Mobile Money Transfer

Understanding Financial Regulation And How It Works

Table of Contents

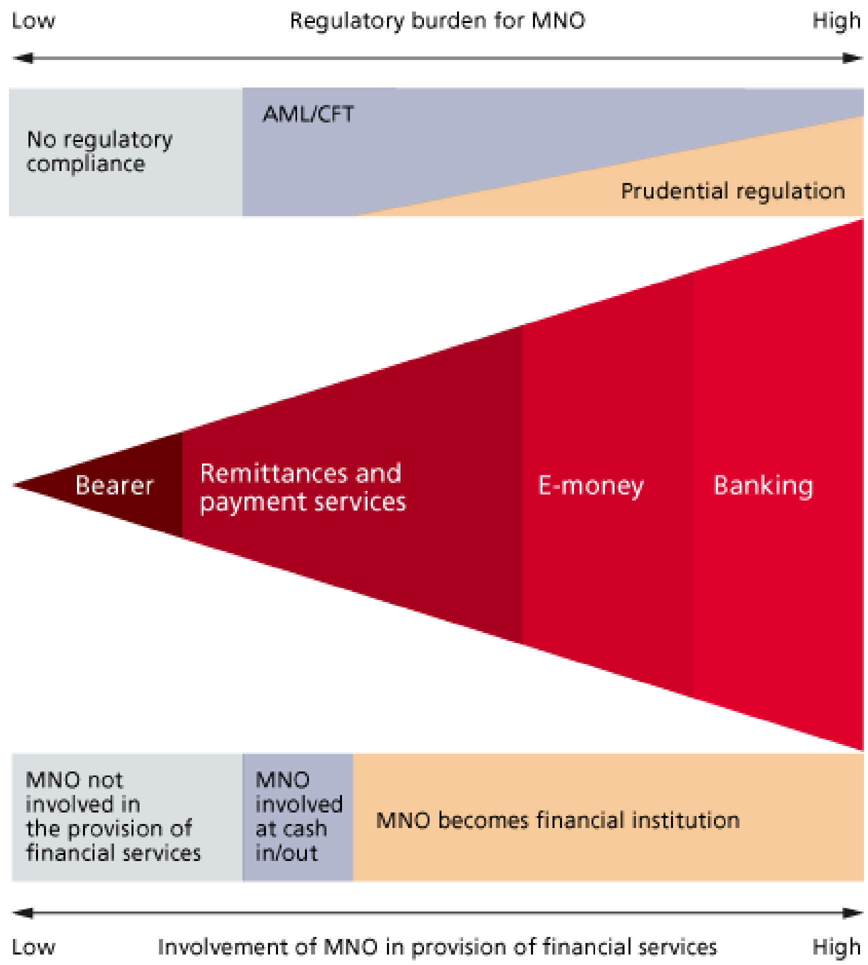
1 An Introduction to the Key Concepts

This document outlines some basic regulatory concepts in financial regulation. The regulatory concepts covered are:

- Anti-Money Laundering (AML) and Combating of Financing of Terrorism (CFT)
- Prudential regulation: deposits, payments and e-money
- Outsourcing and use of agents

Each major regulatory concept is explained in terms of background and purpose, the most important obligations and how mobile operators are likely to be affected.

The document also covers regulatory issues, which may not come from the body of financial regulation, but which may also affect the mobile operator's offering of MMT services. These include amongst others rules around access to the national payment system, data privacy, foreign exchange controls and consumer protection.



As a general rule, the more a mobile operator becomes involved in the provision of financial services, the heavier will be the burden of financial regulation. The first level of financial regulation is AML/CFT compliance, which generally becomes applicable when the mobile operator becomes involved in cash-handling at the consumer interface. The next level of regulation applying to mobile operators is prudential regulation. Prudential regulation becomes applicable when risks increase for the involvement of the mobile operator in the financial transaction, for consumers and for the wider financial system.

2 What is the Outcome?

It is tempting for all parties involved, mobile operators, traditional financial institutions and financial regulators to focus on the status quo of regulation whilst forgetting what we are aiming for.

With the introduction of MMT services, we are aiming for new services, which allow consumers to transfer money securely by using their mobile phone in an easier and cheaper way. We are also aiming for new customers, which include those who will benefit from MMT services particularly, because they are currently un-banked or under-banked.

