

## **DRAFT**

*Please send your comments on or before 18<sup>th</sup> October 2010 to Director  
Payments and Settlements at psd@cbsl.lk*

### **Mobile Payments Guidelines No. 1 of 2010**

#### **1. Introduction**

1.1 The guidelines are issued with the objective of promoting safety and effectiveness of mobile payment schemes and thereby enhancing user confidence of such schemes.

1.2 Under the Payment and Settlement Systems Act No.28 of 2005 (PSSA), the Central Bank of Sri Lanka (CBSL) is empowered to formulate, adopt and monitor the implementation of a payment system policy for Sri Lanka. Such policy is designed to facilitate the overall stability of the financial system, promote payment system safety, efficiency and control risk. Considering the necessity of improving the electronic payment mechanisms in the country with a view to protect the customers, and being guided by the international standards and best practices, on 31 July 2009 Service Providers of Payment Cards regulations No.1 of 2009 (hereinafter referred to as "Regulations") were issued. Acting in pursuance of regulation 21 of the said Regulations, these Mobile Payment Guidelines are issued to regulate the mobile payment industry. These guidelines outline broad principles and standards to be followed by mobile payment service providers and will come in to force with immediate effect.

1.3 Mobile payments may be executed under two systems.

#### **A Customer Account Based System**

- a. Subject to the section c. below, no person other than a Licensed Commercial Bank (LCB), a Licensed Specialized Bank (LSB) or a Registered Finance Company (RFC) licensed under the

Regulations shall operate customer account based mobile payment service. The Customer Account Based System is based on the customer accounts maintained by such financial institutions from which the service can only be offered to account holders. Under this system, account holders are able to operate their own accounts via mobile phones to debit/credit their own accounts or credit accounts of third parties within the same financial institution or across the banking system depending on the regulations/guidelines applicable for such institutions.

- b. This system may offer two types of facilities to customers, namely;
  - i. The basic level;  
Information on balance inquiry, credit/debit status and other information on banking services, which do not relate to fund transfers.
  - ii. The standard level;  
Actual payment services in the nature of fund transactions such as payments, transfers and stop payments etc.
  
- c. Unless otherwise expressly provided herein, in the case of Customer Account Based System, these Guidelines shall apply only to standard level services of mobile payments, provided that basic level services are mentioned specifically as and when required. Financial institutions that provide basic level services of mobile payments are exempted from obtaining licence under these Regulations provided that such financial institutions adhere to the relevant provisions in the Banking Act No.30 of 1988 or the Finance Companies Act No.78 of 1988, as the case may be, and any other legal provisions in operation in this regard.

## **B Custodian Account Based System**

Custodian Account Based System may be operated by non-bank service providers licensed under the Regulations to operate as mobile payment service providers. Under the custodian account based system, service providers may open e-money account for each customer and issue e-money by accepting physical money from the customer. Such non-bank service providers shall operate a custodian account/s with LCB/s and are required to deposit all the funds collected from customers in such account/s and shall maintain the cumulative sum collected from all mobile account holders in the custodian account/s at all times.

## **2. Regulatory Provisions**

- 2.1 Mobile payment services shall be in Sri Lanka Rupees and used only for domestic transactions.
- 2.2 Mobile payment services shall be provided only for Sri Lankan individuals who are above 18 years of age.
- 2.3 Mobile Payment Service Providers (MPSP) shall ensure that they adhere to all applicable laws and regulations, in offering products and services, upgrading and introducing new technologies and software/ hardware to the system.
- 2.4 MPSPs shall adhere to all guidelines issued by any competent authority on customer due diligence

## **3. Marketing of the Mobile Payment Services**

MPSPs shall ensure that marketing strategies of their services including any outsourced functions are designed in accordance with the following guidelines.

- 3.1 Staff assigned to promote or sell mobile payment services shall disclose the official identity card issued by the MPSP at all times when conducting promotional campaigns to the public and during meeting with customers.
- 3.2 Every MPSP shall communicate to its customers in writing or in electronic form clearly and unambiguously regarding the benefits, incentives and rewards of any mobile payment service or reduction of any charges/fees applicable for such service offered by the MPSP in customer preferred language.
- 3.3 Every MPSP shall disclose its own code of conduct/public policy on the operations of mobile payments to customers throughout the marketing process and the same shall be published in their own official websites.
- 3.4 Staff assigned to promote or sell mobile payment services of the MPSP shall provide complete information on mobile payment operations to the public and shall not make false representation on any service/facility, which the MPSP is unable to offer.
- 3.5 MPSP shall not publish/convey misleading and unethical information about its products and services.
- 3.6 MPSP shall not engage in aggressive and hard selling marketing practices during working/office hours or inconvenient hours for customers, except with prior appointments.
- 3.7 MPSP shall seek prior consent of customers when introducing any new chargeable products and/or services.

