BANK OF MAURITIUS

Guideline on

Mobile Banking and Mobile Payment Systems

February 2013
Revised May 2015

Table of Contents **Page**

1 Introduction

The Bank of Mauritius is mandated under the Bank of Mauritius Act 2004 to ensure the stability and soundness of the financial system of Mauritius and manage, in collaboration with other relevant supervisory and regulatory bodies, the clearing, payment and settlement systems of Mauritius.

The objective of this guideline is to promote a sound financial system in Mauritius and regulate the mobile banking and mobile payment systems. It is intended for providers of mobile banking and mobile payment services.

2 Authority

This guideline is issued by the Bank under the authority of Section 50 of the Bank of Mauritius Act 2004 and Section 100 of the Banking Act 2004.

3 Scope of Application

The guideline shall apply to bank-based and non-bank-based mobile banking and mobile payment service providers.

4 Effective Date

This guideline shall come into effect on 18 February 2013.

5 Interpretation

In this guideline –

"Airtime" refers to the communication time stored on a mobile device, denominated in rupees;

"bank" has the same meaning as in the Banking Act 2004;

"Bank" means the Bank of Mauritius established under the Bank of Mauritius Act 2004;

"bank-led model" refers to a mobile banking service model where the customer account relationship rests with a bank;

"deposit" has the same meaning as in the Banking Act 2004;

"financial institution" has the same meaning as in the Banking Act 2004;

"ICTA" means the Information and Communication Technologies Authority established under the Information and Communication Technologies Act 2001;

"Internet banking" has the same meaning as in the Guideline on Internet Banking;

"Mobile banking (M-Banking)" –

(a) includes mobile payment (m-payments) and may involve –

(i) payment through a bank account where fund transfer takes place within accounts held at the bank at the time of payment and the value of the payment is not stored in the device;

(ii) payment through a stored value account, where the fund transfer takes place by debit of a stored value which is located in the mobile device or elsewhere; and

(b) involves access to a broader range of banking services such as account based banking transactions using a mobile communication device which includes the use of Mobile Apps and near field communication (NFC);

(c) but excludes –

(i) the access to banking services through the web browser of a mobile device which is assimilated to Internet Banking;

(ii) the use of a mobile device as point of sale for card based transactions;

"Mobile banking and mobile payment service provider" means a bank or mobile network operator which 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 communication device;

"Mobile Communication Device" means any mobile device having a unique internationally recognized identifier and which is fitted with an integrated circuit for subscriber identification (e.g. Subscriber Identification Module), whether embedded or removable and which can be used as a mobile communication equipment;

"Mobile Payment (M-Payment)" means any financial transaction with fund movement undertaken using a mobile device such as a mobile communication device whether the fund transfer takes place from the stored value in the mobile device, or from a bank account;

"Mobile Network Operator" means a company holding a Public Land Mobile Network licence issued by the ICTA;

"non-bank-led model" refers to a mobile payment service model where the account management functions are conducted by a non-bank which has direct contact with individual customers;

"Retail agents" are third party outlets which act as agents for the provision of mobile banking and mobile payment services to customers on behalf of their principals;

"Service provider" means the mobile banking and/or mobile payment service provider, as the case may be;

"Stored value" means funds or monetary value represented in digital electronics format and stored or capable of storage on electronic media in such a way as to be retrievable and transferable electronically;

"Suspicious transaction" has the same meaning as in the Financial Intelligence and Anti Money Laundering Act 2002;

"Trustees" means a board that controls and manages money from the mobile payment service scheme on behalf of the mobile payment service provider and subscribers;

"Trust account" means a savings account in a bank under the control of the trustees.

6 Application for Mobile Banking or Mobile Payment Services

6.1 The approval of the Bank is required prior to conducting either the bank-led mobile banking and mobile payment model or the non-bank-led mobile payment model.

6.2 Any institution intending to provide mobile banking or mobile payment services shall apply in writing to the Bank provided that :

(a) mobile banking services may only be provided by a bank or a consortium led by a bank in a bank-led model;

(b) a non-bank or mobile network operator or consortium led by mobile payment services in a non-bank led model may only provide mobile payment services.

6.3 Both entry and exit from the payment system by the mobile banking and mobile payment service providers shall require prior written approval of the Bank.

