Mobile Money for the Unbanked

Mobile Money: Methodology for Assessing Money Laundering and Terrorist Financing Risks

GSMA DISCUSSION PAPER

Marina Solin
Andrew Zerzan

January 2010

Co-authors
Marina Solin
Andrew Zerzan

The GSMA represents the interests of the worldwide mobile communications industry. Spanning 219 countries, the GSMA unites nearly 800 of the world's mobile operators, as well as more than 200 companies in the broader mobile ecosystem. To find out more visit www.gsmworld.com. It also produces the premier industry events including the MobileWorld Congress in Barcelona and the Mobile Asia Congress. Visit the congress websites www.mobileworldcongress.com and www.mobileasiacongress.com to learn more.

We thank Thaer Sabri thaer@flawlessmoney.com from Flawless Money for contributing to this paper www.flawlessmoney.com

Table of contents

Executive Summary

Mobile money services are currently being deployed in many markets across the world. There is strong evidence that these services can improve access to formal financial services in developing countries.

However, their rise has prompted concerns that mobile money services will be used for money laundering and terrorist financing (ML/TF). Whilst to date there has been no evidence of ML/TF, mobile money systems could be used for these purposes in the future (as other formal financial services are targeted today).

We believe that now is the right time to discuss how risks can be assessed and mitigated most effectively. Mobile operators offering these new services may not be familiar with the risks of money laundering and terrorist financing. Also the relevant regulators (Central Banks and Financial Intelligence Units) are not often familiar with mobile money services and what money laundering (ML) and terrorist financing (TF) risks they pose.

The aim of this discussion paper is to propose a risk assessment methodology based on the principles of the existing framework of the Financial Action Task Force (FATF) recommendations[1]. Our risk-assessment methodology is intended to provide regulators and industry alike with a flexible and consistent means of assessing and mitigating the risk of ML/TF for mobile money services.

The risk assessment methodology proposed in this discussion paper has been developed based on the following assumptions:

- Regulation should be risk-based and technologically neutral, i.e., 'same risk – same regulation' for everybody (banks, mobile operators and any other payment providers). Whilst we talk about mobile money services in this paper, we believe that the same methodology should be valid for other services and players.
- When assessing the risk and its mitigation, it is critical that the unique 'domino effect' of mobile money is allowed to increase the degree of financial inclusion. Expanding the formal financial sector and shrinking the informal economy directly lowers overall ML/TF risks.
- The digital and traceable nature of mobile money makes it a lower ML/TF risk than cash.
- Financial inclusion and AML/CFT are complementary and support each other.
- Mobile money services should be a regulated activity under the supervision of the financial regulator or other financial regulatory authority.
- Proportionate AML/CFT regulation should emerge from close cooperation between financial regulators and industry. Whilst using the existing FATF framework, proportionate AML/CFT measures should emerge from a collaborative 'test and learn' approach.

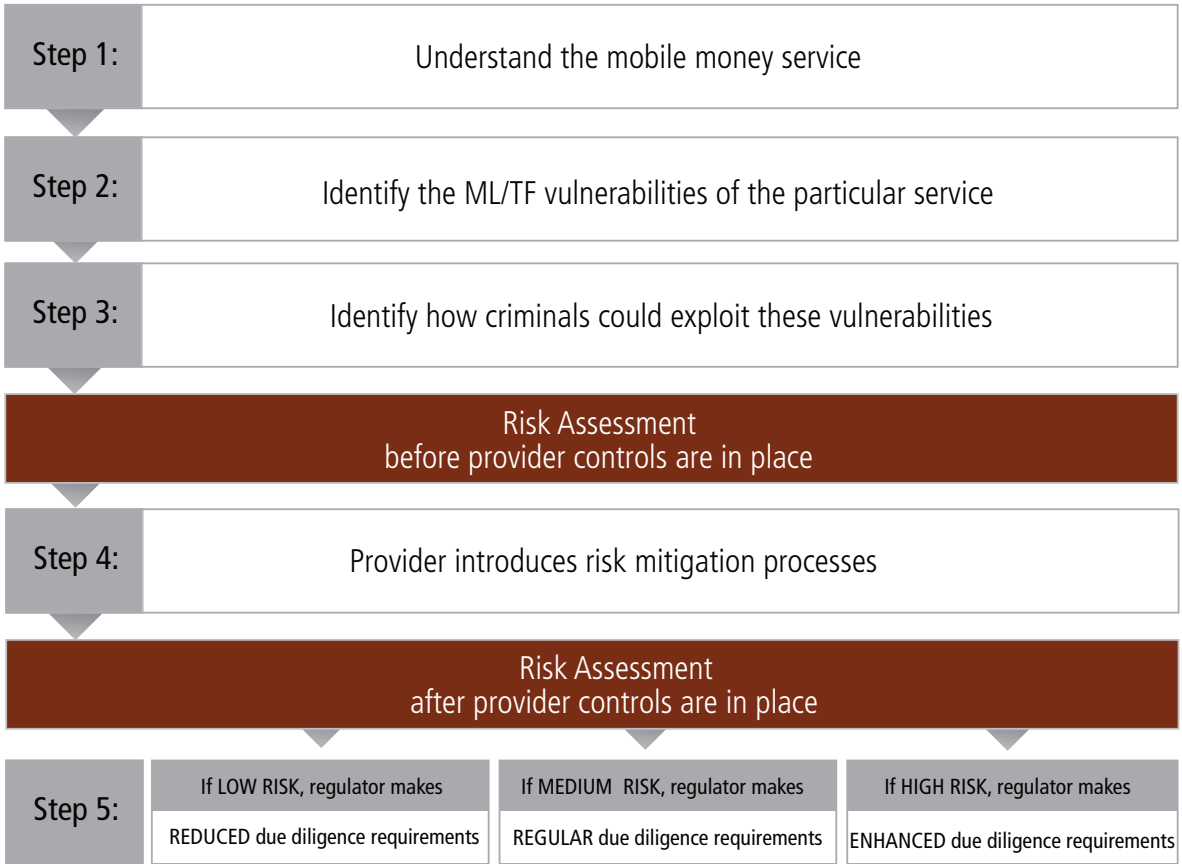
The proposed risk-assessment methodology comprises 5 steps, which we believe help mobile operators and those regulators imposing AML/CFT compliance rules to prevent ML and TF proportionately and effectively. In the first step, the given services, their usage and environment have to be understood. In the second step the vulnerabilities of these services to ML/TF have to be analysed before, in the third step, regulators and industry can develop an understanding of how criminals and terrorist could exploit these vulnerabilities. This will provide an initial risk profile before any controls are put in place.

[1] For instance, FATF Recommendation 5 on Customer Due Diligence. The recommendation calls for control measures to be conducted on a risk-sensitive basis, more controls for higher risk and fewer for lower risk. This paper will discuss how this can be applied to mobile money.

Step 4 is the introdution of control measures that are systems-based. We can then assess the total risk of the service and what futher measures (such as KYC) are necessary via regulation.

Our intended outcome is to encourage the use the whole range of risk-mitigation tools depending on the underlying ML/TF risks.

Summary of risk assessment methodology



There is much to be gained from making it easy for very poor customers in developing countries to use mobile money service whilst at the same time preventing ML/TF. Whilst we do not suggest a 'one size fits all' solution, we do hope that this discussion paper provides a process framework that will be useful to regulators and service providers alike.

1. Introduction

Mobile money services (see definition in Annex 1) are currently being deployed in many markets across the world, and there is strong evidence that they can improve access to formal financial services in developing countries.

Because of the potential to increase access to financial services, the Bill and Melinda Gates Foundation funded the Mobile Money for the Unbanked programme at the GSM Association, which represents the interests of the worldwide mobile communications industry. This project aims to provide, by 2011, financial access via mobile to 20 million unbanked people living below US$2 per day. In many developing countries, mobile operators have been more successful reaching unbanked consumers than banks. In those cases where customers have a mobile phone, but no bank account, mobile money services provide a unique opportunity to bring customers from cash economies into the formal financial system and to provide them with access to financial services.

Studies undertaken in several countries, including Brazil, South Africa, Kenya, Malaysia and the Philippines,[2] indicate that their lower cost is one of the most significant factors driving the adoption of new mobile money services. Speed of delivery and convenience are also important, as are the perceived safety of the money from loss and the security of the transactions.

High take-up numbers where conditions allow consumer-friendly services, such as in Kenya and the Philippines, demonstrate a consumer need for these services. Furthermore, these are a significant rate of penetration among unbanked consumers (on average, one third of mobile money customers are unbanked). The services are characteristically used to perform low-value transactions and are deployed in both urban and rural environments. This paper explores the risk of money laundering (ML) and terrorist financing (TF) with mobile money services in developing countries[3].

