Account Takeover Fraud

At EagleBank, customer security is important. If you have been a victim of Online Account Takeover fraud, it is important that you take action immediately. You have taken the first step by contacting us, but contacting EagleBank is not enough to protect yourself. Reporting any Online Account Takeover attack is important to help the FBI stop the fraudsters from continuing. This type of fraud may also be considered Identity Theft and may be reported to Federal Trade Commission and your local police department.

File a complaint, regardless of monetary loss, with FBI Internet Crime Complaint Center at www.ic3.gov. Be prepared to offer the following information:

- Victim's name, address, telephone, email, and company information
- Date of attack
- Circumstances of attack (email attachment, etc.) at the time the device shut down
- Any information you gather about the perpetrator such as address, phone, email, website, IP address, email header information
- Financial transaction information
- Any other information you think can assist

IdentityTheft.gov is the federal government's one-stop resource for identity theft victims. The site provides streamlined checklists and sample letters to guide you through any recovery processes.

EagleBank has compiled the latest security advice on our Security Page: www.eaglebankcorp.com/security. For ideas to help keep you up to date on the latest fraud protections available for commecial accounts, please visit our Risk Management & Fraud Protection Page at www.eaglebankcorp.com/fraudprotection or speak with your account representative.

Counterfeit or Altered Check Draft

At EagleBank, customer security is important. If you have been a victim of Counterfeit or Altered Check Fraud, it is important that you take action immediately. You have taken the first step by contacting us, but contacting EagleBank is not enough to protect yourself. Reporting any Counterfeit or Altered Check Fraud is important to help law enforcement stop the fraudsters from continuing.

File a complaint, regardless of monetary loss with:

- Your local police department.
- Federal Trade Commission at IdentityTheft.gov

EagleBank has compiled the latest security advice on our Security Page: www.eaglebankcorp.com/security.

For ideas to help keep you up to date on the latest fraud protections available for commercial accounts, please visit our Risk Management & Fraud Protection Page at www.eaglebankcorp.com/fraudprotection or speak with your account representative.

Business E-Mail Compromise

If you have been a victim of Business Email Compromise (BEC) fraud it is important that you take action immediately. You have taken the first step by contacting us.

Now that you have determined you are a victim of the BEC scam you must act quickly:

- Contact your local FBI office (www.fbi.gov/contact-us/field-offices) if the wire or ACH is recent. The FBI might be able to help return or freeze the funds.
- File a complaint, regardless of monetary loss, with the Internet Crime Complaint Center of the FBI at www.ic3.gov. Be prepared to offer the following information:

    - IP and/or email address of fraudulent email
    - Date and time of incidents
    - Incorrectly formatted invoices or letterheads
    - Requests for secrecy or immediate action
    - Unusual timing, requests, or wording of the fraudulent phone call or email
    - Phone number of the fraudulent phone calls
    - Description of any phone contact to include frequency or timing of calls
    - Foreign accents of the callers
    - Poorly-worded or grammatically incorrect emails
    - Reports of any previous email phishing activity

When you contact law enforcement or file a complaint, label your incident as "BEC", provide a brief description, and consider providing the payment instructions.

At EagleBank, customer security is important. We've compiled the latest security advice on our Security Page: www.eaglebankcorp.com/security.

For ideas to help keep you up to date on the latest fraud protections available for commercial accounts, please visit our Risk Management & Fraud Protection Page at www.eaglebankcorp.com/fraudprotection or speak with your account representative.

Identity Theft

At EagleBank, customer security is important. If you have been a victim of Identity Theft, it is important that you take action immediately. You have taken the first step by contacting us, but there is more you should do to protect yourself. You should report any identity theft to the Federal Trade Commission (identitytheft.gov) and your local police department.

Additionally, be sure to visit IdentityTheft.gov, the federal government's one-stop resource for identity theft victims. The site provides streamlined checklists and sample letters to guide you through any recovery processes.

EagleBank has compiled the latest security advice on our Security Page: www.eaglebankcorp.com/security.

For ideas to help keep you up to date on the latest fraud protections available for commercial accounts, please visit our Risk Management & Fraud Protection Page at www.eaglebankcorp.com/fraudprotection or speak with your account representative.

Mail Theft

If you have been a victim of mail theft it is important that you take action immediately. Report any mail theft and take steps to protect you and your business:

- Notify your EagleBank branch immediately to close your accounts if you suspect the thief obtained information such as statements, checks, debit cards, etc.
- Notify your local postal authority inspection service online at postalinspectors.uspis.gov or by calling 1-800-275-8777
- Call your local police agency to report the theft

At EagleBank, customer security is important. We've compiled the latest security advice on our Security Page: www.eaglebankcorp.com/security.

For ideas to help keep you up to date on the latest fraud protections available for commercial accounts, please visit our Risk Management & Fraud Protection Page at www.eaglebankcorp.com/fraudprotection or speak with your account representative.

Ransomware

If you have been a victim of Ransomware fraud it is important that you take action immediately. Reporting any ransomware attack is important to help the FBI stop the fraudsters from continuing.

File a complaint, regardless of monetary loss, with FBI Internet Crime Complaint Center at www.ic3.gov. Be prepared to offer the following information:

- Victim's name, address, telephone, email, and company information
- Date of attack
- Circumstances of attack (email attachment, etc.) at the time the device shut down
- Any ransom demand details, including Bitcoin wallet address information
- Specifics about any money you paid
- Any information you gather about the perpetrator such as address, phone, email, website, IP address, email header information
- Financial transaction information
- Any other information you think can assist.

At EagleBank, customer security is important. We've compiled the latest security advice on our Security Page: www.eaglebankcorp.com/security.

For ideas to help keep you up to date on the latest fraud protections available for commercial accounts, please visit our Risk Management & Fraud Protection Page at www.eaglebankcorp.com/fraudprotection or speak with your account representative.