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.

6. Applicability

This circular is intended for all electronic banking services and products offered by the banks to their customers. Although these are focused on the risks and risk management techniques associated with an electronic delivery channel to protect customers and the general public, it should be understood, however, that not all of the consumer protection issues that have arisen in connection with new technologies are specifically addressed in this circular. Additional issuances may be issued in the future to address other aspects of consumer protection as the financial service environment through electronic banking evolves.

This Circular shall take effect fifteen (15) days after publication in the Official Gazette or in a newspaper of general circulation.

FOR THE MONETARY BOARD:

AMANDO M. TETANGCO, JR.
Governor

01 September 2006

APPENDIX A

AUTOMATED TELLER MACHINE (ATM) SAFETY MEASURES

To minimize/prevent ATM frauds and crimes, banks should, at a minimum, implement the following security measures with respect to their automated teller machine facilities:

- Locate ATM's in highly visible areas;
- Provide sufficient lighting at and around the ATMs;
- Where ATM crimes (e.g., robbery, vandalism) are high in a specific area or location, bank should install surveillance camera or cameras which shall view and record all persons entering the facility. Such recordings shall be preserved by the bank for at least thirty (30) days;
- Implement ATM programming enhancements like masking/non-printing of card numbers;
- Educate customers by advising them regularly of risks associated with using the ATM and how to avoid these risks;
- Conduct and document periodic security inspection at the ATM location, and make the pertinent information available to its clients;
- Educate bank personnel to be responsive and sensitive to customer concerns and to communicate them immediately to the responsible bank officer; and
- Post near the ATM facility a clearly visible sign which, at a minimum, provides the telephone numbers of the bank as well as other banks' hotline numbers for other cardholders who are allowed to transact business in the ATM, and police hotlines for emergency cases.

Banks must study and assess ATM crimes to determine the primary problem areas. Procedures for reporting ATM crime should also be established. Knowing what crimes have occurred will aid the bank in recognizing the particular crime problem and to what degree it exists so that it can implement specific prevention measures to mitigate the risk. In this connection, banks are encouraged to share information involving ATM fraud cases to deter and prevent proliferation of the crime.

APPENDIX B

INTERNET AND WIRELESS BANKING SECURITY MEASURES

1. Network controls

   - Implement adequate security measures on the internal networks and network connections to public network or remote parties. Segregate internal networks into different segments having regard to the access control needed for the data stored in, or systems connected to, each segment.

   - Properly design and configure the servers and firewalls used for the e-banking services either internet-based or delivered through wireless *communication networks (e.g., install firewalls between internal and* external networks as well as between geographically separate sites).

   - Deploy strong and stringent authentication and controls especially in remote access or wireless access to the internal network.

   - Implement anti-virus software, network scanners and analyzers, intrusion detectors and security alert as well as conduct regular system and data integrity checks.

   - Maintain access security logs and audit trails. These should be analyzed for suspicious traffic and/or intrusion attempts.

   - Ensure that wireless software for wireless communication network includes appropriate audit capabilities (e.g., recording dropped *transactions*).

   - Develop built-in redundancies for single points of failure which can bring down the entire network.

2. Operating Systems Controls

   - Harden operating systems by configuring system software and firewall to the highest security settings consistent with the level of protection required, keeping abreast of enhancements, updates and patches recommended by system vendors.

   - Change all default passwords for new systems immediately upon installation as they provide the most common means for intruders to break into systems.

3. Encryption

- Implement encryption technologies that are appropriate to the sensitivity and importance of data to protect confidentiality of information while it is stored or in passage over external and internal networks.

- Choose encryption technologies that make use of internationally recognised cryptographic algorithms where the strengths of the algorithms have been subjected to extensive tests.

- Apply strong "end-to-end" encryption to the transmission of highly sensitive data (e.g., customer passwords) so that the data are encrypted all the way between customers' devices and bank's internal systems for processing the data. This would ensure that highly sensitive data would not be compromised even if the banks' web servers or internal networks were penetrated.