6.4 The application shall include an authority from the applicant authorising any regulatory body, law enforcement body or financial institution, in Mauritius or in a foreign country, to release to the Bank, for use in relation to the application, any information about the applicant, and any of its directors, shareholders, beneficial owners, chief executive officer or other senior officers as may be applicable.

6.5 The documentation and information to be provided to the Bank for conducting mobile banking and mobile payment services are provided in Annex 1.

6.6 For a bank-led model, the application shall be accompanied with the documentation listed in Part I of Annex 1.

6.7 Whereas, for a non-bank-led model, the application shall be accompanied with the documentation listed in Part II of Annex 1.

6.8 A non-bank must also comply with the requirements of Annex 2.

7 Determination of application

7.1 The Bank may, on an application duly made in accordance with paragraph 6 and after being provided with all such information and documents as it may require, determine the application.

7.2 The Bank shall give notice of its determination to the applicant within 60 working days of receipt of a complete application or of the supply of any supplementary information called for by the Bank.

8 Post Application Procedures

8.1 Where the Bank is satisfied with the application submitted under paragraph 6, it may request the applicant to carry out a pilot test regarding the mobile banking or mobile payment services it proposes to conduct.

8.2 The Bank may also request for a certificate from an independent system auditor with regard to compliance with the security norms prescribed in this guideline.

8.3 All processing costs incurred in the application process, including but not limited to the pilot test as well as the system audit, will be borne by the applicant.

8.4 Once the Bank is satisfied with the outcome of the post-application procedures, it shall issue a letter of no objection authorising the applicant to commence business.

8.5 The Bank may seek the assistance of other bodies when considering an application under paragraph 6, including the post-application procedures.

8.6 Where the Bank issues a letter of no objection, it shall provide ICTA with a copy thereof.

9 Cancellation or suspension of approval

9.1 The Bank may, at any time, cancel the approval granted to carry out the mobile banking or mobile payment services if:

(i) the institution fails to commence business within a period of 12 months from the date the approval was issued;

(ii) the approval was obtained by fraudulent means, including but not limited to, forged documents, incorrect statements, anti-competitive practices and misleading information;

(iii) in the opinion of the Bank, the service provider does not operate in the interest of the public;

(iv) the mobile banking or mobile payment service provider violates the provisions of this guideline or any other laws and regulations applicable to it;

(v) in the case of a non-bank led model, the mobile operator's license is forfeited or withdrawn by ICTA; and

(vi) for such other reason as the Bank may deem necessary.

9.2 (a) In the case of a non-bank-led payment model, the approval shall automatically be suspended by the Bank if the mobile operator's license is suspended by ICTA.

(b) The suspension of the approval shall take effect as from the date of the suspension of the mobile operator's licence.

(c) The suspension shall be on such terms and conditions as the Bank may impose.

(d) The suspension of the approval may be lifted by the Bank when the mobile operator's licence is restored by ICTA.

9.3 Where the Bank decides to cancel an approval, the Bank shall serve on the mobile banking or mobile payment service provider a notice of its decision to do so, specifying a date, which shall be not less than 30 days of the date of the notice, on which the cancellation shall take effect.

9.4 The Bank may, where paragraphs 9.1 (i), (ii) and (v) apply, revoke the approval forthwith without being required to serve the notice under paragraph 9.3.

9.5 The service provider may, within 14 days of service of a notice under paragraph 9.3, make representations to the Bank.

9.6 The Bank shall, after considering any representations made under paragraph 9.5, take a final decision on the cancellation and shall notify the service provider in writing of its decision. .

9.7 Where the Bank cancels or suspends an approval, it shall issue a public notice in such manner as it may deem appropriate and it may require the service provider to cause a notice to be published on its website and in three daily newspapers specifying :

(i) that its approval to carry on mobile payment or mobile banking services has been cancelled or suspended by the Bank; and

(ii) the date of cancellation or suspension of the approval.

9.8 Following the cancellation or suspension of the approval, the service provider shall stop providing any mobile banking or mobile payment services to the public and comply with such instructions and terms and conditions imposed by the Bank regarding the handling and/or disposal of the customers' stored money or accounts held with them.

