CORNERSTONE BANK

Business On-line Banking Customer Awareness and Education

Safeguarding Your Privacy

Keeping your financial information secure is one of our most important responsibilities. We value your trust and recognize the importance of handling information about you with care.

We hold our employees to strict standards of conduct to ensure the confidentiality of customer information. We restrict access to nonpublic personal information to those persons who need to know that information in order to service your account or provide you with products and services.

We protect personal information we collect by maintaining physical, electronic and procedural safeguards designed to comply with federal standards to guard nonpublic personal information. However, the internet is not a fully secure environment, therefore we cannot guarantee the security of information transmitted to or from you or us in connection with the use of our online services. Additionally, there is no guarantee that information may not be accessed, disclosed, altered or destroyed by a breach of any of our safeguards.

You play an important role in protecting your information. Taking steps to ensure that you maintain up-to-date computer security protections and ensuring that your passwords and other personal authentication mechanisms are kept secure and confidential, are key components of the protection of personal information. By using our online services, you agree that you are responsible for any additional verification procedures or security you deem necessary.

Third parties who have access to personal information must agree to follow appropriate standards of security and confidentiality. We require those companies we do business with to safeguard customer information and to use it only for the purpose it was provided.

Cornerstone Bank is committed to protecting your information. It is crucial to keep your information safe from criminals who could potentially harm your financial well-being. The techniques used by identity thieves are becoming increasingly sophisticated; however, there are ways to keep your identity from being compromised.

BUSINESS SECURITY

Protect Your Business from Email Phishing

"Email phishing" is a scheme where a fraudster intercepts payment instruction from a legitimate vendor to a business customer, changes the payment beneficiary information, and instructs the unsuspected business customer to make payment to the fraudster's account instead of the vendor's account. The fraudster ends up with the payment while the legitimate vendor does not get paid.

We highly recommend that you implement the following best practices to protect your company from becoming a victim of this scheme:

- Do not follow payment instructions or changes to payment instructions by email.
- If you receive payment instructions or changes to payment instructions by email, implement a callback procedure to contact your vendor or trading partner to verify the authenticity of the request.
- Implement a process that requires additional review and approval of changes to wire templates and payment beneficiary information.
- Never give sensitive data (such as account number or password) in response to an email request, instant message or on a social network site.

These are proven and longstanding fraud management and operating controls that are widely used by companies, including Cornerstone Bank. In addition to the callback procedure above, we also recommend that you continue to use the additional recommendations below to protect your company:

Protect Your Business from Other Threats

- Implement dual control to initiate and release funds transfers, where two employees and two separate computers are required to complete the transfer of funds, either through ACH or wire transfer.
- Establish appropriate dollar limits for ACH and wire transfers, limiting the exposure in case of unauthorized attempts.
- Do not open emails from unfamiliar sources, especially those with attachments or links.
- Maintain current versions of antivirus software, run virus definition updates and virus scans on a regular basis.
- Review employees' user online banking access activity periodically and remove former employees' accounts from your online banking system immediately.
- Make your passwords longer, use a combination of upper and lowercase letters, numbers, and symbols.
- Check for signs that the webpage is secure, for example, a web address that starts with "https" and shows a closed padlock.
- Promptly review Wire, ACH, or other transaction confirmations to ensure authenticity. Notify the Bank immediately at (404) 601-1250 - you notice any discrepancies or error.

Explanation of protections provided, and not provided, to account holders relative to EFT under Regulation E

Regulation E, or the Electronic Fund Transfer Act (EFT), establishes the basic rights, liabilities and responsibilities of (1) consumers who use electronic fund transfer services and (2) financial institutions that offer these services. Much of Regulation E outlines the procedures consumers must follow in reporting errors with EFTs, and the steps a bank must take to provide recourse. Upon opening an account used primarily for personal, family, or household purposes, you received an Electronic Fund Transfer Disclosure and Agreement that fully outlines the terms and conditions related to Electronic Fund Transfer services. Transactions that are covered under this regulation include, but are not limited to:

- Point-of-sale transactions;
- Automated teller Machine (ATM) transactions;
- Direct deposit or withdrawals of funds (automated clearing house(ACH));
- Telephone initiated transfers; and,
- Transfers resulting from debit card transactions, whether or not initiated through an electronic terminal.

Transactions that are EXCLUDED from Regulation E include:

- Checks.
- Check guarantee or authorization.
- Wire or other similar transfer.
- Securities and commodities transfers, if the security or commodity is:
    - Regulated by the Securities and Exchange Commission (SEC) or the Commodity Futures Trading Commission (CFTC)
    - Purchased or sold through a broker-dealer regulated by the SEC or through a futures commission merchant regulated by the CFTC
    - Held in book-entry form by a Federal Reserve Bank or federal agency.
- Automatic transfers by account-holding institution
- Telephone-initiated transfers for any transfer of funds that:

- Is initiated by a telephone communication between a consumer and a financial institution making the transfer
- Does not take place under a telephone bill-payment or other written plan in which periodic or recurring transfers are contemplated.

