Text Message Phishing Scam

At EagleBank, customer security is important to us. There is a quickly-growing phishing phone scam that targets banking customers via text message. Fraudsters use actual bank phone numbers and pretend to be with a bank's fraud department asking about fake "suspicious withdrawals." They may call the account holder about these fake suspicious withdrawals and send them a one-time verification PIN via text to ultimately obtain access to accounts.

If you have been a victim of a Text Message Phishing Scam it is important that you take action immediately. Here are steps you can take to protect yourself further:

- Do not call the number sent by text message but contact your local branch or online banking to confirm the text message. Change your password(s) on everything you can – especially those in conjunction with bank accounts, email, and social media. It is recommended using a device not known to be hacked (cell phone or another Computer). Also consider using one that is not connected to the internet wirelessly.
- File a report with the FBI Internet Crime Compliant Center at www.ic3.gov. The IC3 accepts online internet crime complaints from either the actual victim or from a third-party to the complainant.
- Initiate a local law enforcement investigation by filing a police report. Please ensure that any on-line banking accounts (both personal and business) are noted and perhaps restricted for activity.

EagleBank has compiled the latest security advice on our Security Page: www.eaglebankcorp.com/security. For ideas to help keep you updated on the latest fraud protection available, please speak with your account representative.

Text Message Phishing Scam

At EagleBank, customer security is important to us. There is a quickly-growing phishing phone scam that targets banking customers via text message. Fraudsters use actual bank phone numbers and pretend to be with a bank's fraud department asking about fake "suspicious withdrawals." They may call the account holder about these fake suspicious withdrawals and send them a one-time verification PIN via text to ultimately obtain access to accounts.

If you have been a victim of a Text Message Phishing Scam it is important that you take action immediately. Here are steps you can take to protect yourself further:

- Do not call the number sent by text message but contact your local branch or online banking to confirm the text message. Change your password(s) on everything you can – especially those in conjunction with bank accounts, email, and social media. It is recommended using a device not known to be hacked (cell phone or another Computer). Also consider using one that is not connected to the internet wirelessly.
- File a report with the FBI Internet Crime Compliant Center at www.ic3.gov. The IC3 accepts online internet crime complaints from either the actual victim or from a third-party to the complainant.
- Initiate a local law enforcement investigation by filing a police report. Please ensure that any on-line banking accounts (both personal and business) are noted and perhaps restricted for activity.

EagleBank has compiled the latest security advice on our Security Page: www.eaglebankcorp.com/security. For ideas to help keep you updated on the latest fraud protection available, please speak with your account representative.