NATIONAL PAYMENT AND SETTLEMENT SYSTEMS DIVISION

MINIMUM STANDARDS FOR ELECTRONIC PAYMENT SCHEMES

ADOPTED SEPTEMBER 2010

Table of Contents

Preliminary

These minimum standards may be cited as the "Minimum Standards for Electronic Payment Schemes, 2010". These standards shall apply to all financial institutions and to any other service providing organization that offers direct or indirect electronic payment scheme services. In these minimum standards, unless the context otherwise requires:

"the Act" means the Central bank of Swaziland Order 1974 (as amended);

" Bank" means the Central Bank of Swaziland;

"deposit " means an amount of money paid by one person to another subject to an agreement in terms of which an equal amount or any part thereof will be repaid on demand, on a specified or unspecified date or in circumstances agreed upon;

"electronic money" means monetary value, represented by a claim on the issuer, stored electronically and issued on receipt of funds and generally accepted as a means of payment by persons other than the issuer and is redeemable for physical cash or a deposit into a bank account on demand;

"electronic payment scheme" means any electronic instrument, device and/or system used for the purpose of facilitating payment transfers, through internet and/or wireless communication networks, and by use of service delivery products including but not limited to, electronic cards, electronic transfer systems, mobile banking, internet banking, automated teller machines, point of sale terminals, payment switches and any other type of electronic payment transfer system as may be developed from time to time;

"interoperability" means the ability of software and hardware, implemented by more than one financial institution and/or service provider, to communicate thereby facilitating payments (transfer of value);

"financial institution" means any person licensed in terms of the Financial Institutions Act, 2005;

"oversight" means a public policy activity principally intended to promote the safety and efficiency of payment systems and in particular to reduce systemic risk;

"payment" means a transfer of value, between the payer and the beneficiary, including the related information;

"payment system" means a set of instruments, banking processes/procedures and interbank funds transfer system that ensure circulation of money;

"systemic risk" means the risk that the failure of one participant in the financial system to meet its required obligations will cause other financial institutions to be unable to meet their obligations when due.

1.0 Introduction

1.1. These minimum standards have been issued by the Bank in exercise of powers conferred to it by sections 4 (f) and 42 (b) of The Central Bank of Swaziland Order 1974 (as amended). In terms of this legislation, the Bank is required to promote, regulate and supervise the efficient and secure operation of payment systems to the end of promoting a sound national financial structure; and to supervise clearing houses and other organized systems for the making of payments;

1.2. Based on the powers conferred in the above cited legislation, the role of the Bank becomes that of overseer for payment systems including, but not limited to electronic payment schemes and products. The Bank has a duty to promote safety and efficiency in the National Payment System (NPS) and to ensure that high standards are maintained in the conduct and management of risks in operations of the electronic payment schemes and/or products. The Bank intends the market to use standardized products, with a coherent framework that would ensure interoperability and resilient features for business continuity;

1.3. The Bank takes cognizance of new developments and their impact on the integrity of the NPS and, as far as possible, strives towards minimizing payment system-related risks for all participants. In this regard, to carry-out its oversight function, the Bank always acts in the interest of the system as a whole and not that of any individual stakeholder;

1.4. Accordingly, all financial institutions and non-financial institutions (including but not limited to payment system operators; payment service providers; etc) that have introduced or intend to introduce electronic payment schemes and/or products are required to adhere to these minimum standards.

2.0 Purpose

2.1 The Bank takes a direct interest in the developments and the likely implications of electronic payments, but realizes that emerging e-money products may require regulatory adjustments and/or intervention, which may arise from the need to:

2.1.1 Maintain the integrity and confidence of the NPS;

2.1.2 Limit risks within the NPS;

2.1.3 Assist other regulatory authorities in providing consumers with adequate protection from unfair practices, fraud and financial loss; and

2.1.4 Assist law enforcement agencies in the prevention of criminal activity.

2.2 These minimum standards are intended to provide guidance to financial institutions and non-financial institutions on recommended principles and sound practices for managing risks in their introduction and operations of electronic payment schemes and products;

2.3 It would be important to note that these minimum standards do not provide inclusive principles for risk management in the introduction and operations of electronic payment schemes and products. Financial institutions and non-financial institutions are required to adhere to other prudential and best practice in risk management controls that are appropriate and up to date;

3.0 Bank's Position with Regard to E-money

The Bank considers e-money to be a supplement to physical notes and coin, particularly in the long-run. In order to facilitate the development of e-money products and opportunities they present on a national and regional basis, the Bank will:

3.1 Support the development of a banking industry's vision for electronic substitutes for physical bank notes and coins and paper based instruments (such as cheques);

3.2 Support the development of national standards to enable interoperability of e-money schemes; products and devices; and

3.3 Participate in initiatives aimed at providing secure payment instruments for the general public, including the **unbanked and rural communities** of Swaziland.