What types of accounts are covered?

Regulation E defines accounts as those that include the following:

- Checking, savings or other consumer asset account held by a bank established primarily for personal, family or household purposes.
- Payroll card account, established through an employer, to which EFTs of the consumer's wages, salary or other employee compensation are made on a recurring basis.

Business accounts, escrow or trust accounts (hereafter referred to as business accounts) are not covered.

How does Regulation E apply to a non-consumer using internet banking and/or bill pay?

A business customer using internet banking and/or bill pay is not protected under Regulation E. Because a business customer is not protected by Regulation E special consideration should be made by the customer to review the controls in place to ensure that they are commensurate with the risk level that the customer is willing to accept.

What precautions should a business take since they are not protected by Regulation E?

As a business customer you should perform a risk assessment and evaluate the controls you have in place periodically. The risk assessment should be used to determine the risk level associated with any internet activities the non-consumer customer performs and any controls in place to mitigate these risks. As a non-consumer customer, you should also take advantage of the security controls Cornerstone Bank offers. For ACH and wire originators, we highly recommend you implement dual control for creating and authorizing these transactions. Cornerstone Bank also offers multi-factor tokens to help secure the login process.

Unsolicited Customer Contact

Cornerstone Bank will never contact its customers to request their Online Banking log in credentials such as the combination of a customer's username and password. If someone claiming to be from Cornerstone Bank contacts you to request this information, do not provide it. If you receive an email that appears to be from Cornerstone Bank requesting any type of personal or confidential information, do not respond to the request or click on any links in the email. Please report any activity of this nature to us at (404) 601-1250.

Business Risk Assessment and Controls Evaluation

The following sample internet banking risk assessment and controls evaluation is provided to assist business internet banking users in identifying threats and measuring the strength of their controls.

For each question, select the answers that best represents your environment. Each response has a risk rating associate with it. Add the ratings together, in order to determine your overall risk score. Following the assessment, use the "Control Evaluation - Best Answers and Tips" to evaluate your responses.

Personnel Security

	Risk Rating
1) Are employees required to sign an Acceptable Use Policy (AUP)?	
a) Yes, at least annually or more frequently as needed	(1)
b) Yes, but only at hire	(2)
c) No	(5)
2) Does each employee with access to internet banking complete security awareness training?	
a) Yes, at least annually or more frequently as needed	(1)
b) Yes, but only when initially hired	(2)
c) No	(5)
3) Are background checks completed on employees prior to hiring?	
a) Yes, for all employees	(1)
b) Yes, but only based on position	(2)
c) No	(5)

Computer System Security

4) Is a dedicated computer system used for internet banking activities?

a) Yes, the system is dedicated to only internet banking activities (1)
b) No, the system is used for other business purposes (5)

5) Do your computer systems have up-to-date antivirus software?

a) Yes, all systems (1)
b) Yes, but only critical systems (3)
c) No (5)

6) Is there a process in place to ensure software updates and patches are applied?

a) Yes, a formal process where updates are applied at least monthly (1)
b) Yes, but informally as needed (3)
c) No (5)

7) Are users allowed to act as local Administrators on their computer systems, allowing them access to manage the settings on their computer?

a) No (1)
b) Only those that require it (3)
c) Yes (5)

8) Does a firewall protect the network?

a) Yes (1)
b) No (15)

9) Do you have an Intrusion Detection/Prevention System (IDS/IPS) in place to monitor and protect the network?

a) Yes (1)
b) No (3)

10) Is internet content filtering being used?

a) Yes, internet access on the system used for internet banking activities is restricted to only those sites specifically needed for business functions (1)
b) Yes, internet content filtering is used (2)
c) No (5)

11) Is email SPAM filtering being used?

a) Yes (1)
b) No (5)

12) Are users of the internet banking system trained to manually lock their workstations when they leave them?

a) Yes, and the systems are set to auto-lock after a period of inactivity (1)
b) Yes, but auto-lock is not enabled (2)
c) No (5)

13) Is wireless technology used on the network with the internet banking system?

a) No (1)
b) Yes, but wireless traffic uses industry-approved encryption (e.g. WPA, etc.) (1)
c) Yes, but wireless uses WEP encryption (2)
d) Yes, and wireless traffic is not encrypted (15)

Physical Security

14) Are critical systems (including systems used to access internet banking) located in a secure area?

