ONLINE BANKING - BUSINESS BEST PRACTICES

- Recommend reconciliation of all banking transactions on a daily basis.
- Recommend customers initiate ACH and wire transfer payments under dual control, with a transaction originator and a separate transaction authorizer.
- If possible, and in particular for customers that originate ACH or wires or large numbers of online transactions, recommend commercial banking customers carry out all online banking activities from a stand-alone, hardened and completely locked down computer system from which email, web browsing and access to your company network are not possible.
- Be suspicious of emails purporting to be from a financial institution, government departments or other agencies requesting account information, account verification or banking access credentials such as usernames, passwords, PIN codes, answers to challenge questions and similar information. Opening file attachments or clicking on web links in suspicious emails could expose your computer network to malicious code that could hijack your private information, online banking credentials, and more.
- Never process payment instruction changes from clients, vendors or employees that have not been directly verified. NACHA rules require a valid signed authorization to be on file before a company can originate transactions to both business and consumer accounts. Changes to an authorization should be requested in writing and a new signed authorization should be obtained before implementing any changes. It's also a good idea, if available, to get a blank check with an authorization.
- Install a dedicated, actively managed firewall, if using a broadband or dedicated connection to the Internet, such as DSL or cable. A firewall limits the potential for unauthorized access to a network and computers.
- Create strong passwords that include a combination of characters. The latest guidance suggests using a passphrase such as a favorite line from a movie or a series of associated words rather than a traditional password. The idea is to create a passphrase that can be remembered easily and protect the account — for example, $unWalkRainDriv3.
- Prohibit the use of "shared" usernames and passwords for online banking systems.
- Have procedures in place to control employee access to secure logins and sites if employment status has changed.
- Use a different password for each website that is accessed and change your passwords several times each year. If available, enable multifactor authentication for an additional layer of security.
- Never share username and password information for online services with third-party providers.
- Limit administrative rights on users' workstations to help prevent the inadvertent downloading of malware or other viruses.
- Install commercial anti-virus, spyware detection and desktop firewall software on all computer systems. Free software may not provide protection against the latest threats compared with an industry standard product.
- Ensure security suite software pages and computer programs are patched regularly, particularly operating systems and key applications, such as Adobe products. It is recommended that you utilize the built-in automatic software updates available for most operating systems and software programs.
- Recommend clearing the browser cache before starting an online banking session to eliminate copies of web pages that have been stored on the hard drive. How the cache is cleared will depend on the browser and version. This function is generally found in the browser's options or settings menu.

- Recommend customers verify use of a secure session (https not http) in the browser for all online banking and financial services and the site has a valid digital security certificate.
- Avoid using automatic login features that save usernames and passwords for online banking. This includes using Internet browsers to store password information.
- Make sure computers, scanners, copiers, printers, and other office equipment where the potential for sensitive data is stored is not accessible by unauthorized personnel.
- Never leave a computer unattended, especially when logged into online banking or financial service sites.
- Never access bank, brokerage or other financial services information sites using public Wi-Fi, such as at Internet cafes, public libraries, airports, etc. Using public Wi-Fi increases the potential for unauthorized software to be installed to trap account and sign on information.
- Recommend customers familiarize themselves with the institution's account agreement and with the customer's liability for fraud under the agreement pursuant to the Uniform Commercial Code Article 4A as adopted in the state of Nebraska.
- Recommend developing written security procedures designed to protect your company's network from infection or breach and it is also recommended that you include regular security training for all employees. This is required for ACH origination clients.
- Recommend periodically testing written security procedures and controls to evaluate for potential weaknesses and/or to strengthen processes.
- Stay in touch with other businesses to share information regarding suspected fraud activity. It is recommended that you subscribe to fraud alerts available from sources such as antivirus software companies, credit card processors, government agencies, etc. Also, become familiar with the services your financial institution provides regarding the latest fraud threats and fraud mitigation tips.
- Immediately escalate any suspicious transactions to the financial institution, particularly ACH or wire transfers. There is a limited recovery window for business transactions and immediate escalation may prevent further loss.
- Get into the habit of locking your computer or mobile device when you are not using it. Even if you only step away for a few minutes, that is enough time for someone to steal or destroy your information. For an additional layer of security, computers should have a set time to lock the screen.

Additional Security Tips for Mobile Devices

- Treat your mobile phone with the same care regarding passwords and security as your PC.
- Never save or share your username and password in the mobile phone.
- Enable biometric security features such as facial recognition or fingerprint security.
- Install an antivirus app approved by your phone carrier.
- Keep mobile phones within your sight at all times.
- Activate the mobile phones locking feature after a period of inactivity and use strong passwords.
- Report mobile phone theft immediately.
- Avoid using mobile phones over unsecure Wi-Fi networks.
- Keep Bluetooth out of discovery when not in use.
- Be aware of the potential for fraudulent text messages (SMS/MMS). The bank will never request or invite customers to sign on to its Business Mobile Banking app by sending a text message with initiation from the client.

- Keep your mobile phones operating system and installed apps up to date.
- Download and apply security updates and patches to your mobile phone when they are made available by your wireless or phone provider. These are designed to provide you with the protection from known possible security issues.
- Do not install pirated software or software from unknown sources.

Information provided by NACHA, EPCOR and FS-ISAC (Financial Services Information Sharing and Analysis Center)