdiction.

A. Description of Internet Payment Services

Countries	Short description of NPM
Argentina	Cannot determine the numbers – same regulations than for financial institutions
Australia	A few providers are operating in this jurisdiction but no statistics were available
Belarus	A few providers appear to be operating in this jurisdiction and to fall under same regulations as banks but response to questionnaire was not clear
Belgium	No stats re providers and number of accounts
Brazil	2 providers
Bulgaria	Three providers with a total of about 45 000 accounts
Canada	One Internet payment services provider • Funding through local bank deposits, bank transfers (domestic & international), credit and debit cards • Redemption through prepaid cards, bank transfers (domestic and international) and cheques Four digital currency exchangers
Cayman Islands	No providers – however, such providers would be considered money remitters and therefore would be covered by Cayman Islands' Money Services Law
Colombia	Online payment service providers are not authorised in Colombia, therefore not subject to regulation and supervision; however, some online payment service providers seating in other jurisdictions are active in Colombia
Denmark	No info regarding online payment services
Estonia	11 credit institutions provide online banking services (not covered in this report) – not clear if it also includes online payment services; however, a new legislation which should be effective by the end of May 2010 will cover new payment institutions and electronic money institutions
European Union	18 online payment service providers in the EU (over 90 million accounts but not all active) – two main ones have 65 million and 10 million accounts respectively
France	Few online payment services in France (23 million customers by end of 2009)
Germany	No Internet payment system provider seated in jurisdiction but a number of IPS seated in

Countries	Short description of NPM
	European Economic Area (EEA) conducting business in Germany – licensed through the —European passport"
Gibraltar	No legislation currently in force requiring providers to register
Italy	One main provider – no other info provided
Japan	No info about providers
Lebanon	No providers seating in jurisdiction
Luxembourg	Only one provider – about 60 million in Europe and about 18 million that are active
Macao	Information provided appears to involve online banking services and not online payment services such as IPS providers covered in this report
Mexico	No information provided
Netherlands	One IPS linking customer's bank account to online purchases; also allowing payments to other Dutch bank accounts – 45 million transactions made in 2009 by 10 million bank accounts with a total turnover of 3.4 billion EUR
Norway	Information appears to be referring to online banking services (140 banks and 12 million accounts?)
Peru	No providers seated in jurisdiction and no regulations currently exist but are under consideration
Philippines	No statistics provided as both online banking services (not covered in this report) and online payment services cannot be distinguished; only banks were mentioned for their online banking services
Portugal	Not aware of any online payment service seated in jurisdiction
Republic of Armenia	No providers yet but draft legislation has been prepared to cover such providers
Republic of Poland	No info provided
Russia	About 23 providers – two main ones sharing about 90% of the market; total of about 13 million accounts; accounts can be funded through cash-in terminals (cash is deposited at the terminals and funded into e-money account by providing account number), post office, prepaid cards and e-currency exchangers
Singapore	MAS does not regulate non-FI online payment services and therefore does not have relevant info on them.
Slovak Republic	Provided info on both online banking services (not covered in this report and online payment services) for a total of 21 providers – number of online payment services not clearly identified
South Africa	No providers but Banks Act would cover such accounts since such providers would need to obtain a bank licence or partner with a bank
St. Vincent & the Grenadines	No providers
Sultanate of Oman	23 providers with almost 80 000 accounts – however appears to refer to online banking services and MSB services (*i.e.,* related to remittances?)
Sweden	Swedish credit institutions and Swedish financial institutions are allowed to offer online payment services – no other info provided
Ukraine	No information available as the online payment service is just about to be established
United Kingdom	Three main providers
United States	One main provider reported to have 81 million active accounts, and others are operating in the US

B. Access to Activity

Countries	Registration/Licensing (Y/N)	Supervision (Y/N)	Additional Information
Argentina	Y	Y	
Australia	N	Y	
Belarus	Y	Y	
Belgium	Y	Y	
Brazil	N	N	
Bulgaria	N	N	
Canada	Y	Y	IPS and digital currency exchangers considered money services businesses – and therefore need to register with FINTRAC and required to report suspicious transactions
Cayman Islands	Y	Y	
Colombia	N	N	
Denmark	n/a	n/a	
Estonia	Y	Y	
European Union	Y	Y	
France	Y	Y	
Germany	Y	Y	
Gibraltar	n/a	n/a	
Italy	Y	Y	
Japan	n/a	n/a	
Lebanon	n/a	n/a	
Luxembourg	Y	Y	
Macao	Y	Y	
Mexico			
Netherlands	Y	Y	
Norway	Y	Y	
Peru	n/a	n/a	
Philippines	Y	Y	
Portugal	n/a	n/a	
Republic of Armenia	n/a	n/a	
Republic of Poland	n/a	n/a	
Russia	N	N	

Countries	Registration/Licensing (Y/N)	Supervision (Y/N)	Additional Information
Singapore	n/a	n/a	
Slovak Republic	Y	Y	
South Africa	Y	Y	
St. Vincent & the Grenadines	n/a	n/a	
Sultanate of Oman	Y	Y	
Sweden	Y	Y	
Ukraine	n/a	n/a	
United Kingdom	Y	Y	
United States	Y	Y	Considered money transmitters and therefore covered by AML/CTF regime

C. AML/CFT Provisions

Countries	Customer Due Diligence (Y/N)	Record-keeping (Y/N)	Suspicious transaction Reporting (in 2009)	Other AML Policies & Procedures (Y/N)
Argentina	Y	Y	none	Y
Australia	Y	Y	Yes but no exact number provided	Y
Belarus	Y	Y	n/a	n/a
Belgium	Y	Y	3	Y
Brazil	N	N	none	N
Bulgaria	N	Y	3	Y
Canada	Y	Y	150	Y
Cayman Islands	Y	Y	none	Y
Colombia	N	N	5	N
Denmark	n/a	n/a	n/a	n/a
Estonia	Y	Y	29 received from providers of alternative payment services	Y
European Union	Y	Y	none	Y
France	Y	Y	70	Y
Germany	Y	Y	61	Y
Gibraltar	n/a	n/a	n/a	n/a
Italy	Y	Y	2	Y

Countries	Customer Due Diligence (Y/N)	Record-keeping (Y/N)	Suspicious transaction Reporting (in 2009)	Other AML Policies & Procedures (Y/N)
Japan	n/a	n/a	none	n/a
Lebanon	n/a	n/a	n/a	n/a
Luxembourg	Y	Y	About 500	Y
Macao	Y	Y	7 but possibly related to online banking and not IPS	Y
Mexico	n/a	n/a	317 re Internet fraud	n/a
Netherlands	Y	Y	Only one in 2006	Y
Norway	Y	Y	n/a	Y
Peru	n/a	n/a	n/a	n/a
Philippines	Y	Y	n/a	Y
Portugal	n/a	n/a	n/a	n/a
Republic of Armenia	n/a	n/a	n/a	n/a
Republic of Poland	n/a	n/a	n/a	n/a
Russia	N	Y	n/a	N
Singapore	n/a	n/a	1021 mostly related to goods traded using online payment services	n/a
Slovak Republic	Y	Y	7 between 2005 and 2008, none in 2009	n/a
South Africa	Y	Y	none	Y
St. Vincent & the Grenadines	n/a	n/a	n/a	n/a
Sultanate of Oman	Y	Y	none	Y
Sweden	Y	Y	none	Y
Ukraine	n/a	n/a	n/a	n/a
United Kingdom	Y	Y	73	Y
United States	Y	Y	Over 18,000	Y

D. AML/CFT Cases – Illegal operators

Countries	Legally possible to use service anonymously (Y/N)	Law Enforcement Cases (Y/N)	Illegal Operators
Argentina	n/a	N	n/a
Australia	Y if under low threshold of AUD 1 000	Y	N
Belarus	n/a	n/a	n/a

