CEO and Business Email Compromise (BEC) Fraud Awareness

Identity thieves exploit the personal information and identities of millions of Americans every year. Compromised personal and sensitive information can be used to commit fraud or other crimes that can cost you time, money and potentially destroy your credit. First Bank of Highland Park is committed to protecting the security of your personal and sensitive information.

Please be aware that First Bank of Highland Park will never:

- Require you to enter personal and sensitive information directly into an e-mail or other non-secure webpages
- Ask you to confirm, verify, or update your account, debit/ATM card or billing information via e-mail
- Send "threatening e-mails" stating to close or suspend your account if you do not take immediate action by providing personal information

Here are some ways that CEO Fraud is carried out:

- **Email Spoofing:** This involves the manipulation of an email address to make the sender's email address appear to be sent from someone or somewhere other than the actual source
- **Compromised Email Account:** Cyber criminals send a spoofed email issuing an urgent payment instruction to a staff member. Junior staff members may be targeted and are often instructed not to discuss the email with their colleagues.
- **Company Research:** The criminals use services like LinkedIn to gather information on business relationships, employee names and positions, and even a CEO or other executive's written communication styles

What are some precautionary measures to help avoid this fraud?

- **If something doesn't feel right, it probably isn't:** Be wary and trust your instincts. Ask "Would my CEO actually tell me to do this?" or "Why isn't this supplier submitting an invoice through the normal channels?"
- **Slow down:** Criminals plan their attacks around the busiest periods of the day
- **Initiate a call-back using registered records:** Do not use numbers mentioned in the email
- **Watch for the use of personal accounts:** Criminals may use what appears to be a personal email account so that the "reply-to" field is less suspicious. For example, [CEO name]_personal@gmail.com. This would often not flag spam rules and could appear legitimate. The use of personal accounts, though, should be a warning sign for recipients.
- **Do not access company email via a public device or free Wi-Fi**
- **Be mindful of information shared on social media platforms**
- **Do not respond to a suspicious email without verifying its authenticity:** If you think the email is suspicious, be sure not to click on any attachments or hyperlinks in the email and refer the matter to the appropriate person within your organization

If you believe you have been the victim of phishing or have any additional concerns, please contact your Personal Banker or Lender immediately. For additional information, visit First Bank of Highland Park's Identity Theft Protection page at **www.firstbankhp.com/identity_theft_protection.aspx.**