Mobile Payments Guidelines No. 2 of 2011
for Custodian Account Based Mobile Payment Services

1. Introduction

1.1 The Central Bank of Sri Lanka (CBSL), with a view of facilitating the development of emerging electronic payment mechanisms whilst promoting safety, efficiency and reliability of such mechanisms, has been engaged in providing guidance through building up a regulatory framework for innovative payment systems. Accordingly, in the context of the financial industry exploring and introducing mobile phone based payment applications, CBSL, as the initial step of regularizing the mobile phone based payment systems, issued Mobile Payments Guidelines No. 1 of 2011 for the Bank-led Mobile Payment Services to be complied by banks operating mobile payment systems. As a further measure to broaden the regulatory framework relating to mobile phone based payments and provide guidance to service providers operating custodian account based mobile payment systems, these guidelines are issued by the CBSL to be adhered to, by such service providers.

1.2 Under the Payment and Settlement Systems Act No. 28 of 2005 (PSSA), the CBSL is empowered to formulate, adopt and monitor the implementation of a payment system policy for Sri Lanka, to facilitate the overall stability of the financial system, promote payment system safety, efficiency and control risk. In order to protect the interests of the customers and service providers involved in electronic payment mechanisms and being guided by the international best practices, Service Providers of Payment Cards Regulations No.1 of 2009 (hereinafter referred to as "Regulations") were issued on 31 July 2009. In accordance with the regulation 21 of the said Regulations, these guidelines are issued to outline broad principles and standards for service providers offering custodian account based mobile payment services and will come in to force with immediate effect.

1.3 Custodian account based mobile payment services shall be operated only by service providers licensed under the Regulations to function as service providers of payment cards. Under the custodian account based system, licensed service providers may issue e-money by accepting physical money from customers/merchants. On the other hand, licensed service providers operating custodian account based mobile payment systems may convert e-money into physical money for e-money holders (cash-outs) on their request, directly or through appointed merchants. Based on the transactions made by customers and merchants, it is mandatory that the e-money accounts are updated on real-time basis. Licensed service providers operating custodian account based mobile payment systems shall operate a custodian account/s with Licensed Commercial Bank (LCB)/s and shall maintain the cumulative sum collected from all e-money account holders in the custodian account/s at all times.

2. Regulatory and Supervisory Provisions

2.1 Licensed service providers operating custodian account based mobile payment systems are responsible to ensure compliance to these guidelines.

2.2 Mobile payment services shall be in Sri Lanka Rupees and used only for domestic transactions.

2.3 Mobile payment services shall be provided only for Residents of Sri Lanka who are above 18 years of age.

2.4 Licensed service providers shall ensure that they adhere to all applicable laws and regulations, including but not limited to, Payment and Settlement Systems Act No. 28 of 2005, Financial Transactions Reporting Act No. 6 of 2006, Electronic Transactions Act No. 19 of 2006 and Exchange Control Act No. 24 of 1953, in offering mobile payment services, introducing new technologies and upgrading software/ hardware systems.

2.5 Licensed service providers shall adhere to guidelines on 'Know Your Customer' (KYC) and 'Customer Due Diligence' (CDD) as part of effective Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT). Licensed service providers shall

restrict provisioning of e-money services only to customers who comply with KYC and CDD requirements.

3. Registration of Customers for E-money Services

3.1 Licensed service providers shall have a formal system for registration of customers before providing e-money services and registration of customers shall be carried out through signed documents.

3.2 Licensed service providers shall have one time registration procedure. However, in an event where the customer requests to change his/her mobile number or registered name, producing supportive documents, re-registration should be carried out, terminating the existing registration. If the customer requests for any other data modification with supportive documents, as and where applicable, details of the existing customer account shall be updated.

3.3 Licensed service providers shall enter into agreements with each customer in duplicate, in any of the three languages (Sinhala, Tamil or English) as preferred by the customer, at the time of registration. A copy of the agreement has to be provided to the customer and such agreement shall be protected by service providers at all times.

4. Technology and Information Security Standards

4.1 The technology used for supplying payment service facilities must be safe and secure and shall ensure confidentiality, integrity, authenticity and non-repudiation of the payment related information.

4.2 Licensed service providers shall update and implement the information security policy to adequately address the security requirements of the mobile phone based delivery channels.

4.3 An illustrative but not exhaustive technology framework is given in Annex 1.

5 Operations of the Custodian Account Based System

5.1 Licensed service providers operating custodian account based mobile payment systems shall ensure that customers are notified, on real-time basis, of top-ups made to e-money accounts, cash-outs made from e-money accounts and any other transaction which increases/decreases the value of e-money stored in their accounts.

5.2 Licensed service provider shall open and maintain separate e-money accounts for each customer and a statement of the e-money account shall be made available to the customer electronically or in a print form periodically or upon request.