The aim of this paper is to propose a risk assessment methodology based on the principles laid out in the existing framework of Financial Action Task Force (FATF) recommendations[4]. Our risk-assessment methodology is intended to provide regulators and industry alike with a flexible and consistent means of assessing and mitigating the risk of ML/TF for mobile money services. Adoption of such a methodology could contribute to a proportionate and coherent risk analysis that provides similar results for similar risks wherever it is applied.

This discussion paper has been drafted in response to a number of recurring questions about the risk of ML/TF with mobile money services. Some of these questions are dealt within the risk assessment methodology; others are summarised in Annex 2 in a FAQ. We hope that this paper and the methodology presented in it will be part of an ongoing debate about how best to manage the risk of ML/TF in mobile money.

[2] Data provided by the World Bank in Integrity in Mobile Phone Financial Services (2008) Box 1, page 8 and subsequent research. Also, see the presentation by Pulver, Caroline. (2009) The Performance and Impact of M-PESA: Preliminary Evidence from a Household Survey. Slide 9.
[3] Even developed countries have people who are unbanked. For example, it is estimated that financially excluded adults in the UK range between 3 and 8 million. Whilst the large benefit of a proportionate regulatory approach towards ML/TF risks will accrue to developing countries. The methodology presented in this paper could also be applicable and beneficial to developed countries.
[4] For instance, FATF Recommendation 5 on Customer Due Diligence. The recommendation calls for control measures to be conducted on a risk-sensitive basis, more controls for higher risk and fewer for lower risk. This paper will discuss how this can be applied to mobile money.

1.1 Mobile money in the context of AML/CFT

There are some general trends in the field of mobile money (and in new payment technologies in general). We believe that these trends need to be taken into account when designing AML/CFT regulation and so have derived from each trend a regulatory principle, i.e., a principle which can help the regulator to design effective AML/CFT regulation.

- *Trend: New types of financial service providers are emerging rapidly to meet consumer needs. This technological change is occurring more quickly than regulation is able to adapt.*

Entering an era of innovation where both banks and a plethora of non-banks offer new payment services means that regulation should be tailored to the type of service, not the type of provider. Similarly, for financial crime, the rules that apply to ML/TF have to be the same for everybody offering the same service, varying only in accordance with the risk posed: 'same risk – same regulation'. The risk assessment methodology proposed in this paper should therefore apply to all entities (banks, mobile operators, third party providers) offering mobile money services (and also for any other payment services).

Technological innovations are occurring rapidly and regulation has to remain effective even with such change. In order to keep regulation effective in the future, it should be designed in such a way that takes risk (technological, systemic and operational) into account, without limiting itself to specific technologies. If regulation focuses on the actual risks posed by a particular service, it is more likely to remain effective even if the provider and the technology change. Identifying and mitigating risk of a particular service should be at the heart of anti-money laundering and combating the financing of terrorism (AML/CFT) activity.

Principle: Regulation should be risk-based and technologically neutral—i.e., 'same risk – same regulation'—for everybody.

- *Trend: Mobile money services have a unique 'domino effect' which brings the unbanked into the formal financial system.*

Research shows[5] that mobile money brings unbanked customers operating in a cash economy into the formal sector. Once they have developed trust in mobile money services, they start demanding traditional financial services, such as savings accounts (i.e. customers who are previously unbanked start to ask for savings after they have become sophisticated users of mobile money and can be handed over to banks and traditional banking services). Mobile money therefore has the important function of bringing unbanked customers into the formal financial system. On a mass scale, this will result in formalising the financial system and lowering overall ML/TF risk.

Principle: When assessing risk and its mitigation, it is critical that the unique 'domino effect' of mobile money is allowed to increase the degree of financial inclusion. Expanding the formal financial sector and shrinking the informal economy directly lowers overall ML/TF risks[6].

[5] Paul Leishman 2009, 'Understanding the Unbanked Customer and Sizing the Mobile Money Opportunity'. In Mobile Money for the Unbanked, Annual Report 2009.
[6] Speech by FATF President Paul Vlaanderen at the ESAAMLG 9th Council of Ministers Meeting, Maseru, Lesotho, 21 August 2009

- *Trend: Mobile money is more traceable than cash.*

ML/TF risks of mobile money are often compared to the risks in traditional banking. However, mobile money is most attractive to customers in cash economies. The risk of ML/TF in mobile money services should therefore also be compared with the risk of ML/TF in the cash economy. Mobile money services replace cash payments over time and make them visible and traceable. Mobile money services should therefore be regarded as a service which has the potential to reduce risks compared to cash payments. It is an interim step towards traditional bank accounts and should be promoted by financial regulators.

Principle: The digital and traceable nature of mobile money makes it a lower ML/TF risk than cash.

- *Trend: Financial inclusion and therefore the expansion of the formal financial system has been recognised as a key tool for AML/CFT*

Mobile money services in developing countries promote access to financial services. Access to financial services and the prevention of ML/TF "are complementary; they are by no means conflicting financial sector policy objectives. Without a sufficient degree of financial inclusion, a country's AML/CFT system will safeguard the integrity of only a part of its financial system – the formally registered part – leaving the informal and unregistered components vulnerable to abuse. Measures that ensure that more clients use formal financial services therefore enlarge the legitimate financial sector"[7].

Principle: Financial inclusion and AML/CFT are complementary and support each other.

- *Trend: It is increasingly recognised that mobile money services have to be regulated and supervised by each market's financial regulator.*

Providers should be regulated by the service they provide, consistent with the FATF's functional definition of "Financial Institution".[8] There are a range of existing regulatory tools for mobile money services. On one end of the spectrum there is traditional banking regulation, under which a mobile operator has to enter into a partnership with a bank in order to be able to offer mobile money services. The bank in such a partnership is responsible for the regulated AML/CFT activity. On the other end of the regulatory spectrum, mobile operators in some countries also have the opportunity to apply for an e-money or payments licence from the financial regulator, thus becoming a regulated financial service provider which has to comply with AML/CFT rules itself. This shows that mobile money services are part of the formal financial system and that AML/CFT obligations should always apply to mobile money services. As the service itself is financial, it is increasingly being recognised that it should be regulated by financial authorities, regardless of the provider type.

Principle: Mobile money services should be a regulated activity under the supervision of the financial regulator or other financial regulatory authority.

[7] Speech by FATF President Paul Vlaanderen at the ESAAMLG 9th Council of Ministers Meeting, Maseru, Lesotho, 21 August 2009, quoting Bester, H., D. Chamberlain, L. de Koker, C. Hougaard, R. Short, A. Smith, and R. Walker. 2008. Implementing FATF standards in developing countries and financial inclusion: Findings and guidelines. The FIRST Initiative. Washington, D.C.: The World Bank page vi.

[8] See the glossary of the FATF 40 + 9 Recommendations under "Financial Institutions" and the World Bank paper Integrity in Mobile Phone Financial Services (2008)

- *Trend: There are so far very few cases of substantiated criminal activity through the use of mobile money services.*

Empirically, there have been very few cases of money laundering[9] through mobile money services in countries where these services boomed. What is more, there have been no reports of terrorist financing.[10] Although any payment system is bound to be abused at some point, World Bank research and reports from the GSMA's fraud working group indicate that so far mobile money has been of little interest to criminals or terrorists compared to other payment channels such as cash or internet.

Although no payment system can be 100% free of abuse, it is important to recognise the attractiveness a system has to criminal activity through statistical data.

Whilst this is good news for the time being, vigilance is required to detect newly emerging risks and ML/TF activities. This can only be done by close monitoring by both the mobile money service providers and financial regulators (and/or financial intelligence units). We hope that this risk assessment methodology combined with close cooperation between regulators and the mobile money providers will result in effective regulation.

We propose therefore the 'test and learn'[11] approach: close monitoring and learning in mobile money pilots to assess initial risks on the basis of this ML/TF risks assessment methodology by both industry and regulators in order to decide on proportionate risk mitigation rules.

Principle: Proportionate AML/CFT regulation should emerge from close cooperation between financial regulators and industry. Using a collaborative 'test and learn approach when piloting new services', risks of new services are systematically assessed before deciding on the appropriate risk-mitigation measures.