10 Stored Value Accounts

10.1 The Bank may authorise the issuance of stored value for payments subject to the following conditions:

(i) It is stored in an electronic device;

(ii) It is issued on receipt of funds for an amount exactly equal to the monetary value offered;

(iii) It is redeemed at par with the equivalent conventional money;

(iv) It shall never expire;

(v) Any points/rewards accruing under loyalty schemes cannot be converted into money; and

(vi) Any unclaimed amount which has been left untouched and not reclaimed for 7 years or more and the customer has not responded within 6 months to a letter from the service provider about the unclaimed amount sent by registered post to the customer's last known address, the unclaimed amount, shall be deemed to have been abandoned and shall, without further formality, be transferred forthwith by the service provider concerned to the Bank to be dealt with as decided by the Bank. The procedures set out in Section 59 of the Banking Act with respect to abandoned funds shall apply to these unclaimed amounts.

10.2 The service provider shall inform the customer of any service fees or charges that may be applicable for maintaining the stored value accounts.

10.3 Where a service provider issues stored value for payment, it shall :

(i) Open a trust account with a bank in Mauritius and use that account solely to facilitate mobile payment transactions;

(ii) Reflect all monetary values relating to the mobile payment transactions in the trust account;

(iii) Ensure that interest earned or otherwise accrued to balances in the trust account shall be paid back to the customer in such form as the service provider may deem appropriate. These interests shall not be to the benefit of or otherwise paid to the Mobile Payment Service Provider;

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

(v) 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 be issued;

(vi) Not 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.

11 Restrictions on Use of Airtime

11.1 As airtime is not redeemable at par into cash, is discounted for value added taxes and is subject to expiry, the use of airtime for any payment transaction is not allowed.

11.1A Notwithstanding paragraph 11.1, the Bank may authorise a service provider to make use of airtime for special schemes, on such terms and conditions as the Bank may determine.

11.2 Service providers must keep distinct accounts in the mobile device for communication and payments purposes.

12 Mobile Payment Process

12.1 The service providers shall submit to the Bank a detailed description of the entire business process comprising, but not limited to:

(i) Fund movement and settlement process;
(ii) Customer registration, services and dispute resolution mechanisms;
(iii) Know Your Customer 'KYC' process and internal control systems;
(iv) Information to be disclosed to the customers;
(v) Fees and charges to be applied;
(vi) Finality and irrevocability of payments to be applied; and
(vii) Such other information as may be requested by the Bank.

12.2 The mobile payment service provider shall conform to the following processes:

12.2.1 Customer Registration

(i) Customers must be provided with a written acknowledgment of successful registration;
(ii) Registration of customers must comply with all legal requirements; and
(iii) Enrolment of customers should satisfy KYC requirements as laid down in the Guidance Notes on AML/CFT issued by the Bank.

12.2.2 Activation

(i) Customers must be prompted to activate the payment service by the use of a PIN/password;
(ii) Integrity and security of customer's identity must be ensured throughout the process; and
(iii) It will be the responsibility of the service provider to ensure security and integrity of the entire process.

12.2.3 Transaction Processing

(i) All transactions must produce a ticket with the following minimum features:

a. Unique Transaction reference number within the system
b. Date and time
c. Amount
d. Agent identification
e. Merchant details
f. Payee details

(ii) Confirmations must be provided for all successful transactions to the payer and the payee;

(iii) All transactions must be denominated in Mauritius Rupees. Transactions may be denominated in currencies other than Mauritius Rupees, subject to the prior approval of the Bank.

(iv) Failed transactions must be backed by error message(s) notifications describing the reasons for the failure;

(v) All transaction records shall be retained for a period of at least seven years; and

(vi) The cost of transaction processing, including electronic fund transfer, whether through SMS or any other means shall be separate from the value of the transaction and shall not be higher than the normal cost of the communication medium. Where the service provider imposes fees or charges on any service, such fees or charges may be subject to a cap determined by the Bank.

12.2.4 Settlement

Settlement of transactions must comply with the following conditions:

(i) Settlement shall be final and irrevocable;

(ii) All settlement records shall be retained for a minimum period of seven years.

Notwithstanding (i) above, the service provider shall put in place a dispute resolution mechanism for failed or disputed transactions, which shall make provisions for the conditions for reversals and re-imbursements. The service provider shall inform its customers of the dispute resolution mechanism.

12.2.5 Technology and Security

The mobile payment system shall, at a **minimum**, comply with the following technology standards and such other requirements specified in this guideline.

