SUPERVISORY AND REGULATORY GUIDELINES: PU23-0506
Electronic Banking
6th June, 2006

GUIDELINES FOR ELECTRONIC BANKING

I. INTRODUCTION

The Central Bank of The Bahamas *("the Central Bank")* is responsible for the licensing, regulation and supervision of banks and trust companies operating in and from within The Bahamas pursuant to the Central Bank of The Bahamas Act, 2000 ("the CBA) and the Banks and Trust Companies Regulation Act, 2000 (BTCRA). Additionally, the Central Bank has the duty, in collaboration with financial institutions, to promote and maintain high standards of conduct and management in the provision of banking and trust services.

All licensees are expected to adhere to the Central Bank's licensing and prudential requirements, ongoing supervisory programmes and regulatory reporting requirements, and are subject to periodic onsite inspections. Licensees are expected to conduct their affairs in conformity with all other Bahamian legal requirements.

II. PURPOSE

Electronic banking (e-banking) is defined as the automated delivery of new and traditional banking products and services directly to customers through electronic, interactive communication channels. E-banking includes the systems that enable customers, individuals or businesses, to access accounts, transact business, or obtain information on products and services through a public or private network, including the Internet.

These Guidelines set out the Central Bank's approach to the supervision of licensees' e-banking services, provide licensees with guidance on general principles for risk management of e-banking, outline suggestions for consumer education and security, and introduce the types of internet financial services.

III. APPLICABILITY

These Guidelines apply to all licensees.

IV. SUPERVISORY APPROACH

The Central Bank's supervisory objective is to establish and maintain a prudent regulatory regime for the provision of e-banking services in The Bahamas. The general principle is that licensees are expected to implement the relevant risk management controls that are commensurate with the risks associated with the types, complexity and amounts of transactions allowed (see Appendix 1) and the electronic delivery channels adopted. The risk management controls established for e-banking should be fully integrated into the risk management systems of the licensee.

The Central Bank endorses the principles and recommendations for e-banking outlined by the Basel Committee on Banking Supervision's papers - *"Risk Management Principles for Electronic Banking"* (http://www.bis.org/publ/bcbs98.htm) and the "Management and Supervision of Cross-Border Electronic Banking Activities" (http://www.bis.org/publ/bcbs99.htm) issued July 2003. Licensees are encouraged to read and understand the main principles of these documents.

In keeping with a risk-based supervisory methodology, the Central Bank's supervisory framework for e-banking aims to provide appropriate levels of supervision of its licensees' e-banking activities.

Initial Discussions

Formal approval is not required to launch new e-banking services or make significant changes to existing services; however as with any other potentially significant change in its operations, licensees should notify and discuss plans with the Central Bank prior to implementing such initiatives in light of the possible implications regarding operational and reputational risk, which may affect capital requirements. The Central Bank will generally require the licensee to present and discuss the strategic outlook for launching e-banking services, demonstrating compatibility with the overall strategy of the licensee's operations, the risk analysis for the planned project together with details of risk/reward study. Importantly, management is expected to demonstrate that it has reviewed the current risk profile of its operations, considered the impact of implementing an e-banking service and that 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.

Specifically, the licensee should satisfy the Central Bank that the following issues are properly addressed:-

(1) That there is proper board and senior management oversight;

(2) That major technology-related controls relevant to e-banking have been addressed;

(3) That there are appropriate security measures in place, both physical and logical together with other requisite risk management controls;

(4) That any other relevant supervisory issues related to activities such as outsourcing and cross border e-banking activities have been addressed[1];

(5) That a cost-benefit analysis has been conducted of the provision of the new e-banking service;

(6) That an e-banking 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 e-banking;

(7) That the effectiveness of the plan will be monitored on an ongoing basis and that it will be updated periodically to take account of changes in technology, legal developments and the business environment including external and internal threats to information security;

(8) That risks are monitored on an ongoing basis; and

(9) That the board is satisfied that the licensee has the necessary level of capital vis-à-vis related risks as denoted in section (V) of these guidelines.

Given the dynamic nature of e-banking and related technology, the Central Bank recognizes that the issues to be dealt with will vary with time and from one licensee to another. The preceding list, therefore, is representative of the issues that should be considered rather than being exhaustive.

Ongoing Supervisory Review

The Central Bank will, in the course of its onsite examinations and offsite reviews, determine, as appropriate, the adequacy of the licensee's risk management of e-banking services based on the requirements set out in these guidelines. The Central Bank may implement other monitoring processes to facilitate its ongoing supervision of e-banking.

