Alliance for Financial Inclusion
Bringing smart policies to life

Mobile Financial Services Working Group (MFSWG)

Mobile Financial Services
Consumer Protection in Mobile Financial Services

This guideline note was developed by AFI's Mobile Financial Services Working Group's (MFSWG) Consumer Protection Subgroup to identify the primary consumer protection issues in mobile financial services and discuss options for regulators to address them.

Guideline Note No.13
March 2014

Contents

Recognizing the potential of mobile financial services (MFS), the Mobile Financial Services Working Group (MFSWG) was created to provide a platform within the AFI network for policymaker discussion on regulatory issues related to MFS. The working group promotes the broad use of MFS as a key solution for greater financial inclusion in emerging and developing countries. The group aims to stimulate discussion and learning among policymakers and promote greater coordination between the many different MFS actors, such as financial and telecommunications regulators and bank and non-bank providers.

Context

As mobile financial services (MFS) have evolved in different parts of the world, they have shown great potential to advance financial inclusion. However, consumer demand and adoption of new MFS are driven largely by public attitudes and knowledge about technology and mobile services in general. The image of mobile financial service providers (MFSPs), levels of consumer trust and the value proposition of the services on offer also influence the uptake of products and services. Having effective consumer protection guidelines for MFS in place can help to build consumer trust and confidence, which in turn can improve uptake and usage.

There has been increased attention in recent years to consumer protection in financial services, which has helped to highlight the benefits of empowering consumers to make informed financial decisions, exercise their rights and meet their obligations, and have access to adequate, timely and efficient redress for their complaints. Consumer protection regulations tend to pursue the following broad objectives: i) to ensure that consumers have enough information to make informed financial decisions; ii) to prevent unfair practices by service providers; and iii) to ensure that consumers have access to recourse mechanisms to resolve disputes.[1]

All these objectives should be balanced in a way that does not place onerous restrictions on the provision of the financial products and services and the channels used to deliver them. This is particularly important when the target population is from a low income and/or disadvantaged group, usually a more vulnerable segment of the population, since they may just be starting to use formal financial services and have limited ability or power to protect themselves from unfair practices. However, regulators face a dilemma: protecting consumers without imposing high compliance costs on service providers. High costs can affect the ability of MFSPs to make mobile banking and payment services accessible to this target population and negatively impact their business model.

The first step in achieving this balance is clearly identifying the risks and constraints consumers face when they register with an MFSP, as well as the challenges that may arise when they use MFS, such as those related to language, culture and general knowledge and attitudes about technology and mobile services. Next, regulators should be aware of and understand all the factors that influence the conduct of MFSPs and to manage the risks and inherent costs involved.[2]

To assist regulators in understanding these factors, as well as the risks and the costs associated with the provision of MFS, this guideline note is structured around the various business processes of MFSPs. The central focus of this note is identifying the vulnerabilities, risks and constraints facing MFS consumers.

Purpose and Critical Issues

The purpose of this guideline note is to identify primary consumer protection issues in mobile financial services and the ways in which regulators can address them. One of the main issues is whether the provision of financial services through mobile phones changes the risks consumers face with traditional channels.

Around the world, MFS is showing great potential to dramatically reduce the cost of delivering financial services to consumers and to promote greater financial inclusion, by reaching both new segments of the population and more geographical areas. With lower delivery costs, providers are able to provide services to unbanked customers, which may be unprofitable on their own but together constitute a profitable consumer group.

Providers of payment and transfer services through mobile phones generally depend on customer and transaction volumes to be sustainable. With a broad target market that includes the unbanked, who may be using financial services for the first time, risks come from both the demand and supply side. First, a large proportion of target customers may not be literate in the predominant language of mobile financial services and may also be technologically challenged, both of which can limit the ability of MFSPs to market their products and services. Lack of consumer trust and limited knowledge of new technologies, especially those that transfer money,

[1] This includes looking at institutional arrangements for consumer protection, disclosure and sales practices, customer account handling and maintenance, privacy and data protection, dispute resolution mechanisms, guarantee schemes and insolvency, and consumer empowerment and financial literacy. For more information, see The World Bank, June 2012, "Good Practices for Financial Consumer Protection." Available at http://responsiblefinance.worldbank.org/publications/financial-consumer-protection.