Countries	Legally possible to use service anonymously (Y/N)	Law Enforcement Cases (Y/N)	Illegal Operators
Belgium	n/a	Y	n/a
Brazil	N	N	N
Bulgaria	N	No details provided but mentioned that three cases developed by the FIU involved foreign online payment service providers	n/a
Canada	N	Y	none
Cayman Islands	N	N	N
Colombia	n/a	3 cases but not clear if related to ML through online payment services	n/a
Denmark	n/a	N	n/a
Estonia	N	No details provided but mentioned that typical crimes are phishing and other Internet fraud schemes	N
European Union	Y	N	n/a
France	N	Y	none
Germany	N	Y	Issued two cease-and-desist orders against foreign online payment service providers conducting business in Germany
Gibraltar	n/a	n/a	n/a
Italy	Y	N	n/a
Japan		Y	
Lebanon	n/a	n/a	n/a
Luxembourg	N	Ongoing cases but not able to share info at this point	N
Macao	n/a	n/a	n/a
Mexico	n/a	N	n/a
Netherlands	N/A?	N	5 or 6
Norway	N	n/a	N
Peru	n/a	n/a	n/a
Philippines	N	n/a	N
Portugal	n/a	n/a	n/a
Republic of Armenia	n/a	n/a	n/a
Republic of Poland	n/a	n/a	n/a
Russia	Y (when registering with two main providers, one can choose between anonymous	N	no info

Countries	Legally possible to use service anonymously (Y/N)	Law Enforcement Cases (Y/N)	Illegal Operators
	and registered account – the latter allows more services)		
Singapore		Y	
Slovak Republic	N	N	n/a
South Africa	N	N	N
St. Vincent & the Grenadines	n/a	n/a	n/a
Sultanate of Oman	N	details with Royal Oman Police	N
Sweden	n/a	N	n/a
Ukraine	n/a	N	n/a
United Kingdom	N	N	N
United States	Y	Y	Y (US has prosecuted online payment services that failed to register and failed to obtain licenses)

Mobile Payment Services

The number (16) of countries reporting the presence of mobile payment services providers has tripled in relation to the number (5) reported in 2006. These refer to services that are account-based which can be funded by bank transfers, credit card, prepaid card, and other NPMs. They are the services that use SMS or NFC technology. Two additional countries reported the testing of mobile payment services in their jurisdiction while two other countries only reported online banking services (directly linked to bank accounts) which are really the extension of banking services that are not covered in this report.

Twenty-one out of 37 jurisdictions reported some form of licensing and registration requirements, as well as supervision and AML/CFT provisions for mobile payment services providers. Only three countries indicated that it was possible to open mobile payment service accounts anonymously.

Only three case studies included in this report were provided by two countries. All countries reported that no illegal operator was known to operate in their jurisdiction.

A. Description of Mobile Payment Services

Countries	Short description of NPM	Examples of limits
Argentina	No information provided	
Australia	A number of mobile banking providers are operating in this jurisdiction but no specific statistics were provided regarding the number of accounts	
Belarus	No information provided	
Belgium	One provider recently established offering payments for small purchases and P2P payments; account loaded by bank transfers, credit card or debit card; payments done by SMS or by Internet mobile; considering offering international wire	

Countries	Short description of NPM	Examples of limits
	transfers in the future between Belgium and Northern Africa	
Brazil	One mobile service model is being tested	
Bulgaria	Three providers with a total of about 26 000 accounts	
Canada	Seven providers including five which are an extension of online banking and two that offer mobile banking through SMS – one of the latter, offered by telecommunications company, also offer a prepaid card on which funds can be transferred from mobile banking account; accounts can be funded by credit card, debit or prepaid card, or through wire transfers	Individual transactions limited to 250 CAD and 1 000 CAD is the maximum balance for the account
Cayman Islands	No providers – however, such providers would be considered money remitters and therefore would be covered by Cayman Islands' Money Services Law	
Colombia	No providers in jurisdiction but legislation covers such services which can only be offered by credit institutions	
Denmark	A number of mobile payment providers are available but no details were provided.	
Estonia	3 credit institutions offer mobile banking with over 250 000 accounts (however, nearly 82 000 seem to be inactive); SMS and NFC technology are both used	
European Union	Estimate of 8 providers in EU; accounts can be funded by credit card or bank transfers, and between account holders with the same mobile payment provider; payments done using SMS	
France	No providers yet but mobile payment services using NFC technology are being tested	
Germany	No mobile payments provider available	
Gibraltar	No providers	
Italy	Discussions about offering such services, some initiatives underway but no provider yet established	
Japan	No information provided	
Lebanon	No providers seating in jurisdiction	
Luxembourg	3 providers but no details	
Macao	No information provided	
Mexico	No providers but legislation applied to banking institutions could apply in terms of operational limits	
Netherlands	Two services available that are linked to a bank account and payments are made through SMS; one model using near-field communication (NFC) technology was tested but was not successful	One of them has a limit of 2 500 EUR in payments per year
Norway	2 providers with about 5 million customers	
Peru	Four banks offer online banking services through mobile phones and therefore are covered under AML regime; mobile payment services offered by non-bank entities are not currently regulated but such measures are under consideration	
Philippines	21 providers including banks and one non-bank provider; most of these relate to online banking services done through mobile phones; however, one e-money provider (non-bank institution and a wholly-owned subsidiary of a telecommunications company) offers a digital currency	

Countries	Short description of NPM	Examples of limits
	service (with over 1 million accounts) on mobile phones at the same time as providing digital currency exchange services (cash to e-money and vice-versa); another provider offers SMS technology to banks providing mobile services	
Portugal	Not aware of any mobile payment service seated in jurisdiction	
Republic of Armenia	No providers yet but draft legislation has been prepared and is under discussion.	
Republic of Poland	No information provided	
Russia	A number of different providers with the number of accounts reaching about 15 million in 2009 and the volume of mobile payments reaching about USD 230 million; SMS technology used to purchase services and goods, as well as transferring funds to another mobile payment account holder	
Singapore	There are several mobile payment service operators testing various types of services including ones using NFC technology. MAS does not supervise or regulate such service operators and therefore does not have additional info.	
Slovak Republic	3 providers	
South Africa	One current provider (with 40 000 active accounts) and another one under development	
St. Vincent & the Grenadines	No providers	
Sultanate of Oman	4 providers with over 120 000 accounts offered by telecommunications companies and banks, using SMS at least for one program	
Sweden	Swedish credit institutions and Swedish financial institutions are allowed to offer mobile payment services – no other info provided	
Ukraine	No information available as the mobile payment service is just about to be established	
United Kingdom	The industry has yet to take off in the UK. Mobile phones only used as a communications methods with a payment service provider, rather than the phone being the payment instrument itself.	
United States	Mobile payment services market is still in the start-up stages but some providers are present – some services are linked to bank accounts (extension of online banking) but some are linked to IPS and sometimes offered in combination with prepaid cards or credit card providers	

B. Access to Activity

Countries	Registration/Licensing (Y/N)	Supervision (Y/N)
Argentina	n/a	n/a
Australia	Y	Y
Belarus	n/a	n/a
Belgium	Y	Y
Brazil	N	N
Bulgaria	Y	Y

Countries	Registration/Licensing (Y/N)	Supervision (Y/N)
Canada	Y when offered by banks	Y when offered by banks
Cayman Islands	Y	Y
Colombia	Y	Y
Denmark	Y	Y
Estonia	Y	Y
European Union	Y	Y
France	Y	Y
Germany	Y	Y
Gibraltar	n/a	n/a
Italy	Y	Y
Japan	n/a	n/a
Lebanon	n/a	n/a
Luxembourg	Y	Y
Macao	n/a	n/a
Mexico	Y	Y
Netherlands	Y	Y
Norway	Y	Y
Peru	Y (when linked to bank account)	Y (when linked to bank account)
Philippines	Y	Y
Portugal	n/a	n/a
Republic of Armenia	n/a	n/a
Republic of Poland	n/a	n/a
Russia	Y (banks and telecom companies)	Y (banks) N (telecom companies)
Singapore	n/a	n/a
Slovak Republic	Y	Y
South Africa	Y	Y
St. Vincent & the Grenadines	n/a	n/a
Sultanate of Oman	Y	Y
Sweden	Y	Y
Ukraine	n/a	n/a
United Kingdom	Y	Y
United States	Y	Y

C. AML/CFT Provisions

Countries	Customer Due Diligence (Y/N)	Record-keeping (Y/N)	Suspicious transaction Reporting (in 2009)	Other AML Policies & Procedures (Y/N)
Argentina	n/a	n/a	none	n/a
Australia	Y	Y	none	Y
Belarus	n/a	n/a	n/a	n/a