5.3 The licensed service provider shall not:-

a. grant any form of credit to e-money holder;
b. pay interest or profit on the e-money account balances that would add to the monetary value of 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.

5.4 Individual stored value limits, transaction limits, Merchant's limits and day limits shall be decided with the approval of the CBSL. Any subsequent amendments to such limits shall also be made only with the approval of the CBSL.

5.5 If an e-money holder requires to close his/her e-money account, the licensed service provider shall inform the e-money holder to make a request in writing to redeem the remaining amount of e-money available in his/her e-money account. In such events, redemption shall be made no later than three business days from the date the claim is made, without any additional cost other than what is necessary to complete the transaction. The e-money holder shall be notified with written confirmation by the licensed service provider, after the completion of the process of closing the e-money account.

5.6 In the case of a mobile network operator being licensed under the Regulations as a licensed service provider to operate a custodian account based mobile payment system, such licensed service provider shall ensure that the mobile accounts and e-money accounts of customers are maintained separately. The monetary value of the air time stored in the mobile account is not permitted to be transferred to the e-money account. However, the customer may purchase air time using the balance in the e- money account.

5.7 The licensed service provider operating custodian account based system shall be responsible for the following:

a. Strictly adhere to the KYC and CDD procedures in registering customers and maintaining customer accounts;
b. Monitor and supervise the activities of e-money holders and merchants to ensure that they only engage in permitted services;
c. Submit periodic reports and provide access to the e-money system, as and when requested by the custodian bank, in order to monitor balances and activities of e-money holders;
d. Report to the custodian bank of any suspicious transactions as per the regulations issued by the Financial Intelligence Unit (FIU) established in terms of the Financial Transactions Reporting Act, No. 6 of 2006 (FTRA);
e. Comply to any direction issued by the CBSL and adhere to reporting requirements imposed by the CBSL with regard to the custodian account based system;
f. Handle disputes of all customers and merchants according to the guidelines applicable to the custodian account based system.

6. Arrangements for Maintaining the Custodian Account

6.1 Licensed service providers operating custodian account based mobile payment systems shall open a custodian account/s at a LCB/s and shall deposit funds collected from e-money holders in exchange of e-money, in this account. An agreement including inter alia, the responsibilities given in section 5.7 and 6.2 in these guidelines, shall be signed by the licensed service provider with the custodian bank to ensure that the fund

movements of the system are transparent. However, when a licensed service provider opens multiple custodian accounts with more than one LCB, the licensed service provider shall clearly define the set of e-money accounts related to each custodian account, and such information shall also be provided to the relevant custodian bank.

6.2 The custodian bank shall be responsible for the following:

a. Formulating the KYC and CDD procedures to be adopted by the service provider and ensure the compliance by the service provider;
b. Ensuring the licensed service provider's 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;
c. Monitoring of all transactions made by licensed service provider with the custodian account at predefined periods of time and reporting to the CBSL as per regulations applicable to a regular bank account;
d. Reconciliation of funds held in the custodian account with the cumulative values of all e-money accounts issued by the licensed service provider. Any discrepancy between the e-money accounts and the custodian account shall be reconciled and cleared within 7 days. Discrepancies that cannot be cleared within this period shall be reported to the CBSL for information. However, the custodian bank shall have a mechanism to resolve those discrepancies within a reasonable time;
e. Ensuring that the licensed service provider shall report any suspicious transactions of e-money holders based on the guidelines issued by the FIU established in terms of the FTRA and report such transactions to the FIU as specified by the same Act;
f. Carrying out regular audits of all e-money accounts with the licensed service provider;
g. Monitoring of licensed service provider for compliance with regulations, guidelines of the proposed solution and any other requirements imposed by the CBSL at the time of approval or changes made thereafter;
h. Adhering to the reporting requirements of the CBSL;
i. Reporting the deposits in the custodian accounts as part of the deposit liabilities of the bank;

j. Formulating a proper mechanism for customer protection in the event of a disruption/closure of the licensed service provider's operations.

6.3 When an application is submitted to obtain the licence to carryout mobile payment services, a letter from the respective custodian bank/s has to be submitted with an undertaking that the custodian bank agrees to fulfill the conditions and discharge all responsibilities given in the Section 6.2 above.

6.4 Notwithstanding anything contrary to these guidelines, the custodian bank may be authorized to invest funds in the custodian account, in an interest bearing account. However, licensed service provider shall not have access to funds in the custodian account and shall not use funds in the custodian account as security or collateral at any time.

6.5 Custodian bank may open an interest bearing custodian account for the licensed service provider. However, the interest earned through the custodian account shall be credited to a separate account.

