Best Practices for Online Banking and Electronic Fund Transfers

Online access to financial information allows many conveniences in your day to day operations. Unfortunately, this also leaves your company vulnerable to cyber attacks. Ultimately, you are the first and best line of defense against these attacks. Please use this document to assist you in establishing internal controls to help mitigate both internal and external risk.

Yes, you are a target

Information, whether personal or business related, is becoming increasingly valuable to criminals. If you have a computer, mobile device, an online account, email address, credit card, or engage in other type of online activity, you are worth money to cyber criminals.

Cyber criminals pose a threat to you and your business and could access private and confidential information and steal your money in the following ways:

- **Deceptive Phishing** – This fraud refers to any attack by which a fraudster impersonates a recognized legitimate company. A common fraud attempt is when your company receives an email from a vendor that you typically deal with instructing you to wire or ACH payments to alternate bank account instructions. Anytime a change in bank account instructions is communicated, it is very important that you contact the company via phone call to confirm the new instructions. **NEVER respond directly to the email you received**. If this is a true fraud you are only communicating back to the fraudster who will tell you whatever is necessary to get you to send the electronic funds. **Before you pay a new vendor electronically or change bank instructions on an existing vendor, contact the company directly via a trusted phone number to confirm the instructions.**

- **CEO fraud** – This fraud usually begins with the thieves either phishing an executive and gaining access to that individual's inbox, or emailing employees from a look-alike domain name that is one or two letters off from the target company's true domain name. The victim receives a supposedly legitimate email from someone with authority asking for a wire to be sent. The employee, following the requestor's instructions sends the wire request to the bank for processing. The employee replies back to the same email confirming that the wire has been sent. Unfortunately, since the email address is fake, the true employee is never notified and has no idea that this has taken place until it's too late. **Best practice is to call the requestor directly to confirm the request prior to sending to the bank. It is important that you establish internal controls such as dual control, callbacks to the requestor and signatures to verify the legitimacy of the request. The fraudster's goal is intimidation and that the employee feels they need to immediately process a request without question when the requestor is an executive of the company.**

- **Phishing** - The victim receives a supposedly legitimate email (often claiming to be a bank or credit card company) with a link that leads to a hostile website. Once the link is clicked, the PC can then be infected with a virus.

- **Spear Phishing** – The victim receives an email that appears to be from a known and trusted individual, often someone within the victim's company and generally someone with a position of authority. The Cyber criminal is masked as a familiar person and then requests confidential information or unauthorized access in order to commit fraud.

- **Pop up Ads**- While online, the victim receives a pop up ad claiming that a prize can be collected. The victim clicks on the ad and enters personal information which is stolen by cyber criminals.

- **Cyberstalking** – The victim's personal information is collected from various personal networking sites and used for identity theft.

- **False Websites** - The victim unknowingly downloads a Trojan horse virus from a website which installs a keystroke logger on his or her machine. The keystroke logger allows the hacker to steal private data such as internet banking and email passwords.

In the end, it is very important that you know who you are doing business with. Email is the fraudster's friend!!

When making payments electronically, remember:

- **Any changes in payment instructions or any new instructions communicated through email or on an invoice should be verified prior to sending funds.**
- **Take the time to call the payee directly to confirm payment instructions. A three minute call could save you thousands in loss.**
- **Once funds are sent electronically, the chances of full or partial recovery are low. The fraudster will take the funds as soon as available to them. This is why fraudsters go to choice is wires.**
- **When there are changes to payment instructions via email, do reply directly back to the email. You might just be responding back to the fraudster. If you can't call the company directly, create a fresh email from past communications that you know are legit.**
- **When calling back to the vendor, use a phone number that is known. Many times the fraudster will change the contact information in the email.**
- **Establish internal procedures to include some type of verification process such as call backs, internal dual control, sign-offs on requests etc...**

Best Practices for Meridian Online Banking - NetTeller

User Best Practices

- Tokens should be secured and kept with the designated user at all times.
- Do not share Tokens.
- Users should not share or document their NetTeller credentials (ID and PIN).
- Create strong NetTeller credentials that are at least 8 characters or more and include numbers and symbols.
    - Do not use a name or date that can be easily associated with you
- Change your password regularly.
    - You can change your password in NetTeller by clicking on the Options & Settings Tab.
- Never use the same credentials for NetTeller that you use to access other sites.
- Do not make the answers the same for all three Security Questions.
- Beware of Phishing email attempts.
    - Never open unknown email attachments or suspicious links
    - Never divulge confidential information requested in an email such as passwords or account numbers
    - Verify that the source of an email is valid. It may appear to be from a known individual, but always be aware that scammers can hide behind a supposedly legitimate email address.
    - Watch for suspicious text and grammar that may signal a phishing email
- Log out of online banking properly by clicking on the "Log Out" button.
- Assign one user as the Administrator to:
    - Keep user access up to date
    - Restrict user access when they are on vacation or no longer with the company
    - Keep limits low on users that don't typically perform high dollar transactions
    - Proper training of users is essential. Meridian will provide new employee training and refresher courses upon request.
    - Monitor user activity
    - Maintain written policy/procedure for online access to company's financial information

NetTeller Security Controls

Take full advantage of security controls offered at no charge by Meridian Bank. In order to reduce the risk of fraud, the following controls are recommended:

- Dual Control
- User Limits
- Email Alerts
- IP Address Restriction
- Online Access Time Restriction

Internal Controls

- Internal controls should be established to safeguard against unauthorized transactions.
- Dual Control is the best way to insure accuracy and security for transactions.
- Policies and Procedures should be established internally to define clear and concise responsibilities and to ensure proper use of the designated cash management tools.
- View your account history daily.
- Set up alerts within NetTeller to receive emails when key transactions occur.
- Create a Business Continuity Plan. Address what steps should be taken if a disruption of service occurs at your

place of business or bank. What do you do if you have no access to online banking?