Countries	Customer Due Diligence (Y/N)	Record-keeping (Y/N)	Suspicious transaction Reporting (in 2009)	Other AML Policies & Procedures (Y/N)
Belgium	Y	Y	none	Y
Brazil	N	N	n/a	N
Bulgaria	Y	Y	none	Y
Canada	Y when offered by banks	Y when offered by banks	5	Y when offered by banks
Cayman Islands	Y	Y	none	Y
Colombia	Y	Y	none	Y
Denmark	Y	Y	none	Y
Estonia	Y	Y	none	Y
European Union	Y	Y	n/a	Y
France	Y	Y	none	Y
Germany	Y	Y	none	Y
Gibraltar	n/a	n/a	n/a	n/a
Italy	Y	Y	n/a	Y
Japan	n/a	n/a	n/a	n/a
Lebanon	n/a	n/a	n/a	n/a
Luxembourg	Y	Y	none	Y
Macao	n/a	n/a	n/a	n/a
Mexico	Y	Y	n/a	Y
Netherlands	Y	Y	none	Y
Norway	Y	Y	Cannot distinguish	Y
Peru	Y (when linked to bank account)	Y (when linked to bank account)	none	Y (when linked to bank account)
Philippines	Y	Y	194	Y
Portugal	n/a	n/a	n/a	n/a
Republic of Armenia	n/a	n/a	n/a	n/a
Republic of Poland	n/a	n/a	n/a	n/a
Russia	Y (banks) N (telecom companies)	Y (banks & telecom companies)	Y (banks) – none N (telecom companies)	n/a
Singapore	n/a	n/a	n/a	n/a
Slovak Republic	N	Y	One STR in 2009	Y
South Africa	Y	Y	none	Y
St. Vincent & the Grenadines	n/a	n/a	n/a	n/a
Sultanate of Oman	Y	Y	none	Y
Sweden	Y	Y	n/a	Y
Ukraine	n/a	n/a	n/a	n/a
United Kingdom	Y	Y	none	Y

Countries	Customer Due Diligence (Y/N)	Record-keeping (Y/N)	Suspicious transaction Reporting (in 2009)	Other AML Policies & Procedures (Y/N)
United States	Y	Y	31 (2008)	Y

D. AML/CFT Cases – Illegal operators

Countries	Legally possible to use service anonymously (Y/N)	Law Enforcement Cases (Y/N)	Illegal Operators
Argentina	n/a	n/a	n/a
Australia	Y	N (one case was provided but it was unclear if it was related to the type of mobile payment services covered in this report)	N
Belarus	n/a	n/a	n/a
Belgium	N	N	N
Brazil	n/a	n/a	n/a
Bulgaria	N	n/a	N
Canada	Y	N	N
Cayman Islands	N	Y	N
Colombia	N	N	N
Denmark	Y	N	N
Estonia	N	N	N
European Union	Y	n/a	N
France	N	N	N
Germany	N	n/a	N
Gibraltar	n/a	n/a	n/a
Italy	n/a	n/a	n/a
Japan	n/a	n/a	n/a
Lebanon	n/a	n/a	n/a
Luxembourg	N	N	N
Macao	n/a	n/a	n/a
Mexico	N	n/a	n/a
Netherlands	N	N	none
Norway	N	N	N
Peru	N	N	N
Philippines	N	Y	N
Portugal	n/a	n/a	n/a
Republic of Armenia	n/a	n/a	n/a
Republic of Poland	n/a	n/a	n/a
Russia	Y	N	N
Singapore	n/a	n/a	n/a
Slovak Republic	N	N	N

Countries	Legally possible to use service anonymously (Y/N)	Law Enforcement Cases (Y/N)	Illegal Operators
South Africa	unknown	N	unknown
St. Vincent & the Grenadines	n/a	n/a	n/a
Sultanate of Oman	N	Details available with Royal Oman Police	N
Sweden	n/a	n/a	n/a
Ukraine	n/a	n/a	n/a
United Kingdom	N	N	none
United States	Y	N	none

APPENDIX B: EXCERPTS FROM THE 2006 REPORT ON NEW PAYMENT METHODS

This section provides an overview of the general characteristics and functions of specific New Payment methods, as described in the 2006 typologies report on New Payment Methods. These excerpts are presented in order to provide readers that are not familiar with the general working mechanisms of NPMs, with a general overview of the technical background of these instruments. For more detailed information, interested readers are referred to the 2006 report itself, which contains more information and features additional instructive appendices (www.fatf-gafi.org/dataoecd/30/47/37627240.pdf).

Prepaid cards

Prepaid payment cards provide access to monetary funds that are paid in advance by the cardholder. While there are many different types of prepaid cards that are used in a variety of ways, they typically operate in the same way as a debit card and ultimately rely on access to an account. There may be an account for each card that is issued or, alternatively, there may be a pooled account that holds the funds prepaid for all cards issued. The cards may be issued by, and accounts may be held at, a depository institution or a non-bank organization; pooled accounts would be normally held by the issuer at a bank.

Prepaid cards can be issued for limited or multiple purposes. Limited-purpose or *closed system* prepaid cards can be used for only a limited number of well-defined purposes and their use is often restricted to specific points of sale or for specific services. Examples include merchant-issued gift cards, prepaid long distance service, and mass transmit system cards. These cards may either be limited to the initial value posted to the card (non-reloadable) or may allow the card holder to add value (up to a certain limit) and reuse the card (reloadable). The issuer of the card or its service provider typically operates the network on which the cards can be used. The value on the cards generally is linked to a prepaid account established by the issuer or service provider. Transactions are processed in a similar fashion to transactions involving debit or credit cards.

Multipurpose or *open-system* prepaid cards can be used across a broader range of locations for a wider range of purposes. Such cards may be used on a national or international scale but may sometimes be restricted to a certain geographical area. Multipurpose cards may be used by the person who purchased the card or by someone else. Examples include payroll cards and general purpose "cash cards" for individuals without bank accounts or a credit card. These cards are usually associated with a card payment network, such as Visa or MasterCard, which permits them to be used in the same manner as a debit card to make purchases or to get cash from an automated teller machine (ATM). Some issuers do not require the cardholder to have a depository account. These cards are distributed by merchants, depository financial institutions, and money/value transfer (MVT) systems for a variety of purposes. Most are reloadable.

---

[15] The expression "bank account" used in this box refers to accounts held at financial institutions that are subject to AML requirements.

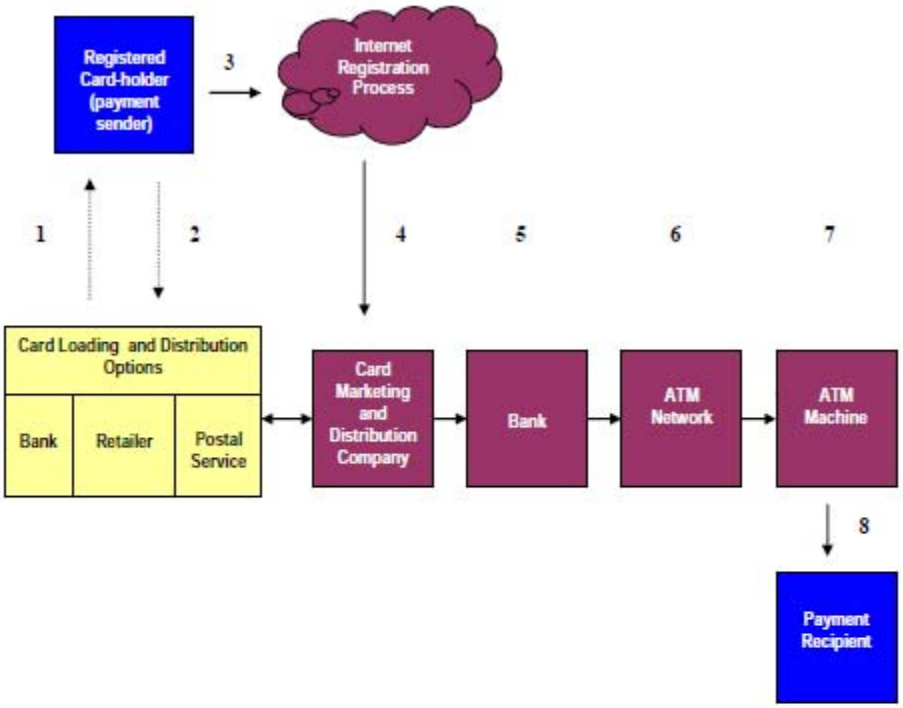


Figure 1 The process of issuing an open-system, magnetic strip, prepaid card varies by issuer. Steps (1), (2), and (3) above may occur in any order. In those three steps an individual completes the registration process for a prepaid card, prepays funds into the card account, and receives the card. Step (4) is the transfer of registration information to the service provider. When a card carries a bank association service mark (as in the case of MasterCard- or Visa-branded cards), the service provider must contract with a bank (5) in order to have access to the global ATM networks (6). Individual ATM machines (7) connect to local networks and often global networks allowing individuals in one country (8) to access funds held in another country.

