Mobile Payments Guidelines No. 1 of 2011
for the Bank-led Mobile Payment Services

1. Introduction

1.1 The Central Bank of Sri Lanka (CBSL) has taken-up the position to encourage electronic payments among the consumers of financial services considering the efficiency, relatively lower cost, safety and the possibility to use in a wider range of transaction situations. Mobile phone based payment applications are explored by the financial industry, as an option to provide electronic payment services in Sri Lanka, due to the rapid growth in the number of mobile phone subscribers. In fact, few banks have already commenced providing the banking services to their customers through mobile phones. Owing to the precautions that need to be taken particularly on the security of such financial transactions, the CBSL have issued this set of guidelines to be adopted by licensed commercial banks.

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. Considering the necessity of improving the electronic payment mechanisms in the country, to protect the customers as well as service providers, and being guided by the international standards and best practices, Service Providers of Payment Cards Regulations No.1 of 2009 (hereinafter referred to as "Regulations") were issued on 31 July 2009. The objective of issuing these guidelines is to promote safety and effectiveness of mobile payment services and thereby enhance user confidence of such services. These guidelines will outline broad principles and standards to be followed by banking institutions providing mobile payment services and will come in to force with immediate effect.

2. Regulatory and Supervisory Provisions

2.1 Banks offering mobile payment services are responsible to ensure compliance to these guidelines. Banks may operate Customer Account based Mobile Payment Systems, through which services can be offered only to their account holders. Under the Customer Account Based System, three types of mobile payment service facilities may be offered, namely;

i. The basic type;

Facility to obtain information on account balance, record of previous transactions, payment orders, which do not relate to fund transfers.

ii. The standard type;

Facility to make fund transfers and stop payments, in addition to the basic type services. Fund transfers may include utility bill payments, own account fund transfers and third-party fund transfers, on the basis of instructions transmitted through the mobile phones.

iii. The extended type – operated through Agents;

In addition to the basic and standard type services, facility to deposit/withdraw cash through agents appointed by the respective banks.

No person other than a Licensed Commercial Bank (LCB) licensed under the Regulations to function as a service provider of payment cards, shall offer customer account based mobile payment services. However, banks that provide only basic type services of mobile payments are exempted from obtaining a licence under the Regulations provided that such banks adhere to the relevant provisions in the Banking Act No. 30 of 1988 and any other legal provisions in operation in this regard.

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 Banks 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 Guidelines on 'Know Your Customer' (KYC) and ' Customer Due Diligence' (CDD) as part of an effective Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) shall be applicable for customers opting for mobile phone based banking services and the banks shall restrict provisioning of mobile payment services to customer accounts which are complied thereon.

2.6 Banks may use the services of agents for providing extended type mobile payment services and shall adhere to all applicable laws and regulations on appointing and obtaining the services of such agents.

3. Registration of Customers for Mobile Payment Services

3.1 Banks shall only offer mobile payment services to their own customers.

3.2 Banks shall have a proper system for registration of customers before providing mobile phone based payment services.

3.3 Customer registration shall be carried out through signed documents.

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 Banks 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 framework is given in Annex 1.

5. Inter-operability

5.1 When a bank offers mobile payment services, it may be ensured that customers having mobile phones of any network operator will be in a position to request for the service.

5.2 The long term goal of the CBSL with regard to mobile phone based payments is to ensure ability to effect fund transfers from anywhere and at any time from an account in one bank to another account in the same or a different bank on a real time basis irrespective of the mobile network that is being used by the customer. Therefore, banks shall note this objective while developing solutions or entering into agreements with mobile payment solution providers.

6. Clearing and Settlement for Inter-bank Fund Transfers

6.1 For inter-bank fund transfers, banks can either have bilateral or multilateral arrangements.

7. Customer Protection

7.1 Banks shall provide the terms and conditions applicable for the utilization of mobile payment 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 banks, account holders and agents with regard to mobile payment services;
c. All applicable fees and charges;
d. Benefits, incentives and rewards of mobile payment 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.

7.2 Banks 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 to the customers in any of the three languages (Sinhala, Tamil or English) as preferred by the customer, through appropriate communication media.

