Mobile Money for the Unbanked

FATF project on financial inclusion: FATF Guidance on AML/CFT and Financial Inclusion

GSMA response to the questionnaire for the private sector

January 2011

Responses to FATF questionnaire

Context of this response

In 2009, the GSMA Development Fund initiated the 'Mobile Money for the Unbanked' (MMU) programme to provide mobile money services to previously unbanked people. MMU has the goal of reaching 20 million previously unbanked people with mobile money services by 2012.

This response is based on our experience of working with the industry in the MMU programme. Since the beginning of the programme we have been in a process of ongoing engagement with the mobile industry in the MMU Working Group.

Q 1) Description of products/services including the connection and interplay with the banking sector and the use of third parties

There are many ways banks and mobile operators can work together when offering financial services for the poor. These business models are constantly evolving and differing from region to region. FATF rules should ultimately be applicable and effective in preventing money laundering and terrorist financing independently from the details of the cooperation between banks and mobile operators. This is best achieved with principles such as technological neutrality, risk-based implementation and ensuring a level playing field between different players in the market (same rules for the same risks).

However, the main challenges we currently see with regard to FATF rules and mobile money arise less from the rules themselves, but more so from their application and implementation. Many regulators shy away from a risk-based implementation of existing FATF principles and remain too conservative, because they lack guidance and are concerned about negative effects of a more flexible approach on their evaluation ratings.

When looking at the connection and interplay between the banking sector and non-banks from an industry point of view, it is important to keep in mind that there is not one way of connection and interplay, but many[1] ways for banks and mobile operators to work together.

This continuum of varying commercial arrangements between banks and mobile operators is determined by two regulatory regimes. At one end of the spectrum, the mobile operator is in control of the service from a regulatory perspective because the operator has the license to provide financial services (i.e. the mobile operator has been granted the e-money or payments license). At the other end of the spectrum, the bank is in control because the regulatory responsibilities, (i.e. the deposit-taking license) generally in the absence of regulation that covers e-money and payment services, are with the bank. In addition to these regulatory possibilities, which determine to some extent how the banks and mobile operators work together, commercial negotiations between banks and non-banks, technological change and innovation will continue to influence the cooperation and lead to improved financial inclusion.

Allowing market forces to interact and find new and more efficient ways to serve customers will best ensure innovation benefiting the unbanked. It is therefore important to keep in mind that FATF rules need to be applicable and effective over time and independently of the exact interplay between different players at this moment in time.

FATF rules need to remain applicable and effective in achieving their aims of preventing money laundering and terrorist financing[2]. This can be achieved by ensuring that FATF rules embrace principles such as technological neutrality, risk-based implementation by national regulators and ensuring a level playing field (same rules for the same activities/risks independently of who offers the service).

However, the main challenge we currently see with regard to FATF rules and mobile money are less the rules themselves, but more their application and implementation. Without guidance and uncertain about the impact of a decision to use a more flexible approach on evaluation ratings, many regulators of financial services remain too conservative. As can be seen in Q 5.1 below, there are very few examples of regulation implementing risk-based exemptions from

[1] Generally, the discussion is focusing on the 'mobile-led versus bank-led' argument. However, this view is too simplistic to capture the full range of existing cooperation between banks and mobile operators. To understand cooperation between banks and mobile operators in more detail we suggest reading our analysis of partnerships between banks and MNOs 'Mapping and Effectively Structuring Operator-Bank Relationships to Offer Mobile Money for the Unbanked' by Neil Davidson http://mmublog.org/global/a-new-mmu-article-on-the-relationships-between-banks-and-mobile-operators/

[2] We note that FATF is taking into account new developments: FATF Report: Money Laundering Using New Payment Methods. October 2010

AML/CFT obligations for low money laundering or terrorist financing risks. This is also an indication that the risk-based approach is actually not being implemented enough to promote financial inclusion.

Q 3) Are there sector-specific AML/CFT exemptions for mobile operators?