4.0 Oversight Function

4.1 The Bank shall conduct oversight inspections and examinations on financial and non-financial institutions and/or service providers to assess the adequacy of risk management;

4.2 The inspections and examinations would be based on the requirements provided in these minimum standards and other assessment processes, developed from time to time, to facilitate its ongoing oversight of electronic payment schemes;

4.3 Financial institutions and non-financial institutions shall promptly report any suspected or confirmed cases of fraud relating to electronic payment schemes, major security breaches, any material service interruption or other significant issues;

4.4 Financial institutions and non-financial institutions shall ensure regular and timely submission of all reports requested by the Bank related to the provision of electronic payment scheme series and/or products.

5.0 Compliance

5.1 Financial and non-financial institutions and/or service providers are required to fully comply with these minimum standards, failure of which shall attract penalties and sanctions as shall be determined by the Bank.

6.0 Application to Introduce Electronic Payment Scheme(s) and/or Product(s)

6.1 Subject to section 6.2 and 8.3, any financial institution or non-financial institution is eligible to operate an electronic payment scheme and/or product provided it meets the minimum requirements stipulated in section 7.0;

6.2 A non-financial institution (such as payment system service providers) that intends to offer an electronic payment scheme(s) and/or product which has **money transfer and/or deposit taking** element shall submit its application through a bank or a financial institution;

6.3 Notwithstanding section 6.1 and 6.2, a financial institution shall submit a written application to the Bank for introducing and operating an electronic payment scheme or product or for expanding the scope of its existing electronic payment scheme or, in the case of 6.2, operating an electronic payment scheme as an agent or partner of a non-financial institution;

6.4 The applying financial institution shall explain in detail how it shall meet the minimum requirements set forth in section 7.0;

6.5 The Bank shall evaluate the application and may grant a license or reject the application if it does not meet the minimum requirements set forth in section 7.0 or for any other reason(s) deemed appropriate by the Bank.

6.6 Any bank wishing to provide e-money services needs to advise the Bank, at least six weeks before the roll out of any pilot, of its intention, and furnish the Bank with full details of its intended proposals

6.7 The Bank reserves the right to request any information pertaining to a payment system, and any person must, on request, provide such information to the Bank in such form and at such time as the Bank may require.

7.0 Minimum Requirements

These minimum requirements are to be observed by all financial and non-financial institutions in applying for and in operating an electronic payment scheme and/or product. Notwithstanding the foregoing, all financial and non-financial institutions shall be required to, at a minimum comply with risk management guidelines stipulated below. The financial and/or non-financial institution warrant(s) that:

7.1 the operation of the electronic payment scheme shall not change or affect its operations, banking license or mandate;

7.2 it has carried out a risk analysis of the project that also details the risk management measures;

7.3 the management has reviewed the existing risk profile of its operations and considered the impact of implementing the electronic payment scheme;

7.4 the board has concluded that there are no undue adverse implications for the safety and soundness of the operations given its resources, risk management systems and technical expertise;

7.5 that there is proper board and senior management oversight over the electronic payment scheme;

7.6 that major technology-related controls relevant to the electronic payment scheme have been addressed;

7.7 that there are appropriate security measures in place, both physical and logical together with other requisite risk management controls and a business strategy has been developed and documented. The strategy should clearly outline the policies, practices and procedures that address and control all of the risks associated with the electronic payment scheme and that it shall be updated periodically to be in tandem with technological changes;

7.8 that issues relating to any outsourcing and/or cross border electronic payment scheme activities have been fully addressed;

7.9 that it shall settle all its inter-bank payments arising from the electronic payment schemes through the Swaziland Inter-bank Payment and Settlement System (SWIPSS) operated by the Bank;

7.10 that the electronic payment scheme(s) shall be open system(s) capable of becoming interoperable with other payment systems in the country and shall comply with the minimum international acceptable standards provided in below Annexure I**;**

7.11 that the electronic payment scheme(s) shall provide an accurate and fully accessible audit trail of transactions from the origin of the payment instruction to its finality;

7.12 that the electronic payment scheme has the potential and capability of providing services to a wider country outreach;

7.13 that the participants to the electronic payment scheme(s) are provided certainty of finality of their payments;

7.14 that an enforceable legal framework for the provision of the services is available which covers all parties in the transaction, the legal framework shall be transparent and shall provide efficient dispute resolution mechanisms;

7.15 that the electronic payment scheme(s) shall be available to its participants at all times, to achieve this, various back up and business continuity arrangements and other legal arrangements to protect the users of the services of the scheme have been implemented;

7.16 that the pricing policies take into account affordability of the services to a wider market reach;

7.17 that the access criteria for participating in the electronic payment scheme(s) is transparent;

7.18 that a cost-benefit analysis has been conducted for the provision of the electronic payment scheme services; and

7.19 that it has considered legal developments (including compliance) and the business environmental (incl. internal and external) threats to information security have been considered in the evaluation of the electronic payment scheme;

7.20 that compliance issues relating to the operation of the electronic scheme shall be monitored on a continuous basis.

