Financial Action Task Force
Groupe d'Action Financière

09-Aug-2010

English - Or. English

FATF/WGTY(2010)11/REV2
For Official Use

Working Group on Typologies

Draft Report on Money Laundering and Terrorist Financing through New Payment Methods

WGTYP, 18 October 2010, OECD Headquarters, Paris

FATF-XXII

Please note that this document is being circulated for comment from delegations with the intention that comments received will be incorporated and a further revision will then be circulated ahead of the October 2010 WGTYP Meeting. The report is complete except for the section concerning oversight of agents in the context of NPM. This section is currently being drafted by the project team and will be available for comment in the next version of the report.

Delegations should be aware that the project team intends to submit the next revised version [FATF/WGTYP(2010)11/REV3] for consultation with the private sector so that relevant input may be gathered prior to the October WGTYP Meeting.

Delegations are asked to submit written comments on this version of the document to the FATF Secretariat by 10 September 2010.

Vincent SCHMOLL, Tel: +33 1 45 24 17 52; vincent.schmoll@fatf-gafi.org
Alexandra ECKERT, Tel: +33 1 45 24 99 50; alexandra.eckert@fatf-gafi.org

JT03287282

English - Or. English

NPM REPORT
(CONCEPT 05-AUGUST-2010)

EXECUTIVE SUMMARY

- After the 2006 NPM report, the growing use of NPMs and an increased awareness of their money laundering and terrorist financing risks has led to the detection of a number of case studies over the last four years.

- Based on the analysis of 30 case studies, the project team has identified three main typologies related to the misuse of NPMs for money laundering and terrorist financing purposes:

    - Third party funding (including strawmen and nominees)

    - Exploitation of the non-face-to-face nature of NPM accounts

    - Complicit NPM providers or their employees

- Most case studies involved prepaid cards or Internet payments systems; among the cases submitted, mobile payment systems (three cases with apparently small amounts involved) only played a minor role.

- In relation to risk assessment, the project team used the same approach as presented in the 2006 NPM report, i.e. to assess the risk of each product or service individually rather than assessing an entire category of NPMs. To this end, the risk matrix presented in the 2006 NPM report has been amended and updated.

- 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 personalized products (i.e. circumvention of verification measures by using fake or stolen identities, or using strawmen or nominees etc.).

- The money laundering and terrorist financing 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.

- There is no uniform standard as to under what circumstances a product or service can be considered to be of "low risk". Some jurisdictions have implemented thresholds for NPM transactions or caps for NPM accounts and allow institutions to apply simplified CDD measures to NPM products that remain below such thresholds or caps; the thresholds and caps can vary significantly from jurisdiction to jurisdiction. Likewise, the assessment of the relevance of risk factors or of the effectiveness of risk mitigants may differ from jurisdiction to jurisdiction, due to respective legal and cultural differences.

- Some of the jurisdictions allow their institutions not only to apply simplified CDD measures in cases of low risk, but grant a full exemption from CDD measures. It is unclear whether such a practice is in line with FATF Recommendation 5.

- 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 Rec. 23; SR VI).

- 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 not subject to regulation and supervision. The concept of agents and outsourcing appears to be only marginally addressed in the FATF 40 Recommendations and 9 Special Recommendations, and there appears to be some inconsistency:

    - On the one hand, the FATF Methodology explains (with regard to FATF Recommendation 9) that an agent is to be regarded as synonymous with the financial institution, i.e. the processes and documentation are those of the financial institution itself. This has led most jurisdictions to the conclusion that there is no need for imposing supervision and legal ANML/CFT obligations onto agents as long as the principal is supervised and subject to AML/CFT obligations.

    - On the other hand, FATF SR VI postulates that agents involved in the provision of a service for the transmission of money or value be licensed or registered and subject to all FATF Recommendations that apply to banks and non-bank financial institutions. It remains unclear whether FATF SR VI is applicable to NPM service providers and their agents.

- Many NPM providers rely on the distribution of their products or services through the Internet, making use of the possibility of non-face-to-face establishment of customer relationships. According to FATF Recommendation 8, such non-face-to-face business relationships or transactions are associated with "specific risks". It remains unclear whether this means "high risk" in the sense of FATF Recommendation 5; if so, this would exclude many NPM providers from applying simplified CDD measures (as according to the IN to Rec. 5, simplified CDD measures are not acceptable whenever high risk scenarios apply).

- 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. 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. 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 NPMs alone.

Table of contents

1. Introduction

The 2006 report

1. 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.

2. 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.

3. 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.

4. 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

5. 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.

6. 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 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. It 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 activities in their business with NPM service providers, in order to increase the number and quality of STRs.

7. Although more case studies are now available, issues surrounding appropriate legislation and regulations for NPMs are still a challenge for most jurisdictions. Consequently, the report identifies those challenges and describes the different approaches currently taken by national legislators and regulators. A comparison of regulatory approaches can help inform other jurisdictions' decisions regarding the regulation of NPM.

8. Finally, this report considers the extent to which NPMs continue to be addressed appropriately by the FATF 40+9 Recommendations.

---

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

Steps taken by the project team

9. 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-six jurisdictions and the European Union Commission submitted a response.

10. The majority of the respondents identified NPMs within their jurisdiction. Prepaid cards were the most common (33 of the countries have such providers), followed by mobile payment services and Internet payment services (IPS) providers with 15 countries offering either one of the two NPM types.[4] Case studies were provided for the three NPMs: 17 cases involving prepaid cards, 12 cases involving Internet payment services and three cases involving mobile payment services.[5] A detailed summary is attached in Appendix A.

11. 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 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

12. 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.

13. 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.

---

[2] See annex for a list of publications used for this report.

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

[4] It should be noted that the statistics provided are based on the presence of each NPM in one country. Therefore, one country may be counted up to three times since it could have reported the presence of all three NPMs.

[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.

[6] Relevant sections of the 2006 report (including definitions) are cited as excerpts in Annex B…

2. Background

"New Payment Methods" and their development since 2006

14. 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.

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

15. New Payment Methods 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 as there was the 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]

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.[9]

Pakistan: Fighting forced more than a million people from their homes in 2009. The Government of Pakistan 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 $300). At the same time, a Pakistani bank and a payment card company installed wireless point-of-sale

[7] The World Bank, the Consultative Group to Assist the Poor (CGAP), the G-20 Access Through Innovation Sub Group and other organizations 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 (see list of publications in Annex … for papers issued by said organisations)..

[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.

[9] http://www.directexpress.org/Media/News_9_3_08_West_Announcement.cfm

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.[10]

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

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:[11]

"*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:[12]

"*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[13] 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."

Other studies on NPMs and ML/TF risks and vulnerabilities

17. 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.[14] In addition, there are a number of recent or ongoing typologies projects of FATF and FSRBs that touch upon this subject.[15] This shows

[10] http://www.currencyofprogress.com/_media/pdfs/case_studies/VISA_Inclusion-Pakistan.pdf

[11] COM(1998)461 final, p. 10;
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:1998:0461:FIN:EN:PDF

[12] SEC(2008)2572, p. 5;
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SEC:2008:2572:FIN:EN:PDF

[13] 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

[14] For a list of related publications see Annex ……..