We prefer risk-based AML/CFT exemptions to sector-specific exemptions, because they are better justified, more transparent and fair. A risk-based approach applicable to all market players equally is also more sustainable in the long-term when technologies evolve.

We are not aware of sector-specific AML/CFT exemptions for mobile operators. In order to create a regulatory framework that encourages competition and that is able to evolve with the development of innovative services, financial regulators should create a level playing field in their respective national markets. Financial services should be regulated in a risk-based manner, independently of who the service provider is (same risks should be regulated with the same regulatory obligations). Equally, exemptions based on low risk services should be also applied on all service providers in an equal manner. For example, every entity providing payments with the same risk-level should have the same CDD obligations. This implies that all providers, be it traditional financial institutions or new entrants, have to apply for and comply with the rules of a payments license when providing payments.

Currently, mobile money services always fall under FATF rules, because they are always offered by a licensed financial institution, be it a mobile operator with an e-money or payment license or be it by a bank with a deposit-taking license. FATF rules therefore always apply.

Q 4.7) What should the customer due diligence (CDD) obligations for undocumented people be like?

Two messages are important in the context of this question:

1) Given a low-risk situation and service, CDD measures for undocumented people should be applied in a risk-based manner with little or no identification, no verification of ID, but instead balanced with limits on transactions, frequency and volume and if necessary with monitoring of suspicious transactions.

2) FATF should provide
   a. positive encouragement for financial regulators to apply a risk-based approach when determining CDD obligations.
   b. clarification of its definitions of low risk with respect to money laundering and terrorist financing.
   c. a process for national authorities which indicates how to conduct a risk-based approach and how to choose appropriate measures for low, medium and high risks.

Assuming undocumented people are poor and are transferring small values, the CDD obligations should follow a tiered approach with simplified or no identification for low risk transactions which are controlled by limits on transaction size, frequency and volume[3]. These limits could be accompanied with the monitoring of transactions[4], which allows the service provider to identify and report suspicious transactions. Monitoring combined with transaction limits also allows the service provider to stop an account with money laundering activity even if the exact name and/or address of the account holder is unknown. Also, compared to cash, the electronic nature of mobile money services has the advantage of traceability.

CDD obligations should increase with the risks associated with larger transaction sizes and volumes.

FATF should provide positive encouragement to national authorities to apply a risk-based approach when determining CDD obligations and should clarify its definition of low risk in respect of money laundering and terrorist financing[5].

[3] These limits are enabled and enforced on the systems level by the mobile operator

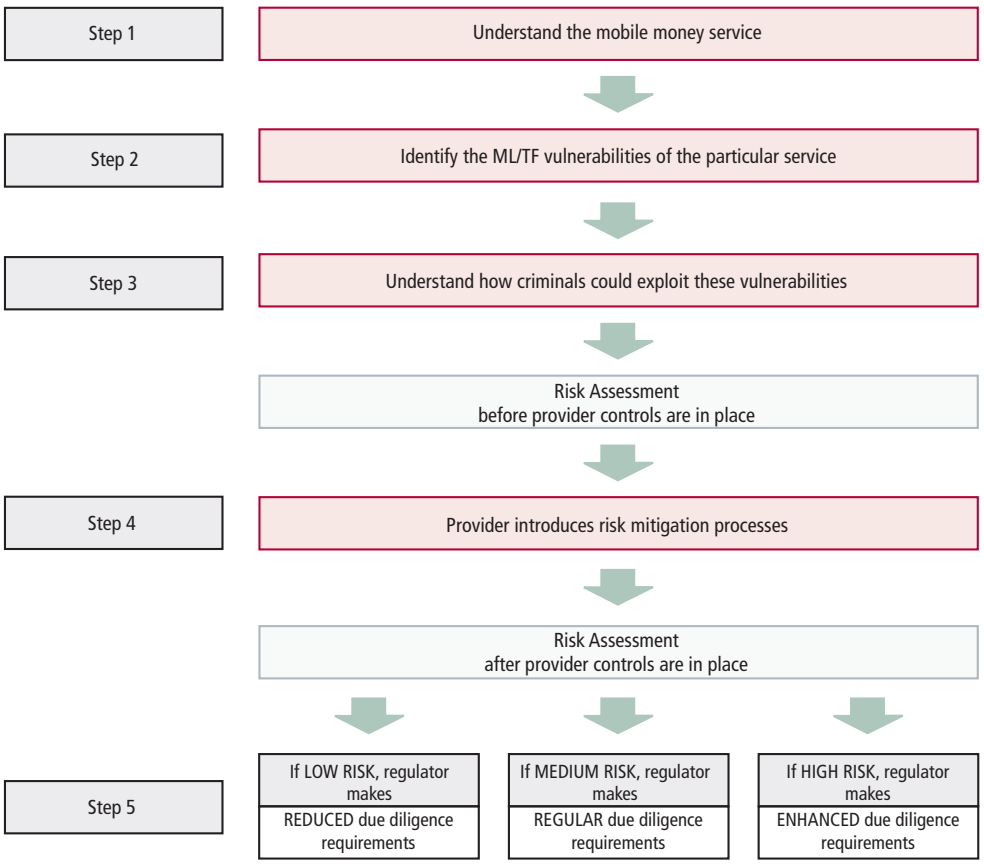
[4] The details of this implementation would depend on the actual risk assessment. For example, there might be no identification necessary in cases of very low risk, in other cases the customer would be identified, but there would be no verification or other CDD measures applied.

