

GUIDANCE FOR A RISK-BASED APPROACH

PREPAID CARDS, MOBILE PAYMENTS AND INTERNET-BASED PAYMENT SERVICES

June 2013



FINANCIAL ACTION TASK FORCE

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

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

www.fatf-gafi.org

© 2013 FATF/OECD. All rights reserved.
No reproduction or translation of this publication may be made without prior written permission.
Applications for such permission, for all or part of this publication, should be made to
the FATF Secretariat, 2 rue André Pascal 75775 Paris Cedex 16, France
(fax: +33 1 44 30 61 37 or e-mail: contact@fatf-gafi.org).

CONTENTS

ACRONYMS 2
I. INTRODUCTION 3
A. Scope and target audience 3
B. Purpose of the guidance 4
II. ROLE OF ENTITIES INVOLVED IN THE PROVISION OF NPPS 5
A. Prepaid cards 5
B. Mobile payments 6
C. Internet-based payment services 9
III ENTITIES COVERED BY THE FATF RECOMMENDATIONS 11
A. FATF definition of "financial institutions" 11
B. Possible risk-based exemption from AML/CFT measures 13
IV. RISK ASSESSMENT AND RISK MITIGATION OF NPPS 13
A. Risk factors 14
B. Risk mitigation measures 21
V. IMPACT OF REGULATION ON THE NPPS MARKET 25
A. FATF Guidance on financial inclusion 25
B. G20 Principles for innovative financial inclusion 26
VI. REGULATION, SUPERVISION & THE RISK-BASED APPROACH 26
A. Risk-based approach to AML/CFT measures and supervision 26
B. Customer due diligence 27
C. Licensing / registration 30
D. Wire transfers 30
E. Supervisory approach and identification of the competent jurisdiction 31
VII. APPROPRIATE AML/CFT REGULATION WHICH ADDRESSES THE RISKS 33
A. Level of AML/CFT measures proportional to the level of risk 33
B. Issues to consider when determining the NPPS provider subject to AML/CFT obligations 34
ANNEX 1 – REGULATORY APPROACHES FOR NPPS 37
BIBLIOGRAPHY 45

© 2013

ACRONYMS

AML/CFT	Anti-money laundering and countering the financing of terrorism
ATM	Automated teller machine
CDD	Customer due diligence
G2P	Government-to-person
IP	Internet protocol
KYC	Know your customer
ML	Money laundering
MNO	Mobile network operators
MVTS	Money or value transfer services
NFC	Near field communication
NPM	New payment methods
NPPS	New payment products and services
P2B	Person-to-busines
P2P	Person-to-person
POS	Point of sale
RBA	Risk-based approach
SIM	Subscriber identity module
TF	Terrorist financing
USSD	Unstructured supplementary service data

© 2013

GUIDANCE FOR A RISK-BASED APPROACH TO PREPAID CARDS, MOBILE PAYMENTS AND INTERNET-BASED PAYMENT SERVICES

I. INTRODUCTION

1. The rapid development, increased functionality, and growing use of new payment products and services (NPPS) globally has created challenges for countries and private sector institutions in ensuring that these products and services are not misused for money laundering (ML) and terrorist financing (TF) purposes. This has attracted the attention of anti-money laundering and countering the financing of terrorism (AML/CFT) authorities as they seek to develop and implement AML/CFT regulation for NPPS. The Financial Action Task Force (FATF) issued typologies reports[1] in 2006, 2008 and 2010 on new payment methods (NPM) which focused on: the potential for NPM to be misused by criminals; the identification of risk factors which can significantly differ from one new payment product or service to another, depending on functionality; and risk mitigants which can be tailored to a particular new payment product or service to address its specific risk profile. The FATF recognises the innovative use of emerging technologies in this area, including decentralised digital currencies. The FATF's discussion reflects these concerns and will continue to consider the risks and measures necessary to mitigate ML/TF risks posed by these.

A. SCOPE AND TARGET AUDIENCE

2. This paper proposes guidance on the risk-based approach to AML/CFT measures and regulation in relation to NPPS of prepaid cards, mobile payments and Internet-based payment services, in line with the *FATF Recommendations*. The guidance is non-binding and does not override the purview of national authorities. The intention is to build on the FATF typologies reports and to complement existing FATF guidance relating to the development and implementation of a risk-based approach to AML/CFT, including in particular the *FATF Guidance on ML/TF risk assessment*.[2] NPPS also play an important role in financial inclusion. This guidance is in line with the *FATF Guidance on anti-money laundering and terrorist financing measures and financial inclusion,* which supports countries and financial institutions in designing AML/CFT measures that meet the national goal of financial inclusion, without compromising the measures that exist for the purpose of combating crime.[3] In this respect, the FATF recognises that applying an overly cautious approach to AML/CFT safeguards can have the unintended consequence of excluding legitimate businesses and consumers from the financial system, thereby compelling them to use services that are not subject to regulatory and supervisory oversight. AML/CFT controls must not inhibit access to formal financial services for financially excluded and unbanked persons. The FATF recognises that financial

1 See FATF (2006), FATF (2008) and FATF (2010).

2 See FATF (2013a). This document outlines general principles that may serve as a useful framework in assessing ML/TF risks at the national level. However, these principles may also relevant when conducting risk assessments of a more focussed scope. The guidance is also not intended to describe how supervisors should assess risks in the context of risk-based supervision.

3 See FATF (2013b).

© 2013

exclusion could undermine the effectiveness of an AML/CFT regime hence, financial inclusion and AML/CFT should be seen as serving complementary objectives.

3. For the purposes of this guidance, NPPS are considered to be new and innovative payment products and services that offer an alternative to traditional financial services. NPPS include a variety of products and services that involve new ways of initiating payments through, or extending the reach of, traditional retail electronic payment systems, as well as products that do not rely on traditional systems to transfer value between individuals or organisations. Given the rapid development and changing nature of such products and services, any attempt to more precisely define what is meant by NPPS will likely unintentionally limit the applicability of this guidance paper. In this respect, it is important to recognize that while this guidance focuses on existing NPPS, it may equally apply to new and emerging NPPS not considered in this paper. To ensure that the guidance in this paper is relevant and practical, it will focus particularly on three categories of NPPS: (1) Prepaid cards; (2) Mobile payment services; and (3) Internet-based payment services. It is important to note that NPPS are increasingly interconnected, both between these three categories and with traditional payment methods.

4. Traditional financial services, such as banking services, are increasingly offered through new and innovative methods, including using the Internet or mobile phone technology. However, while countries and financial institutions should identify and assess the ML/TF risks that may arise in relation to new delivery methods of these traditional financial services[4], they do not fall within the scope of this guidance. Rather, the focus of this guidance paper is on innovative payment methods and the measures to mitigate the ML/TF risks posed by these emerging payment methods.

5. This guidance is primarily addressed to public authorities involved in regulation of NPPS (particularly supervisors and policy makers) and private sector institutions involved in the design, development, and provision of NPPS. This includes financial institutions issuing and managing NPPS, many of which already have CDD and other controls in place to mitigate the risk of money laundering and terrorism financing.

B. PURPOSE OF THE GUIDANCE

6. The purpose of this guidance is to:

(a) explain how new payment systems work, who the entities involved in the provision of NPPS are, and their roles/activities (Section II);

(b) examine which entities involved in the provision of NPPS are already covered by the *FATF Recommendations* (*i.e.,* because they fall within the FATF definition of a *financial institution*) (Section III);

(c) determine the risks involved in the provision of NPPS, including through consideration of any relevant risk factors and risk mitigation measures (Section IV);

(d) consider the impact of regulation on the NPPS market, including whether such regulation would impact financial inclusion and the positive implications of money deposits moving to regulated financial institutions (Section V);

[4] See Recommendation 15.

 © 2013

(e) examine how to regulate and supervise entities involved in providing NPPS, and consider the impact of such regulation and supervision on the effective implementation of AML/CFT measures (Section VI); and

(f) discuss considerations when determining how to apply appropriate AML/CFT regulation of NPPS which addresses the risks, acknowledging that there may be multiple regulated entities, based on the considerations described below in Sections III, IV, V and VI (Section VII).

II. ROLE OF ENTITIES INVOLVED IN THE PROVISION OF NPPS

7. This section explains how new payment systems work, who the entities involved in the provision of NPPS are, and their roles/activities. The structure, characteristics and business models of NPPS vary significantly, many of which serve to address ML/TF risk.

A. PREPAID CARDS

8. Prepaid cards were introduced in the payments market at the end of the 1990s as an alternative to credit cards (which require the card issuer to evaluate the cardholder's minimum level of creditworthiness) and debit cards (which entail the existence of a payment account at a bank or a financial institution). Prepaid cards began as a device used to pay for goods and services where the issuer does not need to conduct any analysis on the cardholder's credit standing, or bear the costs for opening and managing a payment account. Many prepaid cards may now be used to withdraw cash from automated teller machines (ATMs) including internationally. In addition, some of them provide the possibility of person-to-person transfers.

9. The dynamic and evolving nature of the prepaid card market presents particular challenges for AML/CFT regulation in ensuring that it remains relevant and up-to-date. Today, the functionality of prepaid cards varies significantly as they have evolved from a replacement for store gift certificates and limited purpose closed loop applications to, in some cases, embody all the functionalities of a payment instrument tied to a payment account. At one end of the spectrum are gift cards that can only be used for purchases at a single, or among a limited network, of merchants (commonly referred to as closed-loop prepaid cards). These cards do not provide access to the global ATM network and are not able to have cash refund through merchants (commonly known as "cash back"). Given their low-risk characteristics, closed-loop cards, specifically cards which do not allow reloads or withdrawals, remain outside the scope of this paper and the guidance on AML/CFT measures and regulation envisaged in this paper is not intended to apply.[5] At the other end of the spectrum are payment network-branded cards that allow transactions with any merchant or service provider participating in the payment network (commonly referred to as open-loop prepaid cards). For the majority of open-loop prepaid cards, customers use the prepaid cards to access the related funds which are held in an associated payment account. While it is possible to store related funds on a chip on the card, the use of chips on prepaid card cards in this manner has decreased. Some prepaid cards can be funded using cash and other electronic payment instruments, offer similar

[5] The FATF is not taking the position that there is not any ML/TF risk associated with closed loop prepaid cards, but rather the ML/TF risk may be, for example, lessened by the limited use of such cards.

options to those provided by a payment account and related instruments to move funds, may allow cash access via ATMs globally and, in some cases, allow person-to-person funds transfers between users. Between these two extreme cases, there can be a range of products which present some features of an account, but where the adoption of limitations (*e.g.* loading thresholds, limited spending capacity) significantly reduces risks.

10. Many entities can be involved in the provision of prepaid cards. The roles of these entities vary depending on the business model of the prepaid card product and various roles may be carried out by a single entity or through agents. This can create regulatory challenges in determining where to place appropriate responsibility for AML/CFT controls. This paper provides guidance in section VII to assist countries in determining which entity (or entities) could be considered the responsible party (or parties), and therefore subject to AML/CFT regulation, in a given prepaid card business model. Entities involved in the provision of prepaid cards may include the following:

(a) *Acquirer* – The entity which maintains the relationship with the retailer, provides the infrastructure needed for accepting a card payment (*e.g.* access to the point of sale (POS) terminal or the payment services supporting an e-commerce website) and normally operates the account in which the proceeds of the sale transaction are deposited.

(b) *Distributor (including retailer)* – The entity that sells, provides, or arranges for the sale of, prepaid cards on behalf of the issuer to consumers. Distributors may also offer a range of services to their customers.

(c) *Payments network operator* – The entity that provides the technical platform to perform transactions with the card at ATMs or points of sale at merchants.

(d) *Issuer* – The entity that issues prepaid cards and against which the customer has a claim for redemption or withdrawal of funds.

(e) *Programme manager* – The entity responsible for establishing and managing the prepaid card programme in cooperation with a bank or electronic money institution. The programme manager usually markets the prepaid cards and establishes relationships with banks and distributors or customers, and in many cases provides the data processing capability. Some prepaid card issuers also manage their card programmes themselves (*i.e.* without using programme managers).