[15] Recent or ongoing typologies projects include: FATF typologies report on Money Laundering and Terrorist Financing vulnerabilities of commercial websites and Internet Payment Systems (18. June 2008); MONEYVAL workshop on Cybercrime (ongoing); EAG workshop on internet payments (ongoing).

that the awareness of the opportunities and risks associated with NPMs has increased since the publication of the 2006 report.

18. 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.

2.1 Recent Developments Related to Prepaid cards

19. Prepaid cards can be split into two broad categories, open loop cards and closed loop cards.[16] This report focuses mainly on open loop cards[17] 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:

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 US$82,000 in restitution. One defendant was convicted of conspiracy and fraud and sentenced to 45 months imprisonment and 3 years supervised release. The other defendant was convicted of conspiracy and money laundering and sentenced to 5 months imprisonment and 3 years supervised release.

Source: United States

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 organization.

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

[16] For more details see the definition of prepaid cards as given in the FATF 2006 report (included as Annex B.x to this report).

[17] 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.

20. 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.[18] 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 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).[19]

21. 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.[20] For the US, the total funds loaded onto prepaid cards in 2009 are estimated to have been $120.2 billion, according to research commissioned by MasterCard, Inc. and conducted by the Boston Consulting Group (BCG).[21]

22. While about 17% of U.S. consumers have a prepaid card,[22] 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.[23]

23. Prepaid cards have been introduced in a number of countries, both within the EU and elsewhere, 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.[24] The

---

[18] The issue had come up after the mutual evaluation of Brazil; the assessment team had criticized Brazil for applying reduced CDD measures to such cards without having conducted a thorough risk assessment to determine the risk of such products first (MER Brazil 2010, p. 98).

[19] 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.

[20] 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 of consumer debit transactions for purchases of goods and services, with just over 84% of that volume taking place in the United States (Visa 2009 10K Report, Securities and Exchange Commission, Washington, DC, filed 20 November, 2009. (See: http://www.sec.gov/Archives/edgar/data/1403161/000119312509239249/d10k.htm). 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 (MasterCard 2009 10K Report, Securities and Exchange Commission, Washington, DC, filed 18 February, 2010 (see: http://www.sec.gov/Archives/edgar/data/1141391/000119312510034065/d10k.htm).

[21] http://www.paymentsnews.com/2010/07/mastercard-releases-prepaid-market-sizing-report.html

[22] Federal Reserve Bank of Boston, The 2008 Survey of Consumer Payment Choice, (See: http://www.bos.frb.org/economic/ppdp/2009/ppdp0910.pdf)

[23] 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: http://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, The Way We Pay 2010, UK; see http://www.paymentscouncil.org.uk//files/payments_council/the_way_we_pay_2010_final.pdf)

[24] http://www.mastercard.com/us/company/en/newsroom/independent_research.html

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." [25] 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)[26] the number of issued "cards with an e-money function"[27] has grown from 107.6 million in 2004 to 275.28 million in 2008 in selected CPSS countries.[28]

24. 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
Italy	8 million	**Mexico**	2.6 million
Norway	6 million	**Russia**	2 million
Singapore	5 million	**France**	1.3 million

25. 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")[29] are usually still limited to domestic use and often have rather low value limits.

26. 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 traveler 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.[30]

---

[25] First Data, http://www.firstdata.com/en_ae/about-first-data/media/press-releases/11_26_09

[26] Statistics on payment and settlement systems in selected countries – Figures for 2008 (December 2009). (see http://www.bis.org/publ/cpss88.pdf).

[27] 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.

[28] 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).

[29] See definition of e-purses in the FATF 2006 report on NPM, added to this report in Annex B.

[30] See also below in chapter 5.2, "identification of secondary card holders", para. 169 ss.

27. 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

28. 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.

29. 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.

30. 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 transfers.

31. 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 with 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.

32. Furthermore, **cash vouchers** have gained popularity in some markets. These vouchers can be bought anonymously at retailers, gas stations etc. and are usually sold in units ranging from as low as 10 euros up to 500 GBP (approx. 750 euros).[31] Cash vouchers are originally designed for person-to-business (p2b) payments on the Internet, but can also be used for person-to-person (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.

33. **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**.

34. 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

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

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.

2.3 Recent Developments Related to Mobile Payment Services

35. For the purposes of assessing risks and vulnerabilities it is essential to differentiate between mobile payments backed by a bank or securities account held at a financial institution that is subject to adequate AML/CFT regulation and supervision, and those services offered separately from such accounts. In this respect, it may be helpful to use the four categories of mobile payment systems described by the World Bank:[3233]

- 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 a bank or a security account 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.

36. 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).

37. 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.

38. Despite a predicted marked increase in the use and spread of mobile payments,[34] only a few providers have managed to run a successful and profitable business model in the long term so far.[35]

---

[32] World Bank Working paper Nr. 146 "Integrity in mobile phone financial services" 2008, p. 18 ss.

[33] 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.

[34] 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 Working Paper No 146: "Integrity in Mobile Phone Services" 2008). Other sources suggest that mobile phone transaction services will grow at 68% per year reaching almost US$ 250 billion in 2012 (Arthur D Little, Global M-Payment Report Update – 2009). These estimates do not only refer to mobile payments services in the sense of this report, but also include mobile banking services.

39. 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. However for countries providing such statistics, the estimated number of providers varied between one and 21. As for the estimated number of active mobile payment service accounts, it varied between 26,000 and 15 million accounts.

40. 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 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.

3. Risk assessment of NPMs

NPMs: risk vs. opportunity

41. 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.

42. 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.

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

[35] 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 have 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).

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.[36]

Source: United States

43. 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.[37] [38]

44. 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.[39]

NPMs and Terrorist Financing

45. 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 be explicitly noted in the text; otherwise most findings relating to money laundering apply to terrorist financing *mutatis mutandis*.

46. Out of the 30 case studies analysed in this report, only one has an obvious link to terrorist financing (see section 4: "Typologies", ***case 4***). There are reports about a second TF case; however the details of that case were not submitted to the project team.

Common risks of NPMs

47. 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. These shared characteristics and associated risks affect all NPMs:

- 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

[36] http://www.undp.org.af/whoweare/undpinafghanistan/Projects/3rdQ08Reports/2009-01-29%20-%20Third%20Quarter%201387%20Progress%20Report%20-%20LOTFA.pdf

[37] 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).

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

[39] See for example the "cross-border transport of cards" (chapter 4.4, para. 116 ss.) and "ghost employees" (chapter 4.2, para. 111 ss., case 17) examples in the typologies sections.

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"[40] ML/TF risks due to increased impersonation fraud risk and the chance that customers may not be who they say they are.

Assessing individual providers and products, not NPMs as such

48. 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

49. The 2006 report developed a risk matrix which featured several risk factors to assess the risk associated with individual NPM products.[41] 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.