Licensees should promptly report any suspected or confirmed cases of fraud relating to e-banking, major security breaches, any material service interruption or other significant issues related to their e-banking services to the Central Bank.

V. RISKS ASSOCIATED WITH E-BANKING ACTIVITIES

Electronic banking creates new risk management challenges for licensees. Typically, all risks associated with traditional banking and products may be impacted with the

[1] (i.e. the necessary supervisory approvals from the Central Bank or overseas regulatory authority have been obtained.

introduction of e-banking services. However, the Central Bank has identified six major categories of risk specifically associated with e-banking for bank supervision purposes. The risks are strategic, operational/transaction, technology, business, reputation and legal.

(1) **Strategic Risk** is the current and prospective impact on earnings or capital arising from adverse business decisions, improper implementation of decisions, or lack of responsiveness to industry changes. Ideally, an e-banking service should be consistent with the bank's overall financial strategy. The planning and decision making process should focus on how specific business needs are met or enhanced by the e-banking product, rather than focusing on the product as an independent business objective. Strategic vision should determine how the e-banking product is designed, implemented, and monitored. The overall strategic vision of the licensee should influence how the e-banking product is designed and implemented.

(2) **Operational/Transaction Risk** arises from fraud, processing errors, system disruptions, and the inability to deliver products or services, maintain a competitive position, and manage information. In the provision of e-banking services, banks often rely on outsourced software companies. They require the proper management of information systems and the right capacity to service their customers. Contingency and business resumption planning is necessary for banks to be sure that they can deliver products and services in the event of adverse circumstances.

(3) **Technology Risks** are risks related to any adverse outcome, damage, loss, disruption, violation, irregularity or failure arising from the use of or reliance on computer hardware, software, electronic devices, online networks, and telecommunications systems. These risks can also be associated with systems failures, processing errors, software defects, operating mistakes, hardware breakdowns, capacity inadequacies, network vulnerabilities, control weaknesses, security shortcomings, malicious attacks, hacking incidents, fraudulent actions and inadequate recovery capabilities.

(4) **Business Risk** – In some circumstances, due to the more savvy nature of the e-banking consumer, traditional banking risk, such as credit risks, interest rate risk, liquidity risk, and foreign exchange risk are elevated.

(5) **Reputation Risk** arises from negative public opinion. A licensee's reputation can be damaged by e-banking services that are poorly executed or otherwise alienate customers and the public. It is important that customers understand what they can reasonably expect from a product or service and what special risks and benefits they incur when using the system. Customer education along with formal incident response and management procedures can help lessen reputation risk.

(6) **Legal Risk** is the risk to earnings or capital arising from violations of, or non-conformance with, laws, rules, regulations, or ethical standards. The need to

ensure consistency between paper and electronic advertisements, disclosures, and notices increases the potential for legal violations. Regular monitoring of the licensee's websites will help ensure compliance with applicable laws, rules, and regulations.

VI. RISK MANAGEMENT OF E-BANKING ACTIVITIES

The board of directors and management of the licensee are responsible for managing its risks, which become more complex following the introduction of electronic banking activities.

Risk assessment

The Board of Directors or its designated committee should ensure that the risk management of e-banking is an integral part of the licensee's risk management systems (see Corporate Governance Guidelines issued in December 2001). As a result, the applicable risk management policies and processes, and the relevant internal controls and audits as required in the licensee's risk management system should be enforced and carried out as appropriate for the licensee's e-banking services.

In addition, the Board or its designated committee should ensure that the licensee's risk management controls and systems are modified and enhanced as necessary to cope with the risk management issues associated with e-banking. The e-banking-related risk management controls and policies should cover, at a minimum, the following risk management mechanisms:-

Strategic Risk:

- **Cost Benefit Analysis** – Licensees should base any decision to implement e-banking products and services on a thorough analysis of the costs and benefits associated with such action (i.e. lower operating costs, improved or sustained competitive position, increased customer demand for e-banking services, and revenue opportunities). The risk management process requires the board and management to decide on what and how much to invest in security and controls in computer systems, telecommunications and networks. In addition to the obvious costs for personnel, hardware, software, and communications, the analysis should also consider:-

  - Changes to the licensee's policies, procedures and practices;
  - The impact on processing controls for legacy systems[2];

[2] A system in which a licensee has already invested considerable time and expense.