Data Security

- Data should be received, stored, and transmitted in a secure manner.
- All banking information should be encrypted or transmitted in secure sessions subject to changing technology standards (new versions).

Your Customer's Privacy

- Maintain the confidentiality, integrity and security of their information.
- Disclose such information only to authorized personnel.
- Maintain physical, technical, procedural and administrative procedures reasonably designed to ensure the security, integrity and confidentiality of customer's information.

Corporate Account Takeover

Corporate account takeover is the business equivalent of personal identity theft. Small to midsized businesses are the main target of such attacks, however any business can fall victim to these crimes. Corporate account takeover occurs when criminal entities obtain online banking credentials through a variety of tactics in order to drain accounts via ACH or wire transfers. Some common ways that a business' system may be compromised are:

- Clicking on a link in an email that leads to an infected website
- Visiting legitimate websites, such as social engineering websites, that contain infected documents, videos or photos
- Using a flash drive that was infected by another computer
- Opening an infected email attachment

Sound Business Practices

It is important that business owners take steps to protect sensitive financial information and educate all users about cybercrimes. In an attempt to mitigate these threats the following business practices are advised:

- Use appropriate tools to prevent and deter unauthorized access to your network including firewalls, anti-malware and encryption of laptops, hard drives VPN's or other communication channels.
- Install robust anti-virus and security software for all computer workstations and implement multilayered security technology.
- Apply operating system and application updates regularly (patches).
- Do not allow workstations used for online banking to be used for general web browsing and social networking.
- Do not allow the conduct of online banking activities from free Wi-Fi hotspots such as airports or internet cafes.
- Educate all employees to think critically about all phone calls and emails received. If an email is suspicious, do not click on the link or open the attachment.
- Establish users for each employee and limit administrative rights.
- Maintain up-to-date contact information with the Bank.
- Stay informed about cybercrimes. Threats change rapidly and it is important to be aware or current trends in order to ensure your security practices are current.
- Reconcile accounts daily and contact Meridian Bank immediately to report any suspicious activity.

Email Alerts

Sign up for NetTeller Alerts. Receive emails that will notify users when an ACH batch or Wire has been initiated from your company through NetTeller.

Follow these easy steps:

- Sign in to NetTeller
- Select Options & Settings on the toolbar
- Select Alerts
- Select Events
- Check the email box in front of 'ACH Batches Initiated'
- Verify the email address and Accept

What to do in the case of a security breach

- Change your passwords to NetTeller immediately
- Contact the Bank immediately for assistance in securing account information and further guidance

Bank Contact Information

Phone: 484-568-5000

Toll Free: 866-327-9199

Secure Message: Click "Contact Bank" from NetTeller main menu

ATTENTION ALL ACH USERS -

At Meridian Bank, we strive to provide our customers with the latest industry news. We want to take this opportunity to inform you of the ACH Security Framework, affecting all customers utilizing ACH service to disburse or collect funds – known as ACH Originators.

The National Automated Clearing House Association (NACHA) has established The ACH Security Framework that outlines data security obligations for ACH Originators in order to protect sensitive ACH data. This Rule is aimed at protecting the security and integrity of ACH data throughout its lifecycle.

Protected Information is defined as the non-public personal information used to create, or contained within, an ACH transaction. Some examples of personal confidential information include:

- Bank Account Number
- Social Security Number
- Driver's License Number
- Account Balances

To maintain compliance with NACHA's amendments to data security, the following is strongly encouraged:

- Monitor access controls to guard against unauthorized use of Protected ACH Information
  - Implement dual control for initiating ACH transactions
  - Ensure each user has their own login credentials and that passwords and security tokens are never shared
  - Always keep your security token with you

- Protect against anticipated threats or hazards to the security or integrity of Protected information
  - Protect your IT systems from viruses and spyware by using up-to-date antivirus protection and firewalls.

    - Consider dedicating one computer in your office to online financial use, and do not use that machine for general internet surfing or email.
    - Beware of Phishing schemes, do not click on links in suspicious emails
    - Educate employees about cyber-crime and potential threats to security

- Create, verify or update security policies, procedures, and controls related to the initiation, processing, and storage of ACH Entries.
    - Establish procedures for the storage and safekeeping of confidential ACH data
    - Document controls in place to guard against unauthorized use of ACH data
    - Ensure sensitive personal data is only transmitted via secure channels

For more information please visit www.nacha.org.