50. 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).

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 the basis of reliable, independent source documents, data or information (cf. Rec. 5)	Customer's identity is verified on the basis of reliable, independent source documents, data or information (cf. Rec. 5)

[40] If read in conjunction with the Interpretative note to Rec. 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. …

[41] 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 nr. 146 "Integrity in mobile phone financial services" 2008, p. 17 ss.

	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
	Max. amount per transaction (incl. loading / withdrawal transactions)	no limit	no limit	Amount limit
	Max. transaction frequency	no limit	no limit	Transaction limit
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

51. 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.

52. 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

53. **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.

54. 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.[42]

55. For many NPM providers, customer contact is often minimal as a result of business relationships being conducted on a non-face to face basis. According to FATF Rec 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, but may also be relevant for other types of NPMs (e.g. online purchase of prepaid cards).

[42] 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 poit of contact to associate with reports of suspicious transactions.

56. 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").

57. 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 a robust national identification system be implemented as a prerequisite.[43] 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 risk mitigant (para. 98 ss.).

58. 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

59. 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 Rec. 10 nor the IN to Rec. 10 provide 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*."

60. These examples do not explicitly list the IP-addresses of customers initiating a payment transaction through a personal computer; which means that Rec. 10 does not contain an explicit instruction for institutions to collect and keep record of their customers´ IP-addresses.

61. Law enforcement agencies have reported investigation cases where providers had not kept record of IP-addresses at all, or not sufficiently, or had already deleted them before LEA 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

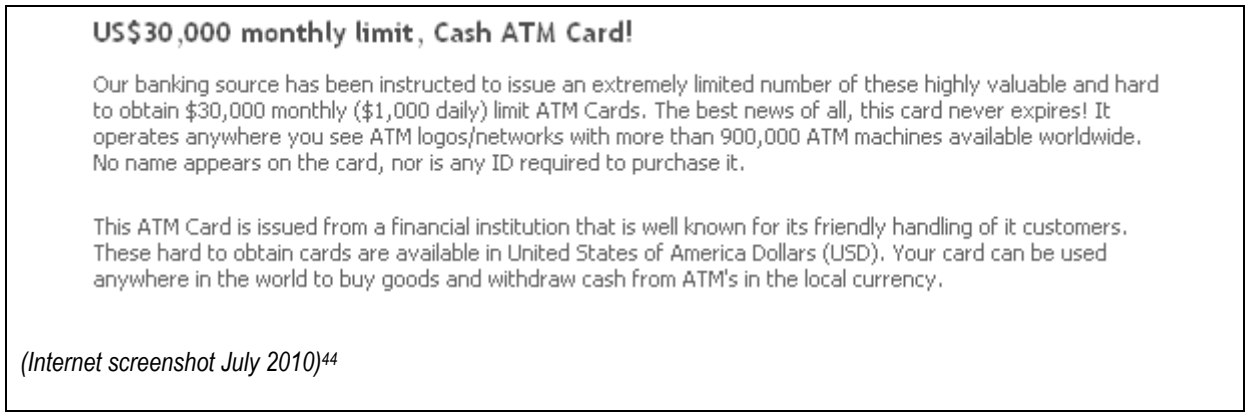
62. The term "value limits" refers to limitations on the maximum amount that can be held in a NPM account or product; or limitations on the maximum amount per single payment transaction; or limitations on the frequency or cumulative value of permitted transactions per day / week /month / year; or a combination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

[43] "Preventing Money Laundering and Terrorist Financing – A practical guide for bank supervisors", World Bank 2009, Annex 1 (A 1.1), p. 173 ss.,

63. 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.

64. 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.

65. 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 100 USD); on the other hand, there are reloadable cards with no or rather high account caps such as 30.000 USD per month.



(Internet screenshot July 2010)[44]

66. Such providers are often located 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, providers of anonymous prepaid cards also operate in jurisdictions whose regulatory regimes and supervision are generally considered robust.[45] Such anonymous cards are often not promoted by the issuing institution itself, but by intermediaries some of which have specialized in founding and selling companies abroad, preferably in tax havens, thus providing a complete "privacy package" to their customers. On the other hand, some of those anonymous prepaid cards have been discovered to be fraudulent.

67. 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

68. 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.

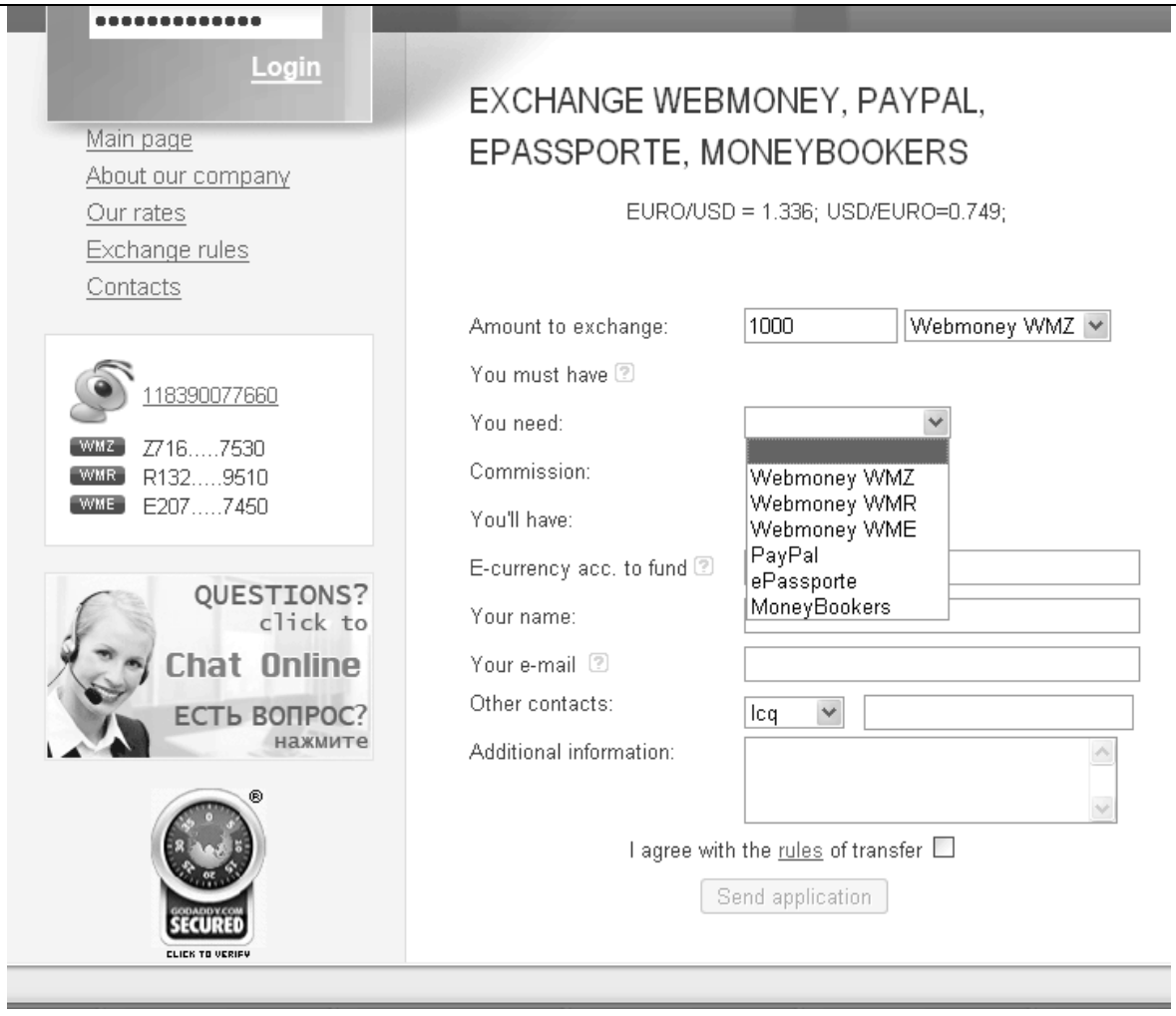
[44] As mentioned above, some offers of anonymous prepaid cards are fraud. The project team did not investigate whether the product advertised by this screenshot is fraudulent or not.