Electronic purse

An electronic purse, or e-purse (also referred to as a "stored value card" as the value is stored on the card), is value stored electronically in a device such as a card with an integrated circuit chip (called a smart card or chip card).[16] Unlike a card with a magnetic stripe, which stores account information, an e-purse actually stores funds on the card's memory chip. The user is literally carrying his funds with him on the card (hence the name electronic purse).

In some e-purse programs value can be transferred from the card directly to participating merchants or another individual without the transaction going through an account at an intermediary. This may limit the amount of

[16] This definition augments slightly the normal CPSS usage of the term "electronic purse" to also encompass the term "electronic money". For the purposes of this report, the term electronic purse is "a reloadable, multi-purpose prepaid card which may be used for small retail or other payments instead of coins" where the "value is stored electronically in a device such as chip card."

identifying information available with such transactions. To obtain funds from an e-purse payment, however, the merchant or individual must redeem the value from an account held by the e-purse provider at the e-purse issuing institution. As the funds are on the card, no online connection and no cardholder identification are needed to make a payment. The electronic purse function was designed to substitute for cash in everyday situations. Today, electronic purses are mainly used for micropayments such as for public transportation, parking tickets or vending machines.

The development and use of card-based e-purses has declined considerably over the past decade so that very few e-purse systems remain in existence. In addition, these few remaining e-purse solutions are generally not interoperable regardless of the market in which they operate. Only one system, the German GeldKarte that operates in the border area of Germany and Luxemburg (See Figure 2), is known to be used in multiple national jurisdictions. Furthermore, e-purses usually have a limited storing capacity for funds (e.g. the German GeldKarte has a load limit of EUR 200).



Figure 2

Mobile Payments

Mobile payments refer generally to the use of mobile phones and other wireless communications devices to pay for goods and services. Payments are initiated from a mobile communications device using voice access, text messaging protocols (such as short/single messaging service or SMS), or wireless application protocols (WAPs) that allow the device to access the Internet. Authorization often occurs by keying in a unique personal identification number (PIN) associated with the customer or mobile device. Adoption of mobile payments varies from country to country. Use of mobile phones as a means to initiate payments is relatively widespread in Southeast Asia and in some European countries.[17]

Most mobile payment services simply use the phone as an access device to initiate and authenticate transactions from existing bank accounts or payment cards.[18] This is the equivalent of using the Internet to initiate a direct debit or credit transfer from a bank account, or a credit or debit card transaction. This is an extension of traditional payment methods.

New mobile payments: Where mobile payment services are not based on an underlying bank or payment card account, the telecom operator typically acts as a payment intermediary to authorize, clear, and settle the payment.[19] Telecom companies engaged in these activities may not be overseen by a country's central bank or other banking regulator but may be subject to AML/CFT measures.

The telecom operator may either allow the phone owner to charge certain transactions to the phone bill (post-paid) or may permit the phone owner to fund an account held by the telecom operator or other service provider for the purposes of making payments (prepaid). Prepaid mobile payments accounts operate in the same manner

---

[17] See CPSS, "Policy issues for central banks in retail payments," BIS, CPSS #52, March 2003, at http://www.bis.org/publ/cpss52.htm.

[18] See CPSS, "Survey of developments in electronic money and internet and mobile payments," BIS, CPSS #62, March 2004, at http://www.bis.org/publ/cpss62.htm.

[19] Telecom companies offering mobile payment services provide for the settlement of the payment transactions completed via their systems through normal banking channels.

as a prepaid card or an electronic purse. When the phone is used in the same manner as a prepaid card, the phone owner uses the phone as a payment system access device to authorize the deduction of value from the prepaid account. When the phone functions as an e-purse, the prepaid value is stored on the subscriber identify module or SIM card within the mobile phone.

Post-paid and prepaid card-like mobile payments are much more common than e-purse mobile payments. In the case of prepaid mobile payments, telecom providers often offer this service in conjunction with a bank. For example, in the Philippines two telecom companies offer mobile payment services, Globe Telecom and Smart Communications. Smart Communications' Smart Money is co-branded with Banco de Oro. The transactions and funds transfers Smart Money users initiate via their mobile phone are authorized against a prepaid account held at Banco de Oro. Smart Money users can also send cross-border remittances by providing relatives with a MasterCard-branded prepaid card linked to the Smart Money account that can be used to withdraw cash from an ATM.

Globe Telecom serves as the intermediary for funds transfers using G-cash and operates without a bank partner. As a result, Globe customers cannot withdraw funds from their prepaid accounts at ATMs but only over the counter at participating businesses. Figure 3 illustrates a G-Cash funds transfer from one Globe Telecom subscriber to another using SMS. Both G-Cash and Smart Money are subject to AML/CFT regulations (including suspicious transaction reporting) and supervision.

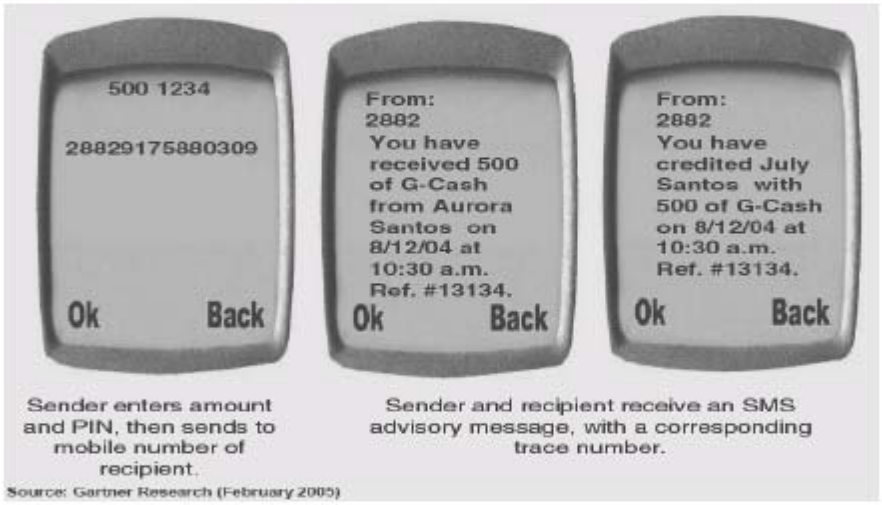


Figure 3 G-Cash Phone-to-Phone Remittance

Internet payment services

The expression "Internet payment services" is generally used to address: (i) payment services that rely on a bank account and use the Internet as a means of moving funds to or from a bank account; and (ii) payment services provided by non-bank institutions operating exclusively on the Internet and that are only indirectly associated with a bank account.

In the former case, Internet payment services refer to traditional payment methods where the Internet is only an innovative channel to exchange the information that is needed to move the funds from one account to another, which allows customers to access their bank accounts from home, 24 hours a day.

Where Internet payment services do not rely directly on a bank account, such as PayPal, individuals can transfer funds, shop online, or participate in online auctions, using a pre-funded account; however, the payment service provider may not be subject to the same AML/CFT measures that apply to banks. The service provider usually

will not have a face-to-face relationship with its customers. Depending upon the accessibility of the Internet payment service, these activities can involve payments or funds transfers across national borders.

Some non-bank Internet payment services allow customers to hold accounts with the payment service provider, while others offer only to send or receive individual payments using the customer's existing bank or credit card account. When non-bank Internet payment services offer customer accounts they may pool those customer funds in a single account at a bank. The account may be held in the name of the service provider. In that case, the bank holding the service provider's account may have no direct relationship with the service provider's individual customers.

