



# *Bangko Sentral ng Pilipinas*

MAYNILA, PILIPINAS

## OFFICE OF THE GOVERNOR

**CIRCULAR NO. 542**  
**Series of 2006**

### **Subject: Consumer Protection for Electronic Banking**

The Monetary Board in its Resolution No. 999 dated 11 August 2006 approved the following rules and regulations concerning consumer protection for electronic banking (e-banking) products and services.

These shall govern the implementation of e-banking activities of the bank for purposes of compliance with the requirements to safeguard customer information; prevention of money laundering and terrorist financing; reduction of fraud and theft of sensitive customer information; and promotion of legal enforceability of banks' electronic agreements and transactions:

#### **1. E-Banking Oversight Function**

- a) Bank's Board of Directors and a senior management committee are responsible for developing the bank's e-banking business strategy and establishing an effective management oversight over e-banking services.**

The Boards of Directors are expected to take an explicit, informed and documented strategic decision as to whether and how the bank is to provide e-banking services to their customers. Effective management oversight encompasses the review and approval of the key aspects of the bank's security control program and process, such as the development and maintenance of security control policies and infrastructure that properly safeguard e-banking systems and data from both internal and external threats. It also includes a comprehensive process for managing risks associated with increased complexity of and increasing reliance on outsourcing relationships and third-party dependencies to perform critical e-banking functions.

It is also incumbent upon the BOD and banks' senior management to take steps to ensure that their banks have updated and modified where necessary, their existing risk management policies and processes to cover their current or planned e-banking services. The integration of e-

banking applications with legacy systems implies an integrated risk management approach for all banking activities.

- b) Bank's Compliance Officer should ensure that proper controls are incorporated into the system so that all relevant compliance issues are fully addressed.**

Management and system designers should consult with the Compliance Officer during the development and implementation stages of e-banking products and services. This level of involvement will help decrease bank's compliance risk and may prevent the need to delay deployment or redesign programs that do not meet regulatory requirements.

## **2. E-Banking Risk Management and Internal Control**

### **a) Information Security Program**

Banks should establish and maintain comprehensive information security program and ensure that they are properly implemented and strictly enforced. They should also encourage the development of a security culture within the organization. The information security program should include, at a minimum, the following:

- Identification and assessment of risks associated with e-banking products and services;
- Identification of risk mitigation actions, including appropriate authentication technology and internal controls;
- Information disclosure and customer privacy policy; and
- Evaluation of consumer awareness efforts.

Banks should adjust or update, as appropriate, their information security program in light of any relevant changes in technology, the sensitivity of its customer information and internal or external threats to information.

### **b) Information Security Measures**

Banks should ensure that their information security measures and internal control related to electronic banking are installed, regularly updated, monitored and is appropriate with the risks associated with their products and services.

**Appendix A** and **Appendix B** provide for the minimum security measures that banks should employ in their ATM facilities and

internet/mobile banking activities, respectively, to protect depositors and consumers from fraud, robbery and other e-banking crimes.

Banks should also take into account other relevant industry security standards and sound practices as appropriate, and keep up with the most current information security issues (e.g., security weaknesses of the wireless environment), by sourcing relevant information from well-known security resources and organizations.

### **c) Authentication**

To authenticate the identity of e-banking customers, banks should employ techniques appropriate to the risks associated with their products and services. The implementation of appropriate authentication methodologies should start with a risk assessment process. The risk should be evaluated based on the type of customer; the customer transactional capabilities (e.g., bill payment, fund transfer, inquiry); the sensitivity of customer information and transaction being communicated to both the bank and the customer; the ease of using the communication method; and the volume of transactions.

Because the standards for implementing a commercially reasonable system may change over time as technology and other procedures develop, banks and technology service providers should continuously review, evaluate and identify authentication technology and ensure appropriate changes are implemented for each transaction type and level of access based on the current and changing risk factors. Account fraud and identity theft are frequently the result of single-factor (e.g., ID/password) authentication exploitation. Where risk assessments indicate that the use of single-factor authentication is inadequate, banks should implement multifactor authentication (e.g., ATM card and PIN), layered security, or other controls reasonably calculated to mitigate those risks.

Banks authentication process should be consistent with and support the bank's overall security and risk management programs. An effective authentication process should have customer acceptance, reliable performance, scalability to accommodate growth, and interoperability with existing systems and future plans as well as appropriate policies, procedures, and controls.

### **d) Account Origination and Customer Verification**

With the growth in e-banking and e-commerce, banks should use reliable methods of originating new customer accounts. Potentially

significant risks may arise when a bank accepts new customers through the internet or other electronic channels. Thus, in an electronic banking environment, banks need to ensure that in originating new accounts, the KYC ("know your clients") requirement which involves a "face-to-face" process is strictly adhered to.

#### **e) Monitoring and Reporting of E-banking Transactions**

Monitoring systems can determine if unauthorized access to computer systems and customer accounts has occurred. A sound monitoring system should include audit features that can assist in the detection of fraud, money laundering, compromised passwords, or other unauthorized activities.

The activation and maintenance of audit logs can help banks to identify unauthorized activities, detect intrusions, reconstruct events, and promote employee and user accountability. This control process also facilitates banks in the submission of suspicious activities reports as required by the Anti-Money Laundering Council (AMLC) and other regulatory bodies.

Adequate reporting mechanisms are needed to promptly inform security administrators when users are no longer authorized to access a particular system and to permit the timely removal or suspension of user account access.

Whenever critical systems or processes are outsourced to third parties, management should ensure that the appropriate logging and monitoring procedures are in place and that suspected unauthorized activities are communicated to the bank in a timely manner.

An independent party (e.g., internal or external auditor) should also review activity reports documenting the security administrators' actions to provide the necessary checks and balances for managing system security.

### **3) Consumer Awareness Program**

Consumer awareness is a key defense against fraud and identity theft and security breach. **Appendix C** provides for the minimum Consumer Awareness Program that banks should convey to their customers.

To be effective, banks should implement and continuously evaluate their consumer awareness program. Methods to evaluate a program's effectiveness include tracking the number of customers who report fraudulent attempts to obtain their authentication credentials (e.g.,

ID/password), the number of clicks on information security links on websites, the number of inquiries, etc.

#### 4) **Disclosure and Business Availability**

- a) **Banks are required to provide their customers with a level of comfort regarding information disclosures or transparencies, protection of customer data and business availability that they can expect when using traditional banking services.**

To minimize operational, legal and reputational risks associated with e-banking activities, banks should make adequate disclosure of information and take appropriate measures to ensure adherence to customer privacy and protection requirements. **Appendix D** provides for the minimum disclosure requirement of the banks.

Likewise, to meet customers' expectations, banks should have effective capacity, business continuity and contingency planning. They should have the ability to deliver e-banking services to all end-users and be able to maintain such availability in all circumstances (e.g., 24/7 availability). Effective incident response mechanisms and communication strategies are also critical to minimize risks arising from unexpected events, including internal and external attacks.

- b) **Banks should apply to e-banking financial transactions and disclosures the record retention provisions required in paper-based transactions.**

A written policy or procedure needs to define vital records relating to e-banking financial transactions and disclosures and the corresponding retention period of these records.

#### 5. **Complaint Resolution**

Banks may receive customer complaint either through an electronic medium or otherwise, concerning an unauthorized transaction, loss, or theft in its electronic banking account. Therefore, banks should ensure that controls are in place to review these notifications and that an investigation is initiated as required. Banks should also establish procedures to resolve disputes arising from the use of the electronic banking products and services.