(f) *Agent* – For the purposes of this guidance, an agent is any natural or legal person providing prepaid card services on behalf of another entity involved in the provision of prepaid cards, whether by contract with or under the direction of the entity. The entities having roles in the prepaid card market may frequently act on behalf of other entities, depending on the business model selected for the prepaid card programme.

B. MOBILE PAYMENTS

11. Mobile payments as they are offered today are the result of an evolutionary process which started with the spreading of the mobile telephony around the world in late 1990s. The first stage of this evolutionary process can be related to the inherent data communication capability of mobile phones, which caught the attention of banks, prompting them to start launching basic inquiry

 © 2013

services like account balance inquiry, and slowly starting expanding the range of functions to also include transaction services such as funds transfer. These sets of services collectively started being referred to as "mobile banking". This stage is mostly characterized by banks being the main actors in the provision of mobile payments services. As noted above, "mobile banking" and other traditional financial services delivered through innovative channels remain outside the scope of this paper. Such mobile banking services are distinct from bank-centric mobile payment models where new products or services are delivered to new customers, as described further below.

12. The second stage is related to the coincidence of a further spreading of mobile telephony and experiences with electronic money products, which motivated various entities to experiment with electronic money products with transaction initiation through mobile phones as a key design aspect, as well as a distribution network of retailers that operate on a prepaid model. In that stage, given that mobile money products are often linked to prepaid accounts, non-banking entities also have been very active. In fact, telecommunications providers have been successful mobile money issuers. During this stage, several jurisdictions have been confronted with these developments and have either allowed their development without specific regulation, regulated them with special licensing or registration requirements, or forbidden their operation. However, in emerging markets forms of mobile money, including mobile payments, are growing and contributing to financial inclusion as these provide under-served and unbanked people with access to a broad range of formal financial services.

13. Today, the financial institutions that facilitate mobile payments, including person-to-business (P2B), person-to-person (P2P) or government-to-person (G2P) transactions, can be traditional payment service providers (banks or depository institutions) or non-bank payment service providers, designated in the FATF glossary as money or value transfer services (MVTS). Depending on the business model and technology used, various types of service providers are essential partners to financial institutions providing mobile payments services. These partners include mobile network operators (MNOs), and may include mobile telephone equipment manufacturers, telecommunications industry standards setting groups, payment networks, and software developers. In terms of technology used, business models use a range of approaches to facilitate mobile payments including text messaging, mobile Internet access, near field communication (NFC), programmed subscriber identity module (SIM) cards and unstructured supplementary service data (USSD).

14. The nature and operation of mobile payment services varies greatly between business models, and commonly involves new technologies and links with other types of NPPS, which presents challenges for countries in developing effective AML/CFT regulation. Business models can vary based on which service provider has the lead role, whether the service is pre-paid or post-paid, meaning the customer pays after receiving the service, and the technical platform used. The description of the models of mobile payment services below is not an exhaustive description and does not describe any particular scheme. Rather, it provides a generalization of typical features of mobile payment services to assist in the development and application of AML/CFT measures and regulation.

15. In a *bank-centric mobile payment model* the customers are account holders of the bank which offers the mobile payments service. However, this differs from the provision of traditional banking

services through the mobile phone as the bank either develops new products offered through the mobile phone to serve the previously unbanked which are tied to limited transaction accounts, or alternatively, is a provider of electronic money that is not tied to a payment account. The bank partners with software developers and a payment processor to allow bank customers to send and receive payment messages via the access mechanism of a mobile phone, with the payments cleared through the domestic automated clearinghouse network or a payment card network. Funds are drawn from and/or deposited to a customer bank or payment card account. The role of the MNO in this example is limited to providing the telecommunication network facility which enables the transfer of payment messages, and it does not manage or hold the customer's funds at any stage. Therefore, the MNO would not require a financial services license as the bank is the payment service provider.

16. Under the *MNO-centric mobile payment model*, MNOs offer mobile payment services as a means to add value to their core communications service. Commonly, customer funds are held in a prepaid account by the MNO itself or a subsidiary. Although in some jurisdictions even if the MNO is the business owner (the entity which assumes the bulk of the financial risk and operational responsibility of offering the service), a partner bank formally holds the license. If the funds are post-paid, the MNO can be considered to be providing short-term credit or payment service to its customers, in the same way as some three-party payment card schemes.[6] In this respect, a prepaid account eliminates credit risk for the MNO, while a customer with a post-paid account has a credit relationship with the MNO. MNOs are often international companies with the ability to extend their services across borders. This may also apply to payment services where there are no legal or technical impediments to the provision of cross-border payment services.

17. Between these two cases, there can be a range of mobile payment services offered by financial institutions and MNOs who have partnered to create agent networks to reach new customers in geographic areas which are typically underserved by the banking system. In such cases, MNO retail outlets and other storefront retailers offer similar services to those of limited-purpose bank branches, signing up customers, taking in deposits, and paying out cash to settle mobile payment transactions. The payment service may be branded under the name of the bank or under the name of the MNO.

18. Mobile payment services are increasingly interconnected with other payment services. MNOs are partnering with electronic funds transfer networks to allow domestic customers to access ATMs for cash withdrawals by entering a code, rather than swiping a payment card. To allow customers international access to cash, MNOs are partnering with payment card issuers to offer open-loop prepaid cards.

19. Mobile payment services that are offered for purchases from a single, or limited number of merchants, with limited value for products related to the use of a mobile phone (such as applications or ringtones) fall outside the scope of this paper. The operation in this way of some

[6] In this model, the issuer (having the relationship with the cardholder) and the acquirer (having the relationship with the merchant) is the same entity. This means that there is no need for any charges between the issuer and the acquirer. Since it is a franchise setup, there is only one franchisee in each market, which is the incentive in this model. There is no competition within the brand; rather you compete with other brands.

 © 2013

mobile payment services is comparable to closed-loop prepaid cards and the guidance on AML/CFT measures and regulation envisaged in this paper is not intended to apply to these services. For clarity, it is not the intention of this guidance to address the creation, sale, transfer or consumption of pre- or post- paid customer 'airtime' balance by MNOs. However, this guidance may apply where 'airtime' funds can be transferred and are accepted for payments or an alternative currency.

20. Many entities can be involved in the provision of mobile payment services. The roles of these entities may vary depending on the business model of the mobile payment service, and various roles may be carried out by a single entity or through agents.[7] This may create regulatory challenges in determining where to place appropriate responsibility for AML/CFT controls. This paper provides guidance to countries in section VII as to which entity (or entities) could be considered the responsible party (or parties), and therefore subject to AML/CFT regulation, in a given mobile payment business model. Entities involved in the provision of mobile payments may include the following:

(a) *MNO* – The entity that provides the technical platform to allow access to the funds through their mobile phone.

(b) *Distributor (including retailer)* – The entity that sells, or arranges for the issuance of funds on behalf of the issuer to consumers, if such funds can be used for payments. Distributors may also offer a range of services to their customers, such as technical support.

(c) *Electronic money issuer* – The entity that issues electronic money. For the purposes of this paper, electronic money is a record of funds or value available to a consumer stored on a payment device such as chip on a prepaid card, mobile phones or on computer systems as a non-traditional account[8] with a banking or non-banking entity.[9]

C. INTERNET-BASED PAYMENT SERVICES

21. The Internet opened up the world of e-commerce and led to the development of various types of Internet-based payment services which emerged in the late 1990s to intermediate between online buyers and sellers (P2B) and for personal transfers (P2P) transactions. During the last decade, financial institutions and retailers have continued to develop electronic payment instruments which use the Internet and are available to a wide range of consumers.[10]

22. Internet-based payment services provide mechanisms for customers to access, via the Internet, pre-funded accounts which can be used to transfer the electronic money or value held in those accounts to other individuals or businesses which also hold accounts with the same provider.

---

7 The entities having roles in the mobile payments market frequently may act as agent for other entities, depending on the business model selected for the mobile payment service.

8 The use of "account" in this definition does not pre-judge the question for countries as to whether business relations are established (see footnote 38).

9 This definition of electronic money is taken from the World Bank's report on *Innovations in Retail Payments Worldwide: A Snapshot* (July 2012). The definition of electronic money should remain flexible and can be further differentiated into network money, M Money, electronic purse, and electronic wallet.

10 See World Bank (2012).

The recipient then redeems the value from the issuer by making payments or withdrawing the funds. Withdrawals occur by transferring the funds to a regular bank account, a prepaid card, or another money or value transfer service. While typically customers hold funds in pre-paid accounts, customers are not required to do so. When the account needs to be funded, this can happen with a debit from a bank account or payment card account, or supplied via another funding source as needed.

23. Many Internet-based payment services use a variety of business models. These services are referred to as digital wallets, digital currencies, virtual currencies, or electronic money. Internet-based payment services can vary significantly in their functionality, structure and procedures. Services may allow individuals to transfer to any individual or business subscribed to the service, or they may limit transactions to a particular merchant or online environment. Internet-based payment services may also be interconnected with other payment methods such as prepaid cards.

24. Digital currency providers may allow third parties to undertake the exchange of national currencies with the electronic currency or value. In such a business model, the electronic currency may be issued and redeemed through such agents. These agents may be affiliated, or unaffiliated, with the provider and therefore acting as a virtual bureau de change. Providers that use this model make their money charging for account-to-account transfers. Exchangers sell digital currency from their accounts, transferring the value from their account to the customer's account. The reverse occurs when a payment recipient wants to cash out. By buying or selling digital currency for cash (or other digital currencies), exchangers act as a virtual bureau de change.

25. Another common form of Internet-based payment service is digital currency providers that sell a digital representation of precious metals online. These service providers sell virtual gold or silver at market prices, claiming to hold actual precious metals on behalf of the customer. Intermediaries, or exchangers as they are often called, buy and sell digital precious metals for their own accounts in transactions with customers. These exchangers determine independently what forms of payment they will exchange for digital currency.

26. Pre-funded accounts that consumers use for online auction payments are among the most dominant Internet-based payment services. Recipients may or may not be required to register with the payment service provider to receive a funds transfer. Customers may pre-fund an Internet-based payment account using a regular bank account. The funds in the Internet-based payment account can be used for transfers to other customers of the same provider, or transferred back to the customer's regular bank account.

27. Internet-based payment services may also be associated with online gambling or virtual worlds for which only a proprietary form of currency can be used to conduct transactions. Participants hold the proxy currency in an account, using the funds for transactions with the proprietor, other participants or retailers in the closed online environment. Recipients of the proprietary currency can exchange it for their national currency on exiting the environment.

28. Internet-based payment services that involve the issuing of electronic money solely for the purpose of purchasing goods and services directly from the electronic money issuer, or within limited number of merchants, with limited value and range of goods and services fall outside the scope of this paper since this is comparable to closed-loop prepaid cards. As noted previously, the

 © 2013

guidance on AML/CFT measures and regulation envisaged in this paper is not intended to apply to these services.

29. The development of alternate online currencies continues to be an issue of consideration for AML/CFT policy makers and the private sector. While some of these currencies may fall outside the scope of this guidance paper, many of the elements of the guidance may apply. Policy makers should be aware of these existing or emerging electronic products, services and forms of currency, and monitor developments in their market in order to understand the potential risks involved and develop suitable policies. Given the developing nature of alternate online currencies, the FATF may consider further work in this area in the future.

30. As described above, Internet-based payment services can be provided by financial or non-financial institutions. This paper provides guidance to countries in section VII as to which entity (or entities) could be considered the responsible provider, and therefore subject for AML/CFT regulation, for Internet-based payment services.

III ENTITIES COVERED BY THE FATF RECOMMENDATIONS

31. This section examines which entities involved in the provision of NPPS are covered by the *FATF Recommendations* (*i.e.,* because they fall within the FATF definition of a *financial institution*).

32. Under the *FATF Recommendations*, countries should ensure that the financial sector and other designated sectors apply preventive measures. While NPPS providers provide products and services that fall within the scope of the *FATF Recommendations*, it can be difficult at times to determine which entity is responsible for the implementation of AML/CFT preventive measures due to the range of entities involved and the complexity of NPPS. Accordingly, this paper provides guidance to countries on the application of the *FATF Recommendations* to NPPS providers.