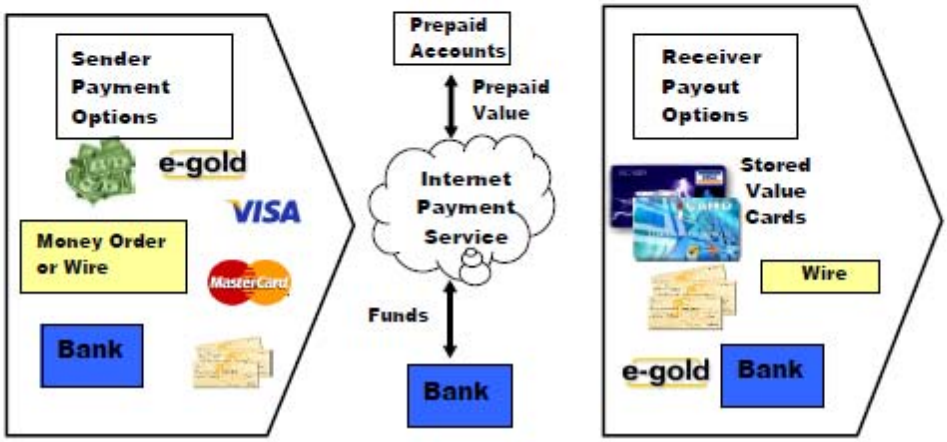


Figure 4

While a limited number of similar products exist in certain countries, PayPal appears to be the most widely used non-bank, Internet-based NPM. PayPal primarily functions as a payments intermediary for individuals and organizations that wish to trade with each other or transfer funds via the Internet. PayPal operates by allowing an individual to set up a pre-paid account in his name with PayPal that can be funded from a credit or debit card or a bank account via a credit transfer. Using those pre-paid funds, individuals can buy items or transfer funds to other PayPal account holders. The payment or transfer of funds occurs as a book-entry transaction between the PayPal accounts. When an individual wishes to access the funds in his PayPal account, he directs PayPal to credit his credit or debit card or bank account via a credit transfer or even a paper check.

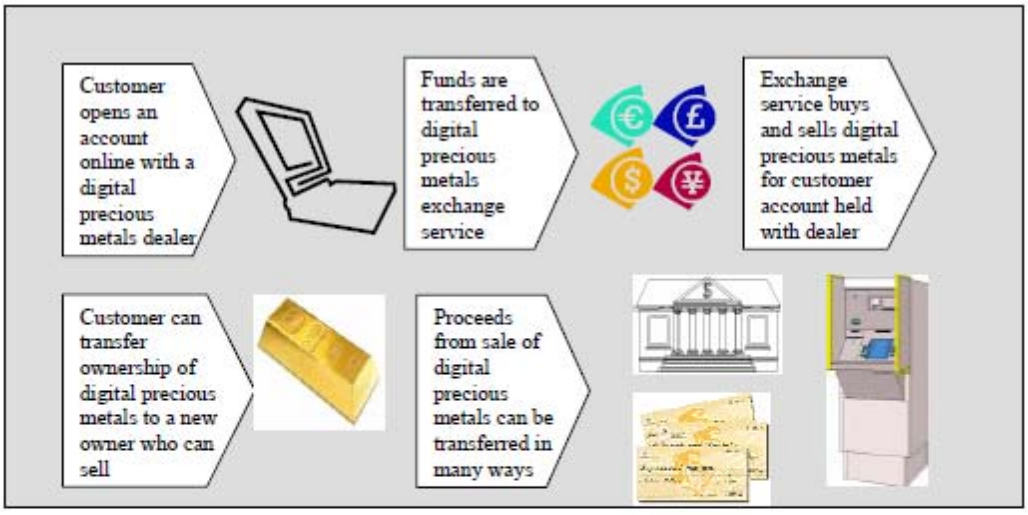
Service providers will differ as to the methods of payment they will accept to initiate a funds transfer, and the methods of payment they will use to distribute funds to the recipient. Figure 4 above illustrates how an individual can use a bank-issued credit card or other traditional payment methods to fund an Internet-based transaction account and subsequently make purchases or transfer all or a portion of the prepaid value to another account holder via book-entry by the service provider. The recipient can then use those funds to conduct additional transactions or withdraw the money via a traditional retail payment method. Online money transfer services set their own terms as what form of payment they will accept from senders and what forms of payment they make available to receivers.

Digital precious metals[20]

Digital precious metals are a relatively new online MVT system that involves the exchange of options or the right to purchase an amount of precious metals at a specific price. These derivatives can be exchanged, like traditional commodity or securities derivatives, between account holders in a digital precious metal service. Consumers purchase a quantity of virtual precious metal holdings based on the current price of the metal on the world commodity exchanges. Once a purchaser has acquired a quantity of the virtual precious metal, those holdings or a portion of them can be transferred either to another individual or a merchant in exchange for goods and services.

The oldest and best known of the digital precious metals dealers is e-gold Ltd., which claims to have almost 2 million accounts.[21] According to e-gold and other digital precious metals dealers, the rationale for using this store of value is to facilitate online transactions without regard for underlying currencies or access to foreign exchange. Transactions involving digital precious metals have immediate finality, which may appeal to online merchants that must pay high credit card interchange fees due to high fraud rates. Some digital precious metals dealers also allow users to maintain anonymous accounts. These traits are concerning to U.S. federal law enforcement agencies.

The transaction process associated with transferring the virtual holdings of precious metals between account holders can involve two separate service providers: the digital precious metals dealer, which maintains the accounts that contain the virtual holdings of precious metals; and the digital precious metals exchange service, which can act as a broker for the digital precious metals that the dealers buy or sell. Some dealers transact directly with account holders. Upon completion of a transaction, the selling account holder transfers ownership of his virtual precious metal holdings to the purchaser and can receive the proceeds of the sale through a variety of traditional and non-traditional payment methods (See Figure 5).



[20] The issuers of digital precious metals use the term "digital currency" to describe the barter arrangement they facilitate. Because of the potential confusion this common industry term would create with the term "e-purse" and "e-money", we have adopted the term "digital precious metals" for this report.

[21] E-dinar is a spin-off of e-gold and is affiliated with the Islamic Mint, a private organization working to revive the gold and silver currencies described in the Koran, the gold dinar and silver dirham. See: www.e-dinar.com.

Figure 5 Buying and selling digital precious metals typically involves working with two separate service provider categories: the digital precious metals exchange service and the digital precious metals dealer.

APPENDIX C: BIBLIOGRAPHY AND RELATED PUBLICATIONS ON NPMS AND ML/TF RISK

- Arthur D. Little (2009), *Global M-Payment Report Update – 2009*, April 2009, www.adl.com/uploads/tx_extthoughtleadership/ADL_Global_M_Payment_Report_Update_2009_Executive_Summary.pdf

- Australian Attorney-General's Department (2006), *Australian AML/CTF Act*, Act No. 169 of 2006 as amended, Table 1, Page 55, Item 23

- Bank for International Settlements (2009), *Statistics on payment and settlement systems in selected countries – Figures for 2008,* December 2009, www.bis.org/publ/cpss88.pdf.

- Basel Committee on Banking Supervision (2001), *Customer due diligence for banks*, section 2.2.6;

- Bester, H., D. Chanberlain, L. de Koker, C. Hougaard, R. Short, A. Smith and R. Walker (2008), *Implementing FATF Standards in developing countries and financial inclusion: Findings and guidelines,* FIRST initiative, South Africa

- Commission of the European Countries (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* and *amending Directive 77/780/EEC on the co-ordination of laws, regulations and administrative provisions relating to the taking up and pursuit of the business of credit institutions*, COM(1998)461 final, p. 10; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:1998:0461:FIN:EN:PDF

- Commission of the European Countries (2008), *Impact Assessment accompanying the Draft Proposal for a Directive of the European Parliament and of the Council amending Directive 2000/46/EC on the taking up, pursuit of and prudential supervision of the business of electronic money institutions*, SEC(2008)2572, p. 5; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SEC:2008:2572:FIN:EN:PDF

- De Koker, Louis: "The money laundering risk posed by low risk financial products in South Africa: Findings and guidelines", 2009, Journal of Money Laundering Control, Vol. 12, No. 4

- Direct Express Media (2008), *U.S. Treasury Introducing Direct Express® Debit Card to Social Security Recipients in Western state*s, www.directexpress.org/Media/News_9_3_08_West_Announcement.cfm

- FATF (2006), *Report on New Payment Methods*, FATF, Paris, www.fatf-gafi.org/dataoecd/30/47/37627240.pdf

