RESERVE BANK OF MALAWI

GUIDELINES FOR MOBILE PAYMENT SYSTEMS

March 2011

Table of Contents

ACRONYMS

DES	-	Data Encryption Standards
DoS	-	Denial of Service
EDGE	-	Enhanced Data GSM Environment
FIU	-	Financial Intelligence Unit
GPRS	-	General Packet Radio System
GSM	-	Global System for Mobile Communication
HSM	-	Hardware Security Module
ICT	-	Information & Communication Technology
IDS	-	Intrusion Detection System
KYC	-	Know Your Customer
MACRA	-	Malawi Communications Regulatory Authority
MITASS	-	Malawi Inter Bank Transfer and Settlement System
PIN	-	Personal Identification Number
RBM	-	Reserve Bank of Malawi
SMS	-	Short Message Service
USSD	-	Unstructured Supplementary Service Data
WAP	-	Wireless Application Protocol

DEFINITIONS

Deposit - Money entrusted to a bank and accepted by it for credit to a depositor's account, which is payable, with or without interest on demand or after the expiration of a stated period of time.

Mobile Network Provider – A mobile phone company licensed by the Malawi Communications Regulatory Authority or any other body with authority in Malawi.

Mobile financial payment service provider – A company that is authorised to provide services that enable the process of money transfer and exchange of money for goods and services between two parties using a mobile phone.

Oversight – Refers to functions by regulatory bodies (e.g the RBM, MACRA and FIU) whereby the objectives of safety and efficiency are promoted by monitoring existing and planned systems, assessing them against the objective and, where necessary, inducing implementation of risk mitigating measures.

Pilot – Refers to a test period of a service prior to live roll out.

Suspicious Transaction – A transaction that does not conform to the knowledge of the system operator or its customer, or is suspected to be used for the commission a money laundering or terrorist financing offence.

Trustees – A board that controls and manages money from the mobile payment service scheme on behalf of the mobile financial payment service provider and subscribers.

Trust account – a savings account in a commercial bank under the control of the trustees

T+1 – Standard settlement period applicable on the MITASS which is the next business day from the date of the transaction.

1.0 Introduction

The mobile payment system in Malawi includes various components that facilitate the delivery of payment to the banked and non-banked population through mobile phones or other similar electronic means. Mobile financial payment service providers shall be required to meet conditions specified in this document.

2.0 Mandate

Pursuant to its mandate under Section 4 (e) of the Reserve Bank of Malawi (RBM) Act 1989, the RBM shall be responsible for promoting a sound financial structure in Malawi, including payment systems, clearing systems and adequate financial services in Malawi.

3.0 Objective

The objective of the guidelines is to promote a sound financial structure including payment systems, clearing systems and adequate financial services. Therefore both entry and exit from the payment system by the mobile financial payment service providers shall require prior written approval of the RBM.

4.0 Scope

These Guidelines shall apply to non-bank based mobile payments models. There are separate guidelines for bank based models.

4.1 Bank-based payment model is where customers have a direct contractual relationship with a prudentially licensed and supervised financial institution – a transaction account, a savings account, a loan, or some combination – even though the customer may deal exclusively with the staff of one or more retail agents hired by the bank to conduct transactions on the bank's behalf.

4.2 Nonbank-based payment model is where customers do not have direct contractual relationship with a prudentially licensed and supervised financial institution. Instead, they exchange cash at a

retail agent in return for an electronic record of value. This virtual account is stored on the server of a nonbank entity, such as a mobile network operator. Once the customers have a relationship with the nonbank service provider, they can order payment of funds to anyone else participating in the system and can receive payments from them on their mobile gadgets.

5.0 Application for RBM Approval

Any institution intending to provide mobile financial payment services shall apply in writing to the RBM. The application shall be accompanied by the following documentation:

5.1 Certificate of Incorporation as a registered company under the Laws of Malawi;

5.2 A copy of license to operate mobile telecommunications services from MACRA or any other body with authority to grant such licenses in Malawi.