12.2.5.1 Authentication

Authentication shall be done through one or a combination of the following methods:

(i) PIN, One Time Code (OTC) or password;

(ii) A card or token in the possession of the customer;

(iii) A unique physiological, genetic or physical trait possessed by the customer such as fingerprint or voice; and

(iv) A secret or private cryptographic key which the customer can access and use to prove his identity.

12.2.5.2 Modularity of Technologies

(i) The technology deployed to deliver mobile payments services shall comprise a set of interoperable infrastructure modules that support at least one major telecom network (GSM or CDMA). There should be an end-to-end connection from user-device through the transport network to the service site;

(ii) Any one or more than one mode of mobile communication may be used;

(iii) Any mode of user interface may be used;

(iv) Plain text SMS may be used solely for 'push transactions', i.e. those category of transactions which are only restricted to the customer's own transactions, or general notification purposes.

(v) Plain text SMS must not be used for any transaction validation message, all such messages must be encrypted;

(vi) Only secure channels must be used, including but not limited to, SMS, USSD, WAP, IVR, Smartphone Apps; and

(vii) The mobile payment solution may be embedded into a SIM card.

12.2.6 Message Format

Mobile payments solutions shall be encrypted end-to-end and shall adhere to the ISO 8583 standards or a variant acceptable to the Bank.

12.2.7 Reliability

(i) The system infrastructure must provide for reliability, redundancy and non-repudiation. The service provider must describe the steps taken to provide for the non-repudiation of transactions. If a transaction is not executed due to technology failure, it must be automatically and immediately reversed;

(ii) Users shall get immediate value and notification for every successful transaction;

(iii) The system shall not have features that lock-in users. Switching from one solution to another should be allowed. The interoperability of the solution shall be implemented in a phased manner.

(iv) The user interface shall be easy and unambiguous. Menus must be used as far as possible;

(v) Where private or personal data in the application are directly accessible through menu or user interface, the access shall be protected;

(vi) Administrative functions, such as, tracing, certification/confirmation of transaction shall be provided;

(vii) PIN shall be encrypted; and

(viii) PINs should not be stored or processed in plain text in a system.

12.2.8 Security

The service providers shall ensure that the overall security framework complies with the following **minimum** standards:

(i) Triple Data Encryption Standard (DES) or Advanced Encryption Standard (AES) or any other recognised encryption standard of equivalent strength must be used at all stages of transaction processing;

(ii) Hardware Security Module (HSM) is used for interaction between all financial or third party service providers;

(iii) Sensitive information, whether in the main system or in the servers of third party systems is restricted with appropriate encryption and hardware security standards;

(iv) Any customer transaction details stored in the handset shall be adequately protected from unauthorised use by means of encryption and/or password protected access;

(v) All accounts activated by the customer on the mobile application shall be linked to a mobile communication device number. This mobile communication device number or an acceptable alternative, shall be used as the second form of authentication for mobile transactions;

(vi) The service provider must ensure that all payment authorisation messages from the handset are triple DES or AES or equivalent recognised standard encrypted and checked for tampering. The service provider must also ensure that any interceptor cannot change the contents of the message;

(vii) Business and technical functions must be segregated;

(viii) Data, systems, application software, utility telecommunication lines, libraries, system software must be controlled;

(ix) The use of state of the art systems with firewall and intrusion detection to control access from the Internet must be used; and

(x) Periodic information security audits and penetration tests of the system must be carried out and shall include but not be limited to the following:

a. Password guessing and cracking;
b. Searching for back door traps in the programs;
c. Checking attempt to overload the system using Distributed Denial of Service (DoS) attacks;
d. Checking if commonly known holes in the software, especially the browser and the e-mail software exist;
e. Carrying out regular penetration testing on the mobile payment system;
f. Ensuring that physical access controls are strictly enforced;
g. Enforcing proper infrastructure and schedules for backing up data; and
h. Maintaining disaster recovery sites and regular testing of its facilities for the purpose of business continuity.

13 Measures to combat Money Laundering and Terrorist Financing

13.1 All service providers shall abide by the requirements of the Guidance Notes on AML/CFT, FIAMLA and other guideline, circulars or directives issued by the Bank to this effect.

13.2 They should have appropriate systems and controls to monitor the transactions of each client in terms of both volume and velocity and to report to the FIU any suspicious transactions.