- FATF (2008), *Money Laundering and Terrorist Financing vulnerabilities of commercial websites and Internet Payment Systems*, FATF, Paris, www.fatf-gafi.org/dataoecd/57/21/40997818.pdf
- FATF (2009a), *Risk Based Approach: Guidance for Money Service Businesses*, FATF, Paris, www.fatf-gafi.org/dataoecd/45/1/43249256.pdf.
- FATF (2009b), *Mutual Evaluation Report of New Zealand*, FATF, Paris, www.fatf-gafi.org/document/28/0,3343,en_32250379_32236963_43998044_1_1_1_1,00.html
- FATF (2010), *Mutual Evaluation of the Federative Republic of Brazil*, FATF, Paris, p. 98, www.fatf-gafi.org/document/53/0,3343,en_32250379_32236963_45538741_1_1_1_1,00.html
- Federal Register (2010), *Financial Crimes Enforcement Network; Amendment to the Bank Secrecy Act Regulations—Definitions and Other Regulations Relating to Prepaid Access, Proposed Rules,* Vol. 75, No. 123, Monday, June 28, 2010, http://edocket.access.gpo.gov/2010/pdf/2010-15194.pdf.
- Finextra (2010), *Safaricom brings M-Pesa to ATMs with Equity Bank partnership*, 18 January 2010, www.finextra.com/news/fullstory.aspx?newsitemid=20963.
- First Data (2009), *First Data Reveals Success Factors for Prepaid Cards in Europe*, 26 November 2009, www.firstdata.com/en_ae/about-first-data/media/press-releases/11_26_09
- Foster K., Meijer E., Schuh S., and Zabek A., (2010), *The 2008 Survey of Consumer Payment Choice*, No 09-10, Federal Reserve Bank of Boston, Boston, www.bos.frb.org/economic/ppdp/2009/ppdp0910.pdf
- Joint Money Laundering Steering Group(2010), *Joint Money Laundering Steering Group Guidance*, Part I Chapter V
- Official Journal of the European Union (2005), *Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (Text with EEA relevance)*, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:309:0015:0036:EN:PDF
- Official Journal of the European Union (2007), *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*, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:319:0001:0036:EN:PDF
- Official Journal of the European Union (2009), *Directive 2009 2009/110/EC of the European Parliament and of the Council 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,* Directive 2009/110/EC; OJ L 267 (10.10.2009), p. 7; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:267:0007:0017:EN:PDF
- Master Card (2010), *Independent Research Forecasts that the European Open-loop Prepaid Market Will Reach $156bn (€127bn) by 2017*, 3 June 2010, www.mastercard.com/us/company/en/newsroom/independent_research.html

- Payments Council (2010), *Payments Council, The Way We Pay 2010, The UK's Payment Revolution,* www.paymentscouncil.org.uk//files/payments_council/the_way_we_pay_2010_final.pdf,

- Payment News (2010), *MasterCard Releases Prepaid Market Sizing Report*, 12 July 2010, www.paymentsnews.com/2010/07/mastercard-releases-prepaid-market-sizing-report.html

- Securities and Exchange Commission (2009a), *Form 10-K, Annual Report Pursuant to Section 13 or 15(d) of the Securities Exchange Act for 1934 for the fiscal year ended September 30, 2009, VISA INC*, commission file No. 001-33977 filed 20 November 2009, Washington, USA, www.sec.gov/Archives/edgar/data/1403161/000119312509239249/d10k.htm, *accessed October 2010*.

- Securities and Exchange Commission (2009b), *Form 10-K, Annual Report Pursuant to Section 13 or 15(d) of the Securities Exchange Act for 1934 for the fiscal year ended September 30, 2009, MasterCard Incorporated*, commission file No. 001-32877, filed 18 February 2010, Washington, USA, www.sec.gov/Archives/edgar/data/1403161/000119312509239249/d10k.htm, *accessed October 2010*.

- South African Government Gazette (2010), *National Gazette No 33241 of 04-Jun-2010,* Volume 540, 002.

- South African Reserve Bank (2008), *Guidance Note 6/2008, Issued in Terms of Section 6(5) of the Banks Act, 1990: Cell-phone banking,* Pretoria, South Africa, 2008-05-07, www.reservebank.co.za/internet/Publication.nsf/LADV/18B4D18670F4E8EC422574520032B728/$File/G6+of+2008.pdf, *accessed October 2010.*

- UN Counter-Terrorism Implementation Task Force (2009), *Tackling the Financing of Terrorism*, CFITF Working Group Report, New York, 2009, www.un.org/terrorism/pdfs/CTITF_financing_ENG_final.pdf

- United Nations Development Programme Afghanistan (2009), *Law and Order Trust Fund for Afghanistan (Phase V), [01-10-2008- 31-12-2008] Quarterly project report [3rd Quarter, 1387]* www.undp.org.af/whoweare/undpinafghanistan/Projects/3rdQ08Reports/2009-01-29%20-%20Third%20Quarter%201387%20Progress%20Report%20-%20LOTFA.pdf

- Visa Corporate Site (2010), *Financial Inclusion - Pakistan eases burden of displaced citizens by delivering financial support through Visa,* www.currencyofprogress.com/_media/pdfs/case_studies/VISA_Inclusion-Pakistan.pdf, accessed October 2010

- World Bank (2008), Working paper Nr. 146, *Integrity in mobile phone financial services*, Washington, 2008, p. 18 ss., http://siteresources.worldbank.org/INTAML/Resources/WP146_Web.pdf

- World Bank (2009a), *Preventing Money Laundering and Terrorist Financing A Practical Guide for Bank Supervisors,* Washington, 2009, http://siteresources.worldbank.org/FINANCIALSECTOR/Resources/PMLTL.pdf

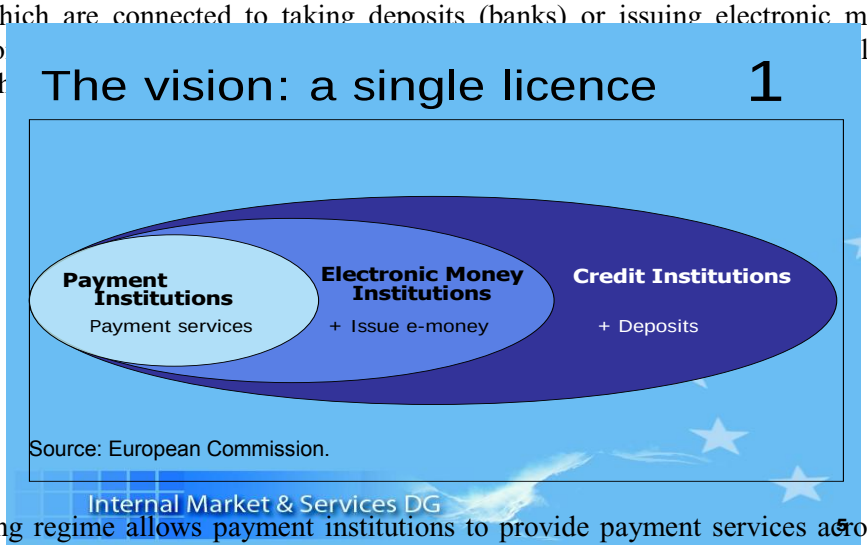
- World Bank (2009b), Working paper Nr. 174, *New technologies, New risks? Innovation and Countering the Financing of Terrorism*, Washington, 2009, http://siteresources.worldbank.org/FINANCIALSECTOR/Resources/New_Technogies.pdf

APPENDIX D: THE EU LEGAL FRAMEWORK FOR NEW PAYMENT METHODS

The EU legal landscape for payments has dramatically changed since 2006: Regulation (EC) No. 1781/2006 transposed FATF SRVII[92]; the Payment Services Directive (2007/64/EC - PSD') provided a supervisory regime for the provision of payment services by non-banks and harmonised the rules governing the provision of payment services across the EU, thus enacting FATF SRVI; the new E-Money Directive 2009/110/EC (the new EMD) will replace the current EMD (2000/46/EC). Besides such reforms, the third Anti-Money Laundering Directive (AMLD) 2005/60/EC[93], adopting a risk-based approach, envisaged thresholds for applying Simplified Customer Due Diligence to electronic money; such thresholds have been revised by the new EMD.