5.3 Description of the mobile financial payment service and its impact on the mobile payment system provider's business strategy;

5.4 Conditions for recruiting network agents and standard copy of the service level agreement;

5.5 A technical proposal, including complete system architecture, of the proposed mobile financial payment service including an indication of interoperability of the proposed solution;

5.6 Proof of availability of the institution's ICT security policies including contingency arrangements and disaster recovery plans for the proposed mobile payment service;

5.7 Description of customer protection procedures such as customer data and financial records;

5.8 Identity and qualifications of directors and senior managers;

5.9 Any other information the RBM may deem relevant in vetting the application.

6.0 Post Application Procedures

6.1 Once the RBM is satisfied with the documentation submitted in Clause 5.0, it may require the applicant to conduct a pilot of the service;

6.2 The pilot phase will be subjected to system audit by an independent systems auditor whose results shall be submitted to the RBM;

6.3 The RBM shall not be responsible for any costs incurred in the application process including that of the system audit.

6.4 Once RBM is satisfied with the outcome of the post-application procedures, it shall issue a letter of no objection authorising the service provider to commence business.

6.5 In the event that it is granted, RBM shall issue the letter of no objection with a copy to MACRA

7.0 Authority of the RBM to Withdraw Approval

The RBM may decide to withdraw approval granted to a mobile payment service provider at any time if:

7.1 The institution has not commenced operations within 12 months of the date on which the *letter of no objection* authorising commencement of business was granted;

7.2 The institution obtained the approval of the RBM through incorrect statements or any other misleading information;

7.3 In the opinion of the RBM, the mobile payment service provider does not operate in the interest of the public;

7.4 The mobile payment service provider violates the guidelines set out in this document or any other laws and regulations applicable to it.

7.4 In the event of MACRA withdrawing the service provider's telecommunications license for whatever reason, then RBM's approval for the mobile payment service is automatically withdrawn.

7.5 For whatever reason the RBM deems necessary

After taking a decision to withdraw approval, the RBM shall notify the mobile payment service provider and shall issue a public notice in such manner as it deems appropriate.

8.0 Roles of the Mobile Payment Service Provider

In addition to generic requirements and those spelt in these guidelines the mobile payment service provider shall;

8.1 Provide and manage the delivery of mobile financial payment services;

8.2 Provide the network infrastructure required to deliver the mobile financial payment service;

8.3 Ensure that the proposed mobile financial payment service meets all the requirements specified in this document and others that may be set by the RBM from time to time;

8.4 Ensure that the service has audit trails and reporting mechanisms that meet operational, financial, regulatory and other reporting requirements;

8.5 Put in place sound risk management framework for the mobile financial payment service;

8.6 Secure interoperability of its system;

8.7 Maintain a trust account with a bank whose usage shall be restricted to facilitating mobile payment transactions;

8.8 Interest earned or otherwise accrued to balances in the trust account shall not be to the benefit of or otherwise paid to the Mobile Payment service Provider

8.9 Reflect all monetary values relating to transactions in the mobile financial payment service in the trust account at the bank;

8.10 Ensure that the balance on the trust account shall at all times be equal to the total outstanding (un-claimed) balance of all holders of the e-money under the service;

8.11 Undertake to the Trustees and system participants that no new or additional e-money other than in return for an equal amount in conventional money being paid to and received by the Trustee shall not be issued;

8.12 Not to effect transfer of e-money from any of its mobile payment account an amount which exceeds the credit balance of e-money in the relevant bank account;

8.13 Not accept deposits from the general public;

8.14 Enable the RBM to conduct oversight activities and system review at any point in time;

8.15 On a monthly basis, submit to the RBM the following:

8.15.1 The number of subscribers who transacted through the mobile financial payment service;

8.15.2 The volume and value of payments made through the mobile financial payment service;

8.15.3 A list of any complaints received relating to service failures of any kind;

8.15.4 Details of action taken to identify patterns in the complaints that may point to general or systemic weaknesses;

8.15.5 Any service breakdowns, such as network outages, giving details of the time the service went down, the reasons and the action being taken to prevent a recurrence;

8.15.6 Any system security lapses, giving details;

8.15.7 Any losses incurred by the mobile financial payment service provider or its customers;

8.15.8 Any loss of confidential data;

8.15.9 Any breach of these guidelines (a record of which should be held by the mobile payment service provider).

Notwithstanding the above reporting requirements, the mobile financial payment service provider shall be required to submit any *adhoc* data specified by the RBM from time to time in its performance of oversight role.

9.0 Mobile Payment Process

The mobile payment service providers shall provide the RBM with a detailed payment management value chain that covers the entire process from agent recruitment and monitoring, customer registration and management, customer service and dispute resolution arrangements to finality of transaction settlement.

