Customer Education & Security Awareness Notice

Security Precautions & Procedures Relating to your Commercial Banking Relationship with NCB

Introduction

National Cooperative Bank, N.A. ("NCB") employs numerous security procedures and other safeguards to protect your information, but we need your help to make your accounts and transactions as safe and secure as possible. This document highlights security precautions that you can take to help protect your accounts, as well as the numerous security procedures NCB has established for its business customers. Working together, we can strengthen the protection of your critical information and reduce the risk of fraud.

How You Can Protect Your Accounts

One of the largest risks to our business customers is Corporate Account Takeover fraud, a form of corporate identity theft in which a company's online banking credentials – usernames, passwords, security questions, etc. – are stolen by malware loaded onto the customer's computers. Criminal entities can then initiate fraudulent banking activity, including wire transfers and ACH payments, on the customer's accounts using the Bank's security procedures. Therefore, it is critical that you guard against such attacks to your company's computers and systems. The steps outlined below will help guard against attacks, and we recommend that you discuss them with your IT team and train your employees regularly, as the diligence of your employees is often a critical factor in stopping an attack before it starts.

Another serious risk is called **Business Email Compromise fraud**, **in which a criminal outsider generates an email to a customer's accounts payable team that appears to be from the customer's CEO or CFO directing the team to pay a fraudulent invoice.** Likewise, your vendors may also fall victim to Business Email Compromise fraud and vendor invoice instructions may be altered without the vendor's awareness. Always validate invoice payment instructions verbally with your vendors at a known contact phone number. Numbers contained on an invoice may be altered. Again, ensuring your email is secure and your employees are trained to be on the lookout for these and similar frauds can limit or stop a loss.

General Operating System Precautions

- ✓ Ensure that you use current anti-virus and anti-malware products to protect yourself against malicious software that is created for the specific purpose of gathering information such as user ID, password, and other critical information that may be stored on your computer.
- ✓ Practice safe internet use. Never click on pop-up messages or links to applications contained in emails. Train your employees regularly with respect to avoiding embedded links and manually going to links that are sent to you. It is estimated that over 80% of malware is obtained from clicking on pop-up ads.
- ✓ Be suspicious of emails claiming to be from a financial institution, government department, or other businesses requesting account information, account verification, or banking access credentials such as usernames, passwords, PIN codes and similar information.
- ✓ Use caution when opening attachments and ensure they were sent from a trusted source.
- ✓ Be suspicious of any proposed transaction that requires you to send an advance payment or deposit by wire transfer.
- ✓ Consider designating a dedicated "locked down" computer to accommodate online banking transactions. The dedicated computer should not be used for email or any other internet activities. This precaution minimizes the opportunity to download malware.

- ✓ Install a dedicated, actively managed firewall, especially if you have a broadband or dedicated connection to the Internet, such as DSL or cable. A firewall limits the potential for unauthorized access to computer networks and computers.
- ✓ Ensure a vulnerability and patch management process is in place to keep your computer software current and can mitigate new vulnerabilities.

Account and Password Precautions

- ✓ NCB's commercial online banking system, Treasury 24/7, requires strong passwords and those passwords must be changed frequently. You should also require passwords to access any of your computer systems and should apply similar requirements. This will help prevent unauthorized use or access, which can lead to bank fraud.
- ✓ Ensure all employees' passwords as well as account information and security responses, are not written where they can be seen or accessed by others. If the information must be written down, it should be secured under lock and key when not being used.
- ✓ Your employees should never share their NCB username or password with anyone for any reason. If it is compromised, contact us to have the ID and/or password disabled or reset.
- ✓ Treasury 24/7 will timeout after a set period of inactivity. You should also make sure your computers have a password protected screensaver with a timeout feature to help prevent unauthorized access to your systems.
- ✓ Similarly, Treasury 24/7 does not permit automatic login features that save usernames or passwords, and you should avoid any such features across your computer systems.

General Business Practices

- ✓ Reconcile your banking transactions daily and look for unusual small amounts such as penny transactions. This may be an indication that your account has been compromised and a fraudulent plan is in progress.
- ✓ Never access bank, brokerage, or other financial services information at internet cafes, public libraries, etc. Unauthorized software may have been installed to trap account numbers and sign on information leaving you vulnerable to fraud.
- ✓ Immediately escalate knowledge of any suspicious transaction to us. Some forms of transactions, such as fraudulent ACH instructions, can be stopped if notice is received in time. Vigilance and immediate action, in the event of suspicious transactions or activity, is critical.
- ✓ Sign up for fraud alerts for fraudulent debit or credit card purchases.
- ✓ Talk to your insurance provider about adding cyber insurance terms to your business insurance policy.

Tips for Protecting Your Mobile Device

As the use of mobile devices continues to climb, cyber criminals are targeting mobile devices more frequently. With the increase in mobile device usage, mobile banking has become more common. It is easy to forget that your mobile device can be vulnerable, but any device connected to the internet is at risk. NCB suggests the following tips:

- ✓ Use the biometric features such as face or fingerprint reader on your smartphone. The use of passcodes should be used on other devices.
- ✓ Log out completely when you finish a mobile banking session.
- ✓ Protect your phone from viruses and malicious software, or malware, just like you do for your computer by installing mobile security software.
- ✓ Use caution when downloading apps. Apps can contain malicious software, worms, and viruses. Beware of apps that ask for unnecessary "permissions."