4. Website and Mobile Banking Authentication

- Authenticate official website to protect bank customers from spoofed or faked websites. Banks should determine what authentication technique to use to provide protection against these attacks.

- For wireless applications, adopt authentication protocols that are separate and distinct from those provided by the wireless network operator.

5. Physical Security

- House all critical or sensitive computers and network equipment in physically secure locations (e.g., away from environmental hazards, unauthorized entry and public disclosure, etc.).

- Implement physical security measures such as security barriers (e.g., external walls, windows); entry controls (e.g., biometric door locks, manual or electronic logging, security guards) and physical protection facilities/devices (e.g., water and fire detectors, uninterruptible power supply (UPS), etc.) to prevent unauthorized physical access, damage to and interference with the e-banking services.

6. Development and Acquisition

- Separate physical/logical environments for systems development, testing and production.

- Provide separate environments for the development, testing, staging and production of internet facing web-based applications; connect only the production environment to the internet.

7. IT Personnel Training

   - Provide appropriate and updated training to IT personnel on network, application and security risks and controls so that they understand and can respond to potential security threats.

8. Service Providers

   - Perform due diligence regularly to evaluate the ability of the service providers (e.g., internet service provider, telecommunication provider) to maintain an adequate level of security and to keep abreast of changing technology.

   - Ensure that the contractual agreements with the service providers have clearly defined security responsibilities.

9. Independent Audit, Vulnerability Test and Penetration Testing

   - Conduct regular audit to assess the adequacy and effectiveness of the risk management process and the attendant controls and security measures.

   - Perform vulnerability test or assessment to evaluate the information security policies, internal controls and procedures, as well as system and network security of the bank. Assessment should also include latest technological developments and security threats, industry standards and sound practices.

   - Conduct penetration testing at least annually.

   - The audit and tests should be conducted by security professionals or internal auditors who are independent in the development, implementation or operation of the e-banking services, and have the required skills to perform the evaluation.

   - For e-banking services provided by an outside vendor or service provider, ensure that the above tests and audit are performed and the bank is provided with the results and actions taken on system security weaknesses.

10. Incident Response

    - Establish an incident management and response plan and test the predetermined action plan relating to security incidents.

APPENDIX C

ELECTRONIC BANKING CONSUMER AWARENESS PROGRAM

To ensure security in their e-banking transactions and personal information, consumers should be oriented of their roles and responsibilities which, at a minimum, include the following:

1. Internet Products and Services

   a) Secure Login ID and Password or PIN

      - Do not disclose Login ID and Password or PIN
      - Do not store Login ID and Password or PIN on the computer.
      - Regularly change password or PIN and avoid using easy-to-guess passwords such as names or birthdays. Password should be a combination of characters (uppercase and lowercase) and numbers and should be at least 6 digits in length.

   b) Keep personal information private.

      - Do not disclose personal information such as address, mother's maiden name, telephone number, social security number, bank account number or e-mail address — unless the one collecting the information is reliable and trustworthy.

   c) Keep records of online transactions.

      - Regularly check transaction history details and statements to make sure that there are no unauthorized transactions.
      - Review and reconcile monthly credit card and bank statements for any errors or unauthorized transactions promptly and thoroughly.
      - Check e-mail for contacts by merchants with whom one is doing business. Merchants may send important information about transaction histories.
      - Immediately notify the bank if there are unauthorized entries or transactions in the account.

   d) Check for the right and secure website.

      - Before doing any online transactions or sending personal information, make sure that correct website has been accessed. Beware of bogus or "look alike" websites which are designed to deceive consumers.

- Check if the website is "secure" by checking the Universal Resource Locators (URLs) which should begin with *"https"* and a closed padlock icon on the status bar in the browser is displayed. To confirm authenticity of the site, double-click on the lock icon to display a security certificate information of the site.
- Always enter the URL of the website directly into the web browser. Avoid being re-directed to the website, or hyperlink to it from a website that may not be as secure.
- *If possible, use software that encrypts or scrambles the information* when sending sensitive information or performing e-banking transactions online.

e) Protect personal computer from hackers, viruses and malicious programs.

