LANB
Creating a better way.

June 13, 2018

Re: Customer Security Awareness / Cyber Security Awareness

Dear Valued LANB customer,

In an effort to protect you against identity theft, we are providing you with information on how to handle unsolicited requests for confidential information regarding eBanking.

Los Alamos National Bank (LANB) will never contact its customers on an unsolicited basis to request their security logon credentials, such as the combination of the customer's username and password. If you receive a request of this type, do not respond to it. Please call us immediately at (505)662-5171 or (800) 684-5262. You may also email us at lanb@lanb.com to report any activity of this nature.

LANB may contact its customers on an unsolicited basis regarding eBanking activity such as:

- Suspected fraudulent activity on your account;
- Inactive/Dormant account;
- To notify you of a change or disruption in service; or
- To confirm changes submitted to your online banking profile.

If you receive an unsolicited contact from an LANB employee for any reason, LANB will always verify your identity through a series of security questions before discussing any specific account information. If you received an unsolicited contact from LANB, you will always have the option of hanging up and calling LANB directly to confirm the validity of our request. Remember, LANB will NEVER ask for your logon security credentials via phone or email, but we will take steps to ensure you are the individual to whom we are speaking.

eBanking Security
LANB is committed to protecting your personal information. Our eBanking / Business eBanking system uses several different methods to protect your information. All information within our eBanking system uses the Secure Socket Layer (SSL) protocol

for transferring data. SSL is a cryptosystem that creates a secure environment for the information being transferred between your browser and LANB. All information transferred through eBanking has a 128-bit encryption which is the highest level of encryption. In addition to the security features put in place by LANB, here are some tips on keeping your information secure:

- Never give out any personal information, including passwords.
- Create difficult/unique passwords which include letters, numbers & symbols when possible.
- Do not use personal information for your user names or passwords, like birth dates or social security numbers.
- Avoid using public access or computers to access your online Banking.
- Do not use the password auto-save feature on your browser.

Mobile Banking Security

It is important to understand the security implications of mobile banking. Please check out the following tips and recommendations to help keep you and your private information safe when using your mobile device for banking.

- Protect your device with a password or passcode, and ensure it is locked when not in use.
- Do not “jailbreak” your phone as this allows some security functions to be overridden or disabled, putting your personal information at risk.
- Always keep your device updated for increased defense against hackers.
- Never send personal information, such as passwords and account numbers, via text messages.
- Be sure to log out of your mobile banking application when you complete your session.

Liability for Unauthorized Transfers for Consumer Accounts (Regulation E)

Contact LANB immediately if you believe your eBanking user ID and Password have been lost or stolen, or if you believe an unauthorized electronic funds transfer (EFT) has been made on your account. If you notify the bank within two (2) business days after you learn of the unauthorized transaction the most you can lose is $50. Failure to notify the bank within two (2) business days may result in additional losses.

If your statement shows transfers that you did not make, including those made with user ID and password or other such means, notify us at once. If you do not notify us within the sixty (60) days after the statement containing such unauthorized transactions was mailed to you, you may not get back any money lost if we can prove that we could have stopped someone from taking the money if you had told us in time. If reasons beyond your control (such as a prolonged hospital stay) kept you from telling us, we will extend the time periods, as applicable.

To report unauthorized activity on your account, you may call (505) 662-5171, or write us at Los Alamos National Bank, 1200 Trinity Drive, Los Alamos, NM 87544.

For a more complete explanation of Reg E, please visit the following link provided by the FDIC: http://www.fdic.gov/regulations/laws/6500-3100.htm

Securing Your Business: Self-Assessment

Is your business keeping Information Secure? Are you taking the proper steps to protect sensitive information? Safeguarding sensitive data in your files and on your computers is a responsible business practice. After all, if that information falls into the wrong hands, it can lead to fraud or identity theft. A sound data security plan is built on five key principles:

1. **Take stock**. Know the nature and scope of the sensitive information contained in your files and on your computer.
2. **Scale down.** Keep only the information you need for your business.
3. **Lock it.** Protect the information in your care.
4. **Pitch it.** Properly dispose of the information you no longer need.
5. **Plan ahead.** Create a plan to respond to security incidents.

LANB strongly encourages our Business eBanking clients to perform an annual self-Assessment focusing on their Business eBanking practices and network security.

The details for the Self-Assessment are provided by the Federal Trade Commission, Bureau of Consumer Protection at the following link: http://www.business.ftc.gov/documents/bus69-protecting-personal-information-guide-business

The measures outlined below can help prevent a business from experiencing losses or ID theft such as a corporate account take-over in which criminals steal your valid

eBanking credentials. The attacks are usually stealthy and quiet and can lead to account-draining transfers.

- Use layered system security measures: Create layers of firewalls, anti-malware software and encryption. One layer of security might not be enough. Install robust anti-malware programs on every workstation and laptop. Keep the programs updated.

- Manage the security of eBanking activity with a single, dedicated computer used exclusively for online banking and cash management. This computer should not be connected to your business network, should not retrieve any email messages, and should not be used for any online purposes except banking.

- Educate your employees about cybercrimes. Ensure your employees understand that just one infected computer can lead to an account takeover. Ensure your employees are very conscious of cybercrime risks, and teach them to ask this question before they open attachments or provide company or personal information: **Does this email or phone call make sense?**

- Block access to unnecessary or high-risk websites. Prevent access to any website that features adult entertainment, online gaming, social networking and personal email. Such sites could inject malware into your network.

- Establish separate user accounts for each employee accessing company financial information and limit administrative rights. Many malware programs require administrative rights to the workstation and network in order to steal credentials. If your user permissions for Business eBanking include administrative rights, don't use those credentials for day-to-day processing.

- Use approval tools in cash management to create controls on payments:
    - Requiring dual control so that two people are needed to issue a payment - one to set up the transaction and a second to approve the transaction - doubles the chances of stopping a criminal from draining your account.

- Review or reconcile your account online daily. The sooner you identify suspicious transactions, the sooner the theft can be investigated.

LANB
Creating a better way.

Additional Resources

The following links are provided solely as a convenience to our eBanking customers. LANB neither endorses nor guarantees in any way the organizations, services, or advice associated with these links:

- https://www.onguardonline.gov/
- http://www.nist.gov/
- https://www.us-cert.gov/
- https://www.fdic.gov/consumers/consumer/ccc/reporting.html
- http://www.fdic.gov/regulations/laws/6500-3100.htm

Protecting your security is a daily task that we take very seriously. We sincerely hope this information has provided valuable tools for your use and can be used to protect your security.

Sincerely,

Los Alamos National Bank