The Payment Service Directive: new entrants in the payments market

The PSD provides the legal foundation for the creation of an EU-wide single market for payments; from a supervisory point of view, it bans carrying out payment services without an appropriate licence or registration. A new category of payment service provider (the "payment institutions") has been created besides those which are connected to taking deposits (banks) or issuing electronic money (electronic money institutio lecommunication companies) will h



The licensing regime allows payment institutions to provide payment services across the entire EU territory. Examination of the AML/CFT scheme by competent authorities is part of the decision-making process following the application to become payment institution. In addition, following a risk-based approach, the PSD provides for a waiver regime[94] whereby natural or legal persons unable to meet all the

---

92 The provisions related to FATF SRVII were not considered relevant by the project team for the purpose of this report.

93 OJ L 309, 25.11.2005, p. 15–36.

94 This waiver regime aims to *"bring all persons providing remittance service within the ambit of certain minimum legal and regulatory requirements*

prudential requirements may nevertheless carry out payment services at national level; AML/CTF measures apply also to waived payment institutions.

A fundamental change introduced by the PSD was the abolition of the exclusivity principle pursuant to which entities engaged in financial activities could not carry out business activities: this reform allows new operators, including telecom or IT providers, to enter the payment market and develop innovative payment services.

To date, the PSD has been implemented in the vast majority of the Member States of the EU/EEA.[95]

The legal framework for e-money issuance

The issuance of e-money has been regulated in the EU since the year 2000. Electronic money can be issued by electronic money institutions or by banks: both categories of financial institutions are subject to prudential supervision.

The definition of e-money provided by the current EMD has posed many problems of interpretation mainly due to its absence of technical neutrality and the lack of clarity with regard to services falling within grey areas. This is why the new EMD refines the definition to substantially cover all situations where the payment service provider issues a pre-paid stored value in exchange for funds, which can be used for payment purposes because it is accepted by third persons as a means of payment[96].

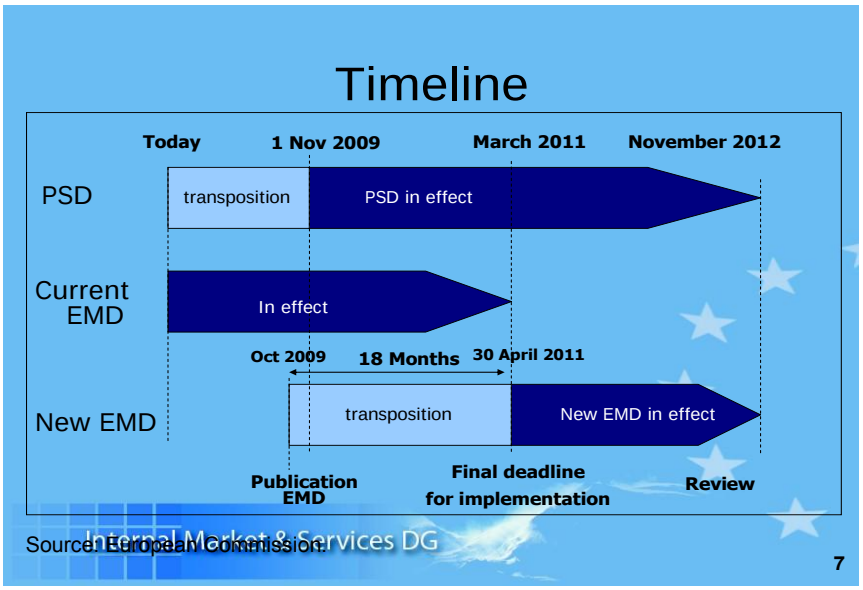
Another significant change introduced by the new directive is the further alleviation of prudential requirements for electronic money institutions and the extension of the activities they may engage in, to cover the full range of payment services and include the provision of credit facilities linked to the payment services provided. As a matter of fact, the too restrictive regime provided for by the first EMD was deemed to be the main cause of the lack of expansion of the e-money market in the EU outside the banking system[97]. The new regime for the issuance of e-money aims at facilitating market access to newcomers, namely telecommunication companies or large-scale retailers who want to engage in the market of e-money. Following the PSD, the exclusivity principle will no longer apply to EMIs. Such increased flexibility will facilitate cross-over of new payment methods (e.g., on-line payment accounts with m-payments) and with traditional payment methods used for the purpose of money remittance (e.g., money remitters with m-payments or prepaid cards).

---

95 The European Economic Area includes all EU Member States, Norway, Liechtenstein and Iceland.

96 In practice, electronic money can be either cards based or server based. In the former case the funds are stored on a chip of a physical smart card, in the latter mostly on a computer hard disk. The cards used for the storage of money can be prepaid-cards or so-called electronic purses. A special type of cards related e-money is the payment by way of using the SIM-cards of a mobile telephone. Server based e-money is also known as software or network money.

97 This legal framework restricted the e-money institutions' activities to the issuance of electronic money and the provision of closely related financial and non-financial services, such as the administering of e-money and the issuing and administering of other means of payment. This implied that activities such as mobile telecommunications services or retailing could not be performed by EMIs. Companies engaged in these businesses and willing to issue electronic money therefore had to split up their activities in two separate entities. Granting any form of credit was also an excluded activity. The framework included a strict prudential regime for electronic institutions, which was designed with the regime for banks as main point of reference.



Source: European Commission.

3. The Third Anti-Money-Laundering Directive (2005/60/EC)

The Third AML Directive (2005/60/EC) is the principal European Act setting Anti-Money Laundering measures; e-money institutions fall under its scope of application. This directive requires financial institutions and other players in key services and sectors to implement, inter alia, Customer Due Diligence (CDD) measures, *i.e.,* identify and verify the identity of their customers. Following a risk-based approach, simplified Customer Due Diligence is allowed in appropriate cases upon discretion of single Member States. Regarding the issuance of e-money products, the AMLD enables Member States to allow e-money issuers to apply simplified Customer Due Diligence where:

- if the device cannot be recharged, the maximum amount stored in the device is not more than EUR 150,
- if the device can be recharged, a limit of EUR 2,500 is imposed on the total amount transacted in a calendar year, except when an amount of EUR 1,000 or more is redeemed in that same calendar year by the bearer.

Most EU Member states define simplified CDD in this sense as applying no CDD measures at all (which is considered in line with the AMLD by the EU Commission). A few member states do not allow their EMI to refrain from CDD completely even in such "low-risk" cases as they believe this would not be in line with Recommendation 5 (cf. crit. 5.9 of the FATF methodology; this is discussed in detail in section 5.2 of the report).

The payments industry expressed some concerns according to which the requirements aimed at countering money laundering and terrorist financing - namely, full application of identification and record keeping requirements - pose a particular challenge in the case of electronic money due to the low average amounts involved in electronic money transactions; this is why the new EMD increases the former threshold for applying Simplified Customer Due Diligence. For non-rechargeable devices the threshold is increased up to EUR 250 (from the current EUR 150). Member States will also have the option to increase such threshold up to EUR 500 for national transactions only. For rechargeable devices the current threshold (EUR 2500) is maintained.

According to the information available to date, the vast majority of Member States has made use of the option for not applying CDD to e-money below the thresholds; with the transposition of the new EMD this choice could be confirmed. In those Member States where the option is not used, as well as in those cases where e-money instruments exceeding the correspondent thresholds are issued, normal CDD measures apply[98].

In all cases where the issuance of e-money instruments is linked to a bank account (*i.e.,* where it is typically the e-money institution itself issuing the product), CDD measures have to be applied when the account is opened and funded. The compliance with these obligations is subject to supervision by national competent authorities.

Notwithstanding the provisions described above, CDD measures must be applied in any case of a suspicion of ML/TF irrespective of the product or transaction.

[98] These obligations apply when: (i) establishing a business relationship; (ii) carrying out occasional transactions amounting to EUR 15 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked; (iii) there is a suspicion of money laundering or terrorist financing, regardless of any derogation, exemption or threshold; (iv) there are doubts about the veracity or adequacy of previously obtained customer identification data.

APPENDIX E: GLOSSARY OF TERMS

Agent

A person or business which acts on behalf of a principal entity in providing payment services. If the principal is a regulated financial institution, it is responsible for the actions of its agent and also remains liable for its own AML obligations. For the purposes of this report, the terms "agent" and "outsource" shall be considered synonymous.