- ✓ Download the updates for your phone and mobile apps.
- ✓ Avoid storing sensitive information like passwords or a social security number on your mobile device.
- ✓ Tell NCB immediately if you change your phone number or lose your mobile device.
- ✓ Be aware of shoulder surfers. The most basic form of information theft is observation. Be aware of your surroundings especially when you are keying in sensitive information.
- ✓ Wipe your mobile device before you donate, sell, or trade it using specialized software or using the manufacturer's recommended technique. Some software allows you to wipe your device remotely if it is lost or stolen.
- ✓ Beware of mobile phishing. Avoid opening links and attachments in emails and texts, especially from senders you do not know. And be wary of ads (not from your security provider) claiming that your device is infected.
- ✓ Watch out for public Wi-Fi. Public connections are not very secure, so do not perform banking transactions on a public network. If you need to access your account, try disabling the Wi-Fi and switching to your mobile network. Consider using a Virtual Private Network (VPN) app to secure and encrypt your communications when connecting to a public Wi-Fi network. (See the Federal Trade Commission's tips for selecting a VPN app.)
- ✓ Report any suspected fraud to NCB immediately. Log into your NCB account often to check your transaction activity and report any suspected fraud to NCB as soon as possible.

Mail Fishing and Check Washing

Mail Fishing happens when thieves steal outgoing mail from U.S. Postal Service blue drop boxes before it can be picked up. There are several ways to commit mail fishing:

- ✓ Thieves will lodge a catching device inside the box and remove it before the scheduled pick up.
- ✓ Thieves may also apply ultra-strength adhesive to a string, tie it to a water bottle or piece of cardboard, and manually pull up the pieces of mail.
- ✓ Thieves may also steal keys to postal drop boxes to access mail.
- ✓ Gift cards, replacement debit or credit cards and/or checks (essentially any documents that can be cashed in, forged, or used to steal person information) are stolen.

Check washing is the process of erasing details from checks to allow them to be rewritten, usually for criminal purposes such as a fraudulent withdrawal from a victim's bank account.

Thieves can also use the account number and routing number from your checks to initiate electronic transfers. What you can do:

- ✓ Make outgoing payments via ACH/Electronic debit
- ✓ If a check must be issued, follow the below tips to avoid mail fishing:
    - ○ Use the letter slots inside your Post Office or hand your mail directly to your letter carrier.
    - ○ For collection boxes: Drop your mail off as close to possible to collection time. Avoid dropping mail in collection boxes at night or during holiday weekends.
    - ○ Check to see if your mail dropped down into the mailbox and is not hung up on any other surface.
    - ○ When dropping off mail, remain observant of cars and people who appear suspicious.

Thieves may also try to steal incoming mail including statements. Statements can provide valuable information to criminals including account numbers and check images that can be used to create fraudulent checks. What you can do:

- ✓ Sign up for online banking/electronic statements:
    - ○ To sign up for online banking go to **https://www.ncb.coop/commercial-banking/cash-management** and click 'Get Started' for either Small Business Online Banking or Cash Management

    - To sign up for e-statements log into your online banking and go to Settings > eStatement Preferences.
- ✓ Enroll in Positive Pay for checks or ACH:
    - Reach out to your account manager or send us a request for information at **https://www.ncb.coop/contact-us**.

COVID-19 Related Scams

Criminals are taking advantage of fears surrounding the COVID-19 pandemic. Scammers are using fake websites direct calls, emails, texts, and social media posts in attempts to get personal information. These communications could be promoting awareness and prevention tips, fake information about cases in your neighborhood, promoting fake work from home opportunities, soliciting donations, offering advice on unproven treatments, or providing fake information about government benefits.

Criminals are also targeting businesses now working in virtual environments and with limited staffing. Cyber-attacks are on the rise. Criminals are looking for vulnerable networks and using emails, texts, and social media posts to install viruses and malware to get access to your computer or other devices. Scams include bogus loans, grants, and relief programs supposedly from the SBA (Small Business Administration).

NCB's Security Procedures

Listed below are various security procedures relating to your accounts at NCB (unless modified or waived in writing). These security procedures are designed to ensure that payment and other instructions provided to us relating to your account are properly authorized by you, and under our account and service agreements, we are entitled to rely on transaction and payment orders originated using these procedures. Therefore, it is so important that you take steps, such as those set out above, to protect your computer systems and credentials.

Usernames and Passwords - When accessing Treasury 24/7, each employee or other company representative with access to accounts has an individual username and password that must be used. We strongly recommend that none of your employees use their Social Security number as their username.

Confirmed IP Address – If Treasury 24/7 does not recognize the IP address of the computer being used to access online banking as being authorized for your Company, the system will require authorization through a separate channel.

Secure Access Code (SAC) – Treasury 24/7 will use a Security Access Code (SAC) as an additional layer of security for certain system functions. To transfer money outside of NCB through Treasury 24/7 will require a SAC as part of the process.

Dual Approvals - Also to transfer money outside of NCB through Treasury 24/7, two users must authorize the payment. You may determine which of the Company's employees is authorized to initiate orders and which are authorized to approve them.

Timed log-off - Treasury 24/7 will automatically log a user off due to inactivity. This reduces the risk of other accessing information from a computer.

In addition to the above security procedures, NCB uses various firewalls and encryption to protect your accounts, and we are constantly updating these to make sure they remain current. We also use software to analyze transactions for unusual activity. Thus, you may get a fraud alert or other communication from NCB inquiring about a recent transaction. While such analytics cannot identify or prevent all fraudulent transfers, they can provide an additional layer of protection.

Should you have any questions or concerns, or believe you are a victim of fraud involving one of your NCB accounts, please contact our Online Banking team at 1-800-322-1251.