[9] Chatain, Pierre; Raul Hernandez-Coss, Kamil Borowik and Andrew Zerzan. Integrity in Mobile Phone Financial Services. World Bank. 2008; De Koker, Louis. 2009. The money laundering risk posed by low risk financial products in South Africa: Findings and guidelines. Journal of Money Laundering Control, Vol. 12 No. 4. 323-339

[10] Zerzan, Andrew. New Technologies, New Risks? Innovation and Countering the Financing of Terrorism. World Bank 2009

[11] The 'test and learn' approach is characterised by very close monitoring by both industry and regulators who cooperatively learn together with initially small and limited pilots to understand risks and all aspects of the mobile money service until all risk elements are understood and satisfactorily mitigated. This permits the regulators to find proportionate and effective risk mitigation tools in the pilot phase. We believe this approach to be more effective than mindless application of existing rules, which may neither be effective nor proportionate. The roll-out and the final decision about the regulatory risk mitigation tools occur after the 'test and learn' phase in the pilot and before a wider roll-out of the respective service. The advantage of the 'test and learn' approach is that the regulator and the mobile operator undergo a process which forces them to deeply understand the risks and risk mitigation tools for a specific service. Both industry player and regulator learn together and from each other in the process.

Regulatory principles for effective AML/CFT regulation

- Regulation should be risk-based and technologically neutral—i.e. 'same risk – same regulation'—for everybody.
- When assessing the risk and its mitigation, it is critical that the unique 'domino effect' of mobile money is allowed to increase the degree of financial inclusion. Expanding the formal financial sector and shrinking the informal economy directly lowers overall ML/TF risks.
- The digital and traceable nature of mobile money makes it a lower ML/TF risk than cash.
- Financial inclusion and AML/CFT are complementary and support each other.
- Mobile money services should be a regulated activity under the supervision of the financial regulator or other financial regulatory authority.
- Proportionate AML/CFT regulation should emerge from close cooperation between financial regulators and industry. Using a collaborative 'test and learn' approach, risks of new services are systematically assessed before deciding on the appropriate risk-mitigation measures.

1.2 Why do we need a risk-assessment methodology?

New mobile money services are emerging all over the world and financial regulators are unfamiliar with the AML/CFT risks arising from these newly emerging services. The current AML/CFT rules are often applied disproportionately to the risks involved, thus hampering the adoption of mobile money services amongst consumers. It is, for example, disproportionate to put a high customer due diligence burden on very poor customers who are transacting very low amounts[12]. Disproportionately strict 'know your customer' (KYC) rules can be impossible for the poor to comply with and may result in their remaining in the informal economy.

The time is right for a global discussion on how to harmonise and fine tune the rules aimed at preventing ML/TF through mobile money services, thus ensuring that these AML/CFT rules are effective and that the benefits of mobile money services reach large parts of the unbanked population.

[12] We are referring here to customers who are the target group of the Mobile Money for the Unbanked project: customers who live below $2 per day and who transact accordingly. We believe applying full customer due diligence on these customers is disproportionate.

2. Characteristics of mobile money services

This chapter considers key characteristics of mobile money services[13]. We break these down these into three parts: (1) what the services are, (2) how they are used and (3) a description of the environment in which they are used. Outlining these characteristics will allow us to then determine ML/TF risks associated with them.

Payment services that are commonly referred to as mobile money services include a range of services: some are simply new means of access to bank accounts, some enable payment from a credit card or other financial services products, and some offer payment from existing accounts held by mobile network operators.

The payment services that are considered in this paper involve the creation of a prepaid account, usually held by the mobile network operator (and in some cases a stand-alone account with a partner bank), and operated as an independent means of payment. They are therefore more than a merely convenient means of access to a bank account, and give rise to stand-alone issues of AML/CFT compliance.

2.1 What services are we talking about?

The following are the most common payment features:

Domestic money transfer: funds remitted from one person to another where both parties are in the same country (also called P2P).

International money transfers: transfers from typically migrant workers abroad to family members in their country of origin.

Funds storage: in some schemes, the account is used as a way to store funds securely, either through a bank account held with a bank or, less commonly, an account held with the mobile network operator.

Retail payments: payments to participating merchants. Merchants can be grocery stores, suppliers of household goods, or the mobile operator itself (from which users can purchase airtime credit or other services).

Payment for utility services: payments for basic utility services such as electricity and water, providing greater convenience and efficiency.

Government payments: payment of salaries, benefits, and similar transactions are expected to develop over the next few years.

2.2 How are the services currently used in practice?

The following gives a profile of how these services are currently used in East Africa (Kenya, Tanzania, Uganda) and Southeast Asia (Philippines, Malaysia) where such services are most prevalent.

Payment values: generally very low, averaging about US$20-$50. The typical user makes a total of only US$500-1000 worth of transactions annually (depending on the GDP of the country).

Frequency of use: as an example, research in Kenya suggests that more than 65% of customers use the service at least once a month, and only 1% do so more frequently than once a week.

Loading and withdrawal of funds: Adding to and withdrawing from an account is done at a variety of retail outlets such as mobile network agents, pharmacies, and grocery stores. In markets where there is a broader traditional financial institution reach, it can be done at a bank branch or remittance agent.

[13] See definitions of mobile money, mobile payments and mobile banking in Annex 1 and also the comparison between mobile money services and banking services in Annex 4.

2.3 What environment do these services run in?

The environment in which mobile money systems currently operate can be described with the help of the example of Kenya[14]:

Geography: generally funds flow from urban to rural areas. Most services currently function only within one country. However, there is great demand for cross-border payments because of the need to cheaply remit money to relatives back home.

Customer demographics: So far, urban users tend to be banked customers who are sending money to their unbanked relatives. Senders typically work in a city and remit funds to family members for regular support. This dynamic creates demand for faster, more secure and more convenient mobile money services and draws unbanked customers into the formal financial system.

Traditional payments and financial services infrastructure: Most people do not have bank accounts or access to a financial institution. In the absence of mobile money services, money transfer is often undertaken through cash and informal channels, including the use of cash couriers and alternative remittance systems.

Public identification infrastructure: whilst in the example of Kenya, there is a mandatory ID system, in many other countries where mobile money services are booming, it is practically unfeasible to verify identity. The lack of national identity infrastructure and documentation affects the majority of people in most markets and prohibits them from entering the formal financial system (see more information in our Annex 3).

Regulatory regime: There is an uneven application of AML/CFT regulations to mobile money services among countries where the service has taken off. According to the World Bank, there has sometimes been a disproportionate implementation of AML/CFT standards because of currently unsubstantiated fears of mobile financial services.[15] Some countries don't have an appropriate regulatory regime or are not effectively enforcing regulations.

The factors set out in the above sections are used in the risk review that follows. We assess them to demonstrate their effect on the overall risk profile of payment products. Two examples of payments service profiles for a classic mobile money service and a traditional banking service are compared in the Annex 4 for illustration purposes.

[14] It is difficult to describe an environment on a global level given that unbanked customers exist all over the world and in all developing countries. For illustrative purposes we have used Kenya as a template, because it is the country where mobile money services so far have been the most successful. Kenya has over 8 million mobile money customers by now.

[15] Chatain, Pierre; Raul Hernandez-Coss, Kamil Borowik and Andrew Zerzan. Integrity in Mobile Phone Financial Services. World Bank. 2008.

3. Risk assessment methodology

There is already some useful literature from the World Bank and CGAP which provides a broad overview of AML/CFT issues in mobile money services[16].

The purpose of the risk assessment methodology in this paper is to provide a proposal for a methodology describing how to analyse ML/TF risks in a systematic way. This gives regulators and industry a practical tool to assess risks and therefore the ability to choose proportionate risk-mitigation responses.

In order to develop this risk assessment methodology we need to assess:

- The vulnerabilities of mobile money to ML/TF risks
- How these vulnerabilities are likely to be exploited by money launderers and terrorists
- What the appropriate tools are to mitigate the identified risks

3.1 How are mobile money services vulnerable to ML/TF risks?

Having identified mobile money service characteristics that have a bearing on the risk of money laundering, the risk review commences by analysing vulnerability of mobile money services to ML/TF risks.

Every payment system has some vulnerability that could facilitate ML/TF. In markets with the highest demand for (and success of) mobile money services cash transactions are the predominant transaction type.

We, therefore, first compare the generic vulnerability of cash and mobile transactions based on the World Bank's risk factors of anonymity, elusiveness, rapidity and lack of oversight[17].

Comparative risks of mobile money if no AML/CFT controls are in place

General risk factors	Cash	Mobile money
Anonymity	***	**
Elusiveness (untraceable transactions)	***	**
Rapidity	*	***
Lack of oversight	***	*[18]

*** indicates risk is highly prevalent
** indicates risk is somewhat prevalent
* indicates risk is low

Anonymity: Even in the worst-case scenario where a mobile customer is not registered, transactions are less anonymous than with cash, since they can be linked to a unique mobile number and since transactions (sender's mobile number, amount, receiver's mobile number, date) are recorded and traceable. This differs from cash where there is neither a unique identifier for the user nor a recorded trace of the payment. In addition, countries[19] are increasingly requiring face-to-face registration with proof of address for the purchase of a SIM card.

Elusiveness: Whilst cash transactions are elusive, mobile money transactions are clearly traceable in the system of mobile operators as part of usual business practice. Telephone number (sending and receiving), time and the amount of the transaction are known to the mobile operator.