3.8 Regular training and awareness sessions shall be conducted by MPSPs for their marketing personnel covering all aspects of mobile payment operations including charges/penalties to be paid by the customers, safety measures, disputes resolution mechanism etc.

#### **4. Eligibility and Registration of Customers for Mobile Payments**

- 4.1 Financial institutions shall offer customer account based mobile payment services on real time basis for the purpose of transferring funds within the same financial institution and/or across the banking system by debiting/crediting the respective accounts.
- 4.2 MPSPs operating Custodian Account Based System may accept funds from e-money holders directly or via appointed merchants and shall make top-ups to relevant e-money accounts immediately, upon receipt of funds.
- 4.3 MPSP shall have one time registration procedure to be followed through signed documents when registering customers. However, in an event where civil status of a customer is changed, re-registration shall be carried out, terminating the existing registration.
- 4.4 The MPSP and the customer shall enter into an agreement in duplicate in the preferred language of the customer, at the time of registration.
- 4.5 A copy of the agreement signed between the MPSP and the customer at the time of registration has to be provided to the customer and such agreements shall be protected by the MPSPs, to ensure access to such documents at any given time.

## **5. Arrangements for Operations of Custodian Based Account System**

- 5.1 The MPSP shall open a custodian account at a LCB and shall deposit funds collected from customers in exchange of e-money in this account. An agreement shall be signed between the MPSP and the custodian bank to operate such accounts.
- 5.2 LCBs maintaining Custodian Account Based System shall ensure that the funds lying in the custodian account shall be blocked in the case of bankruptcy/close of the business of the mobile service provider.
- 5.3 The MPSP operating the Custodian Account based system shall have no claim to the funds lying in the Custodian Account in the case of bankruptcy/close of MPSP.
- 5.4 The LCB maintaining the custodian account shall be responsible for the following:
  - a. Ensure adherence of the MPSP to the KYC procedure;
  - b. Repaying of balances in each mobile account to e-money holder in the event of a disruption/closure of the agent's operations;
  - c. Ensuring the MPSPs responsibility of monitoring and supervising the activities of the appointed merchants to ensure that they will not engage in any unauthorized activities other than the permitted services.
  - d. Monitoring of all transactions made by MPSP with the Custodian Account at predefined periods of time and reporting to DBS at CBSL as per regulations applicable to a regular bank account;
  - e. Reconciliation of funds held in the Custodian Account with the cumulative values of all the mobile accounts issued by the MPSP. Any discrepancy between the accounts of the MPSP and the Custodian Account shall be reconciled and cleared within 7 days. Discrepancies

that cannot be cleared within this period shall be reported to CBSL for information with the steps taken to resolve the issue ;

- f. Ensuring that MPSP shall report any suspicious transactions of e-money holders based on the guidelines of the Financial Intelligence Unit established in terms of the Financial Transactions Reporting Act, No. 6 of 2006 (FTRA);
- g. Carrying out regular audits of all mobile accounts with the MPSP.
- h. Monitoring of MPSP for compliance with banking regulations, guidelines of the proposed solution and any other requirements imposed by CBSL at the time of approval or changes thereafter;
- i. Adhering to the reporting requirements of CBSL.
- j. Reporting the deposits in the custodian accounts as part of the deposit liabilities of the bank

5.5 When an application is submitted to obtain the licence to carryout mobile payment service, each MPSP shall submit a letter from the respective custodian bank, with an undertaking that the Custodian Bank agrees to fulfill the conditions and discharge all responsibilities given in the Section 5.4.

5.6 Individual stored value limits, transaction limits and merchant's limits shall be decided by CBSL at the time of granting approval to the MPSP, based on their risk appetite. Any subsequent amendments to such limit shall be made only with the approval of CBSL.

5.7 A mobile account holder may, during the period of validity, request the operator to redeem the remaining amount of e-money available in his mobile account. In such events, redemption shall be made without any additional cost other than what is necessary to complete the transaction, within three business days from the date the claim is made.