A. FATF DEFINITION OF "FINANCIAL INSTITUTIONS"

33. In applying AML/CFT preventive measures to NPPS, countries should consider which entities fall within the scope of the *FATF Recommendations*. In defining *financial institutions*, the FATF provides a list of financial activities or operations in the glossary to be covered for AML/CFT purposes.

© 2013

Box 1: **FATF Definition of "financial institutins"**

Financial institutions means any natural or legal person who conducts as a business one or more of the following activities or operations for or on behalf of a customer:

1. Acceptance of deposits and other repayable funds from the public.[11]
2. Lending.[12]
3. Financial leasing.[13]
4. Money or value transfer services.
5. Issuing and managing means of payment (*e.g.* credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money).
6. Financial guarantees and commitments.
7. Trading in:
   (a) money market instruments (cheques, bills, certificates of deposit, derivatives etc.);
   (b) foreign exchange;
   (c) exchange, interest rate and index instruments;
   (d) transferable securities;
   (e) commodity futures trading.
8. Participation in securities issues and the provision of financial services related to such issues.
9. Individual and collective portfolio management.
10. Safekeeping and administration of cash or liquid securities on behalf of other persons.
11. Otherwise investing, administering or managing funds or money on behalf of other persons.
12. Underwriting and placement of life insurance and other investment related insurance.[14]
13. Money and currency changing.

34. Providers of NPPS fall within the definition of *financial institution* by conducting money or value transfer services, or by issuing and managing a means of payment, and therefore should be subject to AML/CFT preventive measures as required by the *FATF Recommendations*, including, for example, customer due diligence, record keeping, and reporting of suspicious transactions. There

11 This also captures private banking.

12 This includes *inter alia*: consumer credit; mortgage credit; factoring, with or without recourse; and the finance of commercial transactions (including forfeiting).

13 This does not extend to financial leasing arrangements in relation to consumer products.

14 This applies both to insurance undertakings and to insurance intermediaries (agents and brokers).

 © 2013

can be difficulty, however, in determining which entity (or entities) in the provision of NPPS should be responsible for the implementation of preventive measures and the application of such measures at the national level. This paper provides guidance to countries in section VII as to which entity (or entities) could be considered the responsible NPPS provider, and therefore subject to AML/CFT regulation.

B. POSSIBLE RISK-BASED EXEMPTION FROM AML/CFT MEASURES

35. Countries may exempt the activities listed in the definition of *financial institution* from the relevant preventive measures required by the *FATF Recommendations*, under certain circumstances. The Interpretive Note to Recommendation 1 states that there are two situations in which countries may decide not to apply some of the *FATF Recommendations* requiring financial institutions to take certain actions:

(a) provided there is a proven low risk of money laundering and terrorist financing; this occurs in strictly limited and justified circumstances; and it relates to a particular type of financial institution or activity, or DNFBP; or

(b) when a financial activity (other than the transferring of money or value) is carried out by a natural or legal person on an occasional or very limited basis (having regard to quantitative and absolute criteria), such that there is low risk of money laundering and terrorist financing.[15]

36. Countries should note that the Interpretive Note to Recommendation 1 further states that while the information gathered may vary according to the level of risk, the requirements of Recommendation 11 to retain information should apply to whatever information is gathered. Of further relevance to countries in relation to NPPS is that MVTS cannot benefit from the exemption due to financial activity being conducted on an occasional or very limited basis.[16]

IV. RISK ASSESSMENT AND RISK MITIGATION OF NPPS

37. To implement a risk-based approach to AML/CFT and NPPS, it is essential that countries and private sector institutions identify and assess the ML/TF risks posed by NPPS when developing AML/CFT regulation for NPPS and when designing NPPS. Under FATF Recommendation 1, countries should identify, assess and understand the ML/TF risks for the country[17] and should also require financial institutions to identify and assess ML/TF risks.[18] Of particular relevance for NPPS is Recommendation 15 which requires countries and financial institutions to identify and assess the ML/TF risks that may arise in relation to the development of new products and business practices, and the use of new or developing technologies. In addition, under Recommendation 15 countries

15 See Interpretive Note to Recommendation 1 at paragraph 6, [FATF(2012)].

16 Recommendation 10 states that financial institutions should be required to undertake CDD measures when carrying out occasional transactions that are wire transfers.

17 All references in this guidance paper to *country* or *countries* apply equally to territories or jurisdictions.

18 See Recommendation 1 and Interpretive Note to Recommendation 1 of the *FATF Recommendations*.

© 2013

should also require financial institutions to identify and assess risks of new products, business practices or the use of new technologies prior to their launch.[19]

38. This section features a series of risk factors and risk mitigation measures to assist both countries and private sector institutions in assessing the risk of NPPS. In assessing the risks posed by NPPS, countries should consider the *FATF Guidance for ML/TF risk assessment*.[20] In addition, countries and financial institutions should consider the risk factors outlined in the Interpretive Note to Recommendation 10 on customer due diligence. While these examples are not mandatory elements of the FATF Recommendations, they provide useful examples of risk indicators, many of which are discussed in further detail below with respect to the ML/TF risks posed by NPPS.

A. RISK FACTORS

39. This section of the paper identifies a range of risk factors that help to identify the ML/TF risks associated with NPPS. Many NPPS may have characteristics which mitigate ML/TF risk and these should be considered as part of a holistic approach when assessing the risks associated with a particular NPPS. The level of ML/TF risk posed by a particular NPPS will depend on a consideration of all risk factors, the existence of risk mitigates and its functionality.

i. Non-face-to-face relationships and anonymity

40. As with many banking methods, NPPS can allow for non face-to-face business relationships. Depending on their characteristics, NPPS can be used to quickly move funds around the world, to make purchases and access to cash (both directly and indirectly) through the ATM network. The absence of face-to-face contact may indicate a higher ML/TF risk situation. If customer identification and verification measures do not adequately address the risks associated with non-face to face contact, such as impersonation fraud, the ML/TF risk increases, as does the difficulty in being able to trace the funds.

41. While monitoring and reporting mechanisms can be put in place to identify suspicious activity, an absence of CDD increases the difficulty for the service provider to do so. For example, this impacts on the ability of the service provider to identify instances of customers holding multiple accounts simultaneously.

42. For prepaid cards, the risk posed by anonymity (not identifying the customer) can occur when the card is purchased, registered, loaded, reloaded, or used by the customer. The level of risk posed by anonymity is relative to the functionality of the card and existence of AML/CFT risk mitigation measures such as funding or purchasing limits, reload limits, cash access, and whether the card can be used outside the country of issue. Prepaid cards can be funded in various ways with

19 See Recommendation 15: "Countries and financial institutions should identify and assess the money laundering or terrorist financing risks that may arise in relation to (a) the development of new products and new business practices, including new delivery mechanisms, and (b) the use of new or developing technologies for both new and pre-existing products. In the case of financial institutions, such a risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies. They should take appropriate measures to manage and mitigate those risks."

20 See FATF (2013a).

 © 2013

different degrees of CDD including through banks, the Internet, at small retail shops, or at ATMs. While funding via a bank account or through the Internet normally starts from an account or a payment instrument whose holder has been identified, cash funding or funding through other NPPS is possible and can be fully anonymous. In addition, prepaid cards can easily be passed on to third parties that are unknown to the issuer, including, but not restricted to, 'twin cards' which are specifically designed to allow third parties remittances, and may advertise anonymity as a feature of the product. This is concerning when the providers of these products are based in countries where prepaid card providers are insufficiently regulated and supervised for AML/CFT purposes, but sell their products internationally.[21]

43. Mobile payment services may establish their customer relationships either through agents, online or through the mobile payment system itself. The same channels are used for loading funds into the mobile account. The risk posed by anonymity occurs when the mobile payment service is used or reloaded, and is relative to the functionality of the mobile payment service and the existence of AML/CFT risk mitigation measures such as CDD or funding thresholds.

44. For Internet-based payment services there is typically no face-to-face customer contact. This may increase the risk of identity fraud or customers providing inaccurate information potentially to disguise illegal activity if effective measures to address this risk are not employed. However, this lack of face-to-face contact is often counterbalanced through the adoption of alternative identification mechanisms, which can provide adequate risk mitigation measures. The risk posed by anonymity or not identifying the customer when the Internet-based payment service is used or reloaded is relative to the functionality of the service, the funding mechanisms (if funds come from a regulated account the risks can be substantially reduced) and the existence of AML/CFT measures.

ii. Geographical reach

45. The extent to which a particular NPPS can be used globally for making payments or transferring funds is an important factor to take into account when determining the level of risk.

46. Open-loop prepaid cards often enable customers to effect payments at domestic and foreign points of sales through global payment networks. These cards are accepted as a means of payment everywhere a similarly-branded card (debit or credit) is accepted. Providers of prepaid cards may be based in one country and sell their product internationally through agents or the Internet. These cards can then be used to purchase goods and services, or access cash, internationally. Additionally, some prepaid card programmes allow cardholders to transfer funds from person-to-person. This global reach of some prepaid cards to make payments, access cash and transfer funds are all features that make those products attractive for ML/TF purposes. The compact physical size of prepaid cards also makes them potentially vulnerable to misuse by criminals who use them, instead of cash, to make physical cross-border transportations of value. Prepaid cards which can be used to access funds internationally are particularly vulnerable due to the logistical benefits of transporting a discreet number of prepaid cards that have accounts loaded with high fund values which cannot be determined from the card itself, rather than transporting large, bulky amounts of cash using cash

21 This practice is highlighted in FATF (2010), in Chapter 3, 'Risk Assessment of NPMs'.

couriers. Countries should also consider whether Recommendation 32 applies to certain prepaid access products, such as prepaid cards, that would qualify as bearer negotiable instruments.

47. Mobile payment services and Internet-based payment services that can be used to transfer funds globally, or can be used in a wide geographical area, with a large number of counterparties are more attractive to criminals for ML/TF purposes than purely domestic business models. In addition, NPPS providers located in one jurisdiction may offer these services to customers located in another jurisdiction where they may be subject to different AML/CFT obligations and oversight. This is of concern where the NPPS provider is located in a jurisdiction that has weak AML/CFT controls.

iii. Methods of funding

48. The methods by which a NPPS can be funded impacts on the level of ML/TF risk posed. Anonymous funding methods obscure the origin of the funds, creating a higher ML/TF risk. Cash poses the highest potential risk as cash is anonymous and provides no transaction history. However, while NPPS provide a platform for transaction monitoring, funding a NPPS product via another payment service that does not verify customer identification can also create an anonymous funding mechanism. In addition, NPPS that use a prepaid model means that the absence of credit risk for the provider may reduce the incentive for providers to conduct comprehensive CDD, thereby increasing the ML/TF risk.

49. The ML/TF risk posed by prepaid cards is increased by allowing cash funding and, in some rare cases, reloadability without any limit on the value placed on the card account or CDD requirements. This makes prepaid cards vulnerable to abuse by criminals who can use them, for example, as a means to launder the proceeds of crime by placing those proceeds into the financial system or using the prepaid cards as an alternative to the physical cross-border transportation of cash.

50. Mobile payment services allow accounts and transactions to be funded in different ways; many services, whether bank- or MNO-centric model, draw funds from a bank or payment card account, others allow cash funding through a network of agents. While the former funding method limits ML/TF risk (but also limits potential access), cash and non-bank payment options open up payment system access but also obscure the origin of the funds creating a heightened risk for ML/TF. A mobile payment service that facilitates account-to-account transfers is also permitting funding through third parties, which may increase the ML/TF risk, if the holder of the funding account was not properly identified.

51. Internet-based payment services that allow third party funding from anonymous sources may face an increased risk of ML/TF. A special case of third party funding is the use of exchangers or virtual bureaux de change. Such exchangers can circumvent an Internet-based payment service provider's ban on certain funding methods (*e.g.* a 'no cash funding' policy) if they accept the banned payment methods when reselling the issued digital currency or electronic money funds. Further, the provider will only see the exchanger´s name in its monitoring, but will not see who actually instructed the exchanger to fund the account.