6.6 The licensed service provider and the custodian bank shall ensure that credits/debits to the custodian account are made only to effect changes in the cumulative sum of e-money in the mobile payment system.

6.7 Licensed service providers shall identify dormant e-money accounts and report the amount to be set aside as the dormant deposit from the custodian account with individual e-money holder details to the custodian bank. The custodian bank/s shall report such deposits as per Banking Act Directions No. 5 of 2009 on identifying, reporting, transferring and maintaining abandoned property of LCBs, issued on 02 September, 2009.

6.8 Custodian banks shall ensure that the funds lying in the custodian account shall be blocked in the case of bankruptcy/close of the business of the licensed service provider.

6.9 The licensed service provider 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 business of the licensed service provider.

7. Appointing Merchants

7.1 Licensed service providers may appoint merchants to perform authorized functions related to mobile phone based payments.

7.2 Licensed service provider shall sign agreements with merchants authorized to accept funds and make cash-outs on behalf of the licensed service provider for the purpose of adding/deducting monetary value to/from e-money accounts. All duties, responsibilities and procedures to be followed by such merchants shall be specified in the respective agreements.

7.3 The licensed service provider operating custodian account based system shall be responsible to perform CDD when registering merchants.

7.4 In providing e-money services, licensed service providers shall take all necessary steps to address, mitigate or eliminate merchant-related risks i.e. credit risks, operational risks, legal risks, liquidity risks, reputational risks and risks relating to the safety of funds collected from customers.

8. Customer Protection

8.1 Licensed service providers shall provide the terms and conditions applicable for the utilization of e-money services in an appropriate manner in websites, brochures and registration forms. These terms and conditions should be unambiguous and available in any of the three languages (Sinhala, Tamil or English) as preferred by the customer and shall consist of following, inter alia,

a. Authorized types of payments;

b. Rights and responsibilities of licensed service provider, e-money holder and merchants with regard to e-money services;

c. All applicable fees and charges;

d. Benefits, incentives and rewards of e-money services;

e. Provisions for dispute resolution;

f. Procedure for reporting lost or stolen mobile phones;

g. Procedure for stop payments;

h. Customer service contact numbers.

8.2 Licensed service providers shall ensure that terms and conditions on e-money services shall not vary, amend or modify in any manner except by a prior written notice to the customers, through appropriate communication media, in any of the three languages (Sinhala, Tamil or English) as preferred by the customers.

8.3 Licensed service providers shall maintain the confidentiality of customer information and shall be responsible to ensure that their service providers will also treat customer information as confidential.

8.4 Licensed service providers shall enter into commercial contracts with service providers, in addition to the agreements with e-money holders who subscribe for e-money services. The rights and obligations of each party shall be made clear through these contracts and shall be valid and enforceable in a court of law.

8.5 Licensed service providers shall adhere to the laws and regulations applicable to the security procedure adopted to authenticate users as a substitute for signature, when providing e-money services to e-money holders.

9. Customer Education, Grievance and Redress Mechanism

9.1 Licensed service providers shall educate customers on applying security features and capabilities and the importance of protecting their personal information.

9.2 An appropriate dispute resolution mechanism shall be developed by licensed service providers for handling of disputed payments, transactions and loss of mobile phones.

Licensed service providers shall establish a call centre to respond to customer inquiries and complaints. Each complaint received shall be provided with a reference number and shall be resolved within 3 business days.

9.3 Licensed service providers shall be responsible to address the customer grievances in an event where a customer files a complaint on a disputed transaction. Chargeback procedures for addressing such customer grievances may be formulated by licensed service providers.

10. General Rules and Conditions

10.1 Licensed service providers which intend to operate custodian account based mobile payment systems shall obtain the approval of their respective Boards before offering services to customers. The Board approval shall document the extent of operational and fraud risk assumed by the licensed service provider and the processes and policies designed to mitigate such risks.

10.2 Licensed service providers shall ensure that a consistent notice is displayed in every service outlet, indicating regulatory powers delegated to the merchant and operational instructions for the e-money holders.

10.3 Licensed service providers shall use their best endeavours to use methods consistent with industry best practices to authenticate user identity.

10.4 Licensed service providers shall provide controls that allow customers the ability to receive payment alerts and notifications in accordance with their preference.

10.5 The licensed service provider shall 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 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 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.

10.6 Licensed service providers 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 agents;
d. Proper authorization of functions performed by users and agents.

10.7 Licensed service providers 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 customers. The business continuity plan and disaster recovery site shall be tested and reviewed periodically.

