CENTRAL BANK OF
TRINIDAD & TOBAGO
Eric Williams Plaza, Independence Square,
Port-of-Spain, Trinidad, West Indies
Postal Address: P.O. Box 1250,
Telephone: 625-4835; Fax: 627-4696
E-Mail Address: info@central-bank.org.tt

Guideline on Security Systems for Safeguarding Customer Information

FINAL
May 2005

Table of Contents

1 Introduction 1

1.1 Purpose of Guideline 1

2 Definitions 2

3 Internal Controls and Procedures 2

3.1 Management Responsibility 2
3.2 Role of the Board of Directors 3
3.3 Role of Management 3
3.4 Employee Management and Training 4
3.5 Testing the Programme 5
3.6 Adjusting the Programme 6

4 Security of Information Systems 6

5 Service Provider Arrangements 8

6 Training 8

GUIDELINE ON SECURITY SYSTEMS FOR SAFEGUARDING CUSTOMER INFORMATION

1. INTRODUCTION

1.1 Purpose of Guideline

1.1.1 This guideline is intended to set out a standardized framework for an effective customer information security programme intent on preserving the integrity and confidentiality of customer records and information.

1.1.2 Adequately securing customers' personal information makes good business sense and increases the customer's confidence in the organization. Poorly managed customer data can lead to identity theft[1], fraud and other criminal offenses. Each financial institution must therefore ensure that stringent safeguards are implemented to protect sensitive information and that fiduciary relationships with customers are preserved. This is necessary to maintain the integrity of the financial system.

1.1.3 This guideline requires each financial institution[2] to develop, document in writing and implement an information security programme that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the institution and the nature and scope of its activities. The programme should be designed to ensure the security and confidentiality of customer information and protect against unauthorized access to or use of such information that could result in harm or inconvenience to any customer.

1.1.4 Financial institutions must be mindful of legislative requirements that could impact on security and confidentiality of customer information and implement the necessary measures required under such legislation. For example, the *Proceeds of Crime Act, 2000* requires every financial institution to develop and implement a written programme to monitor compliance with the Act[3], retain relevant records for at least 6 years and appoint a staff member with responsibility for ensuring continual compliance with that Act.

1.1.5 In addition, specific reference is made to financial institutions in the *Electronic Transfer of Funds Crime Act, 2000.* They are prohibited from making available any list of card holders to any person without the proper approval of the card holders except another financial institution for the purpose of credit rating.

[1] Identity theft occurs when someone uses your personal information such as your name, credit card number or other identifying information, without your permission to commit fraud or other crimes.

[2] For the purposes of this Guideline, a financial institution or institution refers to an institution licensed under the Financial Institutions Act, 1993 (FIA) and registered under the Insurance Act, Chap 84:01.

[3] Section 55 of the Proceeds of Crime Act, 2000.

1.1.6 Computers which are used in the provision of banking and financial services are deemed "protected computers" under the *Computer Misuse Act, 2000*. Offences under this and previously referenced legislation carry severe penalties and financial institutions must ensure that relevant requirements are addressed and adequate procedures put in place.

1.1.7 Failure of financial institutions to comply with the provisions of those statutes could lead to the undermining of the integrity of the financial institution.

2. DEFINITIONS

2.1 A customer is defined as one who has sought to establish or has established a business relationship with an institution under which the institution provides one or more financial products or services to the customer.

2.2 Customer information refers to any records containing non-public personal information[4] about a customer, whether in paper, electronic or other form and maintained by or on behalf of the financial institution. In the case of insurance companies, this includes non-public personal health information and non-public personal financial information contained on applications for an insurance product submitted by a consumer, regardless of whether the product is ultimately purchased.

3. INTERNAL CONTROLS AND PROCEDURES

3.1 Management Responsibility

3.1.1 Management should develop and implement control measures that are commensurate with the sensitivity of the information as well as the complexity and scope of the institution's activities. These measures should include a range of system reviews and tests in each area of the institution to validate controls for the protection of customer information. Tests should be conducted or reviewed by staff independent of those that develop and maintain the security programmes. The internal auditor can be used in this capacity.

[4] Non-public personal information does not cover information relating to the financial institution, business customers or to consumers who have not established an ongoing relationship with the financial institution.