 © 2013

iv. Access to cash

52. Access to cash through the international ATM network increases the level of ML/TF risk. Such access to cash may be direct, as in the case of prepaid cards which can allow funding in one country and cash withdrawals in another. Alternatively, mobile payment services and Internet payment services are increasingly becoming interconnected with other NPPS such as prepaid cards which indirectly allow access to cash withdrawals.

v. Segmentation of services

53. The provision of NPPS commonly requires a complex infrastructure involving several parties for the execution of payments. Prepaid cards may involve several parties for the execution of payments including the programme manager, issuer, acquirer, payment network, distributor and agents, while mobile payments service providers must often coordinate with a number of interrelated service providers, and partner with international counterparts to provide cross-border transactions.

54. A large number of parties involved in the provision of NPPS, especially when spread across several countries, can increase the ML/TF risk of the product due to the potential of segmentation and the potential loss of customer and transaction information. This is a particular concern when it is not clearly established which of the entities involved are subject to AML/CFT obligations, who is responsible for complying with such obligations, and what country among those involved in the transaction process is responsible for regulating and supervising for compliance with AML/CFT measures.

55. Using agents and relying on unaffiliated third parties for establishing customer relationships and reloading raises potential ML/TF risks, particularly if the collected information is not shared with the entity responsible for AML/CFT requirements. A service provider that can take responsibility for all aspects of the customer relationship (*i.e.* registration, cash-in/cash-out and transactions) can pose a lower risk. Of relevance is the organizational structure and processes set up for the training, management and control of the network of agents.

56. Additionally, entities providing NPPS often come from sectors, such as MNOs, which are unfamiliar with AML/CFT controls. Consequently, CDD know-how could be limited in comparison to, for example, the traditional banking sector, and CDD generally may remain restricted to analysing atypical transactions and feedback from distributors. In addition, the chain of information could create difficulties in tracing the funds. For example, the chain of information for a single financial transaction could involve more entities; some of which may be located in different countries. This could slow down the investigation process, which is further complicated by the speed of money flows, and the challenges of trying to seize and freeze criminal proceeds which can be quickly transferred or transported to another country using NPPS.

57. NPPS providers maintain bank accounts and use the banking system for periodic transactions to settle accounts with agents and MVTS partners. However, while a bank settling wholesale transactions between NPPS providers has CDD obligations in relation to the NPPS provider, it has no, or limited visibility into the NPPS providers' customers and is unable to oversee transactions between the NPPS provider and their customers.

© 2013

58. Internet-based payment services that handle all aspects of the customer relationship (*i.e.* registration, cash-in/cash-out and transactions) and are subject to AML/CFT requirements may pose a lower risk than de-centralized services. Providers that rely on unaffiliated third parties for the issuance or redemption of electronic currency may also lead to segmentation of services and increased ML/TF risk. The segmentation of Internet-based payment services is particularly concerning as their cross-border nature means that providers may be located in jurisdictions with inadequate AML/CFT regulation and supervision.

vi. Risk matrix

59. The risk matrix below[22] features a series of risk factors that, although not exhaustive, help to identify the risks associated with any type of individual NPPS, including prepaid cards, mobile payments and Internet-based payment services. It is important to take a holistic approach when assessing the risks associated with a particular NPPS. Rather than considering the risk factors listed in the matrix one-by-one, the risks, risk mitigants, and functionality of a particular NPPS should be considered together to determine whether the product poses a high or low ML/TF risk. The risk factors below are intended to be illustrative and some NPPS may contain elements of both higher risk and lower risk factors which should be considered, and combined with the existence of risk mitigants, to determine the overall level of risk.

60. Although the risk matrix applies fully for NPPS, the nature and functionality of the NPPS can vary considerably in comparison to other payment instruments (e.g. credit and debit cards), and product can be tailored in different ways to allow for different uses. For this reason, the risk assessment of NPPS should be developed on a case-by-case basis, taking into consideration the specific features of the single product. In doing so, consideration should be given to the following specific risks which are associated with NPPS.

22 This risk matrix was first published in the FATF typologies report on *Money Laundering Using New Payment Methods* (2010). It is an updated version of the risk matrix which was published in an earlier FATF typologies report, the *Report on New Payment Methods* (2006).

 © 2013

Table 1: **Payment Methods Risk Factors** [1]

Criteria		Cash[2]	NPM Higher risk factors	NPM Lower risk factors
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	Customer's identity is verified on the basis of reliable, independent source documents, data or information (Rec. 10)
	Monitoring	none	none	Ongoing Monitoring of business relationships
Record keeping		Records are generated for authorities through cross border declarations (R. 32)	Electronic transaction records are generated, but not retained or not made accessible to Law Enforcement Agencies (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	Records are generated for authorities through cross border declarations (R. 32)	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/CFT obligations and oversight
Geographical limits		Some currencies are	Transfer of funds or withdrawal across national	Transfer of funds or withdrawal only domestically

Criteria		Cash[2]	NPM Higher risk factors	NPM Lower risk factors
		accepted more widely than others; currencies can be converted through intermediaries	borders	
Usage Limits	Negotiability (merchant acceptance)	Generally accepted	High number of accepting merchants / point of sale (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 countries without appropriate safeguards; lack of oversight and clear lines of responsibility	All processes completed in-house to a high standard

Table notes

1. The risk matrix is taken from the 2010 NPM typologies report and focuses on risk factors, only the headings of two columns have been revised from 'low/high risk' to 'lower/higher risk factors'. This is consistent with the *FATF Recommendations* which also refer to lower/higher risk scenarios.
2. The 'cash' column is provided to allow a comparison between risk factors for NPM and cash, which represents a higher level of ML/TF risk. The controls on cash are with respect to the cross-border transportation of cash which would trigger cash declaration or disclosure obligations pursuant to Recommendation 32. Recommendation 32 may be applicable to certain products if they qualify as bearer negotiable instruments.

© 2013

B. RISK MITIGATION MEASURES

61. The overall degree of risk of a particular NPPS is, in a given context, the cumulative effect of combining each of the risk factors described above. In addition, procedures to mitigate risk should be proportionate to the level of risk posed by the product or service. Adopting proportionality criteria allows the risks posed by a particular NPPS to be addressed, while maintaining the functionality which is aimed at customer convenience and ease of use. Against these considerations, within national or applicable regulatory frameworks, private sector institutions should take into account the ML/TF risks of a product or service while it is still in its project phase, with a view to designing it in such a way that these vulnerabilities are kept to a minimum. This section of the paper provides guidance on possible risk mitigation measures that private sector institutions should take into account during the product design phase.

62. Financial institutions should identify, assess and understand the risks posed by the NPPS they provide before establishing their CDD processes and procedures. In particular, financial institutions should undertake this risk assessment, with a particular focus on ML/TF risks posed by new products and business practices, including delivery mechanisms, and the use of new technologies, prior to their launch. This is an essential step in this process which enables financial institutions to establish appropriate risk-based AML/CFT measures in proportion to the level of risk identified.

i. Customer due diligence

63. CDD is an effective measure to mitigate ML/TF risk associated with NPPS. Under the risk-based approach, the extent to which the NPPS providers should take measures to identify and verify their customer's identity will vary depending on the level of risk posed by the product, in line with the *FATF Recommendations* and the laws in the applicable country.

64. Where the ML/TF risks are lower, financial institutions could be allowed to conduct simplified CDD measures, which should take into account the nature of the lower risk. Simplified CDD never means a complete exemption or absence of CDD measures. For NPPS providers that establish business relations[23], a simplified set of CDD measures may be basic and minimal, but must still respond to each of the four CDD components outlined below in section VI. In line with the risk-based approach, it is the type and the extent of customer and transaction information required, and the mechanisms used to meet these minimum standards that will vary depending on the risk level. In a lower risk context, fulfilling CDD customer identification, verification and monitoring requirements of Recommendation 10 could for example entail less intensive and formal means of information gathering and monitoring and a reliance on appropriate assumptions regarding the intended usage of basic products, or less detailed and frequent information. The *FATF Recommendations* provide examples of circumstances where ML/TF risk can be considered as potentially lower, in relation to particular types of customers, countries or geographic areas, or products, services, transactions or delivery channels.[24] In particular for NPPS, one lower risk example is "financial products or services that provide appropriately defined and limited services to

23 The *FATF Recommendations* do not define this notion. It is left to countries to decide whether business relations are established.

24 See Interpretive Note to Recommendation 10 at paragraph 17.

certain types of customers, so as to increase access for financial inclusion purposes". NPPS providers should also consider the circumstances in which a customer of a NPPS may be considered higher risk and ensure that it has procedures in place to conduct enhanced CDD measures where higher ML/TF risk is identified.[25]

65. It is important to note that the *FATF Recommendations* allow financial institutions in non-face- to-face scenarios to verify the identity of the customer following the establishment of the business relationship (rather than before or during the course of establishing a business relationship) when essential to not interrupt the normal conduct of business and provided that the ML/TF risks are effectively managed.[26]

66. The greater the functionality of the NPPS, the greater the need may be for more enhanced CDD. Non-face-to-face verification of customer identity often requires corroborating information received from the customer with information in third party databases or other reliable sources, and potentially tracing the customer's Internet Protocol (IP) address,[27] and even searching the Web for corroborating information, provided that the data collection is in line with national privacy legislation. It may be appropriate to use multiple techniques to effectively verify the identity of customers. In situations where higher ML/TF risk is identified, enhanced CDD should be carried out in proportion to that risk.

67. In all cases, transaction monitoring and suspicious activity reporting is essential. Its importance is even greater, however, where obtaining reliably information on the customer may be difficult. This may be the case in countries that have no reliable identity card scheme, or alternative reliable forms of identification.

68. Prepaid cards and mobile payment services are commonly distributed using a wide network of agents or distributors which the service provider may then use to undertake the CDD during the face-to-face transaction. In such cases, distributors or agents are carrying out the CDD obligations on behalf of the provider, and the programme manager or issuer should include the distributors or agents in its AML/CFT programme and monitor their compliance with applicable CDD measures.

69. Using an agent gives institutions a chance to conduct CDD while the customer is physically present. When using the Internet, the mobile service provider will have to rely on non-face-to-face identification and verification.

70. Internet-based payment services typically establish their customer relationships through the Internet and the same channel is used for loading funds into an Internet-based payment account. The Internet-based payment services provider will, in such situations, have to rely on non-face-to-face identification and verification.

---

25 See Interpretive Note to Recommendation 10 at paragraphs 15 and 20.

26 See Interpretive Note to Recommendation 10 at paragraph 11.

27 Every time someone connects to the Internet, the Internet service provider assigns, on a dynamic basis, a unique identifying number, similar to a telephone number in that components of the Internet Protocol address correspond to a geographic location and a particular time frame that can be compared to the physical address a person provides in the account registration process. Note: the collection of such information is not required by the *FATF Recommendations*.

 © 2013

ii. Loading, value and geographical limits

71. Placing limits on NPPS can be an effective mechanism to mitigate ML/TF risk, as long as it is combined with other AML/CFT measures such as account and transaction monitoring, and the filing of suspicious transaction reports. Setting geographical or reloading limitations also mitigates the risk that NPPS may be misused for ML/TF purposes. Limiting the functionality of a NPPS product to certain geographical areas or for the purchase of certain goods and services decreases the attractiveness of the product to money launderers or terrorist financiers. Although, it is important to recognise that such limitations can also limit the attractiveness of the product generally, and financial institutions and countries should consider the adverse effect of any limitations on legitimate customer activity. These measures should be considered and implemented, as appropriate, during the design phase of NPPS.

72. Given that the ML/TF risk increases as the functionality of the NPPS increases, financial institutions could consider establishing individual tiers of service provided to customers. This should be developed on a case-by-case basis during the design phase of new NPPS. In this way, financial institutions may consider applying different restrictions, for example thresholds, for NPPS to ensure that a product remains lower risk, therefore allowing them to apply simplified CDD. In such a scenario, the extent of CDD and other AML/CFT measures should increase as the functionality, and therefore risk, increases.