For the purposes of FATF Special Recommendation VI, the glossary to the FATF methodology and the Interpretative Note to Special Recommendation VI define the term "agent" as follows:

"For the purposes of Special Recommendation VI, an *agent* is any person who provides money or value transfer service under the direction of or by contract with a legally registered or licensed remitter (for example, licensees, franchisees, concessionaires). "

Sub-Agent

A person or business acting on behalf of an agent to provide payment services.

"Bank based" business models

For the purposes of this report, bank based models are such models that require each customer to have an individual bank account in order to make use of the NPM service. The term does not stretch out to any business model that has any cooperation with a bank (*e.g.,* many NPM providers need to have a bank account in order to receive funds from customers, or to pay out funds to customers).

Brick-and-mortar exchanger

An exchanger that conducts all business on a face-to-face basis.

Card program manager

The entity responsible for establishing and running prepaid card business models in cooperation with a bank or electronic money institution. The program manager will usually market the prepaid cards and establish relationships with banks and distributors or customers. They typically do not themselves issue electronic money and are therefore not a regulated entity.

Some issuing institutions also manage their card programs themselves, *i.e.,* without cooperation with card program managers.

Cash vouchers

A prepaid product which can be purchased at several retailers and used for person - to -business (P2B) or person-to-person (P2P) transactions on the Internet.

Cash-back

Merchant points of sale (POS) used to withdraw cash by overpaying for purchased merchandise and receiving the overpaid amount in cash.

Customer Due Diligence (CDD)

According to FATF Recommendation 5, the customer due diligence (CDD) measures to be taken are as follows:

a) Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information[4].

b) Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include financial institutions taking reasonable measures to understand the ownership and control structure of the customer.

c) Obtaining information on the purpose and intended nature of the business relationship.

d) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

Digital currency exchanger

(See "Digital currency provider")

Digital precious metals

(See "Digital currency provider")

Digital currency provider (DCP)

A type of internet payment service. Digital currency providers (DCP) keep and administer accounts for their customers, but typically do not directly issue "digital currency" to their customers/account holders. Instead, customers purchase their digital currency from exchangers, who will then transfer the purchased amount of digital currency into the customers DCP account. Funds kept in DCP accounts may be denominated in fictitious currencies or in real currencies. A sub-type of DCP denominates the funds in units of precious metal and supposedly invests funds received in that respective precious metal as a means of deposit protection. These DCP are also called "Digital precious metals providers".

Distributor

A company that sells products produced by other companies to consumers. Distributors may also offer a range of services to their customers, such as technical support.

Intermediary

A very general term for a person or company that acts as a mediator between parties, acting in cooperation with the NPM provider to provide services to customers. The term covers all types of third parties that are in the chain between the NPM provider and the customer, potentially including agents, distributors, retailers, exchangers and others.

(Electronic) Point of Sale – (E)POS

Merchant or shop that accepts a certain payment method as a means of payment. A POS usually requires certain technical devices or terminals in order to be able to make use of the payment method (*e.g.,* a card terminal to swipe the prepaid card, or special software to integrate the possibility for paying via Internet payment services in online shops).

Electronic Money ("E-Money")

While the term "electronic money" is used in the FATF methodology´s definition of *financial institutions*, the glossary does not provide a definition of the term *electronic money* itself.

Some jurisdictions use "electronic money" as a technical term in their legislation. For example, Art. 2 para. 2 of the revised EU Electronic Money Directive defines electronic money as follows:

"„electronic money' means 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 (…)and which is accepted by a natural or legal person other than the electronic money issuer "[99].

Other jurisdictions´ definitions of electronic money may differ.

Electronic purse

An electronic purse, or e-purse (also referred to as a "stored value card" as the value is stored on the card), is value stored electronically in a device such as a card with an integrated circuit chip (called a smart card or chipcard).[100] For the purpose of this report, the term "electronic purses" is folded into the term "prepaid cards", as the method of storing the value (either centrally on a server or on the card itself) is no longer considered of relevance for the risk assessment of the card product.

Internet payment services

---

[99] EU Directive 2009/110/EC (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32009L0110:EN:NOT)

[100] FATF Report on New Payment Methods (www.fatf-gafi.org/dataoecd/30/47/37627240.pdf)

For the purposes of this report, the expression "Internet payment services" is used to address payment services operating exclusively on the Internet that are not or only indirectly associated with a bank account and may also be provided by non-bank institutions[101]. The expression does not include payment services that rely on a bank account and use of the Internet as a means of moving funds to or from a bank account ("online banking").

Merchant

A business that sells goods or services to consumers and maintains an arrangement with an acquirer to process transactions.

Mobile banking

Users can access traditional banking services through their mobile telephone. This is different from mobile payments in the sense that the regulated entity is a bank providing traditional banking services.

- **Mobile financial information services**

  Users may view personal account data and general financial information, but transactions cannot be executed using the service.

- **Mobile bank and securities account services**

  Users may transact in a similar fashion to internet banking.

Mobile payment services

Allows non-bank and non-securities account holders to make payments with mobile phones. However, payment service providers may be non-traditional financial institutions with widely varying controls and supervision measures.

Mobile money services

A subtype of mobile payment service, where subscribers are able to store actual value on their mobile phone (similar to e-purses). They may use phone credits or airtime as tender for payment. Such systems offer versatility but may fall out of regulation and prudential supervision altogether.

Money or value transfer service

Money or value transfer service refers to a financial service that accepts cash, cheques, other monetary instruments or other stores of value in one location and pays a corresponding sum in cash or other form to a beneficiary in another location by means of a communication, message, transfer or through a clearing network to which the money/value transfer service belongs. Transactions performed by such services can involve one or more intermediaries and a third party final payment.[102]

Money remittance

---

101 FATF Report on New Payment Methods (www.fatf-gafi.org/dataoecd/30/47/37627240.pdf)

102 See glossary to the FATF methodology.

A term commonly used to describe international money or value transfers by economic migrants to their home nation.

Negotiability

The level of acceptance across retailers for different payment methods. Some payment methods may have high negotiability because they are widely accepted but others may be very limited.

New payment methods (NPM)

For the purposes of this report, the term "New Payment Methods" encompasses prepaid cards, mobile payment services and internet payment services (IPS).

Open-loop prepaid card

A prepaid card which can be used at a wide range of terminals (vs. closed-loop prepaid cards with limited negotiability)

Outsourcing

An arrangement between a company and a service provider to provide services which would otherwise be carried out by the company itself. It is important to note that responsibility for ensuring compliance ultimately remains with the company. For the purposes of this report, the terms "agent" and "outsource" are used synonymously.

P2B

Person-to-business transaction.

P2P

Person to person transaction.

Phishing

Phishing is a criminal technique used to illegally obtain valuable information. For example, consumers will be sent fake e-mails from addresses that mimic those of banks. These emails will then dupe consumers into entering their account details.

Ponzi schemes

An investment scam that appears to pay high returns to investors. However these returns are paid from the investor's money or by incoming funds from new investors. The fraudster will either disappear with the money invested or the scheme will collapse.

Prepaid card

A payment card pre-loaded with funds. The card can then be used at businesses where the card type is accepted, including on the internet and abroad.

Prepaid card issuer

A bank or other financial institution that issues prepaid cards.

The term issuer is also used in connection with other types of NPM "value", *e.g.,* issuer of electronic money, or of digital currencies. The issuer is the entity that the customer has a contract with, and from whom the customer can demand redemption or withdrawal of funds.

Prepaid internet payment products

Products offered by firms which allow customers to send or receive funds through a virtual prepaid account. In some jurisdictions these firms may not fall within the definition of a "credit institution".

Processor

A company that processes transactions on behalf of an acquirer or merchant.

Red Flags

Indicators of suspicious activity where a product's actual use deviates from its expected usage. Red flags should therefore be tailored to the product's characteristics.

Smart cards

Cards featuring an electronic chip. This is usually used to process additional customer information.

Straw man

A real or fictitious individual used by others as a front for illegal activities such as money laundering and fraud.

Utility

A measure of the variety of payment options offered by a particular type of payment method. For example, some payment methods may offer person to business (p2b) transactions only while others may also allow for person to person (p2p) payments.

Virtual worlds

A simulated world which exists within a virtual environment. This commonly refers to computer games which are based on the internet such as Second Life. Often the economy is based upon a digital currency which can be bought and/or converted into real money.



FATF/OECD
December 2010

www.fatf-gafi.org