The mobile financial payment service shall conform to the following processes:

9.1 Customer registration

9.1.1 Before rolling out, all mobile financial payment service shall seek recognition or authorisation by the RBM;

9.1.2 The solution should be capable of providing the registrants proof of successful registration;

9.1.3 Registration of users shall be subject to Data Protection (Privacy) policy;

9.1.4 Enrolment of consumers should satisfy Know Your Customer (KYC) requirements as laid out in the Money Laundering, Proceeds of Serious Crime and Terrorist Financing Act (2006) and regulations thereto.

9.2 Activation

9.2.1 The solution must prompt the registered user to activate the service by use of a PIN/password before commencement of any transaction processing;

9.2.2 The activation process, which should be through secure messaging systems, should ensure integrity and security of customer's identity;

9.2.3 The mobile payment system provider shall be responsible for the security and integrity of the entire activation process.

9.3 Transaction Processing

9.3.1 The system shall issue a unique transaction reference to any transaction processed within the mobile financial payment service;

9.3.2 All transactions shall have, at a minimum, the following features: transaction amount, transaction type, transaction date and time, and agent identification details;

9.3.3 Every successful transaction must identify a valid payer and payee and the system must produce payment notification to the payer and payee;

9.3.4 The system must produce error message(s) to the payer for every failed transaction indicating the reason for such error(s);

9.3.5 All transaction records shall be retained for a period of at least seven years;

9.3.6 The cost of processing any transaction, including electronic funds transfer instructions whether through SMS or any other means within the mobile financial payment service, shall be denominated in Malawi Kwacha.

9.4 Settlement

Settlement of all transactions shall be subject to conditions specified in this document which include the following:

9.4.1 Intra-scheme settlement shall be effected immediately (in real time);

9.4.2 The service should provide appropriate settlement records for reconciliation of processed transactions;

9.4.3 All settlement records shall be retained for a minimum period of seven years.

10.0 Technology

Security of Information is extremely vital and critical to the mobile financial payment system and its corresponding operations. Therefore, the technology used for mobile payments must be secure and ensure confidentiality, integrity, authenticity, and non-repudiation.

The technology implemented for mobile financial payment service, therefore, shall comply with the following technology standards and other requirements outlined in the provisions of these guidelines.

10.1 Modularity of Technologies

10.1.1 The technology deployed to deliver mobile payments services should comprise a set of interoperable infrastructure modules that work seamlessly across

heterogeneous networks. There should be an end-to-end connection from user-device through the transport network to the service site;

10.1.2 The mobile financial payment services shall use any mode of communication including, but not restricted to, Secure SMS, USSD, EDGE and GPRS;

10.1.3 The mobile financial payment services shall use any mode of user interface, including, but not restricted to, Secure SMS, USSD, EDGE or Menu driven WAP/GPRS application;

10.1.4 The mobile financial payment services shall not use plain text SMS. All messages in transit must be encrypted;

10.1.5 Only secure channels shall be used in providing mobile financial payment services;

10.1.6 The mobile payments solution may be embedded into SIM card and it shall ensure simple initialization of the application.

10.2 Message Format

Mobile payments solutions deployed shall adhere to and adopt the ISO 8583 standards and be encrypted end-to-end.

10.3 Reliability

10.3.1 Payment instruction shall be consistently executed. In the event that an instruction is not effected due to technology failure, reversal of instruction shall be automatic and immediate;

10.3.2 Users shall get immediate value and notification for every successful transaction;

10.3.3 Users should be able to switch between service providers without any bottlenecks. Switching from one solution to another should be as easy as possible;

10.3.4 The user interface shall, at the minimum, be menu-driven;

10.3.5 If private or personal data in the application are directly accessible through such menu, the access to this menu shall be protected;

10.3.6 Administrative functions - for example, tracing, certification/confirmation of transaction shall be provided;

10.3.7 PIN shall be encrypted at the point of entry.

10.4 Security

The overall security framework shall ensure:

10.4.1 That minimum encryption standard specified is Triple Data Encryption Standard (3-DES) encryption at all stages of transaction processing;

10.4.2 That Hardware Security Module (HSM) exists between service providers and all financial or third party institutions that participate in the service;

10.4.3 That any sensitive information stored in third party systems is restricted with appropriate encryption and hardware security standards;

10.4.4 That all transactions on an account shall be permitted only by validation through a minimum of two factor authentication (i.e. mobile number and the PIN associated with it);

10.4.5 That mobile payments application shall not allow the option of saving any customer transaction details on the handset;

10.4.6 That all accounts activated by the consumer on the mobile application is linked to mobile phone number. This mobile number shall be used as the second form of authentication for mobile transactions;