73. Many prepaid card programmes already envisage loading and duration limits to ensure that the outstanding prepaid value does not present undue ML/TF risk. Other common measures include limitations on the amount that is prepaid and accessible via the card as well as a restriction on the ability to reload funds onto the prepaid card. Both loading and duration limits, as well as limits placed on the ability to make cash withdrawals, can make prepaid cards less attractive for criminals. Thresholds are an effective measure for setting the maximum that can be loaded onto a prepaid card, and held on one card at one time or over a defined period. The level of such thresholds should be determined on a risk-sensitive basis and will vary depending on the existence of other AML/CFT measures. Due regard, however, should be given to consumer protection to ensure that customers have access to their funds as they need it, and appropriate recourse should be considered where customers are denied access to funds held on prepaid cards.

74. In addition, the possibility that some prepaid card programmes allow funds to be transferred from person-to-person may represent a high risk of misuse for ML/TF purposes. Especially where it is envisaged that person-to-person funds transfers can be made through a prepaid card, limits imposed on the possible transfers can be an effective measure to mitigate the ML/TF risk, especially if they are treated as cash. This can be enhanced through combining transfer limits with loading or withdrawal limits. In adopting the risk-based approach, the maximum value that can be transferred person-to-person using prepaid cards may also vary depending on the existence of other AML/CFT measures, such as geographical limitations.

75. For mobile payment services, limitations could be placed on the maximum amount that can be held in a mobile payment account; on the maximum amount allowed per single transaction, including cash withdrawals; on the frequency or cumulative value of transactions and cash withdrawals permitted per day/week /month/ year; or a combination of these. Setting geographical

or purchasing limitations further mitigates the risk that the mobile payment service may be misused for ML/TF purposes.

76. Internet-based payment services are commonly provided in a tiered structure to customers and should be considered on a case-by-case basis. Some digital currencies that are primarily designed to allow for P2P transactions within an online environment, such as in a gaming environment, appear to be limit ML/TF risk by operating in a closed system. However, the level of risk posed is increased if the digital currency can be traded with third parties for national currencies.

iii. Source of funding

77. NPPS providers should consider the source of funding when assessing the ML/TF risk of a NPPS and could consider restricting the permissible sources of funding for that product. Anonymous sources of funding such as cash, or even other NPPS that are anonymous, increase ML/TF risk. NPPS providers should take a holistic view to the mitigation of ML/TF risk through these measures and such restrictions could be combined with other limitations outlined above.

78. When cash is used by an individual to add value to one or more NPPS, for which there are limited safeguards, the NPPS provider could consider requiring the person to be identified if the cash exceeds a predetermined cash load limit either for an individual account, either for one or a series of transactions in a day.

iv. Record keeping, transaction monitoring and reporting

79. Transaction and CDD records are key to AML/CFT efforts and support law enforcement investigations. At a minimum the transaction record of a payment or funds transfer should include information identifying the parties to the transaction, any account(s) involved, the nature and date of the transaction, and the amount transferred. The relative size of a transaction does not necessarily equal the value of the transaction record to law enforcement, so recordkeeping should be kept for all transactions irrespective of the value. The records that are retained should be sufficient to allow the tracing of funds through the reconstruction of transactions.

80. The electronic nature of NPPS provides in principle a good foundation for effective record keeping and the monitoring of transactions. NPPS providers should keep all records relating to transactions and CDD information for a minimum period of 5 years, as is required by Recommendation 11, or the length required by the laws in the applicable country.

81. Unique to a mobile payment are the phone numbers of the sender and receiver as well as the sender, and potentially the receiver's, SIM card information. There may also be information captured by the MNO regarding the exact location of the sender and receiver's phones at the time of the transaction. Depending on the size and nature of the transaction, location information may be a useful component of the transaction record. While the collection of such information is not required by the *FATF Recommendations*, providers could consider this, provided that the collection of this data is in line with national privacy legislation, as it may be useful in the monitoring of customer activity.

© 2013

82. NPPS providers should consider putting in place transaction monitoring systems which can detect suspicious activity based on money laundering and terrorism financing typologies and indicators. Such monitoring systems should take into consideration customer risks, country or geography risks, and product, service transaction or delivery channel risks. The transaction monitoring system could also be used to identify multiple accounts or products held by an individual or group, such as holding multiple prepaid cards.

83. NPPS providers should consider analysing the information and records retained to determine unusual patterns or activity. Where the NPPS provider identifies a transaction which it suspects, or has reasonable grounds to suspect, that the funds involved are the proceeds of criminal activity or are related to terrorist financing, it should report its suspicions to the relevant financial intelligence unit in accordance with the *FATF Recommendations* and the laws in the applicable country.

84. NPPS providers should be vigilant to transactions or activity for which there is no apparent legitimate or economic rationale. In particular, providers should consider situations where NPPS appear to be used as a substitute for bank accounts for no apparent legitimate purpose. For example, a prepaid card which appears to be used in an uncharacteristic manner (such as frequent high value transactions), may be considered unusual in some circumstances given that prepaid cards may not offer similar levels of protection (*i.e.* deposit insurance protections) or same benefits (such as interest) that might be provided to bank accounts in many jurisdictions. Providers should consider the rationale for using prepaid cards and the circumstances in the jurisdiction in which they operate. Further guidance to assist in developing an effective transaction monitoring system, particularly in relation to identifying suspicious transactions, is found in the FATF typologies reports on NPM.

V. IMPACT OF REGULATION ON THE NPPS MARKET

85. In developing an AML/CFT regulatory regime for NPPS, countries should also consider the impact of the regulation on the existing NPPS market. In particular, countries should seek to ensure that AML/CFT regulatory measures remain in proportion to the ML/TF risks associated with NPPS and that the regulatory regime does not inadvertently, or unnecessarily, have a negative impact on the operation of existing products nor limit the development of new products. The section considers the impact of regulation on the NPPS market, including whether such regulation would impact financial inclusion.

A. FATF GUIDANCE ON FINANCIAL INCLUSION

86. In June 2011, following the call from the G-20 to standard setting bodies to help countries apply their standards in a way that is consistent with financial inclusion, the FATF published FATF Guidance: *Anti-money laundering and terrorist financing measures and financial inclusion*.[28] Though not focusing on payment methods specifically, this guidance refers to mobile payments and prepaid cards as payment instruments that may facilitate financial inclusion. It should also be noted that some governments are promoting financial inclusion by using NPPS, such as prepaid cards, to pay public subsidies as these methods may be more accessible by the beneficiaries of subsidy payments.

[28] See FATF (2013b).

The FATF guidance on financial inclusion provides support to countries and their financial institutions in designing AML/CFT measures that meet their goal of financial inclusion, without compromising the measures that exist for the purpose of combating crime.

B. G20 PRINCIPLES FOR INNOVATIVE FINANCIAL INCLUSION

87. The *G20 Principles for Innovative Financial Inclusion*[29] issued in 2010 promote the application of the proportionality principle as the right balance between risks and benefits by tailoring regulation to mitigate the risk of the product without imposing an undue regulatory burden that could stifle innovation.[30] On a general basis, the proportionality criteria have already been endorsed by the *FATF Recommendations*. The proportionality criteria allow countries to apply a risk-based approach allowing, for example, the application of reduced or simplified customer due diligence (CDD) measures for certain lower-risk products or even, in justified cases, for an exemption from CDD measures.[31] The G20 Principles also recognise the specific relevance of prepaid cards as a potential tool for financial inclusion, recommending an ad-hoc regulatory regime geared to the risks inherent in the type of service involved.[32] A proportionate regulatory approach may open the market to increased participation by both service providers, and the un-banked/under-banked. This approach can also increase the use of legitimate channels, thereby lowering the risks of ML/TF that are linked to financial exclusion.

VI. REGULATION, SUPERVISION & THE RISK-BASED APPROACH

88. This section of the paper provides guidance to countries to assist in addressing particular issues associated with the application of the *FATF Recommendations* that are specific to NPPS. It examines how to regulate and supervise entities involved in providing NPPS, and considers the impact of such regulation and supervision on the effective implementation of AML/CFT measures.

A. RISK-BASED APPROACH TO AML/CFT MEASURES AND SUPERVISION

89. The *FATF Recommendations* support the development and implementation of a risk-based approach to AML/CFT. This risk-based approach allows countries, within the framework of the FATF requirements, to adopt a more flexible set of measures, in order to target their resources more effectively and apply preventive measures that are commensurate to the nature of risks, in order to focus their efforts in the most effective way. An essential first step of the risk-based approach is that

---

29 See Principles and Report on Innovative Financial Inclusion (2010).

30 See Principle 8 on Proportionality: *Build a policy and regulatory framework that is proportionate with the risks and benefits involved in such innovative products and services and is based on an understanding of the gaps and barriers in existing regulation.*

31 The Interpretive Note to Recommendation 1 at paragraph 6 states: *Exemptions – Countries may decide not to apply some of the FATF Recommendations requiring financial institutions or DNFBPs to take certain actions, provided...there is a proven low risk of ML and TF; this occurs in strictly limited and justified circumstances; and it relates to a particular type of financial institution or activity...* The complete Interpretive Note to Recommendation 1 is available at www.fatf-gafi.org.

32 A proportionate regulatory regime may include for example a combination of maximum allowable transaction turnover, balance thresholds and liquidity and solvency-related requirements.

 © 2013

countries should first identify, assess and understand the risks of money laundering and terrorist financing that they face, as required by Recommendation 1. This is an overarching requirement that applies across the AML/CFT measures required by the *FATF Recommendations*. Also relevant in this context is Recommendation 15 which requires countries and financial institutions to identify and assess the money laundering or terrorist financing risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms and the use of new or developing technologies for both new and pre-existing products. Countries are then in a position to adopt appropriate and proportionate measures to mitigate the risk they have identified with respect to NPPS.

90. The general principle of a risk-based approach is that where there are higher risks, countries must require financial institutions to take enhanced measures to manage and mitigate those risks, and that correspondingly where the risks are lower (and there is no suspicion of money laundering or terrorist financing) simplified measures may be permitted. This means that countries can and should move away from "one-size-fits-all" solutions, and tailor their AML/CFT regime to their specific national risk context. Under the risk-based approach, the intensity of AML/CFT measures depends on the level and nature of the risks identified. The risk-based approach *requires* countries to take a more enhanced and focused approach in areas where there are higher risks, *allows* them to take a simplified approach where there are lower risks, and creates exemptions from certain requirements if there is proven low risk and other conditions are met.[33] It enables countries, within the framework of the FATF requirements, to adopt a more flexible set of measures in order to target their resources more effectively and apply preventive measures that are commensurate to the nature of risks, in order to focus their efforts in the most effective way. A risk-based approach to NPPS furthermore enables countries to mitigate financial exclusion, which represents a ML/TF risk and an impediment to achieving effective implementation of the *FATF Recommendations*.

91. As noted above, the intention of this guidance on the risk-based approach to NPPS is to build on and complement existing FATF guidance relating to the development and implementation of a risk-based approach to AML/CFT, including in particular the *FATF Guidance on ML/TF risk assessment* and the *FATF Guidance on anti-money laundering and terrorist financing measures and financial inclusion*.

B. CUSTOMER DUE DILIGENCE

92. Under Recommendation 10, countries should require financial institutions to perform CDD in order to identify their clients and ascertain information pertinent to doing business with them. CDD requirements are intended to ensure that financial institutions can effectively identify, verify and monitor their customers and the financial transactions in which they engage, in relation to the money laundering and terrorism financing risks that they pose.

93. Pursuant to Recommendation 10, countries should require financial institutions to undertake CDD, including identifying and verifying the identity of their customers, when:

[33] "Low risk" situations refer to cases that may qualify for an exemption from the *FATF Recommendation* is applied, while a simplified AML/CFT regime may apply to "lower risk" cases.

(a) establishing business relations;[34]

(b) carrying out occasional transactions above USD/EUR 15 000 or that are wire transfers in the circumstances covered by the Interpretive Note to Recommendation 16;

(c) there is a suspicion of money laundering or terrorist financing; or

(d) the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.