- Install a personal firewall and a reputable anti-virus program to protect personal computer from virus attacks or malicious programs.
- Ensure that the anti-virus program is updated and runs at all times.
- Always keep the operating system and the web browser updated with the latest security patches, in order to protect against weaknesses or vulnerabilities.
- Always check with an updated anti-virus program when downloading a program or opening an attachment to ensure that it does not contain any virus.
- Install updated scanner softwares to detect and eliminate malicious programs capable of capturing personal or financial information online.
- Never download any file or software from sites or sources, which are not familiar or hyperlinks sent by strangers. Opening such files could expose the system to a computer virus that could hijack personal information, including password or PIN.

f) Do not leave computer unattended when logged-in.

- Log-off from the internet banking site when computer is unattended, even if it is for a short while.
- Always remember to log-off when e-banking transactions have been completed.
- Clear the *memory cache* and *transaction history* after logging out from the website to remove account information. This would avoid incidents of the stored information being retrieved by unwanted parties.

g) Check the site's privacy policy and disclosures.

- Read and understand website disclosures specifically on refund, shipping, account debit/credit policies and other bank terms and conditions.
- Before providing any personal financial information to a website, determine how the information will be used or shared with others.
- Check the site's statements about the security provided for the information divulged.
- Some websites' disclosures are easier to find than others — look at the bottom of the home page, on order forms or in the "About" or "FAQs" section of a site. If the customer is not comfortable with the policy, consider doing business elsewhere.

h) Other internet security measures:

- Do not send any personal information particularly password or PIN via ordinary e-mail.
- Do no open other browser windows while banking online.
- Avoid using shared or public personal computers in conducting e-banking transactions.
- Disable the "file and printer sharing" feature on the operating system if conducting banking transactions online.
- Contact the banking institution to discuss security concerns and remedies to any online e-banking account issues.

2. Other Electronic Products

a) Automated Teller Machine (ATM) and debit cards

- Use ATMs that are familiar or that are in well-lit locations where one feels comfortable. If the machine is poorly lit or is in a hidden area, use another ATM.
- Have card ready before approaching the ATM. Avoid having to go through the wallet or purse to find the card.
- Do not use ATMs that appear to have been tampered with or otherwise altered. Report such condition to the bank.
- Memorize ATM personal identification number (PIN) and never disclose it with anyone. Do not keep those numbers or passwords in the wallet or purse. Never write them on the cards themselves. And

avoid using easily available personal information like a birthday, nickname, mother's maiden name or consecutive numbers.

- Be mindful of "shoulder surfers" when using ATMs. Stand close to the ATM and shield the keypad with hand when keying in the PIN and transaction amount.
- If the ATM is not working correctly, cancel the transaction and use a different ATM. If possible, report the problem to the bank.
- Carefully secure card and cash in the wallet, handbag, or pocket before leaving the ATM.
- Do not leave the receipt behind. Compare ATM receipts to monthly statement. It is the best way to guard against fraud and it makes record-keeping easier.
- Do not let other people use your card. If card is lost or stolen, report the incident immediately to the bank.

