CORPORATE ACCOUNT TAKEOVER INFORMATION FOR ACH ORIGINATORS/BUSINESS INTERNET BANKING CUSTOMERS

Please review this important information regarding the ACH Origination and/or Internet Banking services being provided to your company by First American Bank and Trust.

ELECTRONIC FUNDS TRANSFERS: REGULATION E

The protections provided by Regulation E on Consumer and Sole Proprietor accounts do not apply to your Commercial/Business account(s).

CORPORATE ACCOUNT TAKEOVER

One of the most serious threats which you must be alert for and guard against is the unauthorized transfer of funds from your business account to another location, which activity is referred to as a Corporate Account Takeover (CATO).

HOW CORPORATE ACCOUNT TAKEOVERS OCCUR.

- Criminals target victims using phishing techniques such as mass emails, pop-ups, friend requests, etc. They try to induce your company personnel to click on a link or open an attachment to an email which contains malware. Computers can also be infected with malware by logging onto a legitimate website which has been compromised, and in a number of other ways.
- Malware runs in the background of your computer and obtains information, including passwords, user I.D.'s, account numbers, and the normal pattern of your ACH activities. For example, if the company payroll is processed weekly or bi-monthly in an ACH file, criminals learn how large it is and how frequently it is sent.
- Malware transmits the information it has gathered to cyber criminals, who then use it to try to transfer funds from your bank account to a location of their choosing. They usually try to make it appear as if your company has instructed the bank to transfer funds from your account to a third party, or try to simulate your regular payroll, while changing the routing and account numbers to be credited in the transmission.

CORPORATE ACCOUNT TAKEOVER IS A GROWING PROBLEM.

- It is now estimated that most personal computers in the U.S. are infected with some form of malware.
- CATO was first reported in 2006. Fraud losses due to CATO continue to grow larger each year, and now exceed one billion dollars annually.
- Originally, CATO targeted large companies. Criminals are now targeting smaller business, municipal and non-profit organization accounts.

E-Mail Hijacking

A new and rapidly growing theft threat is criminals hacking into and hijacking your email, posing as you, and sending withdrawal or wire transfer instructions to your financial institution.

CONTACT BY FIRST AMERICAN BANK: ELECTRONIC BANKING CREDENTIALS

First American Bank will never email or call you to ask for your account number, password, or for information on your token. If anyone contacts you requesting that information, do not provide it. Instead, contact First American Bank at 1-800-738-2265 and ask to speak to our Security Officer, Michael Guillot.

RISK ASSESSMENT AND CONTROLS EVALUATION

You should conduct regular and thorough risk assessments on your ACH origination systems and procedures, and to take all action possible to minimize the chances that your employees or third parties access your ACH origination account and transfer funds to an unauthorized recipient. You should place strong controls on ACH transfers from your accounts, and periodically evaluate and update those controls.

RISK CONTROLS

There are a number of things you can do to reduce the risk of CATO and other types of theft or fraud losses in your ACH origination account. NO SECURITY MEASURE OR LIST OF SECURITY MEASURES CAN BE ALL-INCLUSIVE AND FOOLPROOF FOR PREVENTING THEFT. HOWEVER, THE FOLLOWING MEASURES WILL HELP TO REDUCE YOUR RISK OF LOSS, AND MITIGATE THE DAMAGES IF YOUR BANK ACCOUNT IS COMPROMISED:

ONLINE SECURITY MEASURES

- Install and maintain strong anti-virus and anti-malware programs on the computer used to conduct your online banking. The anti-virus and security software on all computer workstations and laptops used for ACH transactions should be robust. You should regularly verify that all anti-virus and security software is current and operating in the manner intended by its licensor. National Automated Clearing House Association (NACHA) rules and your ACH Origination Agreement with First American Bank require that the internet browser used to transmit ACH items support at minimum 128-bit encryption technology.
- Update your anti-virus, anti-malware and computer software frequently. Good patch management practices will ensure that your system protects your account against recent security vulnerabilities and new methods employed by criminals.
- Online banking passwords should be strong, and changed frequently. Passwords should not be stored on the computer used to conduct online banking, or written down and stored near that computer.
- Employees with access to online banking passwords should be instructed not to communicate them to others.
- The computer/device used to originate an ACH file/wire transfer should not be used to scan and fax ACH/Wire confirmations. Fax confirmation should be sent on a traditional paper-fed fax machine. It is recommended that the work station or laptop used for ACH files NOT be used for general web browsing or social networking. If the ACH workstation/laptop is not used for other online activity and is not connected to an internal company network, it is less susceptible to being compromised.
- Use dual control procedures. No one individual should be responsible for creating, sending and confirming an ACH file transmitted to First American Bank. Segregation of duties, particularly requiring that entering and approving of ACH batches be performed by two different persons, reduces the risk of loss due to theft by an employee. If you are unable or unwilling to utilize dual control procedures in ACH originations, you will be required to sign an OPT OUT/HOLD HARMLESS Agreement in favor of First American Bank and Trust.
- Monitor and reconcile your online banking account regularly, especially towards the end of the day. REPORT SUSPICIOUS OR UNAUTHORIZED TRANSACTIONS TO FIRST AMERICAN BANK IMMEDIATELY AT 1-800-738-2265 or VIA ONLINE BANKING MESSAGE.
- Instruct and train your employees on the risks of CATO and how to use online banking systems securely.
- Instruct company authorized online banking users to be alert for warning signs that your system/network has been compromised, which include:
    a. Inability to log into the bank's online banking system.
    b. Dramatic loss of computer speed.
    c. Changes in the way things appear on the computer screen.
    d. Computer locks up or fails to follow commands.
    e. Unexpected rebooting or restarting of the computer.

f. Unexpected requests to enter a password or click on a new link during an online banking session.
g. Unusual pop-up messages which say that the connection to the bank's online banking system is not working.
h. New, unexplained toolbars and/or icons appear on your computer screen.
i. You are unable to shut down or restart your computer.
j. You receive messages purporting to be from the FDIC, IRS, NACHA or another regulatory Agency, asking you to install software, click on a link, or provide personal identifying information. You should assume these are fraudulent in nature until you have confirmed them to be genuine by independently calling the organization, using a phone number obtained independently calling the organization, using a phone number obtained from a source other than the email. You should immediately report such suspicious emails or unauthorized activity on your account to First American Bank by telephone (1-800-738-2265) or via an online banking message.

- Make use of Resources Available for Business Account Holders. The following websites contain useful information on online security:
  a. The Better Business Bureau's website on "Data Security Made Simpler: http://www.bbb.org/data-security
  b. The Federal Trade Commission's (FTC) interactive business guide for protecting data: https://www.ftc.gov/tips-advice/business-center
  c. The National Institute of Standards and Technology's (NIST) https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

- Contact First American Bank immediately to report any of the above warning signs in your computer/system, or if identify a suspicious or unauthorized transaction on your online banking account. **CALL 1-800-738-2265 AND ASK FOR SECURITY OFFICER, MICHAEL GUILLOT OR VICE PRESIDENT KYLE BOURGEOIS.**

TOKENS

First American Bank's ACH Originators are currently required to use security tokens to conduct ACH file transmissions. Tokens are a valuable aid in reducing instances of theft by third parties from ACH Origination accounts, but they are not foolproof. There have been instances where criminals have been able to obtain access to accounts and divert funds despite the use of security tokens.

FACSIMILE CONFIRMATION OF ACH FILES

First American Bank recommends the use of Facsimile Confirmation of your ACH transmission files as an additional security measure. This entails faxing a written Confirmation of each ACH file on company letterhead to First American Bank and Trust with specific information confirming the ACH transmission. The fax should be sent via a traditional, paper-fed fax machine, not an electronic facsimile transmission. This confirmation is signed by an individual properly authorized to do so. In the event you choose not to implement facsimile confirmation of ACH Origination files, you must provide an "Opt Out and Hold Harmless" in favor of First American Bank.

YOU CAN FIND ADDITIONAL INFORMATION ON WAYS TO PREVENT TAKEOVER OF YOUR CORPORATE ACCOUNT AT WWW.NACHA.ORG.

NACHA RULES COMPLIANCE

ACH originators are required to maintain awareness of and comply with all rules of the National Automated Clearing House Association (NACHA). You may find them online at www.nacha.org.

SUB-USER DESIGNATION

The internet banking system allows your authorized Administrator to designate authorized sub-users, and enable them to access your account and initiate ACH files.

In order to do so, you must submit a request to add a sub-user to first American Bank, and that the bank enable the designated sub-user after verifying the request with the appropriate company manager.

FIRST AMERICAN BANK CONTACT

You may contact First American Bank to report suspicious account activity or other events as follows:

Michael Guillot
Security Officer
1-800-738-2265
225-265-2265
mguillot@fabt.com

If you cannot reach Michael Guillot, please contact:

Kyle Bourgeois
1-800-738-2265
225-265-2265
kbourgeois@fabt.com

Version 11.0 (10/8/2020)