[2] While MFSPs must often comply with regulations, there are options that the regulator can consider that may induce MFSPs to act in a certain way, which can range from self-regulation/recommendations (with regulatory oversight in some fashion) to incentives to mandates.

may make low-income clients reluctant to use MFS and potentially increase the risks associated with first-time users.

Second, the use of MFS and agent banking introduces new operational and technical risks, such as new forms of fraud and inappropriate product design and system failures.[3] When technological or operational issues occur and are not handled properly, they can quickly erode consumer confidence in both the service and the provider.

Whereas the first concern relates primarily to demand and the second to supply, both are closely related. For example, low-income households may use basic equipment with low security functionalities, which can increase the opportunity for fraud unless the provider introduces some controls to minimize this risk. Therefore, a good consumer protection policy must include the requirement that the MFSP understands its target market, including literacy and numeracy rates, the types of access channels used, potential risks of fraud, and ways to minimize these risks so that products and operating procedures can be properly tailored to the needs of the target market. At the same time, this policy must ensure that appropriate measures are in place to address various potential risks.[4]

The assumption of this guideline note is that the provision of MFS is regulated and supervised, or there is at least an authority to enforce the general regulatory framework for consumer protection, which may include some rules specific to MFS. This guideline note provides a minimum set of requirements to address the consumer protection concerns arising from the risks of MFS.

Vulnerabilities and Risks for MFS Consumers: Policy Implications

The purpose of this section is to identify potential vulnerabilities and risks facing consumers when they access financial services through mobile phones and agents. Using a structured approach, it begins by identifying the vulnerabilities consumers can be exposed to when using MFS, and then explains the threat of these vulnerabilities and risks to consumers if they are exploited.[5] This process is depicted in Table 1, from the customer acquisition stage to the transaction/usage stage. Finally, other vulnerabilities are identified that can occur at any time, but particularly as more complex, value-added services are offered over time.

Although some of the risks identified here may not be exclusive to MFS, they are included to provide a complete picture of consumer risks. Nor is this an exhaustive list, since risks change depending on the life cycle of a service and technology, as well as the literacy levels of MFS consumers. As Bezuidenhoudt and Porteous (2008) explain, risk identification is the result of measuring the impact and the likelihood of something happening. However, this always depends on the nature of the environment, the types of technology used and consumer demand, among other factors unique to each market.

The Importance of Adequate and Complete Information

During the customer acquisition stage, inadequate and inaccurate information about a new service and the MFSP is a major source of vulnerability. Discrepancies between what consumers understand to be offered and what is actually being offered may foster inaccurate assumptions. Also, lack of trust in new technologies and new MFSPs in the market may result in extremely low service uptake.

Without adequate and complete information about new services, clients risk making errors in both the registration and transaction stages. MFSPs should ensure that all clients are given appropriate and accurate information about the terms and conditions of the service, the list of transactions that can be performed, fees and rates for all types of transaction, transaction limits (if any), available delivery channel options, as well as access to 24/7 customer service operators to ask questions.[6] All information provided to consumers should use clear and understandable terms in the language consumers conduct their everyday business, not just the official national language. In countries with indigenous or

---

[3] In rural areas, limited or ineffective mobile coverage is another source of vulnerability. In other cases, clients not protecting personal identification numbers (PINs) or handing mobile phones with a PIN to an agent to transact can potentially increase risks.

[4] For more information, see the MicroSave article, "Fraud in Mobile Financial Services", which outlines additional risks, some of which can result in customer loss of funds or other harm, and ways to manage them: http://www.microsave.net/files/pdf/RP151_Fraud_in_Mobile_Financial_Services_JMudiri.pdf

[5] This structured approach was used by Bezuidenhoudt and Porteous (2008) to conduct an in-depth analysis of the risks of different MFS technologies and propose possible ways of managing them.

[6] See also http://www.afi-global.org//library/publications/consumer-empowerment-and-market-conduct-transparency-and-disclosure.

other minority groups that speak different dialects or languages, information should also be provided in these languages, along with access to 24/7 customer support and information about options for recourse.[7]

In Bangladesh Bank's 'Guidelines on Agent Banking for Banks,' banks using agents are required to ensure that adequate measures for consumer protection, awareness and dispute resolution are in place. Banks are required to run a call center to receive and process disputes 24 hours a day via telephone, SMS, IVR and mail. Every dispute received by the center must be resolved within three working days. The bank's management should ensure proper controls are in place to log and keep track of all disputes, review the status of each dispute and redress it within the stipulated time. Banks should widely publicize dispute/grievance redress mechanisms through electronic and print media. The banks are required to submit reports regarding disputes/grievances and redress to Bangladesh Bank at regular intervals.