b) Credit cards

- Never disclose credit card information to anyone. The fraudulent use of credit cards is not limited to the loss or theft of actual credit cards. A capable criminal only needs to know the credit card number to fraudulently make numerous charges against the account.
- Endorse or sign all credit cards as soon as they are received from the bank.
- Like ATM card PINs, secure credit card PINs. Do not keep those numbers or passwords in the wallet or purse and never write them on the cards themselves.
- Photocopy both the front and back of all credit cards and keep the copies in a safe and secure location. This will facilitate in the immediate cancellation of the card if lost or stolen.
- Carry only the minimum number of credit cards actually needed and never leave them unattended.
- Never allow credit card to use as reference (credit card number) or as an identification card.
- Never give your credit card account number over the telephone unless dealing with a reputable company or institution.
- When using credit cards, keep a constant eye on the card and the one handling it. Be aware of the "swipe and theft" scam using card skimmers. A skimmer is a machine that records the information from the magnetic stripe on a credit card to be downloaded onto a personal computer later. The card can be swiped on a skimmer by a dishonest person and that data can then be used to make duplicate copies of the credit card.
- Do not leave documents like bills, bank and credit card statements in an unsecure place since these documents have direct access to credit card and/or deposit account information. Consider shredding sensitive

documents rather than simply throwing them away. (Some people will go through the garbage to find this information).

- Notify the bank in advance of a change in address.
- Open billing statements promptly and reconcile card amounts each month.
- Do not let other people use your card. If card is lost or stolen, report the incident immediately to the bank.

b) Mobile Banking

- Do not disclose your Mobile Banking Pin (MPIN) to anyone.
- Regularly change the MPIN.
- Do not let other people use your mobile phone enrolled in a mobile banking service. If the phone is lost or stolen, report the incident immediately to the bank.
- Be vigilant. Refrain from doing mobile banking transactions in a place where you observe the presence of "shoulder surfers".
- Keep a copy of the transaction reference number provided by the Bank whenever you perform a mobile banking transaction as an evidence that the specific transaction was actually executed.

Since customers may find it difficult to take in lengthy and complex advice, banks should devise effective methods and channels for communicating with them on security precautions. Banks may make use of multiple channels (e.g. banks websites, alert messages on customers mobile phone, messages printed on customer statements, promotional leaflets, circumstances when bank's frontline staff communicate with their customers) to enforce these precautionary measures.

APPENDIX D

DISCLOSURE REQUIREMENTS

1. General Requirement

Banks offering electronic banking services have to adopt responsible privacy policies and information practices. They should provide disclosures that are clear and readily understandable, in writing, or in a form the consumers may print and keep.

Banks should also ensure that consumers who sign-up for a new banking service are provided with disclosures (e.g. pamphlet) informing him of his rights as a consumer.

At a minimum, the following disclosures should be provided to protect consumers and inform them of their rights and responsibilities:

- Information on the duties of the banking institution and customers.
- Information on who will be liable for unauthorized or fraudulent transactions.
- Mode by which customers will be notified of changes in terms and conditions.
- Information relating to how customers can lodge a complaint, and how a complaint may be investigated and resolved.
- Disclosures that will help consumers in their decision-making (e.g., PDIC insured, etc.)
- For internet environment, information that prompt in the bank's website to notify customers that they are leaving the banking institutions' website and hence they are not protected by the privacy policies and security measures of the banking institutions when they hyperlink to third party's website.

2. Disclosure Responsibility

- Compliance officers should review bank's disclosure statements to determine whether they have been designed to meet the general and specific requirements set in this circular.

- For banks that advertise deposit products and services on-line, they must verify that proper advertising disclosures are made (e.g. whether the product is insured or not by the PDIC; fees and charges associated with the product or services, etc.). Advertisements should be monitored to determine whether they are current, accurate, and compliant.

- For banks that issue various products like stored value cards, e-wallets, debit cards and credit cards, they must provide information to consumers regarding the features of each of these products to enable consumers to meaningfully distinguish them. Additionally, consumers would find it beneficial to receive information about the terms and conditions associated with their usage. Example of these disclosures include:

  - PDIC insured or non-insured status of the product;
  - Fees and charges associated with the purchase, use or redemption of the product;
  - Liability for lost;
  - Expiration dates, or limits on redemption; and
  - Toll-free telephone number for customer service, malfunction and error resolution.

- Whenever e-banking services are outsourced to third parties or service providers, bank should ensure that the vendors comply with the disclosure requirements of the BSP.