11. Interpretation

In these guidelines unless the context otherwise requires:

a. “Cash-outs” shall mean the process of converting e-money into physical money and issuing to e-money holders;
b. "CDD" means ongoing scrutiny of any transaction undertaken throughout the course of the business relationship with a customer to ensure that any transaction

that is being conducted is consistent with the institution's knowledge of the customer and the customer's business and risk profile etc.;

c. "Custodian Bank" shall mean LCBs which maintain custodian accounts on behalf of licensed service providers;
d. "Customer" shall mean e-money holders;
e. "E-money" shall mean the monetary values stored in the e-money accounts of individuals, to be utilized through the mobile devices for mobile payments;
f. "E-money Account" shall mean individual accounts maintained by licensed service providers under the custodian account based system;
g. "KYC procedure" shall mean the procedure to be followed in accordance with the Financial Transactions Reporting Act No. 6 of 2006;
h. "Licensed Commercial Bank" shall mean licensed commercial bank within the meaning of the Banking Act, No. 30 of 1988;
i. "Licensed Service Provider" shall mean a mobile payment service provider licensed under the Service Providers of Payment Cards Regulations No.1 of 2009;
j. "Merchants" shall mean the institutions/persons appointed by licensed service providers to carryout mobile payment services;
k. "Mobile payments" mean financial transactions effected based on information exchanged through the use of mobile phones;
l. "Service Providers" shall mean mobile payment solution providers and relevant mobile network operators;
m. "Top-ups" shall mean purchase of e-money by paying equivalent amounts of physical money to merchants.

Signed by: P D J Fernando
Deputy Governor
09 March, 2011

Annex 1

Technology Guidelines for Service Providers of Mobile Phone Based Payment Services

1. Technology Constraints, Security Issues, Principles and Practices

Mobile users/customers could 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, licensed service providers must ensure to implement adequate security measures and install reliable systems that address risks, threats and ensure a very high quality of service, regardless of the underlying network and carrier infrastructure used for the service delivery.

Given the dynamic nature and magnitude of security threats in the wireless environment, it is mandatory for service providers to perform periodic independent security vulnerability assessments and reviews of their systems before launching new products/services. Subsequent updates and reviews should also be carried out regularly to ensure adequate mitigation against operational risks. To facilitate such reviews, security architecture information need to be documented and updated regularly. Licensed service providers 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:

a. When customers are required to provide their passwords or PINs for e-money 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.
b. Authentication methods based on more than one factor should be implemented to validate the transactions where, appropriate.
c. Ensure that encrypted and authenticated sessions remain intact throughout the duration of

communications with the customers

d. Authentication processes should be repeated after session failures and subsequent resumptions
e. 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

The licensed service providers shall issue a new mobile pin (mPIN) to facilitate the mobile payments and such PINs may be issued and authenticated by the licensed service provider. Licensed service providers 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 the 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. Licensed service providers 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:

a. Use strong encryption standards for protecting sensitive and confidential information of

the customers while in transit

b. Establish proper information protection systems and incident response procedures
c. Conduct periodic risk management analysis and security vulnerability assessment of the related systems and networks
d. 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
e. 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 licensed service provider and other service providers should have proper wired and wireless data network protection mechanisms.

1.5 Transaction Logs

Mobile 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 six years in duration. Licensed service providers 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:

a. 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
b. 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 service coverage to those where coverage is poor
c. Licensed service providers and other service providers 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

Licensed service providers 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.

2. Other Related Guidelines

Licensed service providers shall also be mindful of the following:

2.1 Security Related Practices

a. The mobile payment servers at the licensed service provider's end or at the service provider's end, if any, should be certified appropriately in compliance with each licensed service provider's security guidelines. In addition, licensed service providers should conduct regular information security audits on all systems used for mobile payments to ensure full compliance with such security guidelines
b. It is recommended that for channels which do not contain the phone number as an identity, a separate login ID and password be provided. Licensed service providers 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 licensed service provider's own risk perception, unless otherwise mandated by the CBSL.

2.2 Minimizing Financial Losses from a Lost/Stolen Phone

a. 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
b. Request a PIN verification for transactions over specified value - any transaction above the maximum contactless payment value defined by the CBSL 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
c. Ensure that contactless payment functions, SIM cards and phone will be disabled immediately, once a mobile phone equipped with payment technology is reported lost or stolen. Any installed financial applications should also be disabled.

2.3 Customer Education

a. 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
b. Customers should be educated on how to maintain PIN safety and not reveal their PINs to another party
c. 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
d. 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
e. 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
f. 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

g. Licensed service providers shall provide clear configuration instructions if their customers are required to manually configure their own mobile phones to access e-money services.
h. Advise customers to take extra precautions when using e-money services.
i. Customers should be educated to enable them to safely check the authenticity of the established connection, before making any payment.
j. Provide advice to customers on dispute handling, reporting procedures and the expected time for resolution.
k. Avoid use of complex, legal and technical jargon in communications with customers.