View the guideline at http://www.bangladesh-bank.org/aboutus/regulationguideline/draft/agent_banking_2013.pdf

New Technology as a Source of Risk

Although the use of mobile phones is widespread, even among low-income households, they are typically used only as a communication device. In many countries, using mobile phones to perform financial transactions is still quite new, and this lack of awareness and experience with new technology can create particular risks for this segment of the population.

The low security functionality of basic mobile phones do not assure end-to-end encryption, which means traffic can be intercepted between the mobile transaction and the point of service, potentially resulting in identity theft and fraudulent transactions. In addition, a customer's lack of technological literacy may produce erroneous transactions (i.e. sending money to the wrong account or paying the wrong bill), failure to complete a transaction, weak PIN choices and carelessness in safeguarding personal information. It is common in low-income households to share mobile phones, which can introduce another level of vulnerability when it is used for financial transactions.

These risks leave MFS users, especially those from low-income households, vulnerable to losing funds either directly or through increased probability of identity theft or theft of authentication parameters. The source of risk can come from the client (demand) side or the operator (supply) side.[8] In both cases, exposure to these risks can have a negative impact on consumer trust in the system, making it difficult for the MFSP to reach the scale it needs to become viable.

Responsibility therefore lies with the regulator to ensure that certain minimum requirements and standards are met and that all MFSPs provide appropriate consumer education and information. Government agencies may also want to play a more proactive role in financial education programs geared toward the base of the economic pyramid to help improve the understanding, opportunities and risks associated with the financial system and its products and services. Finally, MFSPs should be required to mitigate the increased risk that comes with low literacy rates (both language and technological) by adopting certain minimum standards in product design controls (Bezuidenhoudt and Porteous, 2008).[9]

Risks Associated with Agents Providing MFS

The fact that agents are typically used in the provision of MFS, and are often the first point of contact with consumers, is another source of risk. All MFSPs should ensure that appropriate standards are in place to select, manage and train their agents. Contract templates for agents, as well as outsourced agent networks, should be reviewed to ensure that standards are in place, including the following requirements:

(a) MFSPs are responsible for the actions of their authorized agents in the provision of MFS and must provide adequate oversight, observe a minimum set of requirements (established by regulators) to select an agent, provide

[7] See also http://www.afi-global.org//library/publications/consumer-empowerment-and-market-conduct-help-and-redress-financial-consumers

[8] Operator side issues might relate to complicated interfaces which they can address by ensuring that systems are more secure, intuitive, and less susceptible to errors and fraud.

[9] See also "Mobile Financial Services: Technology Risks," http://www.afi-global.org/library/publications/mobile-financial-services-technology-risks-2013

appropriate training to agents and ensure that their authorized agents act in the best interest of consumers.

(b) MFSPs should ensure that agents can be clearly identified by consumers by using appropriate signage and have clear and established customer hotline numbers in place.

(c) MFSPs should ensure their agents maintain consumer confidentiality by having effective data and privacy control standards/mechanisms.

(d) MFSPs should ensure that consumers are provided with accurate and full disclosure of all product services, features and rates at all agent locations.[10]

The size and distribution of the provider's agent network is another factor affecting the quality and convenience of the service. All MFSPs should have sufficient standards in place to ensure liquidity for all agents. This plan should be established prior to initiating services and should be reviewed from time to time to ensure that adequate liquidity levels are in place.

Challenges with New Services and Service Providers

The perception of new MFSPs may generate particular concerns for consumers. New MFSPs providing financial services for the first time, especially in partnership with third party agent networks, may confront more challenges in managing the risk of fraud effectively.[11] These risks may come from product design, processes, weak monitoring/compliance practices, agent-related fraud, or fraud by the MFSP and/or their employees. To prevent this, regulators should ensure that MFSPs are licensed and supervised and operate under an enforceable regulatory framework. This will ensure at minimum that:

- MFSPs follow a licensing procedure that fulfills minimum requirements to ensure minimum capital requirements are met and to ensure that management have sufficient technical skills to manage MFS operations as well as regulatory compliance issues;
- MFSPs have effective internal controls to mitigate fraud or any misuse or misappropriation of consumer funds;
- Consumer funds are segregated, invested in safe liquid assets, are identified as the assets of individual e-money account holders, and are protected in the case of insolvency of the MFSP or issues related to the financial institution managing the funds; [12]
- MFSPs put mechanisms in place to control operational risks, which should consider appropriate security control steps for using mobile phones to access financial services, secure error resolution mechanisms for the access and transmission of funds, software and hardware security measures, appropriate measures to authenticate the identity and authorization of customers of the service, effective business continuity arrangements and contingency planning to ensure service availability, adequate safety measures for data protection, fraud and procedures for preventing service interruption.