In order to achieve this, we need to create the mobile experience.

3 Mobile Experience

The success of mobile telephony is based on two characteristics, which make the service attractive to customers: ease of use and mobility. In order to ensure customer adoption of a MMT service, the service has to be easy to use for customers (ease of use) anywhere at any time (mobility). This is the 'mobile experience'.

This poses the challenge that financial regulation, created with traditional financial institutions in mind, now starts to apply to mobile operators. Compliance requirements with this regulation may sometimes make it impossible to design the MMT service as a 'mobile experience'. However, this is a major impact of financial regulation on mobile operators, as described in the document 'Regulatory Impact on Business Model Choice', which can be found at www.gsmworld.com/mmt.

Financial regulation is necessary to ensure stability of the overall financial systems and prudent behaviour of financial institutions to minimise risks for consumers and financial institutions themselves. Financial regulation also aims at preventing money laundering and financing of terrorism. The result of effective financial regulation is healthy competition amongst providers of financial services, efficiency, innovation and lower prices for consumers.

4 Anti-Money Laundering (AML) and Combating of Financing of Terrorism (CFT)

When mobile operators decide to offer MMT services, they are first confronted with AML and CFT regulation. It applies mostly in situations of cash-in and cash-out of MMT services.

The Financial Action Task Force (FATF)[1] as an inter-governmental body, sets standards and develops and promotes policies to combat money laundering and terrorist financing. AML/CFT standards generally require that institutions implement a wide range of 'Know Your Customer' (KYC) procedures, including specific customer due diligence (CDD) procedures when opening a new bank account or when initiating or receiving a single payment for a client.

5 Summary of Most Important Obligations

Main AML obligations:

- Systems and training to prevent money laundering (train employees, establish procedures of internal control and communication which are appropriate to prevent money laundering).
- Identification procedures (provide satisfactory evidence of identity of customers, take into account the greater risk of money laundering when customers are not physically present when identified)[2].
- Record keeping procedures (keep copy of identification data for at least 5 years on record); money service operator has to register with relevant authority (this in turn gives the authority the power to enter and inspect the premises, order access to recorded information and impose penalties).

Financial institutions should undertake CDD measures in following situations:

- When establishing a business relationship.
- When carrying out occasional transactions.
- When there is a suspicion of money laundering and terrorist financing.
- When there is doubt about previously obtained customer identification data.

Throughout a business relationship, financial institutions have to conduct ongoing due diligence on the business relationship and scrutinise transactions undertaken. The financial institutions have to ensure that the transactions being conducted are consistent with the institution’s knowledge of the customer, their business and risk profile, including, where necessary the source of funds.

[1] FATF Mandate http://www.fatf-gafi.org/dataoecd/14/60/36309648.pdf
[2] The emphasis on KYC checks where the customers are not present is aimed at Internet and mobile situations where the provisions suggest increased risks and therefore stricter rules.

The CDD measures to be taken are as follows:

- Identifying the customer and verifying the customer's identity using reliable, independent source documents, data or information.
- Identifying the beneficial owner and taking reasonable measures to verify the identity of the beneficial owner such that the financial institution is satisfied that it knows who the beneficial owner is.
- Obtaining information on the purpose and intended nature of the business relationship.

6 How are Mobile Operators Affected?

Whilst complying with AML/CFT regulation is standard practice for banks, these rules are not something mobile operators are traditionally familiar with.

AML/CFT rules become typically relevant in situations, where mobile operators start to accept/disburse cash intended for MMT services. At both ends of the transaction (cash-in and cash-out) the mobile operator would have to comply with CDD and AML requirements. This is the case independent of the fact that the actual transaction behind the customer interface is undertaken by a financial institution.

Complying with these rules can be difficult for the mobile operator for following reasons:

- In most countries non-financial institutions are not allowed to undertake CDD and KYC checks on behalf of banks because of the country-specific regulatory framework for agencies (link to agency chapter).
- Often the customer has to come to the store in person and the address has to be cross-checked with an official document. This face-to-face registration can have a negative impact on the speed of enrolment and therefore the cost and customer experience. A 'mobile experience' may not be possible.