[45] 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.

69. 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.)[46] 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.

70. 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 cooperation with money remittance businesses, these may be used to not only fund the customers own personal account, but also to fund the account of third persons.

71. 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.



(Internet screenshot May 2010)

[46] 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.

72. 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.

73. 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 out of 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.

74. While many payment service providers who render cross-border services may cooperate well with their domestic supervisors and law enforcement agencies, some providers may refuse to provide information to foreign agencies unless compelled by formal legal assistance requests. Such 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. 81 ss.).

75. 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.

(Internet screenshot August 2010)

76. 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 accessed (initiated and received) from anywhere in the world. Most IPS providers offer their services globally, thus facilitating cross-border transactions.

77. 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). 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.

78. 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

79. 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.

80. Open-loop prepaid cards, especially when they are based on a well established and widespread technical standard (VISA, MasterCard) may 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 / 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[47] with those of regular 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 effected 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, 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, person to person payments are also facilitated (p2p).

  Most IPS and mobile payment services feature p2p-payments, but some are designed to facilitate person-to-business (p2b) payments for underlying shopping transactions only (e.g. cash vouchers), which generally decreases the ML/TF risk. However, where "merchants"[48] accepting such payments 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").[49] Easy cash access and high negotiability, coupled with the fact that prepaid cards[50]

---

[47] There are controls that countires 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.

[48] Which is a wider term and encompasses more than the classic online shop.

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

are much easier to transport than bulk cash (an ISO standard financial transaction card can be considerably more compact than currency[51]), may make prepaid cards a convenient substitute for cash in bulk cash smuggling ML schemes,[52] assuming a high account limit and/ or no verification of customer identification.

Most IPS and mobile payment services providers restrict the possibility to redeem 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 does not only increase 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 bank) even enables ATM access without the customer having to have neither a bank account nor 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.[53]

Segmentation of services

81. 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 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.

82. Where **agents** are used, this leads to a segmentation of services. Providers often use agents not only for cash acceptance and cash withdrawals, but also to establish new customer relationships. In most jurisdictions agents are under no or only limited supervision; agents usually cannot be sanctioned for breaching AML/CFT obligations as all regulatory responsibilities remain with the NPM provider. 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 one of the most difficult challenges for providers. These problems may exacerbate if a provider uses agents in a foreign jurisdiction.

---

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

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

[52] See chapter 4.4, para. 116 ss..

[53] Cf. www.finextra.com/news/fullstory.aspx?newsitemid=20963.

83. Where **agents** are used, this leads to a segmentation of services. Providers often use agents not only for cash acceptance and cash withdrawals, but also to establish new customer relationships. In most jurisdictions agents are under no or only limited supervision; agents usually cannot be sanctioned for breaching AML/CFT obligations as all regulatory responsibilities remain with the NPM provider. 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 one of the most difficult challenges for providers. These problems may exacerbate if a provider uses agents in a foreign jurisdiction.

84. 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 enhance if the cooperating money remittance business is located in a jurisdiction that does not enforce equivalent AML/CFT standards.

85. 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

86. 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.

87. 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

88. 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.

89. 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 minimize the potential for a customer to access multiple accounts, even if those are anonymous.

90. Some jurisdictions exempt firms from customer due diligence where the perceived ML/TF risk is 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.

91. 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.[54] 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), can add to the AML policies of a provider and help prevent a single customer from opening multiple accounts unnoticed.

92. 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.

93. Where NPMs can be used for p-2-p 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.

Monitoring

94. 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 analyzed, 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.

95. 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; and
- cases where several products are funded by the same source.

[54] Basel CDD paper October 2001, section 2.2.6; Joint Money Laundering Steering Group Guidance 2010, Part I Chapter V;

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

97. Effective Monitoring systems are also the basis for effective reporting of obligated NPM providers.

Value limits

98. 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[55].

99. 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. [56] 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.

100. 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 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.

101. 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".[57] 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

102. 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 personalized payment methods. 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).

103. 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

[55] As in South Africa's FIC Exemption 17 (to be expanded)

[56] See chapter 5.2 ("Degree of reduction of CDD"), para. 140 ss.

[57] See chapter 5.2 („The definition of low risk cases"), para. 139.

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.

4. Typologies and case studies

104. 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.[58]

105. 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.

106. 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 7, 9 and 28***) 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)

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

108. 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, 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.

109. 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 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.

110. 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.

[58] UN Counter-terrorism implementation task force: Working group report "Tackling the financing of terrorism" (October 2009), p. 14.

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 $60,000 in 11 months from his online steroid business. In another case, the defendant laundered about $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 organization involved onshore agents in the United States who recruited gamblers, collected losses, and distributed winnings, and an offshore organization 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 organizers 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 organizers would use the card accounts to make online or phone-based purchases. The online gambling operation earned about $100,000 a month.

Six defendants pleaded guilty to illegal gambling and were sentenced to 3 years probation. One defendant pleaded guilty to illegal gambling and money laundering and was sentenced to 3 years probation and six months home confinement. One defendant pleaded guilty to conspiracy and was sentenced to 4 years probation. One defendant pleaded guilty to bulk cash smuggling and was sentenced to 4 months imprisonment and 3 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

b. Internet Payment Services:

Case 5: 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 6: 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 US$459,000. Local law enforcement found CA$188,000in savings bonds that had been purchased with a portion of the proceeds. The individual was sentenced to two years in jail and fined CA$83,000.

Source: Canada

Case 7: Use of cash vouchers to collect extortion money

An unknown criminal sent an extortionate letter to a food discounter in Germany and demanded 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 8: 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 357,245 euros. Among those, 44 operations were credited via the IPS provider – for more than 300,000 euros. 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 5 years.