[16] See for example CGAP Focus Notes Paper No.56 of August 2009; 'AML/CFT: Strengthening Financial Inclusion and Integrity'; Jennifer Isern and Louis de Koker.
[17] Chatain, Pierre; Raul Hernandez-Coss, Kamil Borowik and Andrew Zerzan. Integrity in Mobile Phone Financial Services. World Bank. 2008.
[18] Mobile operators offering mobile payments have to be licensed by the financial regulators, because this activity is regulated. In some cases mobile operators enter into partnerships with banks who have the regulatory approval to offer mobile payment services. In some cases mobile operators become authorised by the Central Bank independently of banks through a payments or e-money licence. However, we assume that mobile payments are always supervised by the financial regulator. Otherwise they are not permitted.
[19] For example Tanzania, South Africa

Rapidity: Over a distance[20] the electronic character of mobile technology can make transactions much more rapid and effortless than cash. Rapidity is therefore a bigger risk factor for mobile money services than for cash. In the case where there are no automated internal controls, this can provide efficient means for criminals to launder money or fund terrorist activities.

Lack of oversight: Whilst the cash economy lacks oversight, a mobile operator offering mobile money services is usually regulated, either indirectly through a partnership with a bank (financial regulators have therefore oversight of the bank's mobile money activity within the partnership) or directly through becoming a licence holder of a payments or e-money.

In summary, at the outset, we believe that with the exception of rapidity, the vulnerability for ML/TF is greater for cash than for mobile money services. Given that mobile money services are mainly deployed in developing countries/cash economies, mobile money services a priori are an improvement in terms of AML/CTF activity compared to cash.

However, there are still vulnerabilities that criminals might exploit if left unchecked. We will cover these in the next section.

3.2 How could criminals and terrorists exploit these vulnerabilities?

Now that we have identified overall vulnerabilities of mobile money systems, we can apply known ML/TF typologies to test the attractiveness these systems will offer for criminal purposes. Typologies are typical criminal schemes that have been associated with a particular financial service. They assist practitioners in detecting abuse and regulators in assessing the robustness of the provider's systems. In the context of the methodology, they provide an effective way of measuring the degree of risk posed by a payment service and where mitigation measures will be needed.

Because there are very few cases of ML and so far no known cases of TF through mobile money, we will apply typologies used in retail payments and other new payment systems.[21] These have provided much useful information that can be used for this analysis.

The typologies are first broken down into three stages: (1) loading funds into the account, (2) transferring those funds and (3) withdrawing them. They are then set out in terms of opportunities for ML or TF that arise for the different participants in the scheme: consumers, merchants, and partner agents. An analysis of these is laid out in the chart in Annex 5.

Using the four vulnerabilities outlined in the previous section, we can demonstrate how they can facilitate criminal strategies to abuse the system for ML or TF. Although these are just some examples and the comprehensive list is in Annex 5, the samples here will be discussed to illustrate the linkage between ML/TF typologies and the vulnerabilities of a system.

Loading. Perhaps the most noticeable typology applicable to this stage is that of loading illicit monies into the system (also known as the "placement" phase of money laundering).This can be for several reasons, one of which is to continue the process of smurfing, whereby criminals hide the true value of what is being loaded by dividing it into small batches that are more likely to go undetected.

Transferring. Payment services can be abused to "layer". Layering is the strategy criminals employ to complicate the money trail, making it harder to trace.

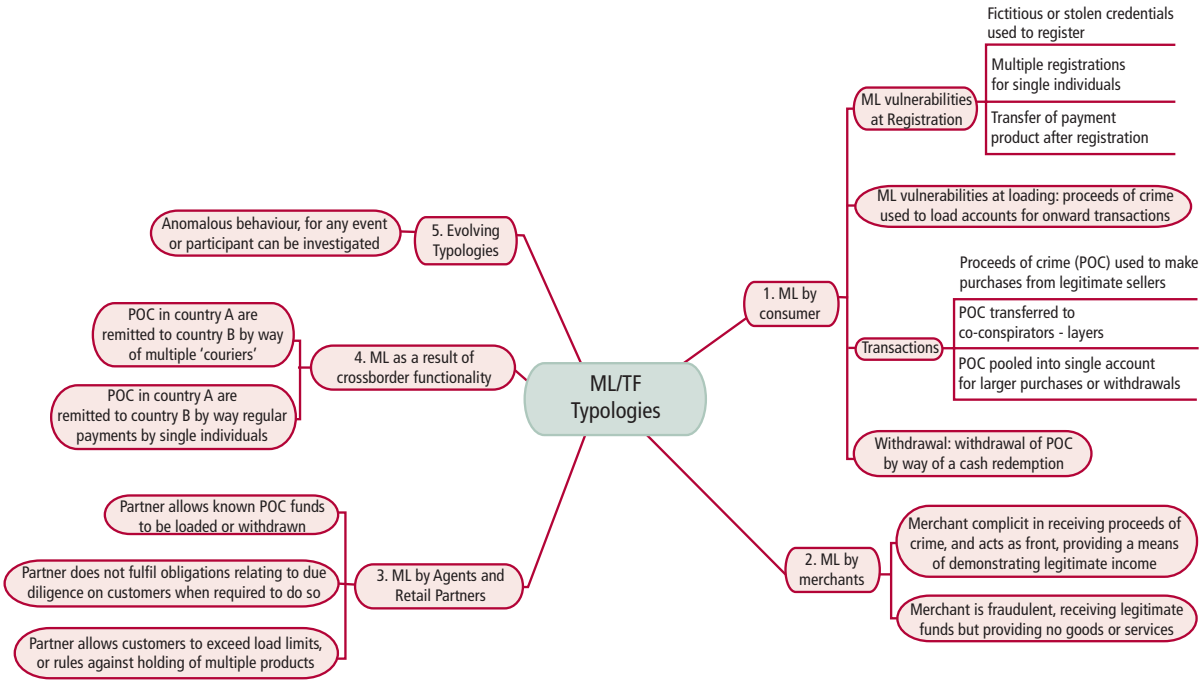
Withdrawing. Perhaps as a continuation of the layering process or as a way to integrate funds of illicit origins, criminals could find the withdrawal stage useful. The rapid movement of funds, coupled with anonymity, from their initial loading to ultimate withdrawal could be used to facilitate either ML or TF.

[20] In a face-to-face-context the handover of cash can still remain as rapid and efficient as electronic technology (and less traceable)
[21] Common issues shared by such services are set out in: FATF "Report on New Payment Methods" of 13 October 2006; FATF "Money Laundering and Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems" of 18 June 2008

General risk factors	Sample exploitation of vulnerabilities at each stage		
	Loading	Transferring	Withdrawing
Anonymity	Multiple accounts can be opened by criminals to hide the true value of deposits	Suspicious names cannot be flagged by system, making it a safe-zone for known criminals and terrorists	Allows for cashing out of illicit or terrorist-linked funds.
Elusiveness	Criminals can smurf proceeds of criminal activity into multiple accounts	Criminals can perform multiple transactions to confuse the money trail and true origin of funds.	Smurfed funds from multiple accounts can be withdrawn at the same time.
Rapidity	Illegal monies can be quickly deposited and transferred out to another account.	Transactions occur in real time, making little time to stop it if suspicion of terrorist financing or laundering.	Criminal money can be moved through the system rapidly and withdrawn from another account.
Lack of oversight	Without proper oversight, services can pose a systemic risk.		

However, looking at potential ways criminals can abuse the system should not be limited solely to the different stages of the payment system. It is also necessary to identify typologies based on the different stakeholders involved.

The typologies are summarised in the diagram and explained in the text below the diagram. The paragraph numbers relate to the numbers on the diagram, which provides a schematic representation of the typologies.



1. **ML/TF by consumers** can take place as part of a conventional transfer of funds that originate in crime or are intended for a crime (such as terrorist financing)[22]. Whilst real credentials may be used at registration, false information can also be presented. It is also possible to use the funding stage to introduce fraudulent value by using stolen credit or debit cards. (This could be regarded as a placement process). Transactions can also be used to move funds amongst co-conspirators, or to move them cross border to jurisdictions where AML/CFT regulation may be less onerous or where the funds can be used to fund further crime. This is then combined with the redemption of such funds for cash, and their extraction for use or onward transfer by other means.

2. **ML/TF by merchants:** these persons may provide a greater risk, as they can receive substantial volumes of payments and extract these as the legitimate product of business (this can comprise integration of funds). Merchants may be fraudulent themselves, defrauding their customers, or may be fronts for the laundering of proceeds of crime from co-conspirators, who can pose as consumers.

