eBusiness Banking
Security Best Practices

First American Bank has robust technology and procedures in place to prevent unauthorized access to your account. In recent months, the financial services industry has seen small and medium-sized businesses suffer data security breaches resulting in fraudsters gaining unauthorized access to the company's online banking platform. First American continues to monitor and adjust our security infrastructure based on the latest threats.

Due to many banks (such as First American) having more sophisticated IT security systems, the computer criminals are turning away from the tightly secured bank computers and are looking toward potentially weaker places in terms of security to attack: the bank client's computer systems. More and more attacks are being committed against small and medium-sized businesses because their computer security is viewed as more lax than large companies/banks, and they typically maintain a higher account cash balance than individual personal accounts.

First American Bank is advising adoption of the online banking best practices listed below. We strongly recommend all of our commercial clients implement the following procedures and tools to help prevent criminals from accessing company accounts:

- It is highly suggested that the Super User/Administrator for the company only use their access for resetting or setting up any sub users.
- The Super User/Administrator should have a separate login for doing Business Banking transactions. The reason this is suggested is, should the Super Users credentials be compromised, the fraudster has access to all controls and even the ability to create sub users allowing access to approve transactions.
- The Super User should be the only user that is permitted to add sub users for the company. Other sub users should not be allowed to add other sub users.
- The Company should allow one designated machine in the office for doing strictly Business Banking transactions. This machine should not be allowed to surf the internet, check email, etc.
- Take advantage of the highest levels of security protection First American has to offer, i.e. token authentication and dual control requirements.
- Pay attention to any fraud alerts posted on First American's website to make sure you are up to date on all hacking and fraud attempts appearing in the industry.
- The Super User Account should only be used on a dedicated machine which should be physically secured and password protected.
    - The criteria for a super user dedicated machine:
        - The computer should be physically secured.
        - The computer should be behind a physical firewall.
        - The computer should be placed on its own subnet if possible.

- All Security Patches MUST BE UP TO DATE.
- Anti-Virus software should be installed and definitions MUST BE UP TO DATE.
- Anti-Spyware / Anti-Malware protection software is also highly recommended.
- **Recommend downloading Malware Detection (Trusteer) on your computer(s) contact** Treasurymanagement@firstamb.com for more information.

- Best Practices should also be followed for any other computer that can approve any wire transfer or ACH transactions.

- Close all other applications and browser windows before initiating online banking.

- Look for any strange or foreign changes on the website. If you see anything different, call First American and verify these changes are legitimate and that you are on the bank's website.

- Verify use of a secure session ("https://" and not "http://"), and avoid saving passwords to a computer.

- Do not use the same password for multiple accounts.
  - Do not share passwords.
  - Use complex passwords
    - 8 – 15 characters.
    - Combine numbers, letters and special characters.
    - Do not write the password down.
    - Change the password at a minimum of every 90 days.

- Monitor your accounts frequently, and monitor and reconcile accounts daily as a best practice; immediately review wire, ACH or other commercial account transactions after receipt.

- Educate all personnel on good cyber security practices, clearing the internet browser's cache before visiting the financial institution's website, and how to avoid having malware installed on a computer.

- Prepare detailed, written procedures covering all processes performed using eBusiness Banking.

- Never leave a computer unattended when using any online banking or financial services, and always lock your computer when you have logged off such sites and leave it unattended.

- Change, revise and re-visit those IT employees who have high access levels for user approval, access rights and deleting/adding new users.

- Never access your financial institution's website for online banking (or any privileged or sensitive computer system) from a public computer at a hotel/motel, library or public wireless access point.

- Understand and carefully control the authorized users and permissions granted to any of your employees who are approved for online banking use and are issued unique User IDs, passwords (and tokens, if applicable).

- Immediately report any suspicious activity in your accounts to First American personnel; there is a limited recovery window and a rapid response may prevent additional losses.

- Do not click on a link in any e-mail purported to be sent from Bank; Bank official e-mails will always instruct you to log in to online banking for updates, instructions, notifications, account statements, etc.

- Be suspicious of e-mails purporting to be from other financial institutions, federal, state or local government departments or agencies, or taxing authorities that request account information, account verification or banking access credentials such as User IDs, passwords, PIN codes and similar information. Opening attachments, or clicking on links in such suspicious e-mails, can also expose your computer to malicious code or malware that will be installed to your computer. Remember, legal process, subpoenas, and information from government agencies still generally comes as regular snail-mail.

- Bank's online banking website is only scheduled for downtime for regular maintenance at certain times late in the evening/early morning, and never during prime business hours. If you log into online banking and receive a message such as "please wait for website update, which will take approximately 15 – 20 minutes," immediately contact Bank personnel to determine if it is a legitimate delay in online banking services caused by the Bank.

- Know about and understand Corporate Account Takeover (CATO)

    - Corporate Account Takeover is an evolving electronic crime typically involving the exploitation of businesses of all sizes, especially those with limited to no computer safeguards and minimal or no disbursement controls for use with their bank's online business banking system.
    - These businesses are vulnerable to theft when cyber thieves gain access to its computer system to steal confidential banking information in order to impersonate the business and send unauthorized wire and ACH transactions to accounts controlled by the thieves. Municipalities, school districts, large non-profit organizations, corporate businesses, and any customers that perform electronic transfers are potential targets.
    - Losses from this form of cyber-crime range from the tens of thousands to the millions with the majority of these thefts not fully recovered. These thefts have affected both large and small banks.
    - This type of cyber-crime is a technologically advanced form of electronic theft. Malicious software, which is available over the Internet, automates many elements of the crime including circumventing one time passwords, authentication tokens, and other forms of multi-factor authentication.
    - Customer awareness of online threats and education about common account takeover methods are helpful measures to protect against these threats. However, due to the dependence of banks on sound computer and disbursement controls of its customers, there is no single measure to stop these thefts entirely.
    - Multiple controls or a "layered security" approach is required.

If you suspect someone is attempting to gain access, or has already gained access, to your Online Banking information, immediately stop using any computers that may be affected and contact Bank personnel at 800-289-6140 to request help in preventing further loss and to aid in the possible recovery of funds fraudulently transferred.