a) Yes, behind a locked door (1)
b) Yes, in a restricted area (2)
c) No, in a public area (5)

15) How are passwords protected?

a) Passwords are securely stored (1)
b) Passwords are written on paper or sticky notes and placed by the computer (15)

Previous Experience

16) Have you experienced fraud through internet banking in the past?

a) No (1)
b) Yes, attempted fraud, but it was detected and stopped (3)
c) Yes (5)

17) Has malware been discovered on systems used for internet banking activities in the past?

a) No (1)
b) Yes (5)

Determining Your Risk Rating

Once you have completed the questionnaire, total the risk scores based on the answers selected to calculate a summary risk rating of your environment. This risk rating is designed to give you a general idea of your risk posture based only on the answers in this questionnaire. Additional factors could either increase or decrease the risk.

The total score based on your responses is: ________________

Overall Risk Rating	
0-20	LOW
21-30	MEDIUM
31-40	HIGH
Over 40	EXTREME

Best Answers and Tips

Below are the best answers to the questions asked above. Review your answers and the tips provided to help protect your systems and information.

1. The best answer is "a) Yes, at least annually or more frequent as needed."

   An Acceptable Use Policy (AUP) details the permitted user activities and consequences of noncompliance. Examples of elements to include in an AUP are: Purpose and scope of network activity; devices that can be used to access the network, bans on attempting to break into accounts, crack passwords, circumvent controls or disrupt services; expected user behavior; and, consequences of noncompliance.

2. The best answer is "a) Yes, at least annually or more frequently as needed."

   Security Awareness Training (SAT) for internet banking users should include, at a minimum, a review of the acceptable use policy, desktop security, log-on requirements, password administration guidelines, social engineering tactics, etc.

3. The best answer is "a) Yes, for all employees."

Companies should have a process to verify job application information on all new employees. The sensitivity of a particular position or job function may warrant additional background and credit checks. After employment, companies should remain alert to changes in employees' circumstances that could increase incentives for abuse or fraud.

4. The best answer is "a) Yes, the system is dedicated to only e-Banking activities."

   It is best to have a dedicated system for high-risk e-Banking activities.

5. The best answer is "a) Yes, all systems."

   Companies should maintain active and up-to-date antivirus protection provided by a reputable vendor. Schedule regular scans of your computer in addition to real time scanning.

6. The best answer is "a) Yes, a formal process where updates are applied at least monthly."

   Update your software frequently to ensure you have the latest security patches. This includes a computer's operating system and other installed software (e.g. web browsers, Adobe Flash Player, Adobe Reader, Java, Microsoft Office, etc.). It is best to automate software updates when the software supports it.

7. The best answer is "a) No."

   Limit local Administrator privilege on computer systems where possible.

8. The best answer is "a) Yes."

   Use firewalls on your local network to add another layer of protection for all devices that connect through the firewall (e.g. PCs, smart phones, and tablets).

9. The best answer is "a) Yes."

   Intrusion Detection/Prevention Systems (IDS/IPS) are used to monitor network/Internet traffic and report or respond to potential attacks.

10. The best answer is "a) Yes, Internet traffic on the system used for internet banking activities is restricted to only those sites specifically needed for business functions."

    Filter web traffic to restrict potentially harmful or unwanted Internet sites from being accessed by computer systems. For systems used for internet banking, it is best to limit Internet sites to only those business sites that are required.

11. The best answer is “a) Yes.”

    Implementing email SPAM filtering will help eliminate potentially harmful or unwanted emails from being delivered to end users’ inboxes.

12. The best answer is “a) Yes, and the systems are set to auto-lock after a period of inactivity.”

    Systems should be locked (requiring a password to reconnect) when users walk away from their desks to prevent unauthorized access to the system.

13. The best answers are either “a) No” or “b) Yes, but wireless traffic uses industry approved encryption (e.g. WPA, etc.).”

    Wireless networks are considered public networks because they use radio waves to communicate. Radio waves are not confined to specific areas and are easily intercepted by unauthorized individuals. Therefore, if wireless is used, security controls such as encryption, authentication, and segregation are necessary to ensure confidentiality and integrity.

14. The best answer is “a) Yes, behind a locked door.”

    Physically secure critical systems to only allow access to approved employees.

15. The best answer is “a) Passwords are securely stored.”

    Passwords should never be exposed to unauthorized individuals.

16. The best answer is “a) No.”

16. The best answer is “a) No.”

    If you have discovered malware on the e-Banking system in the past, ensure the system is clean of all malware. It is best to do this by rebuilding the system.

Please contact us with any questions or concerns at (404) 601-1250 and we will be happy to help. We appreciate your business!