3. **ML/TF by agents, intermediaries and retail partners:** these persons occupy a sensitive position in the payment cycle of mobile services: the loading of cash payments, the point of redemption or pay-out, and also the sellers of the handsets themselves which can be used to make payments. Such persons are therefore in a position to falsify records, ignore suspicions that may otherwise be reported, or simply to be a point of weakness where they do not perform their roles in a diligent manner.

4. **ML/TF through-cross border payments** can enable criminal funds to be moved from the jurisdiction where they are created to another where they may be used to further crime, or to be extracted, or to be moved once again to another jurisdiction. Movement across borders hinders law enforcement investigators and may mask the purpose of the transfer. It is therefore an additional source of risk.

5. **New typologies:** as criminals continue to develop new ways to finance terrorism and launder money, it is important to note that these typologies are not comprehensive.

3.3 How to mitigate identified risks

After identifying potential vulnerabilities (section 3.1) and ML/TF threats (section 3.2) to the system, controls measures can be implemented to mitigate the risks. The details of this can be found in Annex 5 where risks are assessed low, medium or high pre- and post- mitigation measure. The following is a summary of the conclusions:

1. **ML/TF by consumers** can be mitigated to be low-risk with a few simple controls in place. The key mitigation measures can be highlighted in light of the environments in which these services are offered. The first is limits on accounts, transaction frequencies and volumes, and amounts transferred within a certain time period. This may be effective if the transaction amounts and volumes are very low. The second is monitoring of transaction flows on the system level, which alerts the mobile money provider about suspicious transaction patterns (similar to ML/TF systems currently used by banks and the fraud systems used by mobile operators). These measures reinforce each other, because limits force criminals and terrorists to split up the transaction into many smaller ones, which would risk detection by the monitoring system[23]. If customers transact high volumes and with a high frequency, which poses a high ML/TF risk, they can be obliged to register face-to-face and become fully identified. The important notion here is to apply risk mitigation tools which are proportionate to the risks.

[22] FATF, Terrorist Financing Typologies Report 2008

2. **ML/TF by merchants** poses an increased risk to the system. Mitigation by way of enhanced initial and ongoing due diligence can, however, decrease this risk to low. In addition, raising awareness is key: merchants care about the viability of their business, so knowledge of how crime can hurt will reduce their likelihood to participate in it. Other methods to assess and minimise risks are training, testing and 'mystery shopping'.

3. **ML/TF by agents, intermediaries and retail partners:** the greatest risk of ML in the system is posed by agents and retail partners who may provide access to the payment service, allow the loading of value onto the system or undertake due diligence activities on behalf of the payment service provider. This risk can be mitigated, but doing so requires enhanced initial and ongoing due diligence and monitoring for compliance with obligations. For instance, providers can assess compliance and integrity of their agents through the use of 'mystery shoppers' that test agents, they can require agents and retail partners to train front line associates in AML/CFT and provide assistance with and monitoring of that training, and, by monitoring activity on an agent location basis, they can identify unusual activity and investigate an take corrective action.

4. **ML/TF through cross-border transfers:** this can increase risk, but transaction-monitoring tools, limits on value and frequency of transactions combined with proportionate customer due diligence can compensate for it and enable unusual and suspicious transactions to be identified, thus mitigating risk to a low level.

This analysis assumes a risk-sensitive approach. Due diligence and other controls must be applied proportionately to the risks posed by each stakeholder. In the case of consumers with low transaction limits and real-time monitoring systems, the risks would tend to be low. However, merchants and agents pose a greater risk because some controls (i.e. limits) cannot be applied to them in the same way. They require enhanced due diligence processes, training and monitoring.

3.4 Comparative risks of mobile money and cash, before and after controls applied

Linking the implementation of the above-mentioned control measures to our initial analysis of comparing mobile payments to cash, general conclusions can now be drawn about the risks. The chart below is an evolution from section 3.1. It shows sample controls and their mitigating effects on risk.

Implementation of control measures renders the system less attractive to criminal interests. Transactions are necessarily small because of limits, so any attempt to move large sums of money from one location to another would be flagged. The rapidity risk, which was seen as higher than cash before controls were in place, is now lower because of automated internal controls (internal controls enforce limits on transactions, account balance an volume of transactions and even if the ML/TF transactions are broken down to fit within the limits, the monitoring system would be able to detect suspicious transaction patterns on the system level). Customer names can be screened quickly against national and international sanctions lists and flagged automatically. It is interesting to note that this is in many ways more efficient than common financial service providers in developing countries where such screening is often manual and subject to human error.

Comparative risks of mobile money and cash, before and after controls applied

General risk factors	Cash	Mobile money		
		Before	Controls	After
Anonymity	***	**	Customer profile building, includes registration info (name, unique phone number, etc)	*
Elusiveness	***	**	Limits on amount, balance, frequency and number of transactions Real-time monitoring	*
Rapidity	*	***	Real-time monitoring Frequency restrictions on transactions Restrictions on transaction amount and total account turnover in a given period	*
Lack of oversight	***	*		*

*** indicates risk is highly prevalent
** indicates risk is somewhat prevalent
* indicates risk is low

4. Conclusions from the risk review

Assessing the actual risk that mobile money poses is critical to designing controls that (1) effectively target the threat faced and (2) do not unnecessarily prevent the poor from accessing this financial service. AML/CFT and financial inclusion are mutually reinforcing goals. AML/CFT ends where the informal cash economy begins. Cash is untraceable, anonymous and its use cannot be monitored. The expansion of mobile money services is an exciting opportunity to reduce the cash economy, making the market safe while simultaneously improving the lives of the poor.

We hope that this methodology contributes to the discussion between industry and regulators in developing business models and regulations that maximise the reach of mobile money. We believe it is only through a careful analysis of the actual risks posed that appropriate proportionate regulation and controls can be developed and we remain ready to support efforts in the future.

Annex 1: Glossary

What are mobile money services?
Mobile money is a broad term that describes using the mobile phone to access financial services. The term does not assume any specific deployment model, or any particular transaction type; it merely describes a service where a customer uses mobile technology to trigger a financial event. As such, it encompasses information-only services (e.g. a balance enquiry) and transactional services (e.g. the use of mobile technology to send money to another person or to pay for goods and services, as well as government payments of salaries and benefits). **Mobile payments and mobile banking are both part of mobile money.**

What is mobile banking?
Another subsection of mobile money is mobile banking, which is different from mobile payments in the sense that the regulated entity is a bank providing traditional banking services. The mobile element is merely a mobile access channel to a traditional banking service.

Annex 2: Frequently Asked Questions

Question/Concern	Answer
Would it be possible for a criminal laundering money to use a phone once and then dispose of it to keep anonymous?	A criminal has the first choice between cash and mobile money to remain anonymous. Cash is more anonymous than mobile money because the mobile money payment is stored in the system and traceable. Even if the criminal decides to transfer money with mobile money, security limits on transaction volume and size as well on account balance would make it very cumbersome and expensive for a criminal to buy many phones and SIM cards. The monitoring system could flag such an activity as a suspicious transaction. And whilst the sender can change the phone/SIM card the system would record the receiving account, unless those numbers and SIM cards are disposed of after each transaction as well. However, in this case, delivery of cash may be cheaper, safer and more convenient for the criminal than buying large numbers of mobile phones and SIM cards given that only small numbers of low-value payments are possible.
What happens if another person uses the phone instead of the registered user?	The registered user has to disclose a PIN number to the unregistered user in order to make a mobile money payment possible. This is equivalent to existing risks in card payments (ie. where the card owner has to pass on his PIN number to make the card payment possible). The registered user is traceable and ultimately responsible.
It is nearly impossible to detect suspicious activity without knowing the identity of the person behind the transaction. CDD is critical for AML/CFT. How can this work with prepaid mobile money accounts where the user's name has not been verified?	CDD is not limited to solely gathering a customer's name. It is a means to detect connected accounts and flag them all if one is shown to be suspicious. In economies where mobile money has had the greatest success, cash is the dominant means to transact. Cash is entirely anonymous and untraceable. It is impossible for anyone to detect connections between users of cash and monitor activity amongst its users. Mobile money, on the other hand, is inherently traceable. The phone number is a unique identifier that provides more information than anonymous cash, making suspicious transactions more visible.