13.3 They shall be held accountable and responsible for agents' compliance with regulations.

14 Confidentiality

14.1 The service providers and the retail agents shall maintain the confidentiality of all documents and information pertaining to their customers at all times and shall not, on any account and at any time, disclose directly or indirectly to any person, any matter or information relating to their customers unless legally authorised to do so.

15 Compliance Officer

15.1 All service providers shall appoint a compliance officer for ensuring compliance with relevant laws and regulations.

16 Cessation of Mobile Banking and Mobile Payment Service

16.1 A service provider may, with the prior permission of the Bank and subject to such conditions as may be specified by the Bank, cease to provide mobile banking or mobile payment services at any time.

16.2 Any service provider wishing to exit from the mobile payment system shall give 90 days prior notice to the Bank.

16.3 The Bank may, before or after the cessation of mobile banking and mobile payment services, make such inquiry and give such directions as it thinks fit, so as to ensure that the interests of customers and of the public are preserved.

16.4 The Bank may order the service provider to take such action as it deems appropriate.

16.5 The Bank may issue a public notice in such manner as it may deem appropriate in this respect.

17 Loss of device and replacement

17.1 The service provider must clearly disclose, in writing, to the customer information on reporting mechanism for lost or stolen devices.

17.2 The service provider must have clear procedures in place to enable customers to change mobile number. These should be communicated to the customers.

17.3 The service provider shall put in place a hotline for fault, loss or theft reporting on a 24/7 basis.

18 Customer Education, Complaints and Complaints Procedure

18.1 Mobile payment services are based on advanced technology that requires proper customer education. Potential users must be walked through the entire process in order to educate them about the possibilities of misuse or failure of technology, remove psychological hurdles for initiation to such technology and improve user-friendliness.

18.2 The mobile banking or mobile payment service provider will be required to run proper education campaigns and maintain on-going help/advice desks for customers to cover at least the following areas:

(i) Advise customers of the benefits of having different PINs for different online services;

(ii) Provide instructions to customers on how to configure their mobile devices to access mobile and payment applications;

(iii) Advise customers to take security precautions in using mobile banking and payment services;

(iv) Advise customers of dispute handling, reporting procedures and the expected time for resolution; and

(v) Avoid the use of complex, legal and technical jargon in their communications with customers.

18.3 Integrity of staff and fair treatment is central to minimizing grievances and, if possible, a service quality management system should be put in place to ensure that the service standards at the service provider are fair.

18.4 The service provider must have in place a complaints desk and a dedicated complaints officer to attend to customer's complaints. These officers should be adequately trained to address complaints speedily.

18.5 The service provider must inform its customers of the complaint handling procedure when they establish a business relationship with them and ensure that its complaint handling procedures are readily available on its premises and displayed on its website. Customers should be informed via appropriate communications media that –

(a) Complainants should address their complaints to the service provider concerned, in the first instance.

(b) In the case that no reply to their complaint has been received from the service provider within 3 months as from the date the complaint is lodged or that the complainant is not satisfied with the service provider's decision, they may address their complaint to the Bank of Mauritius specifying prominently the address of the Bank of Mauritius where the complaint is to be addressed.

18.6 The service provider may provide for the registration of complaints by

(a) electronic means, as for instance, the website of the service provider where complaints may be registered online.

(b) email, letter, fax or phone.

18.7 The officer who receives the complaint has to log the complaint into a central database.

18.8 Where the complaint can be resolved on the spot, this has to be favoured. Where the complaint cannot be resolved on the spot, the complaint has to be acknowledged within 2 days from the date of receipt thereof and channelled to the officer conversant with the file.

18.9 The complaint has to be addressed and a written reply shall be given to the complainant as soon as practicable but not later than 3 months as form the date the service provider receives the complaint. If the complaint is not resolved within 14 days from the date of its receipt by the officer concerned, the complaint should be automatically escalated higher up through an inbuilt mechanism and even to the Chief Executive Officer, if required. The procedure and stand taken with regard to the complaint has to be reviewed by the Compliance Department of the service provider.

18.10 The service provider shall inform the Bank, on a monthly basis, of -

(i) all complaints received by its complaints desk;
(ii) any remedial action taken to resolve the complaint;
(iii) where the complaint has been resolved, the agreement reached between the parties; and
(iv) if no agreement has been reached, the reasons thereof.