- 5.8 Notwithstanding anything contrary to this guideline the Custodian Bank may be authorized to invest funds in the custodian account in an interest bearing account. However, MPSP shall not have access to funds in the custodian account and MPSP shall not use funds in the custodian account as security or collateral at any time.
- 5.9 Custodian Bank may open an interest bearing custodian account for the MPSP. However, the interest earned through the custodian account shall be maintained in a separate account.
- 5.10 The MPSP shall not:-
- a. grant any form of credit to mobile account holder;
  - b. pay interest or profit on the mobile account balances or anything else that would add to the monetary value of the e-money;
  - c. issue e-money at a discount, i.e. provide e-money that has a monetary value greater than the sum received; and
  - d. any other facility that exceeds the monetary value of the deposit made by the e-money holder.
- 5.11 For the purpose of Custodian Account Based System the MPSP should establish adequate operational arrangements to mitigate operational risks of the respective e-money scheme. Such arrangements shall include but not limited to;
- a. measures taken to ensure safety, security and operational reliability of the e-money including contingency arrangements;
  - b. maintenance of a separate set of records and accounts for its e-money activities excluding any other business activities;
  - c. provisioning of adequate internal controls for systems and personnel administration;

- d. provisioning of a robust clearing and settlement arrangements to ensure that the system will operate in an efficient, reliable and secure manner
- e. maintenance of adequate information and accurate accounting for the purpose of proper reconciliation process and accounting treatment for e-money transactions.

5.12 All foreign inward remittances to the mobile accounts shall be routed through the respective custodian bank/s and credited in LKR, in compliance with existing regulations/procedures.

5.13 MPSP shall open and maintain separate account for each mobile account holder and a statement of the mobile account shall be made available to the mobile account holder electronically or in a print form periodically or upon request.

5.14 MPSP shall sign agreements with merchants authorized to accept funds on behalf of the MPSP for the purpose of adding monetary value to mobile accounts. All duties, responsibilities and procedures to be followed by such merchants shall be specified in the respective agreements.

## **6. General Rules and Conditions for MPSPs**

6.1 MPSPs shall provide the terms and conditions applicable for the utilization of e-money in an appropriate manner in websites, brochures and registration forms. The terms and conditions applicable for the use of e-money should be unambiguous and available in customer preferred language.

The terms and conditions shall consist of following, inter alia

- a. Authorized types of payments with e-money;
- b. Rights and responsibilities of mobile account holders and merchants;

- c. All applicable fees and charges;
- d. Procedure for reporting lost or stolen e-money instruments, provisions of dispute resolution, rules and responsibilities;
- e. Right to redeem unused e-money including conditions, procedures, time frame and applicable fees;
- f. Customer service contact numbers

6.2 MPSP shall ensure that terms and conditions on mobile payment operations shall not vary, amend or modify in any manner except by a prior written notice in preferred language to mobile account holders through appropriate communication media.

6.3 MPSPs shall use their best endeavours to use methods consistent with industry best practices to authenticate user identity.

6.4 MPSPs shall provide controls that allow mobile account holders the ability to receive payment alerts and notices in accordance with their preference.

6.5 An appropriate complaint resolution mechanism shall be developed by MPSPs for handling of disputed payments, transactions and loss of e-money instrument (mobile instrument). MPSPs shall establish a call centre to respond to customer inquiries and complaints on 24x7 basis. Each complaint received shall be provided with a reference number and shall be resolved within 3 business days.

6.6 MPSPs shall educate mobile account holders on applying security features and capabilities and the importance of protecting their personal information.

6.7 MPSPs shall implement a robust security risk management framework to actively identify, assess, reduce and monitor security risk.

The security system shall ensure;

- a. Confidentiality of the sensitive information. All confidential information shall be maintained in a secured manner and protected from unauthorized viewing or modification during transmission and storage;
- b. Accuracy, reliability and completeness of information processed, stored or transmitted;
- c. Proper authentication of users and merchants in the e-money system.

6.8 In providing mobile payment services, MPSPs shall take all necessary steps to address, mitigate or eliminate merchant-related credit risks, operational risks, legal risks, liquidity risks and reputational risks and risks relating to the safety of funds collected from customers in exchange for e-money.

6.9 MPSPs shall maintain a standard business continuity and disaster recovery procedure. In the event of any disaster or operational failure, the disaster recovery site shall be capable to take over the operations without causing any inconvenience to mobile account holders.