3.2 Role of the Board of Directors

3.2.1 Board oversight is critical to the success of the programme and so the Board of Directors should direct management to report at least annually on issues such as risk assessment, risk management, results of testing, service provider arrangements, security breaches and management responses, and recommendations for changes to the information security programme.

3.2.2 The Board of each institution or an appropriate Board committee shall be responsible for: -

3.2.2.1 Approving the written information security programme;

3.2.2.2 Setting policy for overseeing the development of and reporting on the implementation and maintenance of the information security programme, including assigning specific responsibility for its implementation and maintenance; and

3.2.2.3 Reviewing management's status reports on the security programme within an agreed time frame.

3.3 Role of Management

3.3.1 Management is responsible for developing and documenting an operating manual of the policies, procedures and processes of the information security programme. This may take the form of one single document or several separate documents. Regardless of whether the programme resides in one or more documents, management must ensure that all aspects of information security are covered and easily accessible for reference. The following items should also form part of this operating manual:

3.3.1.1 Policies and procedures for storing, retention and destruction of both physical and electronic records and information. This should include the statutory retention requirements for inactive accounts, 6 year retention of records under the Proceeds of Crime Act, 2000 and under the Tax statutes;

3.3.1.2 Policies and procedures for the protection of records and information from potential environmental hazards such as fire and water damage and technology failures should also be outlined;

3.3.1.3 Policies and procedures for the reporting and documentation of incidents of intrusion and misuse of information.

3.3.2 Management with the assistance of internal and external experts, as appropriate, is also responsible for periodically assessing the risk exposure of the institution. In this regard, management should ensure that:-

3.3.2.1 The risks of the institution are properly assessed by identifying reasonable internal and external threats that could result in unauthorized disclosure, misuse, alteration or destruction of customer information or information systems[5] *which store customer data;*

3.3.2.2 The risk assessment of the institution's security requirements is incorporated into the policies and procedures document and form part of a formal programme incorporating timelines and deadlines for the completion or update of systems as necessary; and

3.3.2.3 Each relevant area of the institution's operations is assessed and evaluated for the effectiveness of current safeguards. The risk evaluation should cover all methods used to access, collect, store, use, transmit, protect or dispose of customer information.

3.3.3 Management should prepare a contingency plan which addresses the identified risks and describes the steps to be taken in assessment of any breaches of physical, administrative or technical safeguards. The contingency plan should be reviewed periodically and updated, as necessary.

3.4 Employee Management

3.4.1 The success or failure of the information security programme depends largely on the employees who implement it. It is therefore important that financial institutions: -

3.4.1.1 Check references prior to hiring employees who will have access to customer information;

3.4.1.2 Have every new employee sign an agreement to follow the institution's confidentiality and security standards for handling customer information. This agreement may be renewed annually so that employees have a regular reminder of the institution's policies;

3.4.1.3 Ensure that employees are properly trained in maintaining the security, confidentiality and integrity of customer records and information. Training should be consistent with the user's function;

3.4.1.4 Ensure that employees are competent in the security measures to be taken when accessing, using or exiting information systems;

[5] Information systems include network and software design, and information processing, storage, transmission, retrieval and disposal systems of a technological nature.

3.4.1.5 Ensure that the importance of the following security procedures is fully appreciated by all employees: -

i. **Physical security procedures:** Locking rooms and cabinets where paper records, removable electronic stored files such as diskettes or compact discs and computer equipment are kept;

ii. **Request for information:** Referring calls or other requests for customer information to designated employees with specific training and requiring the requesting individual to provide a proper authorization code other than a commonly used identifier. Financial institutions can also use caller ID or a request for a call back number as tools to verify the authenticity of requests;

iii. **Reporting fraudulent attempts:** Identifying, logging and reporting any fraudulent attempt to obtain customer information such as misrepresentation of identity. The procedures for forwarding such reports to the appropriate law enforcement authority should be known to all employees; and

iv. **Access limits:** Limiting access to information to employees with a business reason only. Dual control procedures[6] should be considered by a financial institution for higher-risk activities and should be adopted only if appropriate for the institution.

v. Reporting of suspicious transactions to the relevant law enforcement authority;

vi Offence of "tipping off" under the Proceeds of Crime Act, 2000.