Question/Concern	Answer
It is more effective to increase financial inclusion through non-technological branchless banking models which do not have the risks of anonymity, elusiveness, rapidity, etc. Why should I consider mobile money services?	Two of the biggest barriers to financial inclusion are cost and distance. These two are often intertwined because travelling distance to the nearest bank branch or remittance provider requires the user to incur cost. Technology, especially mobile technology, offers an opportunity to overcome these two obstacles. Mobile money services eliminate the need to travel to a financial institution and offer much lower fees. There is no non-technological banking model that has these characteristics
Mobile money services are not face to face transactions and as such high risk.	Experience to date indicates no greater risk in mobile transactions versus other channels of payment. Very low transaction limits, account monitoring and other controls can be used to mitigate any attractiveness the services have to criminal activity even if they are not face-to-face.
The speed with which value can be moved electronically and the ease of moving SIM cards present risks that are not present in a cash situation.	The limits that are in place in most mobile money schemes are very low. You could carry much more cash than transfer electronically given most of these limits. Moreover, monitoring systems can detect unusual patterns. For instance, if one account is receiving an unusual amount of money from all over the country, it would be flagged as suspicious and all accounts sending to it would be as well.
Mobile money services deserve a 'lex specialis' treatment with respect to the prevention of ML/TF	The GSMA suggests that full customer due diligence for very poor customer (i.e. who live below $2 per day and transact according) who transact very low amounts with a very low frequency (subject to limits build in the services) is disproportionate. This applies to all service providers and not only to mobile operators. It is a view supported by the FATF's risk - based approach guidance.
What would a solution, derived using the methodology proposed in this paper, look like?	A customer sending very small amounts infrequently (and subject to transaction monitoring to detect suspicious patterns) may qualify for simplified customer due diligence. The service offered to this customer is limited in its functionality. Once this customer is familiar with the service and has developed trust and demands more flexibility for higher transactions, he may only obtain the extension to his service if he registers face-to-face. An agent or intermediary, on the other hand, who is transacting larger amounts may not be able to start using the service without full due diligence, because his risk profile is much higher from the start.
While new payment methods often provide transaction records ('electronic paper trail'), these records are rendered useless if the customer remains anonymous or uses a wrong identity).	Even if the name on the MM account is not verified to the highest level, it is not anonymous like cash. The electronic paper trail links allows the operator and law enforcement to monitor account activity and any collaborators of a crime. If an account is flagged as particularly suspicious, the operator can instantly freeze it and require agents to verify identity to an enhanced degree. The electronic records of MM will improve availability of evidence to law enforcement and prosecutors investigating a crime.

Annex 3: Identification and ML/TF

In some countries, a major obstacle for poor persons in accessing formal financial services provided by banks and non-bank institutions is the overly-rigid implementation of Customer Due Diligence standards set by the Financial Task Force on Money Laundering (FATF).[24] The FATF has created standards rules for customer due diligence which encompass: (a) verification of a customer's identity using reliable, independent source documents or data; (b) collection of information on the purpose and nature of the business relationship; and (c) on-going monitoring of transactions activities.

Client identification and verification is especially a challenge in countries with less developed civil registration systems and none or underdeveloped national identity card systems (henceforth ID systems). The latter are based upon registration of the population. National ID systems are systems, where the government issues ID cards to individuals starting at a specific age, based upon national laws or regulations. These systems can be either voluntary, where individuals may apply for a card if they wish or compulsory, where basically all individuals need to hold an ID card when reaching a specific age.

Recent research conducted by Jentzsch (2009)[25] shows that of a sample of 173 countries[26] a total of 136 countries (79% of the sample) had either mandatory or voluntary ID systems in 2007; 37 countries had no ID system (21%). The numbers are also presented in Table 1. There are also countries with substitute systems such as Australia, Canada, U.S.A and UK, where driver's licenses or social security numbers are used for identification purposes, but these are counted here as having no national ID system.

[24] Bester, H., de Koker, L., and Hawthorne, R., (2003), Legislative and Regulatory Obstacles to Mass Banking, pp 1-116, Genesis Analytics; De Koker, L. 2004. "Client identification and money laundering control: perspectives on the Financial Intelligence Act 38 of 2001," Journal of South African Law 715-746; De Koker, L. 2006. Money laundering control and suppression of financing of terrorism : some thoughts on the impact of customer due diligence measures on financial exclusion, Journal of Financial Crime, 26-50; Isern, J., D. Porteous, R. Hernandez-Coss, and C. Egwuagu. 2005. "AML/CFT Regulation: Implications for the Financial Service Providers that Serve Poor People". Focus Note 29. Washington, D.C.: CGAP; Bester, H., D. Chamberlain, L. de Koker, C. Hougaard, R. Short, A. Smith, and R. Walker. 2008. Implementing FATF standards in developing countries and financial inclusion: Findings and guidelines. The FIRST Initiative. Washington, D.C.: The World Bank; Isern, J., and L. de Koker. 2009. "AML/CFT: Strengthening Financial Inclusion and Integrity." Focus Note 56. Washington, D.C.: CGAP.

[25] Numbers presented herein are an update from Jentzsch, N. (2009). Financial Services for the Poor: Lack of Personal Identification Documents Impedes Access, DIW Weekly Report, 17 / 2009, p. 114-121. The numbers are preliminary.

[26] The selection of countries is based upon the World Bank's Doing Business sample.

Existence and Type of ID Systems

General risk Existence and Type of System	Number of countries	Percentage share in sample
Existence of ID Systems		
Total number of countries in sample*	173	
Existence of either mandatory or voluntary ID system	136	78.61
No ID system	37	21.39
Type of ID Systems		
Total number of observations	135	
- of which have compulsory IDS	112	82.96
- of which have voluntary IDS	23	17.04
Number of countries with no observation	38	

* Uncertainty is associated with the observations for Comoros, Kiribati, Vanuatu, Palau and the Democratic Republic of the Congo. The researcher currently awaits replies from the authorities. There is conflicting information on the existence and type of an ID system in Nigeria, which was counted as not having a system in 2007. Source: Jentzsch (2009), updated.

The type of ID system could be observed for 135 countries only. In this sub-sample, 112 nations had compulsory systems (constituting 82.96 percent of the sub-sample) and 23 countries had voluntary systems (17.04 percent).

The existence of an ID system as well as its compulsory nature does not imply that there is a complete coverage of the economically active population. For a number of reasons, coverage might be incomplete. For instance, the geographical distance to authorities issuing the cards might be great and the means of travelling there too time-consuming, expensive and/or hazardous. Further, civil registries are often incomplete when births are not registered, especially in rural areas, where children are often born outside of hospitals.

In addition, for many poor and very poor persons, the prices of the cards might put this important document out of their reach. Prices can range from 3.41 USD of a new card in Angola to 5.44 USD in Benin and a hefty 68 USD for a new electronic ID card in Central African Republic (exchange rates as of 15 October 2009).[27]

[27] Quotes are based on different sources from the authorities and the Internet.

Existence and Type of ID Systems

Countries	Numbers
Pakistan (mandatory ID card system)	
Total population	172.800.048
Economically active population (15 years and older: 62.2%)	107.481.630
Identified population (with national ID card)	62.000.000
Unidentified population	45.481.630
Share of unidentified population	42%
Indicator of access to financial services[1]	12%
Cameroon (mandatory ID card system)	
Total population	18.060.382
Economically active population (15 years and older: 58.7%)	10.601.444
Identified population (with national ID card)	7.209.916
Unidentified population	3.391.528
Share of unidentified population	31%
Indicator of access to financial services1 (in percent)	24%
Tanzania (no ID card system)	
Total population	39.477.000
Economically active population (15 years and older: 56.1%)	22.146.597
Identified population (with passport)	est. 500.000
Unidentified population	21.646.597
Share of unidentified population	97%
Indicator of access to financial services1	5%

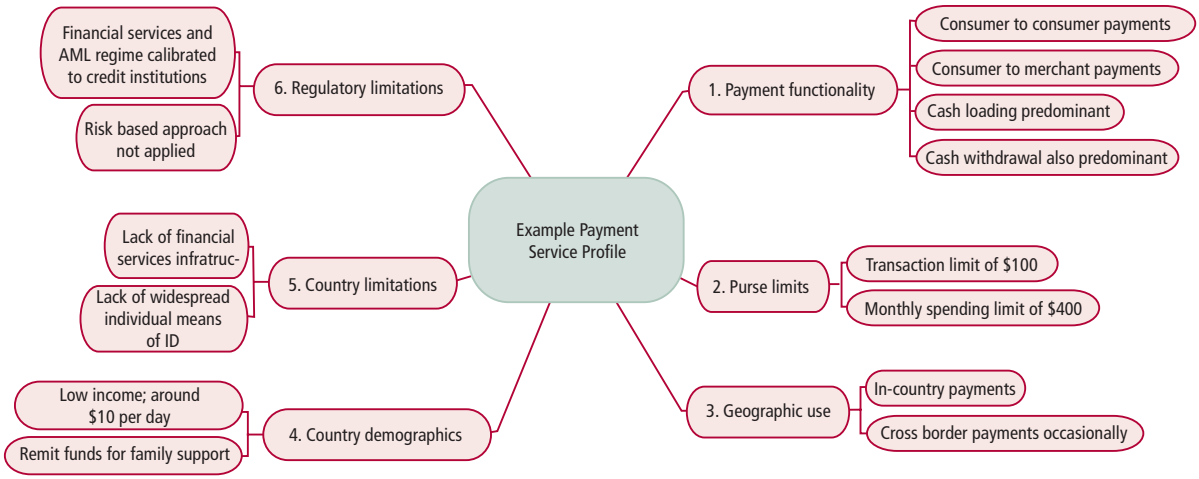
Notes: 1 Percentage of adult population with access to an account at a formal financial intermediary. Sources: 2007 CIA World Factbook; Beck, Demirgüç-Kunt, Martinez Peria (2007); calculations by Jentzsch (2009), based upon numbers issued by local authorities.