- The appropriate networking architecture, security expertise, and software tools to maintain system availability and to protect and respond to unauthorized access attempts;
- The skilled staff necessary to support and market e-banking services during expanded hours and over a wider geographic area, including possible expanded market and cross-border activity;
- The additional expertise and management information systems needed to oversee e-banking vendors or technology service providers;
- Cost of insurance for e-banking activities;
- Potential losses due to fraud; and
- Opportunity costs associated with allocating capital to e-banking efforts.

Operational Risk

- **Business Continuity Considerations** – E-banking services should be delivered on a continuous basis with a reasonable system response time in accordance with the licensee's terms and conditions and anticipated customer expectations. In times of disruption, licensees should have the ability to switch to back-up systems which are protected against similar disruptions. Licensees should also have regard to the requirements for business continuity planning requirements addressed in the *"Minimum Standards for the Outsourcing of Material Functions"* Guidelines issued 4th May, 2004. The e-banking business continuity plan should be documented. The plan should:

  (a) Set out a process for resuming or replacing e-banking processing capabilities, and reconstructing transaction if necessary, in the event of a business disruption;

  (b) Be able to address any dependency on outside service providers (e.g. internet service providers); and

  (c) If an alternate service delivery channel is used for contingency arrangements of a critical e-banking service, licensees should ensure that the alternate service delivery channel can provide an appropriate level of continuous service to its customers, taking into account customers' demands and expectations.

- **Outsourcing Management** – Some licensees may rely on another unit of the same financial group (e.g. the head office) or outside service providers to operate and maintain IT systems or business processes that support their e-banking services. In these cases, licensees should adhere to the controls specified for outsourcing of material functions in the *"Minimum Standards for the Outsourcing of Material Functions"* Guidelines and the requirement for the prior approval of the Central Bank.

Licensees should perform regular due diligence to evaluate the financial soundness and ability of outside service providers to maintain an adequate level of security and to keep abreast of rapidly changing technologies.

The Central Bank also expects licensees to specifically focus on:

- Adopting appropriate procedures for evaluating decisions to outsource electronic banking systems;

- Conducting appropriate risk analysis and due diligence prior to selecting an e-banking service provider;

- Committing adequate resources, with the required knowledge and clear accountability, for the effective oversight of e-banking services outsourced to e-banking service providers;

- Ensuring that the outsourced service is subject to regular independent assessment. In this regard, licensees should have the right to conduct independent reviews or have the right to obtain confirmation that such reviews or audits have been done by an independent party on the e-banking service provider;

- Assessing the internal capacity necessary to evaluate and oversee outsourcing relationships;

- Implementing necessary controls and reporting processes to effectively monitor the outsourced e-banking activity;

- Defining performance expectations under both normal and contingency circumstances; and

- For cross-border outsourcing, ensuring that the arrangements meet the applicable laws, regulations and supervisory standards.

Technological Risk

- **Authentication of customers** –Licensees should select reliable and effective authentication techniques to validate the identity and authority of their e-banking customers and should also have regard to the Guidance provided in the Central Bank's Guidelines on the Prevention of Money Laundering and Countering the Financing of Terrorism for verifying customer identity including instances where there is no face to face interaction with a customer;

- **Confidentiality and Integrity of Information** – E-banking services entail transmission of sensitive information over the Internet and licensee's internal

networks. Licensees should therefore implement appropriate technologies to maintain confidentiality and integrity of sensitive information while it is being transmitted over the internal and external networks and also, when it is stored inside the licensee's internal systems. Cryptographic technologies can be used to protect the confidentiality and integrity of sensitive information. Licensees should choose cryptographic technologies that are appropriate to the sensitivity and importance of information and the extent of protection needed.

- **Application Security** – Inadequate application security in e-banking systems increases the risk of successful penetration or security attacks. Licensees should ensure an appropriate level of application security in respect of their e-banking systems. When licensees select system development tools or programming languages for developing e-banking application systems, they should evaluate the security features that can be provided by different tools or languages to ensure that effective application security can be implemented. In the case of selecting a third-party developed e-banking system, licensees should take into account the appropriateness of the application security of the system.

- **Internet Infrastructure and Security Monitoring** – Licensees should establish an appropriate operating environment that supports and protects their e-banking systems. Licensees should proactively monitor their e-banking systems and internet infrastructure on an ongoing basis to detect and record any security breaches, suspected intrusions or weaknesses.

  Licensees should ensure that sufficient physical controls are in place to deter unauthorised access to all critical e-banking systems, servers, databases and applications.