18.11 The Bank may suspend or revoke the approval of the service provider where it is of the view that it is in the public interest to do so, after taking into consideration the number of complaints received against the service provider.

19 Specific Guidelines for bank–led models

The following shall apply for bank-led models:

19.1 **Information Services**

19.1.1 Banks may offer mobile banking services that are purely informational such as bank advertisements, interest rates, exchange rates and news. Such information is usually available to the public.

19.1.2 Banks shall ensure that the information exchanged with the customer is protected against unauthorised modifications.

19.2 **Bank Account Information**

19.2.1 Banks must ensure that:

(i) Only authorised parties have access to information relative to bank accounts and that such information is conveyed in a manner where confidentiality is maintained; and

(ii) Follow-up actions are initiated regarding customers who modify their profiles.

19.3 **Transfers between Customer's Linked Accounts**

19.3.1 Where bank customers link multiple related accounts to their mobile banking facilities to enable them to perform transactions, including fund transfers on all linked accounts, the bank shall :

(i) institute stringent controls over linking of accounts to a mobile service prior to authorising fund transfers; and

(ii) ensure that the online mobile banking applications implement validation checks to detect and disallow unauthorised transactions.

19.4 **Transfers to Third-Party Accounts**

19.4.1 There are typically two forms of third party fund transfers, namely:

(i) Fund transfers to pre-approved third party transactions; and

(ii) Fund transfers to third party accounts which have not been pre-approved.

19.4.2 Banks shall:

(i) implement two-factor authentication before allowing third party transaction;

(ii) not allow nor rely on third party authentication; and

(iii) ensure that transfers to third party accounts are limited to Rs10,000 per day, or such other amount as may be approved by the Bank.

19.4.3 Any approval granted under paragraph 19.4.2(iii) shall be subject to such terms and conditions as may be determined by the Bank.

19.5 **Payment through third parties**

19.5.1 Banks shall authenticate their customers with respect to payment transactions made by mobile devices and shall ensure that this function is not outsourced to any third-party.

19.5.2 Customers may, through Direct Debit Authorisation schemes, give specific standing authorisations to third parties to charge their accounts.

19.5.3 Banks must ensure that, when operating such arrangements, third parties or service providers must neither obtain, nor store the customers' personal banking IDs, or PINs for the purpose of raising debits.

19.5.4 In case, debit or credit cards are used for making mobile payments, the verifications and validations effected by the issuing bank must be limited to those normally carried out under the terms and conditions governing the usage of debit or credit cards.

19.6 **Agents**

19.6.1 Banks shall when appointing retail agents comply with the Guideline on Outsourcing issued by the Bank and the provisions of the banking laws and guidelines and instructions issued thereunder.

20 Specific guidelines for non-bank led Models

20.1 **Roles of the Mobile Payment Service Provider**

In addition to generic requirements and those spelt in this guideline, the mobile payment service provider shall comply with the requirements and provide the Bank with the information/documents as specified in Annex 2.

20.2 **Agents**

20.2.1 Mobile payment system providers may appoint business entities or agents, to facilitate activities such as registration of subscribers, acceptance of cash, effect payments and effect fund transfers provided that they:

(i) inform the Bank of their appointment;

(ii) have carried out proper due diligence on these business entities or agents.

The Bank may, if it is not satisfied with the fitness and properness of the business entities or agents, instruct the service provider to terminate the agency agreement with them and the service provider shall forthwith comply with the instruction of the Bank.

20.2.2 The service provider shall define the activities restricted to the agents and the latters shall be required to carry out the selected activities in full compliance as expected of the principal under this guideline and other relevant regulations.

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

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

(ii) Collect the following information where the agent is a registered business entity:

a. Copies of Certificate of Incorporation;

b. Board approval to participate in the mobile payments agency arrangement;

(iii) Physical address of head office and list of branches/agencies/kiosks;

(iv) Prescribe e-money limits depending on the nature of the business of the agent.

(v) Maintain an online link with the agent;

(vi) Train agents to ensure that services are efficiently executed;

(vii) Ensure that the agent displays its brand visuals conspicuously at all times for easy identification by customers; and

(viii) 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.