94. An essential question for countries to consider is whether NPPS involve the establishment of business relations. Commonly, NPPS operate in similar ways to an account as referred to in Recommendation 10. The holding and management of an account on behalf of a customer represents the establishment of a business relationship which is a circumstance that, according to Recommendation 10, requires the conduct of CDD measures. In particular, open-loop reloadable prepaid cards increasingly operate in many similar ways to an account as their functionality has increased. Internet-based payment services also commonly hold and manage funds on behalf of their customers, while providers of mobile payment services, whether prepaid or post-paid, typically establish business relationships with customers as envisaged by Recommendation 10 as well.

95. Countries should require financial institutions to undertake the following steps for CDD in line with Recommendation 10: (i) identification and verification of the customer's identity; (ii) identification of the beneficial owner; (iii) understanding the purpose of the business relationship; and (iv) on-going monitoring of the relationship. While countries should require financial institutions to apply each of these CDD measures, the extent to which such measures are applied should be determined using a risk-based approach. It is also important to note, however, with respect to NPPS that operate as accounts, a requirement of Recommendation 10 is that countries should not allow financial institutions to keep anonymous accounts or accounts in obviously fictitious names. When implementing AML/CFT measures on risk-based approach, countries could consider allowing simplified CDD measures where new payment products are lower risk products.

96. The use of thresholds is an important consideration with respect to CDD and NPPS. Thresholds can be used as an effective risk mitigant for a particular product, and therefore as a measure to allow for the application of simplified CDD. The level of threshold will vary between countries, depending on the level of risk posed by NPPS in that country, and should be determined based on a risk assessment.

97. Where NPPS are lower risk and sufficiently low loading or usage limits are applied, countries should still require financial institutions to give sufficient attention to the detection of smurfing and structuring schemes intended to circumvent the thresholds and suspicious reporting requirements. For example, countries could consider applying thresholds to allow the financial institution to carry out the first three steps of CDD by relying on the customers' statements. In this way, countries may consider applying a so called "progressive" or "tiered" KYC/CDD approach whereby low transaction/payment/balance limits could reduce ML/TF vulnerabilities. The stricter the limits that

[34] The *FATF Recommendations* do not define this notion. It is left to countries to decide whether business relations are established.

 © 2013

are set for particular types of products, the more likely it would be that the overall ML/TF risk would be reduced and that those products/services could be considered as lower risks. Simplified CDD measures might therefore be appropriate.

98. In addition, in situations of strictly limited and justified circumstances of proven low ML/TF risk, countries may consider exempting certain NPPS from CDD measures.[35] In such circumstances, a particularly low threshold may be useful in providing an additional safeguard.

99. Countries should ensure that NPPS providers are subject to CDD and monitoring requirements as part of their ongoing CDD to detect suspicious activity. In particular, providers of NPPS with similar functionality to that of accounts should be required to conduct ongoing CDD. The fewer account-like elements or functionalities of a prepaid card, the greater the possibility to apply simplified CDD measures. The application of loading limits can assist in this regard.

100. Countries should note that under the FATF Recommendations, they may allow, as an exception, financial institutions in non-face-to-face scenarios to verify the identity of the customer following the establishment of the business relationship (and not before or during the course of establishing a business relationship) when essential to not interrupt the normal conduct of business and provided that the money laundering risks are effectively managed.[36] Countries could consider this and the examples in the Interpretive Note to Recommendation 10[37] of verifying customer identity after the establishment of business relations, when determining the point at which CDD is required.

101. Applying funding and transaction limits mitigates the risks stemming from the use of retail outlets and the Internet for the distribution of prepaid cards and mobile payment services. Without sufficient CDD, however, acquiring prepaid cards via the Internet could allow for multiple cards to be acquired by the same person using different names. Countries should consider measures to mitigate the risk posed by multiple purchases of a NPPS, such as prepaid cards, under the thresholds, in a single transaction or from multiple retailers. The requirement to report suspicious transactions should apply in such situations. Countries could also consider placing restrictions on the number of cards sold in a single transaction, although the practical difficulties in enforcing such restrictions are recognised. Where prepaid cards or mobile payment services are distributed through retail outlets and those retailers are required to carry out CDD, inaccurate customer identification poses also a risk if the outlet staff is not adequately trained. Where CDD is carried out by electronic verification, providers should ensure information that is relied upon is accurate and from reliable sources.

---

35 The Interpretive Note to Recommendation 1 at paragraph 6 states: *Exemptions – Countries may decide not to apply some of the FATF Recommendations requiring financial institutions or DNFBPs to take certain actions, provided...there is a proven low risk of ML and TF; this occurs in strictly limited and justified circumstances; and it relates to a particular type of financial institution or activity...* The complete Interpretive Note to Recommendation 1 is available at www.fatf-gafi.org.

36 The Interpretive Note to Recommendation 10 at paragraph 11 states that examples may include non face-to-face business, and securities transactions. It is also noted that financial institutions will need to adopt risk management procedures with respect to the conditions under which a customer may utilise the business relationship prior to verification.

37 See Interpretive Note to Recommendation 10 at paragraph 21.

102. In most instances, the customer of the NPPS provider is clear, as the person who has subscribed to the service, or who has purchased the NPPS. Given the limited, or lack of, face-to-face contact with customers of NPPS, there is an increased risk that NPPS will be passed on to, and used by, other parties who have not been identified by the provider. This risk can be addressed according to the risk based approach by applying enhanced measures to ongoing CDD and transaction monitoring. Alternatively, countries could consider other points at which CDD is required such as at the point of re-loading.

103. The role of banks and other deposit-taking institutions that provide accounts to NPPS providers is an important issue for countries to consider. Countries should ensure that financial institutions that hold funds on behalf of NPPS providers carry out CDD on the NPPS provider as required by Recommendation 10, in proportion to the risks posed by the NPPS provider.

C. LICENSING / REGISTRATION

104. Where NPPS fall within the definition of MVTS in the Glossary to the *FATF Recommendations*, the provider should be licensed or registered, supervised and subject to AML/CFT measures. Recommendation 14 provides countries with two options in relation to the licensing or registration of agents.[38] Countries should either require the agent to be licensed or registered, or the MVTS provider should maintain a current list of its agents accessible by competent authorities.

105. Internet-based MVTS are subject to the requirements of Recommendation 14. In particular, as Internet-based MVTS are not subject to territorial boundaries, it is important that countries make clear in both law and guidance that the jurisdictional licensing and/or registration criteria that applies to brick-and-mortar MVTS also applies to Internet-based MVTS, even if the service provider is headquartered offshore. This issue is considered further below.

D. WIRE TRANSFERS

106. Recommendation 16 establishes the requirements for countries with respect to wire transfers. Countries must ensure that financial institutions include relevant originator and beneficiary information on wire transfers and that the information remains with the wire transfer throughout the payment chain as set out in the Interpretive Note to Recommendation 16.[39] In addition, CDD must be carried out on customers sending or receiving wire transfers. It is important to note, however, that countries may adopt a *de minimis* threshold for cross-border wire transfers, below which verification of the customer, and beneficiary, information need not be required unless

[38] Consistent with paragraph 22 of the Interpretive Note to Recommendation 16, MVTS providers should be required to comply with all of the relevant requirements of Recommendation 16 in the countries in which they operate, directly or through their agents. In the case of a MVTS provider that controls both the ordering and the beneficiary side of a wire transfer, the MVTS provider: (a) should take into account all the information from both the ordering and beneficiary sides in order to determine whether an STR has to be filed; and (b) should file an STR in any country affected by the suspicious wire transfer, and make relevant transaction information available to the Financial Intelligence Unit.

[39] In order to ensure that originator information is available in international wires, supervisors should oversee that financial institutions use the screens that are specifically applicable to international wires (and not the domestic wire screens).

 © 2013

there is an ML/TF suspicion.[40] That is, for occasional cross-border wire transfers below USD/EUR 1 000, the requirements of the Interpretive Note to Recommendation 16 apply and the name of the originator and of the beneficiary will be requested, as well as an account number for each or a unique transaction reference number; however such information will not have to be verified.

107. Recommendation 16 applies to cross-border wire transfers and domestic wire transfers,[41] and countries must determine whether these requirements apply with respect to NPPS. Prepaid cards that offer person-to-person transfers have a functionality that is similar to wire transfers and should therefore be subject to Recommendation 16. Recommendation 16 is not intended to cover transfers from a prepaid card for the purchase of goods and services. However, transactions are covered by Recommendation 16 where a prepaid card is used as a payment system to effect a person-to-person wire transfer.[42] Countries should ensure that entities issuing prepaid cards which are used to effect a person-to-person transfer are required to include and maintain required and accurate originator information and the required beneficiary information with the payment message, in line with Recommendation 16. In addition, mobile payment service and Internet-based payment service providers that are MVTS providers should be subject to Recommendation 16.[43]

E. SUPERVISORY APPROACH AND IDENTIFICATION OF THE COMPETENT JURISDICTION

108. Countries should ensure that NPPS providers are subject to adequate regulation and supervision in accordance with Recommendation 26. Supervisors should adopt a risk-based approach where, at a minimum, NPPS providers that are MVTS providers should be licensed or registered and subject to effective monitoring systems.[44]

109. In relation to NPPS that are distributed through agents, countries should ensure that the entity which relies on agents to carry out AML/CFT measures should include those agents in its AML/CFT programme, without exception, and monitor them for compliance. Countries should ensure that under their legal framework, the NPPS provider remains responsible for its AML/CFT obligations and is accountable for the actions of its agents.

110. In establishing the supervisory framework, countries should clearly establish the competent authority that is responsible for the AML/CFT supervision of NPPS providers. In addition,

40 See Interpretive Note to Recommendation 16 at paragraph 5.

41 See Interpretive Note to Recommendation 16 at paragraph 3.

42 Interpretive Note to Recommendation 16 states at paragraph 4: *Recommendation 16 is not intended to cover the following types of payments: (a) Any transfer that flows from a transaction carried out using a credit or debit or prepaid card for the purchase of goods or services, so long as the credit or debit or prepaid card number accompanies all transfers flowing from the transaction. However, when a credit or debit or prepaid card is used as a payment system to effect a person-to-person wire transfer, the transaction is covered by Recommendation 16, and the necessary information should be included in the message*. The complete Interpretive Note to Recommendation 16 is available at www.fatf-gafi.org.

43 Interpretive Note to Recommendation 16 states at paragraph 22: *Money or value transfer services (MVTS) providers should be required to comply with the relevant requirements of Recommendation 16 in the countries in which they operate, directly or through their agents.* The complete Interpretive Note to Recommendation 16 is available at www.fatf-gafi.org.

44 See Recommendation 14.

supervisors should have adequate powers to supervise or monitor, and ensure compliance by, NPPS providers with AML/CFT requirements in accordance with Recommendation 27. Countries should consider the public authority which is best placed, and would be most effective, to regulate and supervise NPPS providers in their jurisdiction, bearing in mind the need for a level playing field and a consistent approach in the supervision of entities offering the same type of services, regardless of sectoral difference that may exist among such entities (*e.g.* banks, telecom companies). The competent authority may be clear in many instances, for example, when a country has a single supervisor for all AML/CFT compliance. However, in other instances, namely when countries consider having different authorities supervising compliance with AML/CFT requirements for different NPPS providers, it is recommended that there are mechanisms in place for effective cooperation between those.

111. In relation to mobile payment services, this is particularly important for MNO-centric payment model given that MNOs are not traditionally supervised by public authorities that are responsible for the supervision of AML/CFT obligations. Countries may, for example, consider making the relevant communications authority the supervising entity for AML/CFT, particularly where there is a large presence of mobile payment services offered by MNOs. However, while the communications authority has a greater understanding of the mobile industry and may already be supervising the relevant MNOs, it lacks the AML/CFT expertise that an existing AML/CFT supervisor possesses. If the communications authority were to be made the supervisor, then training and education in AML/CFT would be required to develop the required expertise. In addition, close cooperation between financial and AML/CFT supervisors is essential to ensure co-ordinated and consistent approaches relating to financial services. Alternatively, the existing AML/CFT regulatory authorities may remain best placed to supervise mobile payment service providers due to their AML/CFT experience. The decision on which authority is best placed to be the AML/CFT supervisor for mobile payment services will depend on the circumstances and existing supervisory structures and expertise of a particular country.