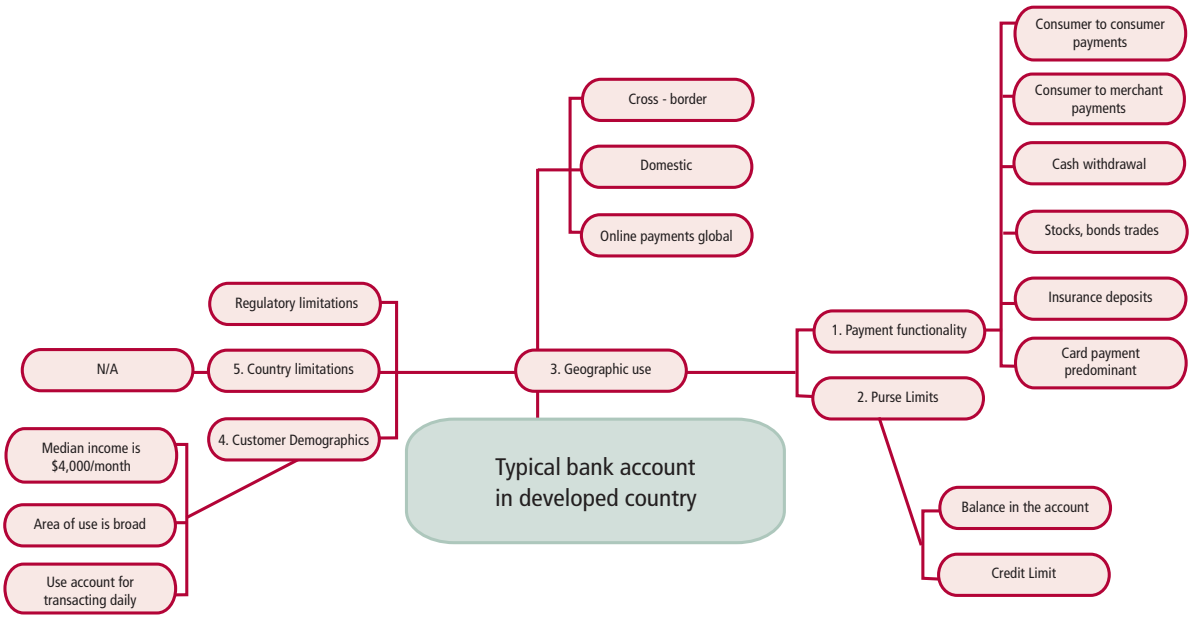
Table 2 shows the percentage of population identified in countries with compulsory ID systems (Pakistan and Cameroon) as well as one with no ID system (Tanzania). The example of Cameroon and Pakistan shows that even in countries with mandatory systems, 30-40 percent of economically active persons are unidentified. In general, there is no international database with information on how many citizens are identified in the individual countries. In a number of countries, there are currently projects underway to roll-out ID cards (such as in Bangladesh or Botswana) or to switch to smart cards that store biometric information (Albania, Republic of Congo). Other nations are planning to roll out multi-purpose cards in the near future (India).

Although most countries are now members in the FATF or FATF-style bodies, there is currently no information on how far it is possible in developing countries to be practically compliant with FATF measures. This area must be left for future research.

Annex 4: Comparison of mobile money and banking service payment profile

Example mobile money service profile





Annex 5 - Table of risks arising from typologies and impact following mitigation

Key: POC = proceeds of crime; DD = due diligence; ML = money laundering

	Typology	Indicator	Vulnerability	Mitigation and comments	Risk following mitigation
1	**ML/TF by consumer**				
a.	Fraudulent registration	Statistical sampling of records and follow up	Medium	Systems should be calibrated to detect fraudulent activity. Account monitoring systems can detect activity that seems abnormal relative to typical behaviour of similar users in a given area. By implementing controls in other parts of the system (strict limits, monitoring, etc.), the risk of fraudulent registration should decrease because the system would be less useful to criminal interests.	Low
b.	Multiple registrations	Transaction patterns may indicate multiple use	Medium	Accounts that are linked to the same person are likely to be detected by the system when very low limits are in place. For example, the system could detect an unusual spike in deposits/withdrawals through a particular agent.	Low
c.	Transfer of service after registration	Use outside of expected geographical area, or contrary to expected profile.	Medium	This is common to all financial services, but mobile services offer a better chance of detection because automated controls are in place to flag and/or freeze highly irregular activities.	Low
d.	Loading with proceeds of crime (POC)	Unusually large loads, frequent loads, or loads just below limit.	Low	Systems conventionally look for such anomalies. Mobile payments are less prone to this typology as the transacted values are small, and frequent use would risk detection. If larger-value payments are routinely transacted, this risk may increase, but would be detected as in conventional payment services.	Low

	Typology	Indicator	Vulnerability	Mitigation and comments	Risk following mitigation
e.	Use of POC to purchase from sellers	Unusually large transactions or purchase of goods/services that make no economic sense.	Low	Systems and processes will need to look for these anomalies. Again, mobile payments are less prone to this typology as the transacted values are small and unusually high transactions would risk detection. If larger payments were commonly transacted, greater emphasis would need to be placed on systems that detect anomalous transactions, where no economic sense could be attributed.	Low
f.	POC transferred to co-conspirators	Transfers are likely to be anomalous to usual geographical transfer patterns. Frequency and value may also be anomalous.	Medium	Systems to detect anomalies will need to be put in place. Account balance limits also make this more difficult as POC would need to be split amongst a great number of mobile money accounts.	Low
g.	POC pooled into single account	Pooling pattern is anomalous unless destination is a retail outlet	Low	Systems to detect anomalies will need to be put in place. Coupled with stringent account limits, monitoring systems are more likely to identify criminal transactions. Account balance limits also make this more difficult as POC would need to be split amongst a great number of mobile money accounts.	Low
h.	Withdrawal of POC by cash redemption	Unusually high or frequent values would be expected.	Low	Anomalous withdrawals can be detected by the most basic systems. Account balance limits also make this more difficult as POC would need to be split amongst a great number of mobile money accounts meaning a criminal would need to withdraw many, many times from an agent. This would likely be flagged.	Low

	Typology	Indicator	Vulnerability	Mitigation and comments	Risk following mitigation
i.	Funds transfer to/from a person linked to terrorism	Identity information of a user matches entry on UN or national sanctions listings	Low	Known terrorists and terrorist financiers can be instantly and automatically screened by the system. If a transaction is detected that could be linked to such individuals, the system can be set to automatically freeze it and flag it for law enforcement. This is a strong deterrent.	Low
2	**ML by merchant**				
a.	Complicit merchant receives POC	(i) Initial and ongoing DD of merchants should reveal fraud, or (ii) Unusual transaction patterns for the type of business	Medium	Ongoing DD is necessary. Systems to detect anomalous behaviour will also be needed, looking for anomalies for the merchant and for the class of merchant.	Low
b.	Fraudulent merchant misappropriates funds	Initial and ongoing DD can seek to identify such incidents	Medium	Fraud cannot be entirely excluded, but good DD processes and transaction monitoring should enable reduction of risk.	Low
3	**ML by agent or retail partner**				
a.	Allows known POC funds to be loaded on or withdrawn from account	Initial DD for partners can provide a good indicator of risk. This can be enhanced given the risk.	High	This is a vulnerable part of the payment chain and additional attention needs to be given to partners. Enhanced due diligence as well as ongoing review of transactions, and periodic audit. For instance, 'mystery shoppers' can be used to test the integrity of an agents' operations.	Low-medium
b.	Partner does not fulfil due diligence obligations, intentionally or negligently	As above	High	This is a vulnerable part of the payment chain and additional attention needs to be given to partners. Enhanced due diligence as well as ongoing review of transactions, and periodic audit. For instance, 'mystery shoppers' can be used to test the integrity of an agents' operations.	Low-medium

