Security Best Practices for Business Online Banking and Remote Capture

We all know online fraud is on the increase. Banks and businesses have not only heard about online fraud but many have experienced it as well. Based on the increased fraudulent activity, we would like to encourage our business customers to use the following security features.

- Token authentication provides an additional layer of security. All users who are set up to authorize a wire or an ACH transaction are required to use the VeriSign credentials.

- Our online banking software acts as a behavioral tool which is built explicitly from the individual user's activity history. The model is dynamic in nature and evolves in real-time according to the user's changing behaviors. The model investigates and analyzes each user's habits, such as when a user typically logs in (time of day), and any computer IP addresses from which a user logs in to their online banking.
    - We have procedures in place to help assure that the validity of the user is real. If at any time the software detects a transaction to be out of its normal behavior we will contact the Fraud Contact on file or an authorized signer/officer on the account.
        - ***Please contact your account officer to review the Fraud Contact information we have on file. This will make the transaction verification process quicker so the transaction is not held up due to invalid contact information for Fraud Contacts.***
    - We will not release a transaction if the customer calls the bank, as phone numbers can be spoofed. We will call back to the phone number listed in our records.
    - We require written follow up to your verbal approval via fax or email for any canceled transactions.
    - It is our goal to respond within 15 minutes of a transaction being placed on hold but certain circumstances (i.e. meetings or training sessions) may increase our response times. Therefore wire transfers should be submitted by 1:00 pm and ACH transaction files should be submitted by 4:00 pm.

We also recommend that you take the following actions immediately to enhance your security.

- While our MFA (multi factor authentication) process is one very good way to protect yourself, you can make it even more secure by doing the following:
    - <u>Allow delivery of the temporary access code (TAC) to phones only</u> – Only allow your employees to have their secure access codes to be delivered via a phone number, cell phone number or via a text message. Delete all methods of TAC via email.

      <u>NOTE:</u> This is particularly useful in the event that a customer's computer is compromised and the user is set up to receive email TAC's.

    - We encourage all customers that use our Cash Management features, such as wire transfers and ACH transactions to receive a TAC code at each login (i.e. don't allow these users to register their computers) - If you force your users to get a TAC at each login and only allow TAC delivery to phones, this will significantly increase the level of security.

Revised: May 2019
Responsible Party: Electronic Banking Department

  - By using our security preference tab, you may also enter in an "anti phishing phrase" to ensure authenticity of our website. Also, inspect the secure delivery methods (TAC) to make sure you have control over each contact. If you see contacts that don't belong to you - contact the bank immediately.

- While all Cash Management customers have limits set within the online application itself, the limits could be more effectively deployed by requiring:
  - Require dual authorization (where appropriate) – All Cash Management applications support the ability to have dual authorization. Each payment type has the ability to turn on dual authorization. For your convenience and ease of use, we have mobile authorization services available. Please contact your account officer if you would like to turn on the dual authorization for your high risk transactions such as wire and ACH.
  - Review your limits – These limits are usually higher than needed. If left unchecked this creates unnecessary exposure.
    - We do perform annual reviews of the limits. However, if you have a significant decrease in ACH activity, you can request the limit be lowered. This helps reduce the exposure of having a higher than necessary limit.

- We highly recommend users with Supervisory access to change transactions or limits, do not register their computers so they will receive the SAC (Secure Access Code) at each login.

- Computer Use – Where practical, the computer used for Cash Management and Remote Capture activities should be dedicated for this purpose ONLY. This is commonly referred to as a "stand alone PC." The computer would only be used to conduct bank business and not used to access email, social media or any other internet browsing activities. This greatly reduces the risk of a virus or malware being loaded on to the computer.

- Virus Protection
  - Virus Protection should be installed with automatic updates, scanning, as well as malware detection software.
  - Never click on a message to install free software.
  - Never open an email attachment without contacting the sender to verify the validity of the attachment.
  - Never click on links in email unless you are expecting the email or have verified the validity with the sender.

- Apply all operating system security patches regularly. This ensures that the security patches are up to date.

- We will delete any inactive users if not active for a period of 6 months. For security purposes this is imperative that you do not have inactive users on the system.

- Limit administrative rights on the computer to help prevent the inadvertent downloading of malware or other viruses.