10.4.7 That payment authorization message from the user's mobile phone shall, at minimum, be triple DES encrypted and checked for tampering by the service provider. It shall not be possible for any interceptor to change contents of the message;

10.4.8 Segregation of duties between the business and technical function;

10.4.9 Existence of logical access controls to data, systems, application software, utility telecommunication lines, libraries, system software, etc. providing the mobile payments solution;

10.4.10 At a minimum, the use of proxy server type of firewall and Intrusion Detection systems (IDS) so that there is no direct connection between the Internet and the service providers' systems. For sensitive systems, a state of the art inspection firewall shall be implemented to thoroughly monitor all packets of information, compare past and present transactions and enable a real time security alert;

10.4.11 That the information security officer and the information system auditor undertake periodic

information security audits and penetration tests of the system, which shall include but not limited to;

10.4.11.1 Password guessing and cracking;

10.4.11.2 Searching for back door traps in the programs;

10.4.11.3 Checking attempt to overload the system using Distributed Denial of Service & Denial of Service (DoS) attacks;

10.4.11.4 Checking if commonly known holes in the software, especially the browser and the e-mail software exist;

10.4.11.5 Carrying out regular penetration testing on the mobile financial payment system;

10.4.11.6 Ensuring that physical access controls are strictly enforced. Physical security shall cover all the information systems and sites where they are housed, both against internal and external threats;

10.4.11.7 Enforcing proper infrastructure and schedules for backing up data. The backed-up data shall be periodically tested to ensure recovery without loss of transactions in a time frame as given out in the security policy;

10.4.11.8 Maintaining disaster recovery sites and regular testing of its facilities for the purpose of business continuity.

11.0 Agents

A mobile payment system provider shall have the option of appointing business entities on a contractual basis to facilitate activities such as registering subscribers, accepting cash, making payments and effecting funds transfers. Being an agent of the principal all activities of the agent must be executed in full compliance as expected of the principal as required under these guidelines and other relevant regulations.

Any principal wishing to appoint an agent shall be required to identify the agent whilst, among other things, observing the following:

11.1 Obtain verifiable name, address, signature and/or bio-data where the proposed agent is an individual;

11.2 Collect the following information where the agent is a registered business entity:

11.2.1 Copies of Certificate of Incorporation;

11.2.2 Board approval to participate in the mobile payments agency arrangement;

11.2.3 Physical address of head office and list of branches/agencies/kiosks;

11.3 Prescribe e-money limits depending on the nature of the business of the agent.

11.4 Maintain an online link with the agent;

11.5 Train agents to ensure that services are efficiently executed;

11.6 Ensure that the agent displays its brand visuals conspicuously at all times for easy identification by consumers;

11.7 Enter into a contract agreement with the agent which, among others, should enable the principal to exercise reasonable control over the activities of the agent;

On their part, agents shall:

11.8 Report any suspicious transactions to the principal;

11.9 Conspicuously display the help line maintained by the principal(s), tariffs and any other relevant information of the mobile financial payments service(s);

11.10 Not be limited to act as agents of one mobile financial payment service for purposes of attaining financial inclusion.

12.0 Transaction Limits

Mobile financial payment services are designed to facilitate retail transactions to both banked and non-banked population. In this regard, institutions shall observe the following transaction limits:

12.1 Maximum transaction value of K20, 000.00 per day for non bank customers trading on the mobile payment;

12.2 Maximum transaction value of K50, 000.00 per day for the banked customers trading on the mobile payment service.

12.3 The limits above are subject to be reviewed from time to time by the RBM

12.4 Organizations will have no limitation on their transaction value provided they seek permission to do so from the Reserve Bank of Malawi. This shall also apply to government.

13.0 Anti-Money Laundering Requirements

All institutions providing mobile financial payment services shall

13.1 Be required, within 3 days, to furnish the Financial Intelligence Unit with information on any transaction having attributes of a suspicious transaction, agent or subscriber.

13.2 Adhere to the Money Laundering, Proceeds of Serious Crimes and Terrorist Financing Act (2006) and FIU regulations as may be issued from time to time

14.0 Cessation of Mobile Payment Service

14.1 Any institution wishing to exit from the mobile financial payment system shall notify the RBM in writing regarding the intention for the discontinuation 90 days before ceasing its operations;

14.2 The RBM shall have powers to order the mobile payment system provider to take any action prior to exiting from the mobile financial payment service.