112. Internet-based payment services pose challenges to countries in AML/CFT regulation and supervision because their cross-border functionality means that providers can be headquartered in a different country to its customers. Payments can be initiated anywhere around the world over the Internet and it is difficult for law enforcement and supervisors to determine whether the provider is operating in a given country. This is particularly a concern when providers base themselves in jurisdictions where they may not be subject to adequate AML/CFT regulation and supervision. Countries should take measures to ensure that providers that offer Internet-based payment services in their jurisdiction are subject to AML/CFT regulation and supervision of that jurisdiction, regardless of where the provider is located. In particular, in line with Recommendation 14, countries should require the licensing or registration of providers of MVTS, and they should take action to identify natural or legal persons that carry out MVTS without such a licence or registration. To determine whether services are offered in a particular country, countries should consider what is the language used and description of the service on the website, which in some instances may indicate the customers who are being targeted by the service provider. To assist in the supervision of services provided in their jurisdiction, countries could consider, consistent with their legal

 © 2013

frameworks,[45] prohibiting Internet-based payment services from offering services in their jurisdiction without a physical presence, in the form of a local office or agent, in that jurisdiction.

VII. APPROPRIATE AML/CFT REGULATION WHICH ADDRESSES THE RISKS

113. This section provides guidance to countries on the issues they should consider when determining which entity in the provision of NPPS should be responsible for AML/CFT measures, particularly in relation to prepaid cards, mobile payment services and Internet-based payment services.

A. LEVEL OF AML/CFT MEASURES PROPORTIONAL TO THE LEVEL OF RISK

114. The level of AML/CFT measures required should be in proportion to the risk posed by the NPPS. As an example, the closer the functionality of a NPPS is to a bank account, the greater the need to apply comparable regulation, including the application of full CDD measures. In particular, as the functionalities NPPS become more like an ongoing relationship of a depository nature, comparable AML/CFT obligations should apply.[46]

115. What makes a NPPS functionally similar to that of a bank account could be the presence of one or more of the following features:

(a) the NPPS can be reloaded an unlimited number of times;

(b) no or very high funding, loading or spending limits are envisaged;

(c) it is possible to make and receive funds transfers cross-border, and within the country where product is issued;

(d) the NPPS can be funded through cash, and cash can be withdrawn through the ATM network; or

(e) the ability to add or withdraw funds to the account using cash or cash equivalents, whether directly or through another provider or intermediary.

116. These factors should be taken into account in the application of a risk-based approach to AML/CFT regulation. The approaches taken by national regulators with respect to NPPS differ significantly, and some specific examples are provided at Annex 1. Countries may find these examples useful when considering AML/CFT approaches to NPPS; however, it is ultimately the responsibility of each country to ensure that its AML/CFT regime complies with the *FATF Recommendations*, taking into consideration its own circumstances and risk profile.

---

45 For examples of legal frameworks, see annex 1 (section on internet payment services).

46 It is worth noting that a proportionate and tailored approach was endorsed by the private sector in the *Wolfsberg Guidance on Prepaid and Stored Value Cards* which was issued in October 2011. This paper concluded that the closer a prepaid card is to a bank account (*e.g.* it can be reloaded, has no loading/spending limits, and enables funds transfers to be sent and received), the greater the need to apply comparable regulation.

B. ISSUES TO CONSIDER WHEN DETERMINING THE NPPS PROVIDER SUBJECT TO AML/CFT OBLIGATIONS

117. Given the range of entities that can be involved in the provision of NPPS, countries should ensure that their legal frameworks specify clear legal responsibilities for the oversight and control of relevant entities subject to AML/CFT requirements (collectively, "NPPS providers"), and ensure that such NPPS providers are subject to adequate regulation and supervision in accordance with Recommendation 26. In addition, NPPS providers which fall within the definition of MVTS providers should be licensed or registered and subject to effective monitoring systems as required by Recommendation 14.[47]

118. As stated above, under the *FATF Recommendations* entities that provide NPPS that are MVTS, or that operate as a means of payment, should be subject to AML/CFT obligations. Where there are multiple entities involved in the provision of the NPPS or service, and it is not clear which entity is the provider, countries should consider the following factors in determining the appropriate NPPS provider(s):

(a) the entity which has visibility and management of the NPPS;

(b) the entity which maintains relationships with customers;

(c) the entity which accepts the funds from customer, and

(d) the entity against which the customer has a claim for those funds.

119. Depending on the business model, especially is there is a strong segmentation of services, there can also be more than one entity responsible for the provision of NPPS and therefore subject to AML/CFT requirements. Further guidance is provided below for prepaid cards, mobile payment services and Internet-based payment services. In particular, this guidance is based on the operation and role of entities involved in the provision of NPPS outlined in Section I.

i. Providers of prepaid cards

120. In some business models, the prepaid card programme is effectively run by a programme manager who provides the payment service under contract with the issuer and the issuer is responsible for customers' funds. Where it maintains relationships with the customers, the prepaid card programme manager should be directly subject to AML/CFT regulation as it is the entity with the visibility and management of the provision of the prepaid cards or indirectly subject to AML/CFT regulation as an agent of the issuer. In other instances, the card issuer also acts as the programme manager and maintains the relationships with customers and monitors use of the cards. In such instances, it is the card issuer that should be subject to AML/CFT regulation.

---

47 The glossary to the *FATF Recommendations* states that "MVTS refers to financial services that involve the acceptance of cash, cheques, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MVTS provider belongs. Transactions performed by such services can involve one or more intermediaries and a final payment to a third party, and may include any new payment methods. Sometimes these services have ties to particular geographic regions and are described using a variety of specific terms, including *hawala*, *hundi*, and *fei-chen*."

 © 2013

121. Prepaid card providers in practice, commonly use their distributors or agents to carry out the relevant AML/CFT measures. In these circumstances, the prepaid card provider clearly retains ultimate responsibility for complying with the AML/CFT measures. In this scenario, the distributor of a prepaid card is carrying out activities on behalf of the NPPS provider and would therefore be considered an agent of the prepaid card provider , whether or not the prepaid card is considered an MVTS. In such instances, the prepaid card provider would also be liable for any non-compliance with these AML/CFT obligations due to the actions of their distributors or agents.

122. In some instances, countries could consider imposing AML/CFT regulation on NPPS provider, as well as the distributors or agents. Under this approach, the distributors or agents would be subject to legal liability and are directly supervised by the respective supervisory authority. This approach may be particularly beneficial in situations where: there is no contractual relationship between the distributors, and NPPS providers; or that entity is located in another country which creates difficulties in effectively supervising that entity. Such a situation is common where an issuer uses wholesale distributors who, in turn, use a large number of distributors or agents.

ii. Providers of mobile payment services

123. Providers of mobile payment services fall within the definition of *financial institution* as either MVTS or by issuing and managing a means of payment depending on the nature of the service. Mobile payment services that allow P2P transfers are MVTS and countries should ensure that they are subject to AML/CFT measures, including the requirements relating to licensing or registration under Recommendation 14.

124. On the other hand, mobile payment services that provide for P2B transfers fall within the *FATF Recommendations* as the providers are issuing or managing a means of payment. AML/CFT measures should apply to these providers. However, while countries may choose to require the licensing or registration of providers, the requirements under Recommendation 14 would not apply.

125. The entity which should be responsible for AML/CFT obligations will depend on the model and structure of the mobile payment service. Under the *bank-centric mobile payment model*, the bank which manages the funds and the relationships with customers is the financial institution and should be subject to AML/CFT measures.

126. In the *MNO-centric mobile payment model*, the MNO or its subsidiary is the financial institution for the purposes of the *FATF Recommendations*. In this model, the MNO, or its subsidiary provides the service, manages the relationship with the customer, holds the customers' funds, and the customer holds a claim to the funds against the MNO or its subsidiary.

127. As with prepaid cards, providers of mobile payment services may use a wide range of distributors, as agents, that have direct contact with customers at the point of sale, and are in a position to carry out AML/CFT measures (such as CDD) on behalf of the provider. This can be the case for loading prepaid money into a prepaid account or issuing of mobile money. In this scenario, the distributor is carrying out activities on behalf of the mobile payment service provider and would therefore be considered an agent of that entity, whether or not the mobile payment service is considered an MVTS.

© 2013

iii. Providers of Internet-based payment services

128. Providers of Internet-based payment services fall within the definition of *financial institution* as either MVTS or by issuing and managing a means of payment depending on the nature of the service. In general, Internet-based payment services allow P2P transfers and therefore are MVTS. In this case, countries should ensure that they are subject to AML/CFT measures, including the requirements relating to licensing or registration under Recommendation 14.

129. However, some Internet-based payment services that issue electronic currency as a means of payment for goods and services, and do not allow P2P transfers, fall within the *FATF Recommendations* as they are issuing or managing a means of payment. AML/CFT measures should apply to these providers, and while countries may choose to require the licensing or registration of providers, the requirements under Recommendation 14 would not apply.

130. The provider of the Internet-based payment service is the entity which accepts the funds, currency or other value from a customer and either:

(a) transfers, or arranges the transfer, of funds, currency or other value to another location using the Internet to transmit the payment message, or

(b) issues the electronic currency which can be used for the making of transfers or payments.

131. While various business models exist for Internet-based payment services, in general the entity which provides the service also manages relationships with customers. In such models, the customer holds a claim to the funds against that entity. Countries should ensure that this entity is responsible for AML/CFT obligations and subject to supervision.

© 2013

ANNEX 1 – REGULATORY APPROACHES FOR NPPS

This annex contains examples of regulatory approaches taken by FATF member countries with respect to NPPS. These regulatory approaches have not been assessed against the *FATF Recommendations* adopted in February 2012 and their inclusion in this guidance paper does not indicate their level of compliance with the *FATF Recommendations*. Their presentation can therefore not amount to an endorsement by FATF. Countries may find these examples useful when considering AML/CFT approaches to NPPS. However, it is the responsibility of countries' to ensure that their AML/CFT regimes are fully compliant with the *FATF Recommendations* taking into consideration their own risk profile.

PREPAID CARDS

Argentina

In 2011, Argentina established AML/CFT measures and procedures for issuers of prepaid cards (reloadable or non reloadable). These Argentinean regulations establish CDD measures that companies should implement with regards to clients, and require, among other obligations, that companies report to the FIU in a monthly basis the issuance of non reloadable prepaid cards for amounts over ARS 4 000 (approximately EUR 700).

European Union

The European experience is particularly interesting with respect to prepaid cards – which fall within the broader definition of electronic money – since the regulatory framework, which originally considered electronic money as very close to a deposit, was gradually made lighter. This was achieved through the introduction of a simplified CDD regime for electronic money by the third AML Directive in 2005, and later through the revision of the prudential regime applicable to institutions that can issue electronic money, which lightened prudential requirements significantly but did not amend the essential AML/CFT obligations. The combination of these two regulatory interventions, aimed at fostering the development of electronic money in the European market, gained significant success as the data provided by the European Central Bank shows. In the euro area, the number of transactions made with electronic money increased from 386 billion in 2006 to 1 024,56 billion in 2010[48]. However, it should be noted that closed-loop prepaid cards, that is, where acceptance is limited to the issuer of the card such as in the case of gift cards by a specific merchant, do not fall within the definition of electronic money in the EU Directive. Closed-loop cards still constitute the majority of prepaid cards.

It is interesting to note that the introduction, through the third AML Directive, of an option for single EU member States to apply a simplified CDD for electronic money followed a consultation with the

48 See European Central Bank (nc).

market operators who claimed that the application of full CDD measures to electronic money was disproportionate and was one of the reasons for the very slow take-up of the electronic money market. On the demand side of the market, there was also a legitimate need for a swift and low-cost payment instrument to facilitate the payment needs of persons who may not have an interest in, or opportunity of, opening a bank account to access payment systems (for example, minors and migrants). As of 2004, there was also an increasing interest and commitment on the part of governments globally to improve the quality and reduce the price of remittance services. Electronic money products including prepaid cards seemed to have the potential to serve this purpose as well. The European regulator acknowledged the claims of the operators and allowed single Member States to apply a simplified CDD for electronic money up to certain thresholds: EUR 150 when electronic money could not be reloaded and a yearly turn-over of up to EUR 2 500 when electronic money could be reloaded. The second electronic money Directive in 2009 raised the threshold for electronic money which cannot be reloaded to a maximum of EUR 250.