Source: France

Case 9: 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 4500-6000 EURO. 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. 500 EUROS 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

c. Mobile Payment Services:

Case 10: 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 G-cash (e-money account linked to mobile phone) to pay doctor's or hospital's bill.

Source: Philippines

Case 11: 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 G-cash to pay for taxes related to prizes.

Source: Philippines

Case 12: 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

111. Many NPMs rely on a business model where face to face custonmer contact is minimal or non existent. This can facilitate abuse by criminals for money laundering purposes.

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.

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.

112. 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).

113. 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 #24, 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 13: 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 $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 14: 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 $19,967.43 in illegally obtained funds. The defendants have not yet been tried.

Source: United States

Case 15: 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 16: 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 5,000 euros (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 17: 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 US$200,000. The defendant has not yet been tried.

Source: United States

Case 18: 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 US$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 unauthorized access devices. He was sentenced to 61 months imprisonment and five years supervised release.

Source: United States

Case 19: 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 US$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 20: Fraud and money laundering

In 2007, three defendants were prosecuted for illegally accessing a payment processor and initiating fraudulent transactions resulting in approximately $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 $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 21: Fraud and money laundering

In 2009, three defendants were charged with stealing $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 $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 22: 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 740,000 yen (US$8,300) to a digital currency exchanger to get "WebMoney" e-currency units. Then, the suspect sold off a portion of the WebMoney 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 23: 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 US$ 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 24: 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

114. 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.

115. In some instances (case studies #25, #27 and #28), both IPS and prepaid card providers were suspected to be complicit and colluding in facilitating the laundering of illicit proceeds.

a. Prepaid Cards

Case 25: 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 26: Embezzlement activities and money laundering

In 2007, a defendant was prosecuted for embezzling more than $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 27: 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 distributors / operators (in Canada and the United States) were knowingly or unknowingly used in this complex money laundering scheme.

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[59] 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

Case 28: 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 29: 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 US$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 30: 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

[59] 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.

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

116. 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 $500 and $1,500, allegedly depositing more than $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.

117. 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 US$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.

While the 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.

Two of the case studies submitted (***cases 19 and 25***) 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).

4.5 Red Flags

118. The analysis of the case studies identified red flags which are relevant to NPM products and services in general. In addition, a small number of red flags appear to be mostly associated 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.

119. 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 16***)
- Individuals who hold an unusual volume of NPM accounts with the same provider (***cases 18 and 20***)
- 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 5, 6, 13 and 14***)
- Multiple reference bank accounts from banks located in various cities used to fund the same NPM account (***case 24***)
- Loading or funding of account always done by third parties (***cases 1 and 3***)
- Multiple third party funding activities of a NPM account, followed by the immediate transfer of funds to unrelated bank account(s) (***cases 8 and 23***)
- Multiple loading or funding of the same accounts, followed by ATM withdrawals shortly afterwards, over a short period of time (***cases 15 and 16***)
- Multiple withdrawals conducted at different ATMS (sometimes located in various countries different from jurisdiction where NPM account was funded) (***cases 4 and 21***)
- NPM account only used for withdrawals, and not for POS or online purchases (***cases 15 and 16***)
- Atypical use of the payment product (including unexpected and frequent cross-border access or transactions) (***cases 2 and 21***)

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 25***)
- Prepaid card company located in one country but holding accounts in other countries (unexplained business rationale which could be suspicious) (***case 25***)
- 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 27***)
- 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 27***)

5. Legal issues related to NPMs

120. This chapter addresses how the provision of NPMs is regulated in different jurisdictions. **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

121. According to FATF Rec. 23, "*countries should ensure that financial institutions are subject to adequate regulation and supervision and are effectively implementing the FATF Recommendations.*" Similarly, FATF SR VI 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.*"

While the provision of NPMs can be considered a financial service in nature, not all jurisdictions consider all providers of such services a financial institution in the sense of Rec. 23 or a money transfer service in the sense of SR VI. Some providers are classified differently depending on the jurisdiction in which they operate. Where NPM providers are not regulated, they are unlikely to be subject to AML obligations. It is therefore important to understand how different NPM providers are regulated and supervised for AML and, more generally, prudential purposes.

122. 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 traditional financial institutions also applies to NPM providers, or they are subject to new regulatory regimes specific to NPM providers.

5.1.1 Not subject to regulation

123. In some jurisdictions certain NPMs are not subject to regulation. The degree of regulation differs depending on the type of NPM.

124. 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.[60]

125. However, where there is a segmentation of services through the use of third parties that are not "issuers" and do not fit into the traditional definitions of financial institutions, such third parties are usually not subject to regulation (e.g. card program managers, retailers etc.). The use of such third parties is usually regarded as either making use of agents or outsourcing. This issue is discussed in more detail below (See chapter 5.2 ("The use of agents / Outsourcing CDD measures"), para. 152 ss.).

126. 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.[61] 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 as the one provider mentioned before.

[60] See Annex A, table B for prepaid cards.

[61] See Annex A, Table B for Internet Payment services

127. 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.

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.

128. The provision of **mobile payment services** is regulated in most of the 15 jurisdictions that have identified domestic providers of such services.[62] 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,[63] 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 (...)."

129. 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 not subject to regulation.

5.1.2 Subject to regulation for traditional financial services

130. 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.

131. 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.

132. 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.[64]

133. 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.

---

[62] See Annex A, table B for mobile payment services.

[63] World Bank working paper no. 146 "Integrity in mobile phone financial services", May 2008, p. 53.

[64] See Annex A, ……

134. While 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.

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[65] 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.[66]

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.[67]

5.1.3 Subject to specifically designed regulation

135. Some jurisdictions have implemented a dedicated regulatory regime for providers of NPMs. For example, the EU has enacted an "Electronic Money Directive" which has 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 their activity.

The EU concept of "electronic money"

According to Article 2 no. 2 of the revised EU Electronic Money Directive(EMD)[68] 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;...*"

[65] The term „mobile payment" used by the Mexican authorities is not identical with the term „mobile payment" used in this report; see glossary.

[66] See chapter 5.2 ("The definition of low risk cases"), para. 139 or more details.

[67] Guidance note 06/2008; http://www.reservebank.co.za/internet/Publication.nsf/LADV/18B4D18670F4E8EC422574520032B728/$File/G6+of+2008.pdf

[68] 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

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[69]; 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 can not 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.[70]

136. The United States is currently considering the introduction of a new subtype of money services business called "provider of prepaid access".[71] 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.

5.2. Specific issues in regulation and supervision of NPM

137. 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
    - Definition of low risk cases
    - Full exemption from CDD?
    - Simplified CDD acceptable for non-face-to-face business models?
- Digital currency providers: the use of exchangers
- The use of agents / outsourcing CDD measures
- "Hybrid" service providers
- Law enforcement and supervisory action against providers seated abroad
- Identification of secondary card holders

[69] Directive 1007/64/EC; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:319:0001:0036:EN:PDF

[70] For more details on the EMD and its interconnectivity with the Payment Services Directive, see Annex …

[71] See above para. … on FinCen´s Notice of Proposed Rulemaking.