[5] Aligning FATF standards and financial inclusion: questions to consider when FATF standards are clarified. Louis de Koker, 20 December 2010.

In addition, FATF should determine a process for national authorities on how to conduct a risk-based approach. This process should include guidance which indicates how to choose appropriate measures for low/medium and high risks. In this context, the GSMA has developed a risk assessment methodology based on existing FATF principles which could lead to a uniform process for assessing risk and choosing the resulting level of customer due diligence. Whilst all FATF principles apply, GSMA's methodology introduces risk mitigation processes developed by the service provider. This allows for additional risk mitigation processes on the business level. Only after these measures are introduced by the service provider (see step 4 in diagram below) the remaining money laundering and terrorist financing risks are then addressed with regulatory compliance obligations (step 5). This approach enables cooperation with the regulator and therefore a better understanding of risks on the side of the regulator as well as proportionate and effective regulation.

Such FATF guidance should be based on principles/guidelines rather than on specific standards, so that the national authority has some scope to take into account national differences and the risks of the offered services.

Example of GSMA Risk Assessment Methodology



Q 5.1) Examples of simplified CDD

South Africa's AML/CFT regime is an example for exemption and risk-based due diligence[6]. Subject to limits and risk indicators, a customer can open their bank account with the mobile. The identification requirements become more onerous as the transaction sizes and risks increase.

Key for reaching the unbanked population is not only overcoming hurdles with regard to identification, but also enabling immediate account opening. The customer should be able to start using the service immediately by transacting small amounts without going to a bank branch to provide a proof of address. Otherwise the hurdle of starting to use the service may not be overcome and customers will not gain access to formal financial services.

There are very few existing examples[7] of exemptions or simplified CDD procedures. In the regulatory work stream of the MMU programme, the industry has been discussing positive examples of regulation promoting mobile money services. One of these positive regulatory examples is South Africa's AML/CFT regulation[8].

South Africa shaped a simplified AML/CFT regime based on the following risk indicators:

- The **type of customer** – the products are only available to natural persons.
- The **type of service provider**[9] – the exemption is restricted to deposit-taking institutions and money remitters.
- **Nationality** of the customer – the customers must be South African citizens or residents.
- **Domestic transactions** – cross-border transfers may not be made, except for point of sale payments or cash withdrawals in the Rand Common Monetary Area.
- **Monetary limits** – there is a daily limit as well as a monthly limit on withdrawals, transfers and payments. If the product is an account, a limit is placed on the balance that may be maintained in the account. The latter limit is reinforced by restricting the customer not more than two such accounts at the same institution.[10]

