

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 not 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.