Simplified Customer Due Diligence

138. Several jurisdictions allow financial institutions to apply only 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 can CDD measures be reduced in designated cases of low risk?

The definition of low risk cases

139. Several jurisdictions have introduced in their legislation a concept of low risk scenarios where simplified due diligence can apply. Most jurisdictions rely mainly on value limits and transaction thresholds to define low risk scenarios. However, such limits and thresholds differ significantly among jurisdictions, ranging from USD 700 per month to USD 1,000 per day:[72]

EU:

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[73] as amended by the second e-money Directive[74], according to which 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."

USA:

According to the aforementioned Notice of Proposed Rulemaking[75], 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 $1,000 maximum value that can be initially loaded at the time of purchase of the prepaid access;

(ii) Not to exceed $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

[72] 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.

[73] 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; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:309:0015:0036:EN:PDF

[74] DIRECTIVE 2009/110/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:267:0007:0017:EN:PDF

[75] See. Para. 159.

(iii) Not to exceed $1,000 maximum value that can be withdrawn from the prepaid access device on a single day; "[76]

The reason for exempting such prepaid programs is that it is believed "*that the potential for misuse is slight*".[77]

South Africa:

When the South African anti-money laundering regulations were drafted in 2002, the Minister of Finance made an exemption under the Financial Intelligence Centre Act 38 of 2001 (FICA) to ensure that the lack of a verifiable residential address did not bar low income persons from access to appropriate financial services. This exemption, known as Exemption 17, relaxes the standard customer due diligence requirement that financial service providers must identify and verify a client's residential address. Exemption 17 was amended in 2004 to facilitate the launch of a basic bank account, the Mzansi account. This account was designed to meet the needs of the majority of South Africans who did not have access to financial services.

Currently Exemption 17 applies to all banks, mutual banks as well as the Postbank and the Ithala Development Corporation. It also extends to money remitters, but only in respect of remittances that originate and terminate in South Africa.

The exemption applies when the following conditions are met:

a) The customer must be a natural person who is a citizen of, or resident in, South Africa;

b) The business relationships and single transactions must not enable the customer:

(i) to withdraw or transfer or make payments of an amount exceeding R5 000,00 (USD 500) per day or exceeding R25 000,00 (USD 2500) in a monthly cycle; and

(ii) to effect a transfer of funds to any destination outside South Africa, except for a transfer as a result of a point-of-sale payment or a cash withdrawal in a country in the Rand Common Monetary Area.[78]

c) Should the business relationship outlined above, entail the holding of an account:

(i) the balance maintained in that account must not exceed R25 000,00 (USD 2500) at any time; or

(ii) the same person must not simultaneously hold two or more accounts which meet the criteria referred to above in a) and b), and are similar in nature, with the same institution.

d) If the balance in such an account exceeds R25 000,00 (USD 2500) or the customer acquires more than one such account with the same institution, no debit from that account may be effected before:

(i) the normal prescribed identification and verification steps are completed; and

(ii) the normal record-keeping requirements are met.[79]

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,

[76] NPRM (see para. 159), p. 75.

[77] Ibidem, p. 40.

[78] This refers to South Africa, Lesotho, Namibia and Swaziland.

[79] De Koker, L. (2009), "The money laundering risk posed by low risk financial products in South Africa: Findings and guidelines", Journal of Money Laundering Control, Vol. 12 No, 4

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.[80]

"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.[81]

Degree of reduction of CDD: full exemption from CDD?

140. FATF Recommendation 5 provides for the opportunity of applying simplified or reduced CDD measures in low risk cases, but does not specify the degree to which CDD measures may be reduced.

141. Several jurisdictions interpret Rec. 5 as granting a full exemption from CDD where the money-laundering and terrorist financing risk is low. 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.[82][83] As a result, several NPM products issued in the EU are effectively anonymous.[84]

142. This approach has been criticized in some mutual evaluations:[85]

Assessed country	**Quote from the evaluation report**
Luxembourg (February 2010)	*"Ceci est contraire aux normes du GAFI qui n´autorisent pas d´exonération de vigilance, mais*

[80] The file requires to be integrated only with the client basic data (name, address and birth date) and it is notrequired 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.

[81] 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.

[82] The European Commission has confirmed this interpretation of Art. 11(5)(d) of the third AMLD 2005/60/EC in its response submitted to the project questionnaire.

[83] 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.

[84] Mainly cash vouchers and some prepaid cards (open loop and closed loop), whereas IPS providers usually ask at least for the customers name (which may remain unverified though).

[85] Over the last five years, more than ten jurisdictions have been criticized for granting full exemptions from CDD rather than application of simplified or reduced CDD; the jurisdictions presented in this table have been chosen exclusively for the very clear wording used in their reports, i.e. the assessors explicitly stating that a full exemption is not in line with FATF Rec. 5. The assessments did not necessarily relate to NPMs, but to all types of financial services where there might be scenarios for low risk and simplified CDD.

	uniquement l´application de vigilances simplifiées ou réduites." (p. 126)
South Africa (February 2009)	*"The FATF Recommendations allow for simplified or reduced CDD measures where there are low ML/FT risks. However, parts of the following exemptions do not comply with the FATF Recommendations in that they fully exempt certain accountable institutions – which should be subject to the FATF Recommendations – from all CDD requirements (as well as some or all record keeping requirements)."* (p. 100)
Canada (February 2008)	*"These exemptions mean that, rather than reduced or simplified CDD measures, no CDD measures apply whatsoever for these cases, which is not in line with the FATF requirements that only permit reduced or simplified CDD in certain circumstances."* (p. 132)

On the other hand, that same approach was either not criticised in other evaluations, or did not have a negative impact on the rating of Rec. 5. As a result, there remains uncertainty whether full exemptions of CDD in cases of low risk can be considered in line with FATF Rec. 5 or not. This is currently being considered by other working groups within FATF.

Simplified CDD acceptable for non-face-to-face business models?

143. Another issue related to simplified CDD is the question whether according to the FATF 40 Recommendations it is acceptable to apply simplified CDD to non-face-to-face business models.

144. The Interpretative Note to Rec. 5 states:

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

Consequently, there would be no room for simplified CDD for non-face-to-face business, if it had to be assessed as a "specific higher risk scenario".

145. Non-face-to-face business is currently addressed by FATF Rec. 8,[86] 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."