It should also be noted that in some countries, electronic money systems have been carefully introduced through controlled and supervised pilot projects that gather information and test and correct mistakes and limitations before allowing services to scale up.

The Bangko Sentral ng Pilipinas (BSP) has collaborated openly with e-money issuers, including addressing how to handle consumer protection issues. Through controlled pilots using a "test and learn" approach, the BSP helped to ensure that major risks were identified early on. This allowed pilots to operate under a letter of "no objection" for a specified period of time and with a limited number of clients in order to properly test various risks prior to finalizing regulations and allowing e-money services to be fully rolled out.

[10] See the Consumer Empowerment and Market Conduct Working Group's (CEMC WG) Guideline Note 7 on Sales and Marketing Practices: http://www.afi-global.org//library/publications/consumer-empowerment-and-market-conduct-sales-and-marketing-practices

[11] It should be noted that some new MFSPs might have better systems for detecting certain fraud risks (such as those led by MNOs), and banks might be better in other areas, but both may have weaknesses related to MFS that need attention.

[12] E-money funds held for clients, especially in non-bank MFSPs, should be held in trust rather than as a deposit in a financial institution to protect against the risk of insolvency of the MFSP and the bank or other financial institution managing the funds. See Trust Law Protection for E-Money Customers http://www.afi-global.org/library/publications/trust-law-protections-e-money-customers

Consumer Privacy Concerns with MFS

During the registration and transaction stages, MFSPs and their agents collect and store personal customer information. Regulators should ensure that MFSPs have internal control mechanisms and appropriate standards in place to carry out proper consumer protection practices. These standards should include:

- Clearly disclose to customers that their information belongs to them and that the MFSPs and their agents will uphold the privacy and confidentiality of all customers' information, data and transactions;
- State the conditions/circumstances under which such data may be shared (with the explicit consent of the customer);
- State or disclose to the customer the process for correcting or deleting inaccurate or unsolicited information;
- Establish a mechanism for a data retention period;
- Set up appropriate hotlines at the MFSP to address consumer questions and complaints; and
- Establish an external consumer complaint service either within the regulator or within an appropriate government agency.

Outsourcing and Third Party Service Providers

The provision of MFS usually involves one or more third party service provider(s), often the financial institution, agents/agent network operators and telecommunications companies. When an MFS customer encounters a problem, it may not always be clear which partner is ultimately responsible for addressing it. At minimum, the regulators should ensure that:

- The principal MFSP clearly assumes full responsibilities in handling consumer complaints and is able to have a complaint resolution system in place that records and tracks the nature and resolution of the complaints;
- If a problem is not resolved in the first instance, there is a clear, defined process for escalating complaints; and
- For issues relating to the mobile channel and external complaint resolution, there is close coordination between the financial and the telecom regulator, ensuring there are clear protocols to resolve and address complaints.[13]

The Central Bank of Nigeria (CBN) guidelines for MFS require that mobile payment operators must maintain a functional dispute and complaints resolution desk, which should be equipped to receive complaints through phone calls, e-mails and personal visits/ contact with the customer. The complaints desk is required to be well advertised through various media and conspicuously displayed at agent locations. All mobile payments scheme operators should ensure that complaints are acknowledged with a case identifier issued to the complainant within 24 hours and resolved within three working days of registering a complaint. Complaints must be logged and phone conversations with the dispute/complaint resolution desk should be recorded and maintained until the dispute is resolved.

Consumers are allowed to contact the CBN to intervene if they are not satisfied with the bank's response to their complaints, and the CBN's Consumer Protection Department will mediate to resolve the complaint

See: http://www.cenbank.org/OUT/CIRCULARS/BOD/2009/REGULATORY%20FRAMEWORK%20%20FOR%20MOBILE%20PAYMENTS%20SERVICES%20IN%20NIGERIA.PDF

[13] Ideally, consumers should approach one external regulator/agency as a last resort to address complaints that are not handled properly by MFSPs.

