IMPORTANT INFORMATION ABOUT ELECTRONIC BANKING SECURITY

What is Regulation E? What protections are provided, and not provided, to account holders relative to electronic funds transfers under Regulation E? What types of accounts with internet access are provided these protections?

Regulation E is a consumer protection law that protects consumer customers using electronic funds transfers (EFT). Regulation E covers accounts such as checking or savings, established for personal, family, or household purposes. Non-consumer account owners, such as Corporations, Trusts, Partnerships, or LLCs, (among others), are not protected by Regulation E.

An EFT is any transfer of funds that is initiated through an electronic terminal, telephone, computer, or magnetic tape for the purpose of ordering, instructing, or authorizing a financial institution to debit or credit a consumer's account. The term includes, but is not limited to, transfers initiated by telephone and transfers initiated through internet banking and electronic bill pay.

To maximize their protection under Regulation E, the consumer should notify their financial institution as soon as possible when they discover that an unauthorized or suspicious EFT on their account or if they do not have possession of their ATM/Debit card.

Because a non-consumer is not protected by Regulation E, they should perform a periodic risk analysis to ensure that they have implemented controls adequate to mitigate the risk of unauthorized transactions.

For more information, please refer to the Electronic Funds Transfer Disclosure you received when you opened your account. If you would like an additional copy of this disclosure, or if you are unsure if your account is protected by Regulation E, please contact us.

Under what, if any, circumstances and through what means may the bank contact a customer on an unsolicited basis and request the customer provide their electronic banking credential?

Please be aware that legitimate calls from the bank are made, but we will only ask for confirmation of certain information.

The Bank will never contact you requesting personal information such as your social security number, credit, debit or ATM card numbers, PIN numbers, passwords, usernames, or account numbers. Under no circumstance will the bank request this type of personal information.

We may also respond to an email request or similar electronic request submitted by a customer.

Should commercial online banking customers perform a risk assessment and controls evaluation periodically? Is any additional training for the customer's staff recommended?

Because a non-consumer is not protected by Regulation E, management should perform a periodic risk analysis to ensure that they have implemented controls adequate to mitigate the risk of unauthorized transactions and corporate account takeovers.

Management of the organization should also ensure that all employees have received adequate training in internet security procedures prior to transacting business on the internet. Management should also ensure that employees receive periodic training concerning corporate account takeovers.

The bank will provide commercial customers with additional information and training, upon request or as needed.

What risk control mechanisms should customers consider implementing to mitigate their own risk? Does the bank have any available resources where such information can be found?

General Security Tips

- 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
- Keep accurate records of banking transactions
    - Regularly obtain, review and reconcile your bank accounts
    - Immediately notify the bank of any unauthorized entries or transactions in the account.

Telephone Security Tips

- Never respond to a phone call or voice mail asking you to provide account information or reactivate a bank service.
- Do not provide your personal information to an unsolicited caller.
- If you receive an email or a phone call requesting you to provide information to the bank, do not provide the information. Do not call a number left in a message
    - If contacted by a bank representative, get their name and terminate the call
    - Return the call at the number listed on your statement or in the phone book.
- Remember that the bank will never contact you by phone requesting personal information such as your social security number, credit, debit or ATM card numbers, PIN numbers, passwords, usernames, or account numbers.

Computer Security Tips

- Protect your computer by using anti-virus software and a firewall and keeping them up to date.
- If using a Wi-Fi connection, make sure that the connection is password protected.
- When banking online, be aware of bogus or look alike websites
    - Always log in from your bank's homepage. Check the homepage for security features and information.
    - Always make sure your browser address begins with https and that a padlock icon, or similar security feature, is displayed in the browser. Double click the icon to display the website security certificate.
- Always log off from your online banking session.
- Avoid using shared or public computers for internet banking.
- Never respond to an email, or similar electronic communication, asking you to provide account information or reactivate a bank service.
- Remember that the bank will never contact you by email requesting personal information such as your social security number, credit, debit or ATM card numbers, PIN numbers, passwords, usernames, or account numbers.

The bank has an active customer education plan. Please be sure to look for information that may be contained in statements (both mail and electronic), lobby displays and phone on hold messages. If you have any security concerns or would like additional resources, please contact the bank at 432-264-2100.

What are the bank's contacts points for customers use in the event they notice suspicious account activity or experience customer information security-related events?

If you believe you are a victim of fraud or have been the recipient of suspicious communication, contact the bank immediately at 432-264-2100 or 432-264-2146. You may also email us at custserv@statenb.com or fweber@statenb.com.