FATF Rec. 8 does not explicitly speak of "higher" risks. However, the Interpretative Note to FATF Rec. 5 (para. 7) suggests that financial institutions should refer to the Basel CDD paper (section 2.2.6) for specific guidance, which says:

[86] FATF Rec. 8 is currently being revised, and the issue of non-face-to-face business may be removed from Rec. 8 and addressed elsewhere; cf. ……

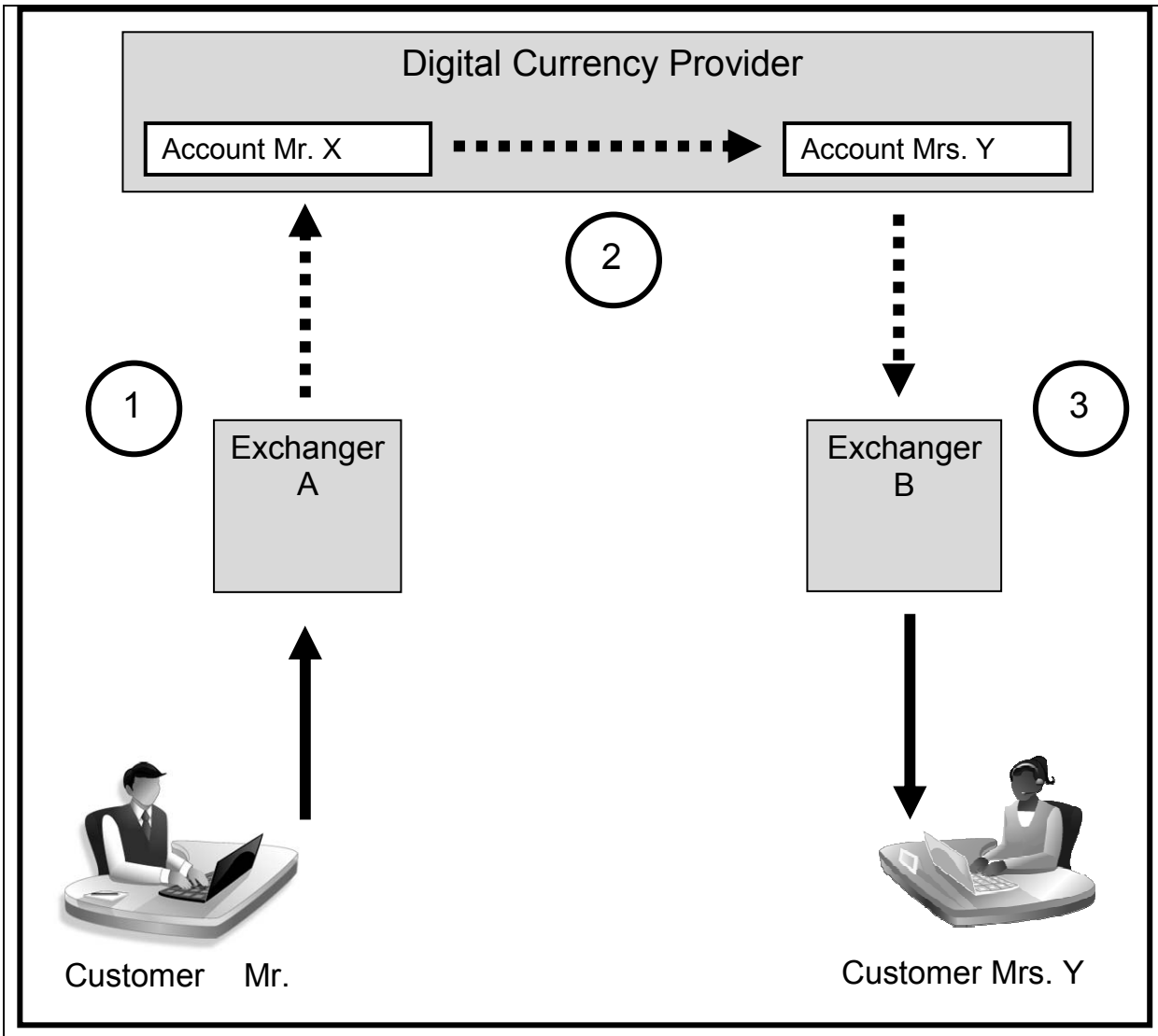
"*48. In accepting business from non face-to-face customers (...) there must be specific and adequate measures to mitigate the* ***higher risk***."

146. It remains unclear whether non-face-to-face business is a "specific higher risk scenario" in the sense of the Interpretative Note to Rec. 5. If so, simplified CDD measures would be not acceptable for such business models; instead, according to FATF Rec. 5, institutions carrying out such activities should even perform enhanced due diligence. This would affect several existing business models that rely on non-face-to-face business and apply simplified CDD to their products and services.

Digital currency providers: the use of exchangers

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

148. 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:



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

149. 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.

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

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.

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.

151. 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[87]

152. Another issue related to the segmentation of services is the use of agents or the outsourcing of AML obligations / CDD measures respectively. The FATF 40+9 Recommendations address this issue in two different contexts, namely in Recommendation 9 and SR VI.

153. 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, as explicitly explained

[87] For the purposes of this report, the terms „agent" and „outsource" shall be used synonymously. The FATF WGEI has set up a working group on Rec. 9 that has worked on providing greater clarity on the delineation between agency, outsourcing agreements and third party introduction.. The group has come to the preliminary conclusion that the concepts of agency and outsourcing "differ from one country to another, and even sometimes from one financial activity to another" (FATF document WGEI(2010)45, p.3).

in the Methodology: "*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.*"[88] Accordingly, Recommendation 5 only subjects financial institutions to CDD measures, but does not mention agents and outsources.

154. Therefore, agents of financial institutions are not normally subject to AML legislation or regulation themselves, thus having no legal AML/CFT obligations of their own.[89] Instead, the principal (or outsourcer), being a regulated institution, will remain solely responsible for meeting its own AML/CFT obligations. 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.

155. The only Recommendation explicitly mentioning agents is SR 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 SR 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).*" It is unclear whether the rules and definitions of SR VI apply to the providers of NPMs.

156. 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 directly. The term "agent" in this sense may cover many different activities, including for example card program managers or sellers of prepaid funds.

Card program managers

157. In some business models, the prepaid card program is effectively run by card program managers, while the issuing bank´s role is reduced to providing access to the technical card platforms. The card program manager may have ownership and control of the business model and take any important business decisions. As a result, their role is greater than that of the traditional outsource or agent.[90] Under such circumstances, the traditional principal and agent model no longer applies, and there is a risk that effective supervision is compromised: the card program manager is not supervised and outside the scope of AML legislation, while the issuing financial institution alone retains legal and regulatory liability. This situation is exacerbated if the card program manager and the issuing bank are located in different jurisdictions, e.g. the card program manager in a jurisdiction with a robust regulatory regime (to which the card program manager is not subject though) and the issuing bank in a jurisdiction whose AML/CFT standards are not equivalent to the FATF recommendations.

---

[88] Footnote 16 of the FATF Methodology for assessing compliance with th FATF 40 Recommendations and the FATF 9 Special Recommendations.

[89] Agents are often subject to contractual AML/CFT responsibilities that are imposed on them by the agency contract with their principal. However, as explained above, 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.

[90] The definition of "agents" for the purpose of SR 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.