7.21 that the period for retention of records should not be less than five years.

PART IV

RISK MANAGEMENT STANDARDS

8.0 Risk Management Standards

8.1 the Bank expects that, in addition to the recommended risk management measures set forth herein, each financial and/or non-financial institution shall implement the relevant risk management controls that are commensurate with the risks associated with the electronic payment scheme adopted by the financial and/or non-financial institution.

8.2 these risk management standards follow the relevant principles laid down by the Basel Committee on Banking Supervision, the principles are herein grouped into main risk categories and specific guidelines are drawn on them.

8.3 these standards do not contain specific detailed security requirements or intend to provide detailed and exhaustive risk management guidelines, rather, they provide general guide for financial institutions to develop effective risk management measures commensurate to their electronic payment scheme business or strategic alliances.

9.0 Risk Category and Management Standards

9.1 Institutional Management Issues for Operating Electronic Payment Scheme(s)

The board of directors and senior management (Institutional Management) of a financial institution and/or non-financial institution are responsible for developing the institution's business strategy. The financial and/or non-financial institution's management shall at minimum ensure that:

9.1.1 there is a board resolution made mandating the institution to provide e-banking transactional services before beginning to offer such services;

9.1.2 electronic payment scheme plans are clearly integrated within corporate strategic goals;

9.1.3 a risk analysis of the proposed electronic payment scheme activities is performed, appropriate risk mitigation and monitoring processes are established for identified risks, and ongoing reviews are conducted to evaluate the results of electronic payment scheme activities against the institution's business plans and objectives. Additionally, risk management measures are introduced to address risks of provision of financial services over the internet and ensure adherence to international cybercrime laws;

9.1.4 ensure that the operational and security risk dimensions of the institution's electronic payment scheme business strategies are appropriately considered and addressed;

9.1.5 that the financial institution's existing risk management processes, security control processes, due diligence and oversight processes for managing the institution's outsourcing relationships and other third –party dependencies supporting electronic payment scheme(s) are appropriately evaluated and modified to accommodate electronic payment scheme services;

9.1.6 it establishes effective management oversight over the risk associated with electronic payment scheme activities, including the establishment of specific accountability, policies and controls to manage these risks; and

9.1.7 it reviews and approve the key aspects of the bank's security control process, which include establishing appropriate authorization privileges, logical and physical access controls, and adequate infrastructure security to maintain appropriate boundaries and restrictions on both internal and external user activities.

9.2 Managing Security Risk

The management of electronic payment scheme service provider has the responsibilities for ensuring that appropriate security control processes are in place for the scheme in addressing issues of authentication, non-repudiation, data and transaction integrity, segregation of duties, authorization controls, and maintenance of audit trails and confidentiality of key financial institution information. As a general guide, the financial institution shall at minimum ensure that:

9.2.1 it establishes appropriate measures to authenticate the identity and authorization of customers with whom it conducts business over the adopted network. Effective Know Your Customer (KYC) and/or Regulation of Interception of Communications and Provision of Communication (RICA) principles should be applied using reliable methods for verifying the identity and authorization of new customers as well as authenticating the identity and authorization of established customers seeking to initiate electronic transactions;

9.2.2 it establishes formal policy and procedures identifying appropriate methodology(ies) to ensure that the financial institution properly authenticates the identity and authorization of an individual, agent or system by means that are unique and , as far as practical, exclude unauthorized individuals or systems. Financial institutions can use a variety of methods to establish authentication, including Personal Identification Numbers (PINs), passwords, smart cards, biometrics, and digital certificates. Banks can use single or a combination of these methods;

9.2.3 it determines which authentication methods to use based on its assessment of the risk posed by the electronic payment scheme as a whole or by the various subcomponents;

9.2.4 it establishes robust customer identification and authentication processes for cross-border electronic payment schemes given the additional difficulties that may arise from doing business electronically with customers across national borders.