Complying with AML/CFT is costly. "... the costs of the requirements on industry to have effective procedures and controls are very large, and it is not easy to measure the benefits (beyond 'successful' deterrence) in real terms. For example, the total number of suspicious reports in the UK in 2002 was 64,000. Of that number only 12 were considered sufficiently significant for further action to be taken. The same trend can be observed in other Member States."[3]

Example of good AML regulation: Third EU Anti-Money Laundering Directive[4]

This EU Directive allows for simplified CCD for e-money institutions, where

- if the device cannot be recharged, the maximum amount stored in the device is no more than EUR 150, or where,
- if the device can be recharged, a limit of EUR 2,500 is imposed on the total amount transacted in a calendar year, (except when an amount of EUR 1,000 or more is redeemed in that same calendar) year by the bearer
- any other product or transaction represents a low risk of money laundering or terrorist financing which meets the technical criteria established in accordance with the Directive[5]

Mobile operator check list for regulatory compliance

☑ Establish the national regulatory regime with regard to KYC.

☑ Are the systems and training in place to prevent money laundering?

☑ Are the identification procedures in place?

☑ Are the record keeping procedures in place?

☑ What CDD measures have to be implemented?

[3] http://www.epfsf.org/meetings/2004/briefings/briefing_10mar2004.pdf)

[4] DIRECTIVE 2005/60/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing

[5] as specified according to Article 40(1)(b) of the Directive.

7 Prudential Regulation: Deposits, Payments and E-money

Prudential regulation ensures that regulated entities are financially sound and promotes their prudent behaviour. The key aim of prudential regulation is protecting the interests of consumers and the quality of an institution's systems for identifying, measuring and managing the various risks in its business.

Prudential regulation can apply in various measures depending on the risks.

From a mobile operator perspective following thresholds of prudential rules depending on the risks involved seem useful:

- Payment regulation (low risk – light prudential rules)
- E-money (medium risk – medium heavy prudential rules)
- Deposit taking, i.e. banking (high risk – heavy prudential rules)

However much such a risk-based approach would be desired, it is not the rule, and in many countries banking regulation applies to the majority of financial services offered independently of the risks involved (link to overview in level 1 report).

7.1 Payment Regulation (Low Risk – Light Prudential Rules)

Background and purpose

One of the examples of risk based payment regulation is the EU Payment Services Directive (PSD), which will be adopted by November 2009 across the EU. It was introduced to remedy the lack of competition with regard to payment services in the EU. The EU Commission argued that the current regulatory situation seems to create a lack of competition in many payment services with banks often enjoying a privileged competitive position in payment markets. The objectives of this Directive are to generate more competition, increase market transparency for providers and users, and standardise rights and obligations of providers and users of payment services.

Following activities are authorised under the Directive:

- Money remittance.
- Payment transactions carried out by mobile operators.
- Full range payment services providers (credit transfers, direct debits, card payments).
- Payment related services such as foreign exchange service, safekeeping activities, operation of payment systems for the payment service.

Summary of most important obligations

- A payment service provider has to fulfil qualitative and quantitative requirements, which ensure both financial stability and sound and prudent management of the payment institution.
- The authorisation for operating as a payment service provider requires capital requirements on ongoing and initial capital. These capital charges are based on the lower risk of payment services and are in comparison lower than the capital requirements of banks.
- The Directive sets out the requirements on payment service providers to provide information to consumers in order to ensure transparency.

How are mobile operators affected?

There is little experience about the impact on mobile operators at this stage because the Directive will only be implemented in the EU in November 2009. However, the most important aspect of the Directive to allow non-banks such as mobile operators to offer payment services is positive.

This specific regulatory framework is also only available in the EU, whereas most other countries require a banking licence for the same service. This effectively prevents mobile operators from offering this service without partnering with a bank.

An example of good regulation

The success of the actual implementation of the PSD remains to be seen. However, the regulatory principle to allow non-banks to offer payments services is positive for the mobile industry and consumers. New services and business models – especially for consumers with no or limited access to the current banking system – become possible. This is likely to increase competition in the payment services market to extend the range of services offered.