158. A related issue is market entry. As card program managers are currently not subject to regulation and supervision, they do not have to meet market entry requirements like fit-and-proper tests. This means that the only obstacle criminals face when setting up their own prepaid card program is to find an authorised financial institution to formally issue the card on the criminals´s behalf. Criminals have been successful in doing so[91] as evidenced by case studies in the typologies section (see above section 4 "Typologies", *cases 19 and 25*).

159. 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.[92]

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 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 recognized 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 "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.

[91] Regulated institutions may enter into such a co-operation either collusively or negligently, or be deceived and tricked into such a cooperation.

[92] http://edocket.access.gpo.gov/2010/pdf/2010-15194.pdf.

Other agents

EU

Within the EU Committee on Money Laundering and Terrorist Financing (CPMLFT), it is currently discussed to which Financial Intelligenc Unit reporting should be done in cross-border situations, as well as issues of attribution 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.

160. Beyond the issue of program managers, there is also discussion whether traditional agents should be subject to immediate legal AML obligations and supervision or not.

161. As mentioned above regarding program managers, wherever agents are used, there is a risk that effective supervision is compromised, especially if the agent and the principal are located in different jurisdictions. This may be further exacerbated if the agent itself makes use of further agents ("sub-agents"). While this phenomenon has not yet been observed with NPM service providers, it has become apparent in the latest WGTYP typologies report on money service businesses.[93]

Sellers of prepaid funds

162. 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. A discussion has started whether such "agents" need to be subject to AML obligations and supervision or not.

USA

In the Notice of proposed rulemaking (NPRM) described above,[94] FinCEN proposes to impose direct AML/CFT obligations not only on the issuing bank and the "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 od 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

[93] (Quote report; not published yet)

[94] See above, para. …

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."

"Hybrid" service providers

163. 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 in the sense that due to their financial activities in many jurisdictions 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.

164. 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.

Example EU

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 other lines of business activity ("ringfencing").

Law enforcement and supervisory action against providers seated abroad

165. 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 located.

166. 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.

167. 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 29**) and in the Caribbean (see above **case 30**). 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.

168. 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

169. 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.

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

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

New Zealand MER 2009

According to the MER at the time the assessment was conducted, where there were three or more "facility holders" (=account or card holders) financial institutions in New Zealand were generally "only required 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 criticized by the assessment team and affected the rating for Rec. 5 (MER New Zealand 2009, p. 84, 93).

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

"419. 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."

172. While generally all 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 of customers has been criticized as not in line with Rec. 5,[95] 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).

6. Conclusions and Issues for Further Consideration

173. 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.

174. New types of NPMs will most likely emerge in the future. Because of the convergence and combination of NPMs it will be more complex to assess if such payment systems are vulnerable to ML/TF purposes. The continued development of NPMs therefore requires an appropriate and 'future proof' FATF framework.

175. In addition to the risk assessment (section 3) and the evaluation of typologies (section 4), the present report intends to examine whether recent technological and regulatory developments in the field of NPMs requires any updates or amendments of the FATF 40 + 9 Recommendations or any related changes in policy.

The project team has come to the conclusion that the FATF Forty Recommendations and Nine Special Recommendations provide a reasonable framework to address the vulnerabilities associated with new payment methods, although there is uncertainty about the scope and interpretation of some of the relevant Recommendations. Uncertainty exists in two main areas, namely the application of simplified CDD and the treatment of agents.

176. It is the project team´s conclusion that it would be desirable for FATF to provide more clarity on these issues. It is understood that some of those issues are already being addressed in preparation of the fourth evaluation round. 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

[95] See above chapter 5.2 ("Degree of reduction of CDD: full exemption from CDD?"), para. 140 ss.

informal to the formal sector, promotion of competition and economic growth in national markets) in order to find an appropriate balance. Furthermore, in all cases the cost/benefit ratio should be taken into account, i.e. does the AML/CFT benefit justify the extra costs end efforts that may arise for institutions as well as for supervisors, FIUs or other agencies.

Questions relating to simplified CDD:

1. Should complete anonymity of the customer be allowed for "low to non risk products"? (Rec. 5)

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

178. Furthermore, Recommendation 5 recommends that "*financial institutions* ***should apply each of the CDD measures*** *(as listed in Rec. 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***."

179. Based on the risk-based approach provided for in Recommendation 5, a number of jurisdictions currently grant institutions a full exemption from CDD measures in designated low risk cases. This has been criticized to be not in line with Recommendation 5 in some mutual evaluations, while in other mutual evaluations the issue was not raised or did not have a negative impact on the rating for Rec. 5. It would be desirable for FATF to give binding clarification on this issue in a central document, for example by amending the wording of Rec. 5 or its Interpretative Notes, or by complementing the Methodology. The following aspects should be taken into account:

180. Exemption from verification:

- 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.

- 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.

181. 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)?

- …

182. The FATF may want to consider providing guidance about business models that it considers to be a "low risk scenario" according to Recommendation 5, for example in a Best practice Paper. Such guidance could grow by continuously adding assessments taken from future mutual evaluations.

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

183. Recommendation 5 recommends that "*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.*"

184. The Interpretative Note to Rec. 5 states that "***simplified CDD measures are not acceptable whenever*** *there is suspicion of money laundering or terrorist financing or* ***specific higher risk scenarios apply.*****"**

185. Accordingly, simplified CDD would not be acceptable for non-face-to-face business models, if these were to be classified as a "higher risk scenario". The FATF 40 Recommendations are not entirely clear about this. Recommendation 8 does not explicitly speak of high risk, but of "***specific*** *risks associated with non face to face business relationships or transactions.*" However, the Basel CDD paper, which is referenced by the Interpretative Note to Rec. 5 (para.7), says in section 2.2.6:

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

186. It would be helpful if FATF could provide clarity whether the assessment "higher risk" from the Basel CDD paper needs to be applied to non face to face business models; and whether that means that those business models cannot apply simplified CDD, but would rather have to perform enhanced CDD according to Recommendation 5. When making this decision, the following aspects shold be taken into account:

- 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.

- 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.

<u>Question relating to the treatment of agents:</u>

3. Should agents be subject to regulation and own AML/CFT obligations? (Rec. 23, SR VI)

187. [*Still under discussion within the project team*]

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

188. 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 by a subgroup of FATF WGEI EGA.

189. Secondly, it is yet unclear which types of activities can be considered as creating an agency relationship between the NPM provider and the acting entity. 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. As there is disagreement amongst jurisdictions as well, FATF guidance would be helpful.

Other issues:

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

190. SR 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."

191. 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 much in the past.

192. 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 SR 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 SR IX) are only applicable to currency and bearer negotiable instruments, which means that prepaid cards do not have to be declared when crossing borders.[96]

193. 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 SR IX. In order to be able to subject these cards to cross-border controls, it would therefore be necessary to widen the scope of SR IX (and resulting from that national custom laws) to include such cards as well. When considering expanding the scope of SR IX, the following aspects should be taken into account:

- 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 SR 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

[96] 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).

funds. It should be examined further whether the reasons that excluded credit and debit cards from the scope of SR 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 that is value 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.

6. Updating this study

194. 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 (two years). 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).