Reputational Risk

- **Incident Response and Management** – Licensees should put in place formal incident response and management procedures for timely reporting and handling of suspected or actual security breaches, frauds or service interruptions of their e-banking services during or outside office hours. The incident response and management procedures should allow the licensee to quickly identify the origin of the weakness and contain the damage, assess the potential scale and impact of the incident, escalate promptly to senior management where warranted, identify and notify affected customers, and collect and preserve forensic evidence as appropriate to facilitate the subsequent investigation and prosecution of suspects and intruders if necessary. Furthermore, the incident response procedures should include strategies for dealing with adverse media and customer reactions in a timely way.

  Licensees should report any suspected or confirmed cases relating to e-banking, major security breaches, any material service interruption or other significant

issues related to their e-banking services to the Central Bank. Licensees should ensure that the specific mechanisms for ensuring this notification to the regulator are in place.

Legal Risk

- **Terms and Conditions** - Licensees must set out clearly, in their terms and conditions, the respective rights and obligations between the institutions and their customers. These terms and conditions should protect the interests of both the institutions and the customers.

  The terms and conditions should be readily available to customers who use the internet banking feature. On initial logon or subscription to a particular service or product, the licensee should require a positive acknowledgement of the terms and conditions from the customer.

- Licensees should perform appropriate assessments of the legal and reputation risks associated with their e-banking services. Based on the risk assessment, licensees should have proper controls in place to manage the legal and reputation risks. For example, the controls may include:

  - Proper terms and conditions of e-banking services;

  - Appropriate disclosures and disclaimers prominently posted on the e-banking websites or other relevant documents so as to address the applicable legal requirements and potential reputation issues. In particular, terms and conditions governing outsourced activities and other critical third party relationships; and

  - Consideration of the need to use appropriate insurance coverage to address residual legal risks.

VI. CUSTOMER SECURITY AND EDUCATION

An important aspect of customer security and risk management is customer education. Therefore, licensees should pay special attention to the provision of easy-to-understand and prominent advice to their customers on e-banking security precautions. The Central Bank suggests the use of multiple channels, such as websites, messages printed on customer statements, promotional leaflets, or even direct staff communication with customers, to reinforce certain key precautionary measures.

Security precautionary advice for customers should cover, at a minimum, the following issues:-

- Password and user ID selection and protection;

- Customers should be reminded not to disclose their personal information to unauthorised persons or to any doubtful websites; and

- Reminders not to access e-banking services through public or shared computers.

VII. CROSS BORDER ELECTRONIC BANKING ACTIVITIES

Before engaging in cross-border e-banking transactions, licensees should ensure that adequate information is disclosed on their websites to allow potential customers to make a determination of the licensee's identity, home country, and whether it has the relevant regulatory licence(s) before they establish the business relationship. This information will improve transparency and minimize legal and reputational risk associated with cross border e-banking activities.

END

Appendix 1

TYPES OF INTERNET FINANCIAL SERVICES

Due to the open and dynamic nature of the Internet, the risks associated with providing online services via the Internet are greater and far more extensive than closed networks and proprietary delivery channels.

Specific security and control measures have to be formulated to tie in with the risk management process. It is important that licensees set appropriate control and security benchmarks for the Internet operations.

The level of e-banking risk is directly linked to the type of services provided by licensees. The licensee's management should chose a level of e-banking services provided to various customer segments based on customers needs and the institution's risk assessment considerations. Typically, e-banking services can be classified into information service, interactive information exchange service and transactional service.

1. Information Service

This is the most basic form of online e-banking service. It is a one-way communication whereby information, advertisements or promotional material are provided to the customers. Although the risks associated with such online services are low, these websites are often the targets of hacking which vandalizes and mutilates the original information being provided. A licensee may suffer reputational harm resulting from its website being hacked.

Where a licensee purchases advertising space from a third party, regular monitoring should be made not only of the licensee's advertisement, but also the associated contents of the service provider. Reputational damage may be caused by association with unsavoury advertising being hosted on the same service.

2. Interactive Information Exchange Service

This form of Internet services offers slightly more customer interactions compared with the former. Customers are able to communicate with the bank, make account enquiries and complete application forms for additional services or purchase new products offered. The risks pertaining to these websites depend on whether they have any direct links to the licensee's internal network. These risks range from low to moderate according to the connectivity between the Internet and the internal network and the applications that the customer could access.

3. Transactional Service

This category of Internet services allows customers to execute online transactions such as the transfer of funds, payment of bills and other financials transactions. This is the highest risk category that requires the strongest controls since online transactions are often irrevocable once executed and the bank's internal systems may be exposed to external attacks if controls are inadequate.