6.10 MPSPs shall adhere to the technological guidelines in annex 1 hereto.

## **7. Interpretation**

In these guidelines unless the context otherwise requires:

- (a) “Customer” shall mean account holders or e money holders
- (b) “Custodian Bank” shall mean commercial banks who appoint agents in terms section 12 A of the Banking Act.
- (c) “E-money” shall mean the monetary values stored in devices for mobile payments

- (d) “Financial Institutions” shall mean licensed commercial banks, licensed specialized banks and registered finance companies that operate account based systems
- (e) “Licensed Commercial Bank” and “Licensed Specialized Bank” shall mean licensed commercial bank and licensed specialized bank within the meaning of the Banking Act, No 30 of 1988
- (f) “Merchants” shall mean the institutions/persons appointed by MPSPs to facilitate the Mobile Payment Systems.
- (g) “Mobile Account” shall mean Individual Accounts maintained by non-bank service providers under the Custodian Account Based System
- (h) “Mobile payments” means the payments that can be made using any mobile phones device.
- (i) “MPSPs” shall mean Mobile Payment Service Providers
- (j) “Non Bank Service Providers” shall mean public companies other than LCBs, LSBs and RFCs eligible to apply for a licence to operate as a service providers of payment cards
- (k) “Registered Finance Companies” shall mean finance companies registered in terms of the Finance Companies Act No 78 of 1988

-----<<◇>>-----

## **Annex 1**

### **Technology guidelines for Banks and Mobile service providers**

#### **1. Technology constraints, security issues, principles and practices**

Mobile users/customers can face security issues and poor quality services while making mobile payments due to certain technological constraints and characteristics of wireless technologies, which should be minimized to avoid any negative impact on customers and the financial system. Therefore, MPSPs must implement adequate security measures and install reliable systems that address risks, threats and ensure a higher quality of service, regardless of the underlying network and carrier infrastructure used in delivering their services.

Given the dynamic nature and magnitude of security threats in the wireless environment, MPSPs shall perform periodic independent security vulnerability assessments and reviews of their systems which should be carried out before launching new products/services. Subsequent updates and reviews should also be carried out regularly. To facilitate such reviews, security architecture information should be documented and updated regularly.

The technology used for mobile payments must be secure and should ensure confidentiality, integrity, authenticity and non-repudiability. Accordingly,

- Information Security Policy of the MPSP may be suitably updated and enforced to address the security controls required specially for mobile phone based delivery channels
- MPSP shall evaluate service delivery channels in terms of security and risks involved and offer appropriate services, mitigating risks involved.

##### **1.1 Authentication and non-repudiation.**

The following guidelines with respect to authentication and ensuring of non-repudiation should be adhered to:

- When customers are required to provide their passwords or PINs for banking services, these should be encrypted immediately at the point of entry. No sensitive data should be allowed to be displayed as clear text on the mobile screen
- Authentication methods based on more than one factor should be implemented to validate the transactions where, appropriate
- Ensure that encrypted and authenticated sessions remain intact throughout the duration of communications with the customers
- Authentication processes should be repeated after session failures and subsequent resumptions
- Details of all transactions, including those that are incomplete or aborted, should be logged and such logs should be reviewed daily for abnormality or aberrations that might constitute security breaches.

## **1.2 PIN security**

Security in mobile payment schemes shall prevent misuse and eliminate fraud by unauthorized users. In cases of direct access to bank accounts through the mobile channel, a high level of security is required.

The banks shall issue a new mobile pin (mPIN) to facilitate the mobile payments and such PINs may be issued and authenticated by the bank or by the MPSP appointed by the bank. Banks and the various service providers involved in mobile payments should comply with the industry accepted security principles and practices with respect to issuance and usage of the mPIN.

In case of non-mobile network operator based mobile proximity/contactless payments, a second factor authentication shall be used along with mPIN. It is suggested that either card number or OTP (one time passwords) be used as the second factor authentication rather than the mobile phone number.

### **1.3 Cryptographic key management**

Proper key management is vital for the effective use of cryptography and digital certificates. MPSP must establish adequate control measures and procedures to enable crypto keys to be created, stored, distributed, replaced, revoked or destroyed, securely. Periodic audits and compliance reviews should be carried out to maintain a high degree of confidence in relevant security procedures.

### **1.4 Network and System Security**

The following guidelines with respect to network communications and system security should be adhered to:

- Use strong encryption standards for protecting sensitive and confidential information of the bank and customers while in transit
- Establish proper information protection systems and incident response procedures
- Conduct periodic risk management analysis and security vulnerability assessment of the related systems and networks
- Maintain proper and regularly updated documentation of security practices, guidelines, methods and procedures used in mobile payments and payment systems based on the risk management analysis and vulnerability assessment carried out
- Implement appropriate physical security measures to protect the system gateways, network equipment, servers, host computers, and other hardware/software used from unauthorized access and tampering. The data centre of the bank and service providers should have proper wired and wireless data network protection mechanisms.