Mobile operator check list for compliance

- ☑ Establish the national regulatory regime with regard to payments regulation
- ☑ Can a mobile operator become a payment service provider?
- ☑ What are the regulatory requirements for a mobile operator to obtain an authorisation?

7.2 E-money (Medium Risk – Medium Heavy Prudential Rules)

Background and purpose

There are several examples of regulatory regimes allowing non-banks to accept money from a customer and to store it on an electronic device. We call it e-money in this toolkit. The risks with e-money services compared to payment services increase, because the e-money provider holds customers' monies over some time. And if the e-money provider were to go bankrupt, the risk is that the customers' monies would be lost.

This regulatory framework imposes prudential supervision of e-money institutions to the extent necessary for ensuring their sound and prudent operation and their financial integrity. Some of the main principles are summarised below.

Summary of most important obligations

- Structural separation: a mobile operator offering e-money services has to set up a separate company, because electronic money institutions issuing electronic money are restricted to offer only services closely related to the issuance of e-money.
- The Directive requires initial capital and ongoing own fund requirements.
- Limitations on investment: Electronic money institutions have to have investments of an amount of no less than their financial liabilities related to outstanding electronic money in zero credit risk and sufficiently liquid funds.
- Sound and prudent operation for management, administrative and accounting procedures and adequate internal control mechanisms.
- E-money has to be redeemable in cash.
- The E-Money Directive requires compliance with money laundering regulation.

Please note that the EU E-Money Directive is currently being re-negotiated on EU level at the time of writing this report.

How are mobile operators affected?

Activities classified as e-money in the EU are in many countries traditionally regarded as deposit taking. This has the de facto impact that mobile operators as non-banks cannot enter the market and offer e-money services without setting up a bank or partnering with a bank.

The reason for banking regulation applying to e-money services is that traditional banking regulation has not taken into account recent developments with regard to technology and innovations in financial services.

Mobile payment services are much smaller payments than traditional banking services both in terms of size of transactions and volume of payments. Therefore, instead of applying traditional banking regulation, regulators should look at the actual risk of a service offered and regulate the service proportionately to the given risk. Acknowledging the smaller risks attached to mobile payments will lead to the creation of new and proportionate regulation allowing non-banks to offer payment services under proportionate regulation. We need a balanced approach for payment regulation for mobile operators wishing to offer services independently from banks – currently in some countries we have too much payment regulation and in some countries no payment regulation at all.

Mobile operator check list for compliance

☑ Establish the national regulatory regime with regard to e-money regulation

☑ Can a mobile operator become an e-money institution?

☑ What are the regulatory requirements for a mobile operator to obtain an e-money authorisation?

Difference between an e-money institution and a bank

The difference between e-money and deposit-taking is still a grey area, which may become clearer over time as more countries start to introduce the e-money regime and as more experience with e-money institutions and their activities. The following distinction has been drawn on the basis of the principles of the e-money regime in the European Union and also on the basis that e-money and deposit taking entail different activities and therefore different risks from a prudential perspective.

1. Activity

Deposit taking by a bank in general terms can be defined as: accepting funds from the public with a view to deploying them by way of lending or investment. From a customer perspective, this constitutes a savings account.

E-Money is an electronic surrogate for coins and banknotes, which is stored on an electronic device and intended for effecting payments of limited amounts. Unlike the bank deposit, e-money is immediately exchanged for electronic money, which remains with the customer to use at any time. From a customer perspective, this constitutes a purse.

2. Risks

Banks accept money from the public and hold deposits which they use for a variety of risk-taking activities. These risks, i.e. credit risk (i.e. offering credits, which may not be paid back), market risk (i.e. possible losses incurred when trading) and operational risk (i.e. risks for people, processes and systems) can pose systemic risk to the wider financial system.

E-money institutions incur less risk than a bank, because:

- the volume of money flows the e-money institution is dealing with, is very low compared to a bank (difference between purse and savings account).
- e-money institutions can not use customers' monies to finance its payment activities, such as lending the accepted e-money on as credit. The customers' monies are backed by high quality, low yielding, Qualifying Liquid Assets. This means the e-money in circulation with customers is matched by the same amount in a secured and liquid float.