9.2.5 it establishes audit trails in the electronic payment schemes to facilitate detection of errors, fraud and tempering incidences and proper documentation of the same should be kept;

9.2.6 it monitors and adopts industry sound practices in the area of authentication to keep pace with the changes in technology and the market;

9.2.7 it uses transactions authentication methods that promote non-repudiation and establish accountability for electronic payment scheme transactions;

9.2.8 electronic payment schemes are designed to reduce the likelihood that authorized users will initiate unintended transactions and that customers fully understand the risks associated with any transactions they initiate;

9.2.9 appropriate measures are in place to promote adequate segregation of duties within electronic payment schemes, databases and applications;

9.2.10 it continuously reviews and adapts segregation of duties commensurate with the electronic payment scheme to ensure that an appropriate level of control is maintained.

9.2.11 the architecture of the straight-through processes and adequate audit trails are emphasized.

9.2.12 proper authorization controls and access privileges are in place for electronic payment schemes, databases and applications.

9.2.13 appropriate measures are in place to protect the data integrity of electronic payment scheme transactions, records and information, by ensuring *inter alia* electronic payment scheme transactions are conducted in a manner that makes them highly resistant to tampering throughout the entire process;

9.2.14 take appropriate measures to preserve the confidentiality of key electronic payment schemes information. Measures taken to preserve confidentiality should be commensurate with the sensitivity of the information being transmitted and /or stored in databases; and

9.2.15 Clear audit trails exist for all electronic payment schemes transactions.

10.0 Managing Legal and Reputational Risk

Financial institutions and/or non-financial institutions have the responsibility of providing their customers with a level of comfort regarding information disclosures, protection of customers' data and business availability. In achieving this, financial institutions are required to address the following issues; privacy of customer information, capacity, business continuity and contingency planning to ensure availability of electronic payment scheme services, and incident response planning.

11.0 Minimum Standards **for Managing Legal and Reputational Risk**

The financial institution shall at minimum ensure that:

11.1 adequate information is provided on their websites to allow potential customers to make an informed conclusion about the financial institution's identity and regulatory status prior to entering into electronic payment scheme transaction;

11.2 take appropriate measures to ensure adherence to customer privacy requirements in accordance to statutory and contractual obligations;

11.3 it has effective capacity, business continuity and contingency planning processes to help ensure the availability of electronic payment scheme and services; and

11.4 it has developed appropriate incident response plans to manage, contain and minimize problems arising from unexpected events, including internal and external attacks, that may hamper the provision of electronic payment systems and services.

ANNEXTURE 1

MINIMUM STANDARD REQUIREMENT

12.0 Relevant De facto International Standards

12.1 Payment Cards

All payment cards used in electronic payment schemes will be expected to adhere to internationally acceptable standards for each of the following:

12.1.1 Physical characteristics, dimension and location of contacts, type of electronic signals, transmission protocols and inter-industry commands for interchange transfer, application identification for contract cards;

12.1.2 Physical characteristics, radio frequency interface, transmission protocols and transmission security features for "remote coupled" contactless cards;

12.1.3 Electronic interchange of messages relating to financial transactions between systems;

12.1.4 Transfer of messages between payment cards and cards accepting devices, for both contacts and contactless technology;

12.1.5 Security architecture of financial transaction systems using integrated circuit cards covering issues on card life cycle, transaction process, cryptographic key relationships, secure application modules, use of algorithms, cardholder verification, key management, general principles and overview; and

12.1.6 Personal identification number (PIN) protection principles and techniques in the banking industry.

12.1.7 Furthermore,

12.1.7.1 De facto standards that support international interoperability between cards, terminals, related devices and software should be generally observed;

12.1.7.2 Developments undertaken by Euro pay, MasterCard and Visa (Electronic Magnetic Verification specification internationally referred to as "EMV spec.") on integrated circuit card, terminal and application specification for payment system should be considered, where necessary.

12.2 Minimum Standard for Other Electronic Schemes

12.2.1 Internet Payments

Developments on Secure Electronic Transaction (SET) specification for Internet payments should also be considered; particularly any impact of such specifications on operations of electronic payment schemes in Swaziland should be evaluated and addressed.

12.3 Switches

12.3.1 De facto standards that support international interoperability between electronic switches for ATMs, cards, terminals, related devices and software should be generally observed.

12.3.2 General observation of standards for securities industry.

12.3.3 General observation of standards for financial transaction card originated messages

13.0 References

Bank for International Settlements, Basle Committee on Banking Supervision. *Risk management for Electronic Banking, 2003;*

Swaziland Government Gazette, *The Central Bank of Swaziland (Amendment) Act, 2004 (Act No.1 of 2004);*

Swaziland Government Gazette Extraordinary, *Financial Institutions Act, 2005;*

Bank of Tanzania, *Electronic Payment Schemes Guidelines, 2007*;

South African Reserve Bank, *Position Paper on Electronic Money, 2009;* and

http://www.iso.org/

Joleen Young Consulting (Pty) Ltd

http://www.govinfosecurity.com/articles.php?art_id=2345