Table 1: Vulnerabilities and Risks Facing MFS Consumers at Each Stage

Marketing stage: Consumer is informed about service availability

Vulnerability: Lack of consumer knowledge or understanding of the new service and MFSP. Lack of awareness or misperception about the nature/gravity of different risks of using the service (including the comparison to current informal options).

Threats:
- Gap between a customer's expectations and the services actually offered
- Uncertainty about which party is ultimately the responsible MFSP[14]

Risks:
- Potential for fraud
- Errors in making decisions
- Lack of trust, failure to adopt service

Regulatory implications:
Create a requirement that MFSPs provide clear, adequate, accurate and complete information to consumers about the responsible MFSP and "key facts" related to registration, transactions and product/service features

Registration stage: Client receives information about the service, fills out a registration form and selects a PIN

Vulnerability	Threats	Risks	Regulatory Implications
• Insufficient agent training • Lack of client knowledge and awareness of risk • Inadequate data security platforms and processes	• Poor services • Lack of adequate information from agent • Weak security of selected PIN or storage of personal information in the mobile phone • Inadequate handling of customer data at agent's premises (including both privacy and data security concerns)	• Reputational risk • Operational risk: identity theft or theft of authentication parameters, which can lead to a loss of funds	• Disclosure of information and operator support • Accessible, complete, clear, plain and understandable language[15] • Client education and awareness programs • Consumer complaints and redress mechanism

Transaction stage: Customer performs cash-in/out transactions, payments and transfers

Vulnerability	Threats	Risks	Regulatory Implications
• Low-income/ indigenous population with limited access to information or low levels of literacy/ numeracy (e.g. Terms and Conditions) • Shared mobile phone usage within the family or community • Transactions facilitated by agents or others • Customer interface is overly complex and not intuitive	• Inaccurate/uninformed decisions • Potential for fraud	• Erroneous transactions • Vulnerability to fraud • Loss of trust	• Disclosure of information • Accessible information • Consumer education • Improvements in business processes that reduce the risks (e.g. contact/address book appears to facilitate transaction or the receiver's name appears before the person confirms the transaction, to reduce transactions sent to an unintended third party)

[14] This is especially important when agents, telecom operators, or other third party providers are engaged to support the services provided by the principal MFSP.

[15] Including information and operator support for all major dialects and other main languages spoken in the country

Table 1: Vulnerabilities and Risks Facing MFS Consumers at Each Stage *(continued)*

Transaction stage: Customer performs cash-in/out transactions, payments and transfers			
Vulnerability	**Threats**	**Risks**	**Regulatory Implications**
Provision of MFS relies on:			
i. Client equipment with low security functionality and lack of end-to-end encryption ii. Client skill in following procedures and security measures	• Interception of traffic between mobile phone and point of service • Inaccurate transactions	• Identity theft, wrongful access, used to conduct transactions • Erroneous transactions • Loss of client funds	• Minimum security requirements for mobile phones • Product design and business process improvements • Appropriate risk management policies • Customer service support • Consumer complaints and redress mechanisms • Educational campaigns
iii. Communication network	• Failures in the system, inability to complete transactions	• Reputational risk • Incomplete or delayed transactions • Possible loss of funds	• Minimum standards • Required alpha/beta system tests • Redundancy and contingency plans • Ensuring real-time transaction services are in place and must be used
iv. Agent network	• Fake agents • Agent misconduct and poor service • Lack of agent liquidity	• Potential for fraud • Perception that the service is unreliable	• MFSP liable for agent services and conduct • Agent training and oversight (to improve compliance with SOPs, reduce opportunities for and improve sanctions against agent misconduct and abuse) • Minimum requirements, proper signage, training and support for agent networks • Liquidity management/ support • Disclosure of transaction limits • 24/7 operator support • Consumer complaints and redress mechanism

Table 1: Vulnerabilities and Risks Facing MFS Consumers at Each Stage *(continued)*