Note: The FATF recognises that the 4th EU AML Directive is currently being developed and encourages readers to monitor the development and implementation of this directive.

Germany

It should be noted that some EU Member States did not follow the option in the third AML Directive for a simplified CDD, but instead designed their own stricter simplified due diligence regime for electronic money. For example, in Germany, legislation was introduced in December 2011 which only allows for an immediate and complete exemption of prepaid card products from CDD if the following criteria are met:

1. The product has a threshold of EUR 100 (which is considerably lower than the thresholds in the EU Directive);
2. The product does not enable customers to carry out person-to-person transactions;
3. The product cannot be reloaded by other electronic money products and cannot be used to reload other electronic money products; and
4. The product does not allow for cash withdrawals beyond EUR 20.

Prepaid cards that do not meet these criteria may still benefit from simplified CDD or even exemption from CDD. This, however, requires a formal application to the supervisory authority which will then assess the risk of the individual prepaid card product and determine what degree of CDD is appropriate for it. Such risk assessment is not exclusively based on thresholds but takes into account all relevant risk factors. On the other hand, where the supervisory authority concludes that a prepaid card bears a high ML/TF risk, it can issue instructions and take additional measures against the issuers and distributors, including a ban of the product. This also applies to prepaid cards that were issued by an operator abroad.

© 2013

South Africa

In South Africa, card association branded payroll prepaid cards are issued to some workers to pay salaries. The prepaid cards can be used at ATMs to withdraw cash and at point of sale devices to purchase goods. No additional funds (deposits) may be uploaded onto the prepaid card by either the cardholder or other external parties, and no debit orders may be processed against these cards or the employer's balances held at the bank. An employer can apply to participate in the payroll programme. On approval, the employer is subjected to the full Financial Intelligence Centre Act (FICA) requirements with respect to CDD and is required to keep records of the identities and residential addresses of each cardholder. An internal bank account is then opened for the employer which is used for settlement purposes and at any given time reflects the aggregate credit balances remaining on the prepaid cards. The employer transfers the aggregated amount of salaries/wages to the employer's prepaid card bank account before payday and notifies the bank of the transfer and provides instructions for the transfers to each prepaid card.

India

Pre-paid payment instruments (PPIs) issued by banks and non-bank entities have been gaining popularity as a means of payment in India. The pre-paid payment instruments that can be issued in the country are classified under the three categories viz. (i) Closed system payment instruments (ii) Semi-closed system payment instruments and (iii) Open system payment instruments. Both banks and non-banks are allowed to issue PPIs but only banks can issue open system PPIs, i.e., those that allow cash withdrawal from ATMs.

Proposal for issuance of PPI by banks are approved after getting clearance from the concerned regulatory department of RBI. All other persons proposing to operate payment systems involved in the issuance of PPIs need authorization from Reserve Bank of India (RBI), under the Payment and Settlement System Act 2007. All other persons should have a minimum paid-up capital of INR 10 million (USD 0.18 Million approx) and positive net owned funds.

The maximum value permitted for any category of PPIs is INR 50 000 (USD 900approx). Eligible PPIs can be reloaded through cash and / or debit to bank account or credit card at bank branches/ATMs/authorized outlets/through agents of banks and non-bank entities. Proper due diligence of agents authorized for sale/reloading of PPIs is mandatory.

Banks, which have been permitted to provide mobile banking transactions by RBI, are permitted to launch all types of mobile-based PPIs (mobile wallets & mobile accounts). Other persons are permitted to issue mobile phone-based semi-closed PPIs subject to a limit of INR 5000 (USD 90 approx) and without any facility of person-to person transfer of value.

Banks are also permitted to issue PPIs for credit of cross border inward remittance under the Money Transfer Service Scheme (MTSS) of RBI, subject to KYC and other conditions. The use of PPIs for cross border transactions is subject to foreign exchange management rules. A risk-based approach has been adopted for KYC of PPIs in that the degree of due-diligence of the customer varies with the monetary limits and nature of the instruments. Following three types of semi-closed PPIs can be

issued:

1. Semi-closed system prepaid payment instruments can be issued up to INR 10 000 by accepting minimum details of the customer provided the amount outstanding at any point of time does not exceed INR 10 000 and the total value of reloads during any given month also does not exceed INR 10 000 These can be issued only in electronic form;
2. Semi-closed system prepaid payment instruments can be issued from INR 10 001 to INR 50 000 by accepting any 'officially valid document' defined under Rule 2(d) of the Prevention of Money Laundering Act. Such PPIs can be issued only in an electronic form and should be non-reloadable in nature;
3. Semi-closed system prepaid payment instruments can be issued up to INR 50 000 with full KYC and can be reloadable in nature.

Funds transfer to cards issued by same issuer or any banks account has been permitted from all three categories of cards. Entities other than banks are permitted to issue mobile phone-based semi-closed PPIs subject to a limit of INR 50 000 (USD 900 approx). These cards can be used only for domestic transactions.

Persons issuing PPIs are subject to record-keeping and reporting requirements under Prevention of Money Laundering Act, 2002.

© 2013

MOBILE PAYMENT SERVICES

European Union

In Europe single Member States are allowed to apply simplified CDD for regulated electronic money services up to certain thresholds: EUR 250 when electronic money cannot be reloaded and a yearly turn-over of up to EUR 2500 when electronic money can be recharged. The provisions apply to mobile payments when the funds are prepaid (in which case they are considered electronic money), not when they are paid after the transaction has taken place.

'Direct Billing' is exempted from being a payment service if the product or service purchased falls within certain exemptions in the Payment Services Directive and Second Electronic Money Directive. One exemption is if the product or service is bought through a mobile phone and delivered to and is to be used through a telecommunication, digital or IT device (*e.g.* ring tones, music or digital newspapers), provided that the MNO does not act only as an intermediary between the customer and the supplier of the product or service.

United States

The AML/CFT electronic money regulatory model used in the United States treats all new payment technologies equally without making a distinction among payment card-, mobile- or Internet-based payment technologies.[49] The U.S. requires all providers of MVTS, wherever they may be based in the world, to be licensed and registered in the U.S. if the MVTS provider offers services in the U.S.

India

In India bank-led model is adopted to give customers access to banking services beyond remittance. Only banks which are licensed and supervised by Reserve Bank of India (RBI) and have a physical presence in India are permitted to offer mobile banking services. The services are restricted only to customers of banks and/or holders of debit/credit cards. Customers have to register for Mobile Banking with their bankers. The banks have to put in place a system of document based registration with mandatory physical presence of their customers, before commencing mobile banking service.

The Immediate Payment Service (IMPS) developed and operated by National Payments Corporation of India (NPCI) has also enabled real time transfer of funds through the medium of the mobile phone between accounts in different banks. Only Indian rupee based domestic services are provided. Use of mobile banking services for cross border inward and outward transfers is strictly prohibited.

Banks can also use the services of Business Correspondents (persons and entities that act as an extension of the physical banking infrastructure) for extending this facility to their customers. The guidelines issued by Reserve Bank on "Know Your Customer (KYC)", "Anti Money Laundering (AML)" and "Combating the Financing of Terrorism (CFT)" from time to time would be applicable to mobile based banking services also.

Banks are permitted to offer mobile banking facility to their customers without any daily cap for

[49] The U.S. regulation refers to electronic money providers as providers and sellers of prepaid access.

transactions involving purchase of goods/services. In case of fund transfers involving cash a payout, the maximum limit of Rs 10 000/- (approximately USD 185) will also be applicable for mobile banking. Banks can place a suitable cap on the velocity of such transactions, subject to a maximum value of Rs 25 000/- (approx USD 460) per month, per customer. Banks should carry out proper due diligence of the persons before appointing them as authorized agents for such services. Banks are required to maintain secrecy and confidentiality of customers' accounts.

© 2013

INTERNET PAYMENT SERVICES

Argentina

New regulations of the "Electronic Media Payments" system (MEP) establish the need to identify the recipient and the payer (both with Tax/Labour Identification Number and accounts CBU). A field was included to indicate whether the payer is PEP. This will introduce controls on the transfer of funds, including this as a risk factor. MEP is an electronic payment system administered by the BCRA which is generally used in operations with considerably high amounts. In that sense, financial entities which offer Internet payment services must identify the recipient and the payer and whether the latter is PEP.

European Union

In Europe, Internet-based payment service providers are regulated by the Second E-Money Directive 2009/110/EC if they issue electronic money ('electronic money institution') or else by the Payment Services Directive (2007/64/EC) if they provide payment services without issuing electronic money ('payment institution'). All authorized payment service providers offering Internet-based payments are subject to the full range of AML/CFT measures. In the case of Internet-based prepaid accounts, the funds placed on such accounts are considered as e-money and thus a simplified CDD is required when: (i) the loading limit is below 250 euro for accounts which cannot be reloaded; (ii) the yearly turnover is not higher than 2,500 euro in the case of accounts which can be reloaded. Internet-based payment service providers operate under the passporting provisions of the Payment Services Directive (2007/64/EC) which allow services to be offered throughout the European Union on the basis of the authorization granted in one Member State. The Directive requires a public register of authorized payment institutions, their agents and branches to be kept in the Member State where the payment service provider is established, and requires Member States to cooperate for supervisory purposes and provides for exchange information with authorities in other Member States responsible for authorization and supervision.

In the context of payment services offered over the internet, the Electronic Commerce Directive (Directive 2000/31/EC) sets up an Internal Market framework for electronic commerce, which provides legal certainty for business and consumers alike. It enables providers of so-called "information society services" (which also include financial services offered via the internet) to supply services throughout the Union on the basis of the legislation prevailing in the Member State in which they are established, without the need for an established physical presence in other EU Member States, and in principle does not allow the receiving (or host) Member State to impose licensing or registration obligations on companies established in another EU Member State and providing cross-border services.

© 2013

United States

The U.S. requires all providers of MVTS, wherever they may be based in the world, to be licensed and registered in the U.S. if the MVTS provider offers services in the U.S. This obligation has particular relevance for Internet-based MVTS providers that may have no easily identifiable physical business presence anywhere.

India

Only such banks which are licensed and supervised by Reserve Bank of India (RBI) and have a physical presence in India are permitted to offer Internet banking products to residents of India. Banks can open accounts only after proper introduction and physical verification of the identity of the customer even though request for opening account could be accepted over Internet. Banks are required to keep the data relating to Indian operations segregated and made available to RBI inspection / audit as and when called for. Banks have to report to RBI every breach or failure of security systems and procedures and the RBI, at its discretion, may decide to commission special audit / inspection of such banks. As regards foreign exchange transactions, banks have to comply with the Foreign Exchange Management Act (FEMA) regulations relating to cross-border transactions, operations and maintenance of vostro accounts in India. Banks are required to institute adequate risk control measures to manage risks and maintain secrecy and confidentiality of customers' accounts.

© 2013

BIBLIOGRAPHY

Relevant FATF material (all available at: www.fatf-gafi.org)

FATF (2006), *FATF Report on New Payment Methods,* FATF, Paris

FATF (2008), *FATF Report: Money Laundering & Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems*, FATF, Paris

FATF (2010), *FATF Report: Money Laundering using New Payment Methods*, FATF, Paris

FATF (2012), *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation - the FATF Recommendations, FATF Recommendations,* FATF, Paris

FATF (2013a), *FATF Guidance on ML/TF risk assessment*, FATF, Paris

FATF (2013b), *Guidance on anti-money laundering and terrorist financing measures and financial inclusion*, FATF, Paris

OTHER USEFUL SOURCES:

European Central Bank (nc), *Payment and terminal transactions involving non-MFIs, total number of transactions: 5. E-money purchase transactions,* www.ecb.int/stats/payments/paym/html/payments_nea_n_IEM.NT.Z0Z.Z.en.html accessed on 22 June 2013.

World Bank (2012), *Innovations in Retail Payments Worldwide: A Snapshot*.

The Wolfsberg Group (2011), *Wolfsberg Guidance on Prepaid and Stored Value Cards*.

© 2013