20.2.4 Principals shall ensure that their agents:

(i) Abide by the provision of this guideline and any other relevant laws, rules and regulations; and

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

20.3 **Transaction Limits**

20.3.1 Payments through mobile devices are expected to be in the category of low value retail transactions. In this regard, service providers shall observe the following transaction limits:

(i) Maximum transaction value of Rs5,000 per day for unbanked customers trading on the mobile payment; and

(ii) Maximum transaction value of Rs10,000 per day for the banked customers trading on the mobile payment service, provided the mobile money account is linked with a bank account.

20.3.2 Notwithstanding paragraph 20.3.1, the Bank may, upon the request of a service provider, authorise push transactions in excess of the prescribed limits to specific bodies and for specific purposes.

20.3.3 The limits specified above may be reviewed from time to time by the Bank.

21 Review of the Guideline

21.1 This guideline may be subject to periodic review by the Bank.

21.2 The Bank shall inform service providers of any amendment which it may bring to any section, part or paragraph of this guideline.

22 Transitional Period

22.1 Where a service provider is, at the coming into operation of the guideline, already providing a mobile banking or mobile payment service, it may apply to the Bank for a transitional period to comply with the guideline.

22.2 The service provider shall in the application state the reason why it is unable to comply with the guideline.

22.3 The Bank may consider the application and grant the service provider with a transitional period of up to 6 months following the date of coming into force of this guideline, to comply with the provisions of the guideline.

Bank of Mauritius
February 2013

Annex 1 : Information requirement for conducting mobile banking and mobile payment services

Part I : Bank-led Model

1. Information on accounting and control systems;
2. A complete description of the mobile banking and payment system;
3. A technical proposal, including complete system architecture, DR and Business Continuity plans of the proposed mobile payment service including an indication of interoperability of the proposed solution;
4. Description of customer protection procedures such as customer data and financial records;
5. Conditions for recruiting network agents and standard copy of the service level agreement, if applicable; and
6. Any other information the Bank may deem relevant in vetting the application.

Part II : Non-bank led Model

Certified copies, where applicable, of the following documents :

1. The certificate of incorporation;
2. The shareholding structure of the company, the composition of the board and organisation structure;
3. Information on fitness and propriety criteria for directors and senior managers;
4. Information on accounting and control systems;
5. Qualifications and experience of directors and senior managers, where applicable;
6. A copy of license to operate mobile telecommunications services from ICTA for each network partner;
7. A complete description of the mobile banking and payment system;
8. A technical proposal, including complete system architecture, DR and Business Continuity plans of the proposed mobile payment service including an indication of interoperability of the proposed solution;
9. Description of customer protection procedures such as customer data and financial records;
10. Conditions for recruiting network agents and standard copy of the service level agreement, if applicable; and
11. Any other information the Bank may deem relevant in vetting the application.

Annexe 2 –Requirements for non-bank led models

The mobile banking or mobile payment service provider shall:-

1. Be required to comply with the operational, financial, regulatory and other reporting requirements set by the Bank;
2. Ensure that the proposed mobile payment service meets all the requirements specified in this guideline and any other instructions issued by the Bank from time to time;
3. Provide and manage the delivery of mobile payment services;
4. Provide, maintain and operate the network infrastructure required to deliver the mobile payment service;
5. Put in place sound risk management framework for the mobile payment service;
6. Secure interoperability of its system;
7. Not accept deposits from the general public;
8. Enable the Bank to conduct oversight activities and system review at any point in time, including but not limited to on-site examinations and access to its books, accounts, records and financial statements
9. On a monthly basis, submit to the Bank the following:
    a. The number of subscribers who transacted through the mobile payment service;
    b. The outstanding volume and value of payments made through the mobile payment service;
    c. A list of any complaints received relating to service failures of any kind;
    d. Details of action taken to identify patterns in the complaints that may point to general or systemic weaknesses;
    e. 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;
    f. Any system security lapses, giving details and activities;
    g. Any losses incurred by the mobile banking and mobile payment service provider or its customers;
    h. Any loss of confidential data;
    i. Any breach of these guidelines (a record of which should be held by the mobile payment service provider).
10. Provide the Bank with the following:
    a. an auditor's certificate attesting that they are compliant with the guideline on mobile banking and mobile payment system;
    b. not later than three months after the end of its financial year, its audited financial statements for the financial year, prepared in accordance with the International Accounting Standards and such guidelines as may be issued by the Bank; and
    c. any other on-line data to the Bank in the format specified by the Bank.
11. Not debit the customer’s account with any fees or charges which the customer has not expressly agreed to.