Acquisition, transaction or more complex value-added stages			
Vulnerability	**Threats**	**Risks**	**Regulatory Implications**
• Diverse MFSPs • New financial service providers as MFSPs	• Misuse of funds • MFSP insolvency • Inadequate management of fraud risks	• Fraud • Loss of client's stored value funds • MFSP bankruptcy	• All MFSPs under supervision • Protection of funds and investment policies (i.e. trust agreements) • Both internal and external consumer complaint and redress mechanisms
• Personal and transaction information known to MFSP or agents	• Client privacy Issues	• Reputational risk • Fraud and/or identity theft	• Data privacy and client secrecy regulations • Internal and external consumer complaint and redress mechanisms
• Outsourcing part or all MFS to third parties	• Customers unclear about which party is responsible and where, how and whom to address complaints • Complaint is not handled adequately	• Reputational risk	• Clear customer communication re: who the MFSP is and who is responsible for each of the services provided • 24/7 customer support • Internal and external consumer complaint and redress mechanisms (and standards to ensure they are adequate and consistent) and reporting requirements to allow the supervisor to monitor potential trouble spots or poorly performing MSFPs in the market

Responsibilities of the MFSP

The responsibilities of the MFSP should be clearly stated in the regulations and at minimum should require that the MFSP:

- Demonstrate that they understand the target market and have conducted appropriate market research analysis (on capabilities, processes and security levels) to design products that satisfy the needs of the market, reduce potential threats and mitigate the risks they might face;
- Have appropriate processes in place to educate consumers about their rights, duties and responsibilities in the use of MFS, including consumer education and risk awareness programs that inform them of the consequences of not being prudent and responsible when accessing the service (providing clear examples of acts of negligence or misconduct);
- Comply with the regulation that aims to ensure services are provided in a safe, reliable and transparent way;
- Ensure adequate management of operational risks by having appropriate operational manuals, internal control procedures and contingency plans in place that can be reviewed by regulators;
- Ensure they have appropriate contracting manuals and an operational manual that explains how to carefully screen, train and monitor agents and/or outsourced agent network operators; and
- Have a fair and effective internal complaints/ redress system.

It is important to point out that while complaints and various questions about MFS may arise, particularly those targeted at low-income, indigenous, disadvantaged or unbanked populations, the basic approach of the MFSP should be to build consumer trust by developing clear and simple mechanisms to address complaints and ensure appropriate compliance and follow-up.[16]

In general, responsibility for appropriate customer protection lies with MFSPs as well as with consumers. Providers that have taken appropriate actions to educate consumers should not be liable in cases of clear customer negligence. Customers must be advised of their shared responsibility when using MFS.

Responsibilities of the Financial Regulator

Regulators must also be aware of and keep pace with developments in information and communication technology in general, and in the mobile financial services industry in particular. Financial regulators must actively pursue programs that continually build the competencies of its personnel or improve the organization's internal capacity to better understand and properly regulate the industry.

Regulators play a critical role in consumer protection by defining policy and appropriate regulations for the MFS industry. They must ensure they are properly equipped to support improved client protection practices by providing appropriate regulations and ensuring these policies are properly enforced. Regulators must also strike an appropriate balance between protecting consumers and creating an enabling environment for MFS to be viable. They must also ensure they are not "over regulating," as this may prevent vulnerable and underserved consumers from accessing services from well-regulated providers.

Only properly regulated MFSPs should be allowed to offer MFS and be appropriately supervised under rules and policies designed to ensure the sound and safe provision of MFS. MFSPs should operate under license of one regulator, although some of the services they offer may fall under the responsibility of more than one regulator.[17]

When designing the regulatory framework, regulators should take into account that MFS provide multiple benefits to consumers, including greater access, convenience, reduced costs and security. However, due to their technical nature, these services can pose new threats. Regulation should therefore ensure both minimum proportionate risk standards while at the same time allowing for innovation. In addition, regulators should ensure that mandated rules are enforceable and that the financial authority has the capacity to provide appropriate supervision and oversight.

Regulators should ensure at minimum that:

- A regulatory framework for consumer protection that takes a proportionate risk-based approach to prudential standards is in place, but which also allows for innovation and aims to achieve the overall objective of financial inclusion;
- MFSPs are all licensed to operate under clear rules to protect consumer funds from misappropriation by the MFSP, insolvency, fraud or any operational risk;
- MFSPs operate on a level playing field that promotes competition to boost efficiency and increase consumer choice;
- There are appropriate and accurate standards for disclosure of information;
- There are simplified consumer protection rules for low-value transactions under the guiding principle of proportionate risk-based policies;
- MFSPs are required to be responsible for all their services whether provided directly to the consumer through a mobile network carrier or through agents;
- Clear data privacy and confidentiality rules are in place and properly enforced by the regulator;

[16] MFSPs should provide effective complaint and redress procedures, ensuring that channels for handling complaints are easy for consumers to access (some examples include a 24/7 toll-free call center that offers multiple language support, as well as mobile numbers that consumers can contact with inquires or complaints via SMS.