A South African citizen or resident can register for domestic mobile banking services by opening his/her bank account with a mobile phone. There is no need to go to a bank branch initially if the customer has a valid South African identity number and if the following limits are observed:

- daily transfer limit of approx. US$100 (approx)
- monthly transfer limit of approx US$2,500 (approx)
- maximum balance of US$2,500

This approach is proportionate to risk measured in terms of the value transacted. The identification requirements become more onerous as the transaction sizes increase. The customer has to provide identification when transacting daily up to US$500 with the same monthly limit and maximum balance of US$2,500 respectively. If the customer wants to transact higher amounts, a full identification and proof of address has to be provided in person to a bank representative.

The appropriateness of the actual daily/monthly transfer limits as well as balance limits may depend on the risks of the service and on the customer group. In addition, different transaction limits may be appropriate in different markets. However, the underlying principle of low transaction sizes constitute low risk for money laundering and should be less onerously regulated than higher transaction sizes which constitute higher risk, is what is key for a proportionate regulatory solution – especially if it is to benefit the financially excluded.

[6] There are a few caveats to discussing the South African AML/CFT regime:
a) We don't see strong evidence of services reaching the unbanked in South Africa
b) We ignore the negative impact of the Regulation of Interception of Communication-Related Information Act (RICA) , which was introduced at a later stage and which facilitates interception of information passed over electronic communications channels.

[7] Indonesia, Mexico and BCEAO (as per FATF's overview of October 2010)

[8] http://mmublog.org/africa-south/industrys-favourite-regulatory-solution-south-africas-aml-regulation/

[9] While the GSMA supports a tiered, proportional approach to KYC based on risk indicators and restrictions, we respectfully disagree with the way in which the type of service provider is employed as a restriction in South Africa. We believe that such restrictions should be service-focused rather than provider-focused to prevent unfair and unequal market and regulatory conditions.

[10] The money laundering risk posed by low-risk financial products in South Africa – Findings and guidelines by Louis de Koker School of Law, Deakin University, Geelong, Australia http://www.emeraldinsight.com/journals.htm?articleid=1817094

It is important to understand that key for reaching the unbanked population is not only to overcome hurdles with regard to identification, but also to enable immediate account opening. The customer can start using the service by transacting small amounts without going to a bank branch to provide an address. From a business perspective it takes a lot of marketing spend to actually get people to decide to try these new services. Especially as formal financial services are new to them and they often don't trust traditional financial service providers. Having to go to a point of sale and not being able to immediately try out the account (because it cannot be activated before some papers are authorized) creates a cumbersome customer experience and ruins the investment involved in setting up of the service, as it can lead to low uptake. The customers are more likely to remain in the informal sector, which has no benefits from FATF's perspective.

Q 7) What are the main challenges with regard to keeping records of identification data?

> Overly prescriptive rules can be a burden to some players in the market. Technological neutrality should be a principle of FATF regulations. Some market players prefer paper records of identification data whereas others prefer digital records. As long as the purpose of record keeping is achieved, there should be some choice for the provider with regard to the technology they wish to choose.

FATF standards do not require identification documents to be copied, but some countries understood that as best AML practice. This is for instance the case in relation to South Africa where the Financial Intelligence Centre advised in 2009 that copies of relevant documents must be made.

Some members of our MMU working group find it difficult to make a photocopy of the ID if the service is offered in a remote rural area without electricity, let alone photocopying machines. Others are accustomed to paper copies of identification data; converting to digital copies would result in unnecessary costs. It would therefore be helpful, if FATF rules would encourage the regulator to allow several options as long as the purpose of data retention is adequately achieved. This could easily be ensured by incorporating the principle of 'technological neutrality' in the FATF framework. The 'principle of technological neutrality' has several advantages. It takes away the focus on specific technologies and who the service provider is and moves to focus on the actual goals of the FATF framework. The FATF framework becomes better placed to remain effective with technological developments. For example, it doesn't matter in what form records of IDs are kept as long as they are kept in a way that complies with and achieves the purpose of AML/CTF regulations.

