ELECTRONIC BANKING CONSUMER AWARENESS PROGRAM

NobleBank's Commitment to Security

NobleBank will NEVER request personal information by email or text messaging including account number, passwords, personal identification information or any other confidential customer information. Fraudulent emails may be designed to appear as though they are originated by NobleBank. Do not respond to any email communications which request any type of personal or confidential information and do not go to any links listed on that email. These emails are not originated by NobleBank. Never give out any information that the bank already has to any caller, texter, or email sender. If you contact us we may verify the last 4 digits of your SSN to confirm your identity but we will never contact you and ask for your debit card number or your full SSN. If we need to contact you, it will always be done in a manner that protects your personal confidential information and we work diligently to do so. We always work with the local regulatory and law enforcement departments to be certain any type of illegal activity is stopped as soon as possible. We have multi-layer security to protect your confidential information and will continue to be vigilant in protecting it. Immediately report any suspicious emails or websites to NobleBank.

If you suspect identity theft or have any questions regarding this notice, please contact NobleBank at 256-741-1800.

To ensure security in your e-banking transactions and personal information, please be aware of the following guidance:

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 ebanking 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 or POS terminals. Stand close to the ATM/POS 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 or POS terminal.
- 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.