- We recommend clearing the browser cache before and after accessing Remote Deposit Capture to eliminate copies of web pages that have been stored on the hard drive.

- Never leave the computer unattended or unlocked when using online banking or Remote Deposit Capture. If you need to walk away, always log out of the website or lock the computer.

- Never access your online banking using a public Wi-Fi connection, such as an airport, internet café, public library, etc. These connections are not secure and unauthorized software could be installed to capture account and login information.

- Passwords
    a. All Cash Management users are required to change their passwords every 90 days. The changing of passwords will help protect against fraudulent activity.
    - We will **never** ask you for your password.
    - Password Complexity – We highly recommend that you use complexity measures to strengthen your password using upper, lower case letters, numbers and or symbols. We recommend that you do not use recurring letters or numbers i.e.: sss or 111 and that you do not use your passwords alternating by a single letter or number 121212 or ababab.
    - Sharing your password – Do not share your Login ID or password with anyone. This includes third party providers such as computer repair professionals or hardware technicians.
    - Using the same password – We highly recommend that you do not use the same password as your do for your online banking, email or any social networking accounts.
    - Avoid using automatic login features – Some browsers and programs will store passwords so you do not have to enter them upon each login. This poses a significant security risk.

- Mobile Banking – If you use our mobile banking or Advanced mobile applications for iPhone or Droid, you are safe and secure. You are still using your online banking Login ID, password and Mobile Authorization Code (MAC) code for any transfers.

    - Do not store your passwords on your phone unencrypted.
    - Do not store unencrypted personal information on your cell phone or any other unsecure application.
    - Critical data should be stored in a digital wallet or password manager with strong encryption, such as 256 bit AES to keep the data safe, secure and accessible.
    - When finished using mobile banking remember to sign off before accessing another application.
    - If you lose your phone, call your cell phone provider immediately so they can deactivate your phone.
    - If you lose your phone it is also imperative that you call us right away at 530-722-3940 to disable your Login ID and remove your cell phone number for your SAC (Secure Access Code) delivery method.
    - Utilize the “passcode” or auto-lock options available on your particular device.
    - If available, use the option that will erase or “wipe” your phone after too many unsuccessful passcode attempts.
    - If available, turn on the option to track and remotely erase your device if lost.

    Please see our “Mobile Banking Security Best Practices” for additional recommendations.

- Remote Deposit Capture

a. Ensure that the **firewall is turned on** for any computer access Remote Deposit Capture.
b. Do not retain checks longer than 45 days.
c. Checks should be stored in a locked, secure environment.
d. Do not leave checks unattended.
e. Checks should be stamped with the endorsement stamp
f. The scanner should be properly maintained so that the ink spray on the back of the check is legible both physically and on the check image. This provides extra security against checks being processed multiple times

- On a ***daily basis***, all Cash Management users should be verifying their online activity. ACH transaction files are pending until the daily cutoff time of 5:00 pm. Review all transactions prior to the cutoff time and contact us immediately at (800) 421-2575 if unauthorized transactions appear.

- All online banking users will be required to receive the following security alerts either by phone or text message:
  - Alert me when a computer/browser is successfully registered
  - Alert me when a new user is created
  - Alert me when an invalid password for my login ID is submitted
  - Alert me when my login ID is changed
  - Alert me when my security alert preferences are changed
  - Alert me when a recipient is added

- We have numerous alerts that we encourage all customers to use such as:
  - Alert me when forgot password is attempted for my login ID
  - Alert me when my password is changed
  - Alert me when a user profile is updated
  - Alert me when my user login is locked out
  - Alert me when the forgot password process is attempted unsuccessfully

- We also have transaction alerts that will notify you when transactions are authorized, cancelled, drafted, processed successfully or failed to process. We encourage all of our customers set up the following:
  - Change of address
  - External transfer
  - Bill Pay
  - Check Reorders

- When you're on our website logging into online banking we will never ask you for:
  - Your name
  - Your date of birth
  - Social Security number
  - Account number
  - ATM or PIN number

  If you are ever asked for any of this information at the time of login, STOP and do not login. Chances are you have been redirected to another site.

- Ensure that you have a qualified computer technician review your computer and network at least annually.

- We suggest that all Cash Management customers perform a risk assessment and evaluate their business at least annually.