[17] Considering that payment and transfer services are financial services, licensed MFSPs generally operate under license from the financial regulator. Even though telecommunications regulators may regulate fees and information related to telecommunications services such as SMS or USSD services, it is best to have the MFSP supervised directly by the financial regulator. Nevertheless, the financial regulator and the telecommunications regulator should agree to cooperate both formally and informally on complaints that involve the use of mobile channels. This includes clearly ensuring that appropriate protocols are in place to resolve complaints related to both telecommunications and financial issues. The responsibilities of each regulator should be clearly defined in a set of regulations and/or legal instruments, as well as spelled out in a Memorandum of Understanding between the two regulators.

- There are appropriate channels for handling complaints, both internally by MFSPs and relevant external complaint resolution services via the regulator or appropriate government agency;[18] and
- Relevant data has been collected, both quantitative and qualitative, to assist the regulator in fine-tuning the consumer protection regulation based on evidence.[19]

References

The World Bank. June 2012. Good Practices for Financial Consumer Protection. http://responsiblefinance.worldbank.org/publications/financial-consumer-protection

Bezuidenhoudt, Johann and David Porteous. 2008. Managing the Risk of Mobile Banking Technologies. Bankable Frontier Associates LLC. http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2012/03/2008-Managing-the-risk-of-mobile-banking-technologies.pdf

Collins, Daryl. 2010. Consumer Experiences in Branchless Banking. Bankable Frontier Associates LLC. http://www.microfinancegateway.org/gm/document-1.9.50593/Consumer%20Experiences.pdf

Dias, Denise and Katharine McKee. September 2010. Protecting Branchless Banking Consumers: Policy Objectives and Regulatory Options. CGAP Focus Note 64. http://www.www.st.gsma.com/mobilefordevelopment/wp-content/uploads/2012/06/fn_64_rev_d_10.pdf

Gilman, Lara and Michael Joyce. 2012. Managing the Risk of Fraud in Mobile Money. GSMA Mobile Money for the Unbanked Annual Report. http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2012/10/2012_MMU_Managing-the-risk-of-fraud-in-mobile-money.pdf

Mudiri, Joseck. 2013. Fraud in Mobile Financial Services. MicroSave. http://www.microsave.net/resource/fraud_in_mobile_financial_services#.Uw2-33nZ2vI

[18] Complaint resolution and customer service support should be made available so that low-income, indigenous or other disadvantaged groups can easily access it and in a language they are comfortable with.

[19] See MFSWG Guideline Note No. 11 http://www.afi-global.org//library/publications/mobile-financial-services-indicators-measuring-access-and-usage-2013

About AFI Mobile Financial Services Working Group Guideline Notes

The AFI Mobile Financial Services Working Group guideline notes are based on the experience of group members and attempt to provide guidance on the definition of common standards, approaches, and practices for MFS regulation and supervision within AFI member institutions. The notes are not summaries of best practices nor do they propose new principles or revisions to existing core principles. Instead, they highlight key MFS policy and regulatory issues and identify challenges to be addressed. The definitions here are intended to complement rather than replace similar MFS definitions drafted by International Standard Setting Bodies (SSBs).

About AFI

The Alliance for Financial Inclusion (AFI) is a global network of financial inclusion policymaking bodies, including central banks, in developing countries. AFI provides its members with the tools and resources to share, develop and implement their knowledge of financial inclusion policies. We connect policymakers through online and face-to-face channels, supported by grants and links to strategic partners, so that policymakers can share their insights and implement the most appropriate financial inclusion policies for their countries' individual circumstances.

Learn more: www.afi-global.org

Alliance for Financial Inclusion

AFI, 399 Interchange Building, 24th floor, Sukhumvit Road, Klongtoey - Nua, Wattana, Bangkok 10110, Thailand
t +66 (0)2 401 9370 **f** +66 (0)2 402 1122 **e** info@afi-global.org www.afi-global.org
www.facebook.com/AFI.History @NewsAFI