E-money issuers are subject to interest rate risk and foreign exchange risk and may use derivatives to hedge these risks although their freedom to do so can be carefully circumscribed to limit the possible risks. The remaining risk for e-money institutions is operational risk with regard to people, processes and systems. However, this can be regulated proportionately and effectively without having to impose compliance with banking regulation from the e-money provider.

7.3 Deposit Taking, i.e. banking (High Risk – Heavy Prudential Rules)

Banks hold deposits which they use for a variety of risk-taking activities, including providing credit, and can pose a systemic risk to the wider financial system.

Banks are regulated under Basel II with rules ensuring financial stability and that depositors can be repaid on demand. General principles of bank regulation are reserve requirements, capital requirements, restrictions on activity and affiliation and payment system requirements. More information can be found at: http://www.bis.org/bcbs/

8 Outsourcing and Use of Agents

Background and purpose

Regulation on the use of agents determines if entities other than banks are allowed to handle cash at both ends of the remittance transaction, whether on behalf of banks or non-banks (i.e. remittance providers). In cases where regulation permits the outsourcing of the cash handling function, entities which already handle cash, such as retailers, may act as agents for financial institutions.

From a mobile operator perspective agency rules become relevant with regard to two situations:

1) Can the mobile operator become an agent? Becoming an agent allows the mobile operator to use its own distribution chain to accept/disburse cash at both ends of the MMT service.
2) Can a mobile operator operating a payment service or e-money use other retailers as agents for MMT services?

Summary of most important obligations

It varies from country to country whether non-bank agents such as mobile operators are allowed to accept or disburse cash on behalf of a bank or a money remittance provider. In those cases where the mobile operator operates the MMT service the agency rules also become relevant with regard to the scope the mobile operator can use other retailers to become agents of the MMT service.

How are mobile operators affected?

Mobile operators are likely to be affected by the same rules governing the use of agents in situations where they want to handle cash at both ends of the remittance transaction. It is often easier for a mobile operator to become an agent for a remittance provider than for a bank.

An example of good agency regulation

In 2006 in Brazil 95,000 agents [retail outlets, equipped with POS and bar code readers] processed 1.53 billion transactions, valued at US$ 104 billion, 78% of which were bill payments and delivery of government benefits in Brazil. The remainder included deposits, withdrawals, loan repayments/ disbursements. 6 million new accounts were opened in 2006.

In Brazil virtually any entity can be engaged as an agent. The most common types are lottery kiosks, post offices, grocery stores and other merchants. Banco Central do Brasil has issued comprehensive regulations governing other aspects of the business (particularly to protect consumers), but the lack of prohibitions on who can be agent seems to have opened up the field for innovation and allowed rapid growth. http://cgap.org/portal/site/Technology/research/technology/agents/

Mobile operator check list for compliance

☑ Establish the rules of the national regulatory regime with regard to outsourcing of cash-in/out activities on behalf of banks and remittance agents.

☑ Can the mobile operator become an agent of a bank?

☑ Can the mobile operator become the agent of a remittance provider?

☑ Can the mobile operator use other retailers as agents for the MMT service (cash in/out and registration)?

9 Other Aspects to Bear in Mind

Payment system

Rules about the payment system/s in a country govern who has access to the systems, whether they are required to interoperate as well as covering operational aspects like the basis of settlement and clearing. The laws covering the payment system affect whether and how a mobile operator may access existing payment systems, or set up its own payment service. This has an effect on the business model.

If a mobile operator is deemed to conduct a payment business when offering MMT services, these laws will apply to them; in addition, they will affect the mode through whom the mobile operator may seek to access existing payment systems. As an example, MTN South Africa had to partner with a bank in order to get access to the South African payment systems.

Data Privacy

Data privacy laws are relevant because they can potentially restrict the ability of financial providers and mobile operators to transfer, release or make use of client data other than for purposes initially agreed by the client. This issue could occur when both the financial institution and the mobile operator expand their initial scope of service provision when offering MMT services.

Foreign exchange regime

Foreign exchange controls impose transaction limits on the amount that can be sent / received by a customer in the relevant country.