	Typology	Indicator	Vulnerability	Mitigation and comments	Risk following mitigation
c.	Partner allows customers to exceed load or withdrawal limits	Systems can instantly flag.	Medium	System should prevent this and record incidents for follow up. Provider can implement measures to deter abuse by agents (e.g., 'Mystery shopper' technique)	Low
4	**ML as a result of cross border functionality**				
a.	POC remitted cross border using multiple users' accounts	Unusual frequency or value of remitted payments to/from same location.	Medium	Collusion may be apparent from agent location data, as well as the size and frequency of transfers. Systems can be calibrated against a baseline of transfer patterns, and geographic information may yield additional data to identify collusion (e.g. unusual values/frequencies of transactions from/to same agent or nearby agents)	Low
b.	POC remitted by single individual	Unusual frequency or value of remitted payments.	Medium	It would be difficult to launder any significant amount of money without departing from the normal pattern for such payments. Systems can be calibrated against a baseline of transfer patterns and flag them.	Low
c.	Funds remitted for terrorist financing	Unusual destination or origin profile. Destination flagged by UN/ FATF/national listings.	Medium	The automatic and instant flagging and freezing tools available make mitigation relatively easy and the channel less attractive than other means to transfer funds.	Low
5	Evolving typologies	Systems can detect abnormal behaviour against a baseline. This could be values, volumes or geographical parameters or type of business or consumer etc.	Medium	Systems that seek anomalous behaviour should be deployed to address ongoing risk of ML. Given the low values transacted, the overall risk will remain low as long as systems seek to identify anomalies.	Low

Annex 6 – Table of Most Relevant AML/CFT Obligations for Mobile Money Providers

FATF Recommendation	Requirement	How to comply & possible challenges	Means of resolution
Due Diligence Measures			
Recommendation 5	(i) Prohibition on anonymous accounts and accounts in obviously fictitious names (ii) Undertaking customer DD when establishing business relationship or qualifying one-off transaction. Similarly, where there is a suspicion of money laundering. (iii) Identify beneficial owner and verify identity (iv) Information on the purpose of the business relationship (v) Ongoing due diligence during the lifetime of the business relationship and scrutiny of transactions	Mobile money accounts are generally registered to the name of the user. Verification of identity is difficult in many countries where most of the population has no identity documentation. These accounts are limited in transaction size and frequency which makes ML/TF through these channels ineffective. However, mobile money providers face a huge burden to implement full CDD measures in environments of such low risk.	It is important to distinguish the level of DD necessary for different categories of users (customers, agents, merchants) as risk will depend on the services each uses. Full due diligence should be standard for agents and merchants. For customers, where the means of verifying identity through a national ID document is available, this can be used to enable registration. Where verification of ID cannot be undertaken in a conventional way, then alternative forms of due diligence is required (e.g. a letter of reference or a utility bill). However, there are cases where simplified or reduced due diligence may be appropriate because of the low risk posed. For instance, low risk might be achieved by applying account limits and careful monitoring of account activity. See R15
Recommendation 6	Enhanced DD for politically exposed persons (PEP)	All merchants, agents and users should be screened against commercial databases of PEPs to identify them.	
		Once flagged, senior management should approve the establishment of the business relationship and perform enhanced and ongoing due diligence on a risk-sensitive basis. The source of funds should be identified and recorded.	

FATF Recommendation	Requirement	How to comply & possible challenges	Means of resolution
Recommendation 8	Risk of anonymity stemming from new payment methods that favour non-face-to-face relationships.	The present review is intended to address such risks in particular.	This methodology is intended to assist in the assessment and mitigation of risk. There are ways to significantly lower risk in non-face-to-face situations. For instance, a robust system of limits and activity monitoring.
Recommendation 9	Reliance on regulated third parties for the performance of some DD obligations. Conditions relating to availability of data and supervision of the third party are set out.	This recommendation does not apply in the case of contractual arrangements in which the agent is obligated to carry out CDD for the financial institution. (See FATF Methodology.) Typically agents are contracted. In cases where a financial institution relies on telco data for the CDD process, the financial institution is to verify the process and be satisfied that it is appropriate and immediately available for inspection. Ultimately, the financial institution holds responsibility for the entire CDD process.	
Special Recommendation VII	Inclusion of originator information in money transfers to mitigate the risk of terrorist financing and other crimes.	This applies for cases of large money transfers between accounts at two different financial institutions. It is not relevant to most domestic mobile money services and markets. Domestic and international payments above a specified threshold (FATF sets this at €$ 1000) must contain the name of the sender plus at least one other piece of personal information (address, date of birth, customer ID number, etc) There are certain further exemptions for domestic payments outlined by the FATF.	Control measures need to be commensurate to the risk. Higher level transactions (i.e. high frequency or amount allowances) can be higher risk so a greater level of CDD should be applied.

FATF Recommendation	Requirement	How to comply & possible challenges	Means of resolution
Customer and Account Records			
Recommendation 10	Record keeping of transaction data for five years and DD information for five years from end of business relationship.	This should be applied in all cases. Telcos generally hold records on their clients but for a shorter length of time (typically one year for call records).	Financial information, including CDD data, should be kept for at least 5 years as is consistent with the FATF standard.
Recommendation 11	Records of unusually complex, large, etc. transactions should be kept for at least 5 years and be easily accessible to help authorities.	Payment service providers should be able to undertake this obligation relatively easily because transactions and records are electronically processed.	
Reporting			
Recommendation 13	Reporting of suspicions of ML or terrorist financing to financial intelligence unit.	All mobile money providers, whether telco or bank, should report suspicious activities to the competent authorities.	
Recommendation 19	Reporting of transactions above a given threshold.	In most countries where mobile money has taken off, this is a non-issue. Typical transaction amounts are very low and account balance and transaction limits are well below the FATF threshold. This issue has only emerged in South Korea where mobile money users are permitted to transact large amounts but under enhanced due diligence.	
Customer Activity Monitoring and Staff Training			
Recommendation 15	Monitoring systems and training to deter and detect ML and vulnerabilities.	Mobile money providers will naturally have sophisticated computer systems to process customer activity. These systems can be tailored to detect transactions that have unusual traits.	

FATF Recommendation	Requirement	How to comply & possible challenges	Means of resolution
Submission to Oversight			
Recommendation 23	Prevention of criminals from positions in the financial institutions.	Mobile money providers are already under the supervision of financial regulators either through their partnerships with a licensed bank or through their own registration/licensing as an e-money or payment system provider.	The licensing process should include a check whether criminals are in crucial positions in management.
Special Recommendation VI	Licensing/registration of value transfer services to prevent TF/ML.	Mobile money providers should be licensed or registered with competent authorities before allowing transactions.	

Sample risk assessment (not representative of any particular country and for illustration purposes only)

Factor		Effect on ML/TF risk
Payment functionality	Person to person money transfer	Ability of individuals to both make and receive payments **increases risk**
	Person to merchant	Limitation of payments made to merchants confines the scope and therefore **lowers risk**
	Limits on the value of payments	**Lowers risk** by setting a ceiling for payments and a threshold that would limit amounts that could be laundered
Service characteristics	Low value payments	**Lower risk**, as low payments in absolute terms make laundering less feasible
	Infrequent use	**Lowers risk**
	Cash loading and withdrawal	**Increases risk** as cash is not traceable
	Single country use	**Lowers risk** as the movement of funds can be more easily followed
	Cross-border use	**Increases risk** as borders act as hurdles in following the flow of funds
	Payments made to family	Where this is the predominant purpose, the use of the funds can be easily discerned and measured. This is therefore associated with **lower risk**
Customer demographics	Low income	**Lowers risk**, as payments will also be low in value or frequency
	Rural	Customers in rural environments are usually known in the community, and are less able to conceal crime. **Lowers risk**
	Urban	**Increases risk**, as urban environments offer better opportunities for criminals to conceal their activities
Financial services infrastructure	Good regulated branch network	**Lowers risk**, as this enables use of trained personnel, familiar with financial services
	Informal, unregulated network	**Increases risk**, as staff with knowledge of financial services and requisite training are absent
Public ID infrastructure	Good penetration of public ID cards	**Lowers risk**, as this can be used to verify the identity of customers
	Lack of public ID infrastructure	**Increases risk**
Regulatory regime	Present and enforced	**Lowers risk**
	Present but inconsistent or disproportionate	**Increases risk**
	Not present	**Increases risk**

The factors considered above are not intended to be comprehensive or to act as a reference to risks that could attach to mobile payments. They illustrate the type of issues that would be considered as part of a risk review, and demonstrate the competing effects that would be encountered. (It is also worth noting that the present list focuses on payment services deployed in developing and lower-income countries.)

Risk factors need to be placed in a meaningful context, where the relative and compensating influences can be understood and the overall risk profile of the service developed. The present methodology proposes to achieve this by using money laundering typologies (that is, known and projected money laundering scenarios) as a reference against which factors can be assessed.