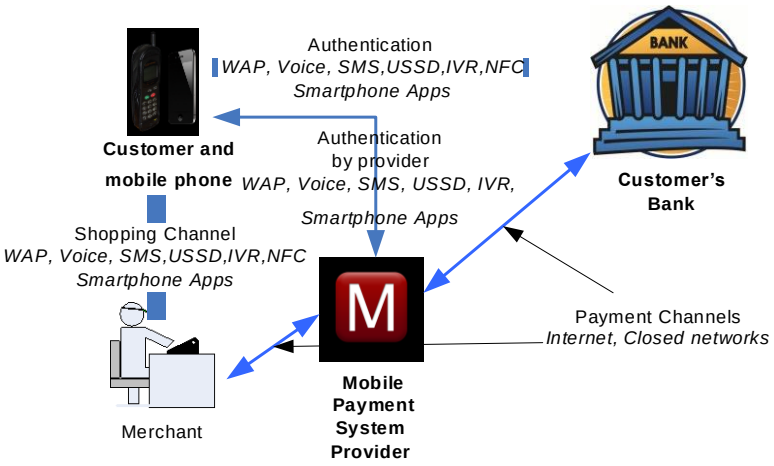
Notwithstanding the above reporting requirements, the mobile service provider shall be required to submit any *adhoc* data specified by the Bank from time to time in the performance of its oversight role.

Annex 3 : Overview of the Mobile Banking and Mobile Payment Service Providers Models

An overview of the bank-led mobile banking and mobile payment model as well as the non-bank led mobile payment model is provided hereunder. **Both models are solely for the purposes of illustration and are not prescriptive.**

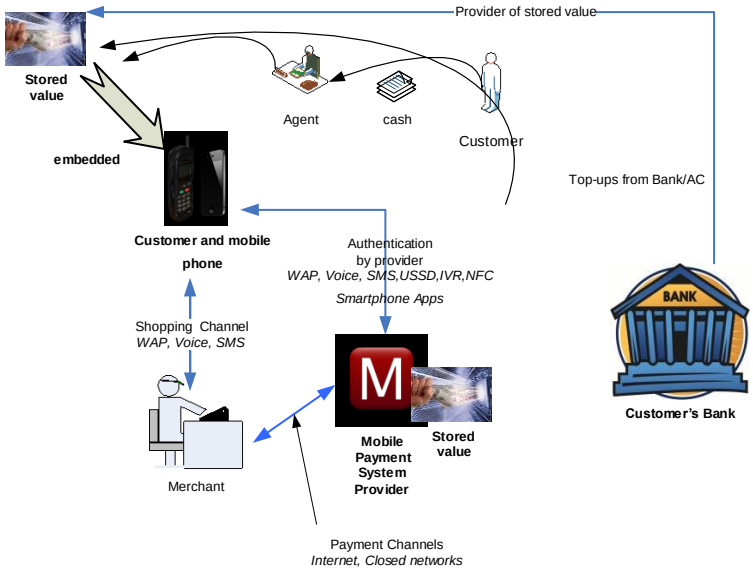
I. Bank-led mobile banking and payment model

In bank-based mobile banking and payment model, customers have direct contractual relationships with a bank which is licensed and supervised by the Bank. In this model, the financial institution may provide information services, bank account information, fund transfers, airtime purchase as well as payment services to its customers via mobile communication device.



II. Non-bank led mobile payment model

In this model, the customers need not have a direct contractual relationship with a bank which is licensed and supervised by the Bank. The service provider, subject to the authorisation of the Bank, takes the lead and creates a stored value account. Customers transfer funds into these accounts for the purpose of making periodic or frequent payments by means of cash at a retail agent.



ACRONYMS

AES	Advanced Encryption Standard
Bank	Bank of Mauritius
CDMA	Code Division Multiple Access
DES	Data Encryption Standards
DoS	Denial of Service
DR	Disaster Recovery
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 Technologies
IDS	Intrusion Detection System
IVR	Integrated Voice Recognition
KYC	Know Your Customer
ICTA	Information & Communication Technologies Authority
MACSS	Mauritius Automated Clearing and Settlement System
NFC	Near Field Communication
PIN	Personal Identification Number
PLMN	Public Land Mobile Network
SMS	Short Message Service
USSD	Unstructured Supplementary Service Data