



# RECOGNIZING BUSINESS FRAUD AND HOW TO TAKE ACTION

If fraud happens to you we are here to help! Follow the steps outlined below if you believe you are the victim of fraud.

## Common Types of Digital Fraud



### BUSINESS EMAIL COMPROMISE

Wire fraud occurs when criminals use fake emails or phone calls to impersonate an individual or business you may have an existing business relationship with. Wire transfers, once initiated, are extremely difficult to reverse. If you receive a suspicious email, or feel you might be a victim of wire fraud, please follow the steps outlined below.

#### **If you believe you have suffered a Business Email Compromise and your email was compromised:**

- ❑ Notify your IT team of the situation to determine any steps that need to be taken.
- ❑ Reset your email password. If you've used the same password for other programs/systems, reset those passwords as well.
- ❑ A review will be done to determine if a new account needs to be opened or if digital banking needs to be restricted. If your full account number was available in an email, the account will be restricted and a member of our Treasury Management Team will reach out to you to discuss options.
  - Once resolved a new username and password will be required.
  - Once accounts are set up with Treasury Management services they will be removed from a restricted status.
  - If Treasury Management services are declined a new account will need to be opened and the Fraud Protection Disclaimer will be provided to you.
- ❑ Please work closely with your NBT branch to let them know any outstanding checks that need to be paid. Due to the restricted status all items will be reviewed to determine if they should be paid or returned.
- ❑ Complete attestation sent to you by the fraud department to re-enable digital banking.

#### **If you have fallen victim to a Business Email Compromise and sent funds to a fraudulent account:**

- ❑ Provide the email header information to your local branch or at [reportfraud@nbtbank.com](mailto:reportfraud@nbtbank.com).
- ❑ NBT will reach out to the receiving financial institution to inquire if funds are available to return.
- ❑ An Internet Crime Complaint Center (IC3) form can be completed at [IC3.gov](https://www.ic3.gov). This can be done by you or the bank.



# Common Types of Digital Fraud



## ACH FRAUD - BUSINESS

Automated Clearing House (ACH) Fraud can occur when account number and routing number are used to initiate debits through the ACH network. If you suspect your business account has been compromised or see suspicious or unauthorized electronic transfers, please follow the steps below.

- Complete disputes for unauthorized transactions by contacting your local branch or NBT Customer Service at 1-800-628-2265.
- The affected account will be restricted and if any unauthorized logins occurred digital banking will be restricted.
- The NBT Treasury Management Team will be contacting you about adding Fraud Prevention products (Check Positive Pay and ACH Positive Pay) to your current account. This will allow the account to remain open and enable you to authorize any future ACH payments to your account.
  - Once accounts are set up with Treasury Management services they will be removed from a restricted status. Digital banking can be enabled with a new username and password.
  - If Treasury Management services are declined a new account will need to be opened and a Fraud Protection Disclaimer will be provided to you.

Please work closely with your NBT branch to let them know any outstanding checks that need to be paid. Due to the restricted status all items will be reviewed to determine if they should be paid or returned.



## DEBIT CARD FRAUD

If your business debit card was lost, stolen, or you think your debit card is compromised in any way, please follow the steps below.

- Complete a dispute for all unauthorized transactions.
  - A new card will be issued, and the impacted card canceled.



## STAY AWARE



Visit our Business Fraud Information Center for the latest information, tips, and resources related to business fraud:  
[www.nbtbank.com/businessfraudinfo](http://www.nbtbank.com/businessfraudinfo)



Monitor your accounts daily and report any fraud concerns immediately to  
[reportfraud@nbtbank.com](mailto:reportfraud@nbtbank.com)



To learn more about NBT Bank's Fraud Protection Tools, contact us at 1-833-NBT-4BIZ option 5 or  
[www.nbtbank.com/treasurymanagement](http://www.nbtbank.com/treasurymanagement)