3.4.1.6 Ensure that employees are updated on any security risks that exist and how to deal with them appropriately;

3.4.1.7 Impose disciplinary measures for any breaches of security policies by employees.

3.5 Testing the Programme

3.5.1 Regular testing of the key controls, systems and procedures of the information security programme should be carried out. The frequency and nature of such tests should be determined by each institution's risk assessment. The process used for testing should be logical, supportable and appropriate for the institution. Testing should be conducted or reviewed by independent third parties[7] either within or outside the institution and should ascertain the sufficiency of policies, procedures and other arrangements in place to control risks.

[6] Dual control procedures refers to a security technique that uses two or more separate persons, operating together to protect sensitive information. Both persons are equally responsible for protecting this information and neither can access the information alone.

[7] Independent of those that develop or maintain the security programme.

3.6 Adjusting the Programme

3.6.1 Each financial institution is expected to monitor, evaluate and adjust, as appropriate, its information security programme in light of any relevant changes in technology; changes to the sensitivity of its customer records and information; internal and external threats to information; and the institution's own changing business arrangements such as mergers and acquisitions, alliances and joint ventures, and outsourcing arrangements.

4. SECURITY OF INFORMATION SYSTEMS

4.1 Electronic customer information should be stored on a secure server that is protected by passwords or other security protections[8]. Servers should be kept in a physically secure area;

4.2 Sensitive customer data should not be stored on computers accessible by an Internet connection. If sensitive data is stored on such computers, appropriate software and firewall protection and intrusion detection devices should be utilized;

4.3 Secure backup media should be maintained and archived data kept secure;

4.4 All systems should be password protected and automatically locked once there has been no activity for a specified period of time. Passwords should be changed regularly and times of log on and off should be recorded;

4.5 Access to physical locations containing electronic customer information, such as buildings, computer facilities and records storage facilities should be restricted to authorized individuals only;

4.6 Procedures should be designed to ensure that modifications to customer records and information are monitored and recorded and that checks are in place to detect and/or prevent and deal with unauthorized modification;

4.7 Encryption of electronic customer records and information should be utilized when transmitting data over private networks and the internet;

4.8 Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into information systems should be in place;

[8] Note sections 9 and 10 of the Computer Misuse Act, 2000.

4.9 Response programmes that specify actions to be taken when the institution suspects or detects that unauthorized individuals have gained access to information systems should be in place;

4.10 When electronic media is being discarded, all data should be erased from computers, diskettes, magnetic tapes, hard drives or any other electronic media that contained customer information;

4.11 An accurate inventory of all computers and other electronic hardware should be maintained;

4.12 Anti-virus software that updates automatically should be used;

4.13 Up-to-date firewalls should be maintained particularly if the institution uses broadband Internet access or allows employees to connect to the company's network from home or other off-site locations;

4.14 Software vendors should be consulted regularly to obtain and install patches that resolve software vulnerabilities.

5. SERVICE PROVIDER[9] ARRANGEMENTS

5.1 Due to the specialized expertise needed to design, implement and service new technologies vendors may be needed to supply resources that the institution is unable to provide on its own. However, the Board and senior management remain responsible for the performance and action of these vendors while they are performing work for the institution;

5.2 Each financial institution should exercise appropriate due diligence in selecting and contracting its service providers. Research of outsourcing arrangements should include consideration of potential vendors' financial condition, reputation and expertise, years in business, history of service interruptions and recoveries and future business plans;

5.3 Service providers should be required, by contract, to implement appropriate security measures designed to meet the objectives of this guideline and the information security programme of the financial institution. These contracts should clearly define responsibility for maintaining and sharing of records and information and any resulting liability for unauthorized use or disclosure of such information;

5.4 Financial institutions should monitor service providers to confirm that they have satisfied their obligations. As part of this monitoring, the institution should conduct or review audits, summaries of test results or other equivalent evaluations of its service provider(s).

6. TRAINING

6.1 Management should be instructed to train staff at least annually on the institution's information security policies and procedures. Documentation of training should be maintained for review by auditors and the regulatory authorities;

6.2 Employees should be properly trained in maintaining the security, confidentiality and integrity of customer records and information. Training should be consistent with the user's function;

6.3 All new employees should be apprised of the security policies and procedures and should be trained in maintaining the security, confidentiality and integrity of customer records and information within two months of joining the institution.

[9] Service provider refers to a person or entity that maintains, processes or otherwise is permitted access to customer records and information through its provision of services directly to the financial institution.