## **1.5 Transaction Logs**

Mobile banking and payment systems should maintain detailed transaction logs to enable processing audit trails to be reconstructed in the event of any disputes or errors. The retention period of logs should be .....years in duration. The MPSPs shall ensure that such information is protected from any loss or damage. Security safeguards should also be implemented to protect the information from unauthorised modification or destruction.

## **1.6 Data Confidentiality and Integrity**

The following guidelines with respect to data confidentiality and integrity should be adhered to:

- End-to-end application layer encryption of sensitive customer details and authentication data such as PINs should be implemented to ensure keeping intact such data from the data-entry device right through to the host end
- Software for wireless applications should implement adequate measures to avoid duplicate transactions resulting from intra-session delays or session failures when customers move from areas with good wireless coverage to those where coverage is poor
- MPSPs should install adequate security measures, firewalls, intrusion detection/prevention systems, surveillance control procedures to ensure capability for immediate recovery. They should also implement integrity checks on systems, files and code, to ensure the reliability of systems. All changes to such systems should be properly authorized.

## **1.7 System Availability and Recoverability**

MPSPs shall ensure that proper recovery and back-up plans are in place to minimize disruption to services due to system failures. Such plans shall cater for single points of failure to ensure speedy recoverability and an acceptable level of high system availability. Mobile traffic and system capacity should be closely monitored to ensure that any service degradation due to capacity problems are addressed in a timely manner.

## **1.8 Inter-operability**

When a bank offers mobile payment services, it may be ensured that customers having mobile phones of any network operator should be in a position to request for such services. To ensure inter-operability between banks and their MPSPs, it is recommended that banks adopt the standard message formats available.

## **2. Other related guidelines**

MPSPs should also be mindful of the following:

### **Security related practices**

- The opening up of banking systems to MPSPs to facilitate mobile payment services may place knowledge of bank systems and customers in a public domain. Therefore, it is imperative that sensitive customer data, and security and integrity of transactions are protected
- The mobile payment servers at the bank's end or at the MPSP's end, if any, should be certified appropriately in compliance with each bank's security guidelines. In addition, banks should conduct regular information security audits

on all systems used for mobile payments to ensure full compliance with such security guidelines

- It is recommended that for channels which do not contain the phone number as an identity, a separate login ID and password be provided which is different from the internet banking ID. Banks are required to implement appropriate risk mitigation measures such as transaction limits (per transaction, daily, weekly, monthly), transaction velocity limits, fraud checks, AML checks etc., depending on the bank's own risk perception, unless otherwise mandated by the CBSL.

## **2.2 Minimizing financial losses from a lost/stolen phone**

- Strengthen security measures to prevent criminal activity while using Near Field Communication (NFC) based mobile payment systems. Action to prevent criminals abusing new mobile phone technology, which allows the mobile to be used like debit/ credit and pre-paid stored value cards, must be agreed by all stakeholders
- Request a PIN verification for transactions over Rs..... - any transaction above the maximum contactless payment value will require additional security measures/verification, such as a PIN code. This shall also be applicable if more than a certain number of low-value transactions are carried out consecutively in quick succession
- Ensure that contactless payment functions, SIM cards and phone will be disabled within..... hours once a mobile phone equipped with payment technology is reported lost or stolen. Any installed financial applications should also be disabled.

## **Customer Education**

- Ensure that the PIN request is activated in customers' mobile phone. The PIN code should also be changed immediately after a new mobile phone is purchased
- Customers should be educated on how to maintain PIN safety and not reveal their PINs to another party
- On some mobile phone units, PINs entered may be recalled through redial menus. Instructions should be given to customers to erase PINs immediately from the phone memory to prevent PIN discovery by accessing previously dialed numbers
- Customers should be advised not to use the same PIN for different delivery channels or systems as they have different security levels and implications depending on the security risks attached to each of them
- Ensure that customers refrain from saving any confidential information such as passwords, credit card, bank card PINs etc. in mobile phones. Customers shall also be advised to delete such information when the phone is sold or given away
- Advise customer to keep the mobile phone's IMEI code in a separate place in case the mobile phone gets lost. Customers can prevent making of unauthorised payments using their lost/stolen mobile phone, by reporting the phone's IMEI code to the mobile network operator
- MPSPs shall provide clear configuration instructions if their customers are required to manually configure their own mobile phones to access mobile banking and payment services.
- Advise customers to take extra precautions when using mobile banking and payment services.

- Customers should be educated to enable them to safely check the authenticity of the established connection, before making any payment.
- Provide advice to customers on dispute handling, reporting procedures and the expected time for resolution.
- Avoid use of complex, legal and technical jargon in communications with customers.