Foreign exchange controls are relevant for mobile operators when they offer remittance services, because they have to comply with the imposed transaction limits and reporting and authorisation requirements. In the context of foreign exchange controls, receiving remittances is often less restricted than sending remittances. For example, in South Africa, when sending remittances, there is a yearly limit for South African residents not to exceed 22,700 US$ per calendar year. In Pakistan, outward remittances, generally require permission of the State Bank of Pakistan.

Controls which impose onerous requirements on sending or receiving foreign remittances may make the MMT service unviable to mobile operators or customers (whether they can do it at all will affect all remittance providers equally).

Consumer protection

Electronic means of payment may bring new risks to consumers, arising for example from loss of payment instrument i.e. the mobile phone, fraudulent transactions, identity theft, loss of funds through bankruptcy or fraud by the MMT provider etc. Financial regulators looking at MMT services will be interested in understanding how consumers can be protected. Whilst mobile operators will also be interested to keep consumers satisfied with the MMT service.

So far little systematic work has been undertaken to identify the exact regulatory requirements in this area. The reason for this is that MMT services are still in their infancy and hence any failures with regard to consumer protection are still largely not experienced in the market.

The starting point of the analysis should include following considerations:

- Depending on the country, there are potentially three bodies of consumer protection in place: general consumer protection, telecom-specific consumer protection and consumer protection emerging from financial service regulation.
- Given the largely uncoordinated consumer protection regulation in those three areas, which are starting to converge, it needs to be assessed where there is unnecessary duplication of regulation, which may also bring contradictory compliance requirements for mobile operators. However, this analysis will also show areas, where the consumers may not be adequately protected.

Once it is clear, where regulation needs to be simplified and where the actual risks for consumers are, following principles should be included in the final regulatory decisions:

- Proportionality: any consumer protection measures should be proportionate to risks.
- Mobile experience: any consumer protection measures should consider that the MMT service has to remain a ‘mobile experience’.
- Consultative approach: any new consumer protection regulation should be designed by consulting the industry and looking for new ways to reduce both risks for consumers as well as regulation. This will also allow the creation of regulation, which addresses real problems as they emerge.

The mobile industry has a vested interest in ensuring that consumers like using MMT services, that they perceive these services as safe, reliable and easy to use. Any problems, where consumers experience the service negatively will have a negative impact on the success of these services.

Consumer protection – next steps:

☑ Comprise all consumer protection measures, which apply already (general consumer protection, telecoms-specific consumer protection, financial services consumer protection).

☑ Establish duplication, contradiction and gaps.

☑ Adapt consumer protection rules where necessary, whilst allowing for adapting them proportionately to the risks given and also allowing for a ‘mobile experience’ of the MMT service.

☑ Develop the future regulatory rules for consumer protection in a consultative approach with the mobile industry to ensure timeliness, feasibility and appropriateness of the future rules.

E-Commerce

Electronic forms of payments require new regulatory frameworks such as e-commerce regulation. These regulatory frameworks are often not yet developed in those countries which would benefit the most from receiving remittances.

Telco/mobile operator regulation

Any new payment regulation applying to mobile operators when offering payment/remittance services is added to the already existing regulatory framework of telecommunications regulation. This bears the danger of over-regulation and inappropriate/disproportionate rules in overlapping regulatory areas, i.e. customer identification, restrictions to offer non-telecommunications services, etc.

Competition

Several competition issues can arise when introducing MMT services in the market. Mobile operators offering MMT services can be affected by difficulties to access bank clearing systems, pre-existing market power of banks, and by lack of interoperability enabling inter-network transfers[6] of competing mobile operators.

Financial access

MMT services are closely related to issues of providing access to financial services to the poor. The GSMA's strategic partnership (link to toolkit chapter on strategic partners) is aimed at benefiting the poor in the receiving countries by allowing funds remitted over MMT to reach new and so far unbanked segments of the population.

Taxation of financial transactions

Mobile services and financial services can be taxed differently. In some countries VAT does not apply to financial services such as person–to–person transfers, whereas it can apply to telecommunications services. If these rules are not coordinated, they can make a service offering by the mobile operator unviable if there is no level playing field between mobile operators and financial institutions.

---

[6] Competition issues in the development of m-transactions systems, George Houpis, James Bellis, Frontier Economics, The Transformational Potential of M-Transactions, Moving the debate forward, The Policy Paper Series, Number 6, July 2007