Q 12) Licensing and registration of mobile operators

> Licensing mobile operators or any other non-banks offering financial services creates a level playing field in which the rules are the same for all market players. The respective licenses (e-money, payments, deposit- taking) are awarded based on the risk of the services offered and are therefore the same for all market players. This allows for a truly risk-based approach. Such a risk-based approach increases competition and consumers benefit from a wider choice of services and cheaper prices. A broad range of licensing activities (i.e creating new frameworks for e-money/payments and moving beyond traditional regulation of every financial service as a deposit taking activity) brings non-banks into the realm of financial regulation ensuring that national authorities have greater control and understanding of services and associated risks in their market. This is favourable for preventing money laundering and terrorist financing.
>
> Mobile operators bring huge advantages to the effort to improve financial inclusion: their distribution and marketing capabilities can reach a large part of the population, which is too costly for the banks to serve directly. Mobile financial services are therefore well placed to connect the unbanked population to financial services. Such services bring activity from the informal unregulated sector, into formal regulated financial services – and this enhances the effectiveness of AML/CTF regimes.

The motor of financial inclusion is competition. Competition between service providers offering different business models and technologies leads to innovation and cheaper prices for consumers. With that in mind, we believe financial regulators should choose to offer many models, by licensing banks and non-banks in a risk-based way.

This approach has several advantages. Firstly, this approach creates a level playing field in which the rules are the same for all market players. The respective licenses (e-money, payments, deposit-taking) are awarded based on the risk of the services offered and therefore the same for all market players. This allows for a truly risk-based approach.

Secondly, innovation will accelerate when banks and non-banks have the choice to work together or to compete with each other. Consumers will ultimately benefit from a wider choice of services and cheaper prices.

Thirdly, the national authorities have greater control and understanding of the services and associated risks in their market. Relying on, for example, a traditional bank-based deposit-taking model only, where the bank can be the only recipient of a license from the financial regulator, bears the danger that both the financial regulator and the bank don't fully understand the risks in mobile money services, because they only control parts of the value chain. Such an approach stifles innovation in this area and ultimately leads to the unbanked being financially excluded, as traditional financial services have not met their needs.

Licensing non-banks directly, with progressive and appropriate regulation based on the services they provide (such as e-money, which is recognised by the European Commission as not being a 'deposit' taking activity[11]) provides the financial regulator with more oversight on innovative developments and regulatory frameworks that are better equipped to realise the objective of financial inclusion. This means the financial regulator is also in a much better position to be aware of newly emerging money laundering and terrorist financing risks.

Fourthly, the distribution and marketing capabilities of mobile operators reach a large part of the population, which is too costly for banks to serve directly. Mobile financial services are therefore well placed to connect the unbanked population to financial services.

Q 13) Supervision and oversight of mobile money providers

> To avoid confusion and complications that could arise from the same activity being regulated twice, mobile operators should be regulated only by the financial regulator for any financial services they are offering, just as any other provider of financial services would be. Only the financial regulator has the know-how and the responsibility for regulating financial services.

We observe in the market unnecessary confusion with regard to this question. Mobile operators are licensed for their telecommunications services by the national authority responsible for telecommunications.

However, when offering financial services, the mobile operator should be regulated by the financial regulator for those services, because only the financial regulator has the know-how and the responsibility for regulating financial services.

Whilst the two competencies of the financial and telecommunications regulators should be kept separate, it is preferable to have an open dialogue between these two regulators so that they are each informed of the latest developments.

In markets where telecommunications regulators get involved in regulating financial services, we sometimes observe paralysis in the necessary decision-making processes, because the telecoms regulator doesn't understand financial services and a bureaucratic layer is added, which does not add any value. The same logic would apply if the financial regulator would attempt to regulate telecommunications services.

[11] http://ec.europa.eu/internal_market/payments/emoney/index_en.htm

For further information please contact

mmu@gsm.org

GSMA London Office

T +44 (0) 20 7356 0600