7.3 Banks shall maintain the confidentiality of customer information and shall be responsible to ensure that their service providers will also treat customer information as confidential. Banks shall institute appropriate and adequate risk control measures to manage the risk of liability to the customers on account of breach of secrecy, for which the banks may be exposed due to the high level of information security risk associated with mobile payments.

7.4 Banks shall enter into commercial contracts with service providers, in addition to the agreements with account holders who subscribe for mobile payment 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.

7.5 Banks shall adhere to the laws and regulations applicable to the security procedure adopted to authenticate users as a substitute for signature, when providing mobile payment services to account holders.

8. Customer Education, Grievance and Redress Mechanism

8.1 Banks shall educate customers on applying security features and capabilities and the importance of protecting their personal information.

8.2 An appropriate dispute resolution mechanism shall be developed by banks for handling of disputed payments, transactions and loss of mobile phones. Banks 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.

8.3 Banks shall be responsible to address the customer grievance in an event where a customer files a complaint on a disputed transaction. Chargeback procedures for addressing such customer grievances may be formulated by banks.

9. General Rules and Conditions

9.1 Banks which intend to operate 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 bank and the bank's processes and policies designed to mitigate such risks. Banks which have already started offering mobile

payment services shall review the position and comply to these guidelines within a period of five months from the issuance of the same.

9.2 Banks which provide extended type mobile payment services shall ensure that a consistent notice is displayed in every service outlet, with the logo representing the bank and the mobile service provider and indicating regulatory powers delegated to the agent and operational instructions for the customers.

9.3 Banks which provide extended type mobile payment services shall ensure that appointed agents only provide services of taking deposits and permitting withdrawals, only for the customers of the bank. Banks shall not permit agents to provide any other banking service without obtaining prior approval of the CBSL. Banks shall also specify transaction limits and day limits for agents with the prior approval of the CBSL.

9.4 Banks which provide extended type mobile payment services shall ensure that deposits and withdrawals made by customers at appointed agents are accounted on real-time basis.

9.5 Banks shall monitor and supervise the appointed agents to ensure that they will not engage in any unauthorized activities.

9.6 Banks shall use their best endeavours to use methods consistent with industry best practices to authenticate user identity.

9.7 Banks shall provide controls that allow customers the ability to receive payment alerts and notices in accordance with their preference.

9.8 Banks 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.

9.9 In providing mobile payment services, banks shall take all necessary steps to address, mitigate or eliminate agent-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.

9.10 Banks 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.

10. Interpretation

In these guidelines unless the context otherwise requires:

a) "Agents" shall mean the institutions/persons appointed by banks to carryout mobile payment services;
b) "Customers" shall mean account holders;
c) "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;
d) "Licensed Service Provider" shall mean a mobile payment service provider licensed under the Service Providers of Payment Cards Regulations No.1 of 2009;
e) "Mobile payments" means information exchange between a bank and its customers for financial transactions through the use of mobile phones;
f) "Service Providers" shall mean mobile payment solution providers and relevant mobile network operators.

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, banks 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 service delivery.

Given the dynamic nature and magnitude of security threats in the wireless environment, it is mandatory for banks 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.

Banks 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 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.
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

A high level of security is required when bank accounts are directly accessed through mobile channel, to prevent misuse and eliminate fraud by unauthorized users. 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. 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 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. Banks 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 bank and 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 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 six years in duration. Banks shall ensure that such information is protected from any loss or damage. Security safeguards should also be implemented to protect the information from unauthorized 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. Banks and 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

Banks 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

Banks should also be mindful of the following:

2.1 Security Related Practices

a. The opening up of banking systems to service providers 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
b. The mobile payment servers at the bank's end or at the service provider'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
c. It is recommended that for channels which do not contain the phone number as an identity, a separate log-in 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

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 prepaid stored value cards, must be agreed by all stakeholders.
b. Request a PIN verification for transactions over a 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 unauthorized payments using their lost/stolen mobile phone, by reporting the phone's IMEI code to the

mobile network operator.

g. Banks shall provide clear configuration instructions if their customers are required to manually configure their own mobile phones to access mobile banking and payment services.
h. Advise customers to take extra precautions when using mobile banking and payment 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.

<<<<<<<<<<◇>>>>>>>>>>