eTreasury+ Security Checklist

Protection, Alerts and Controls:

- **Password Protection:** A unique password or token PIN is the first step of securing your online information. Select a password/PIN that is easy for you to remember but not quickly guessed, like birthdays, sequential numbers or street addresses. Do not write down passwords and never click "save my password." Do not share your password/PIN with anyone. Our employees will never ask for your password.
- **PC and Anti-Virus Protection:** For all company PCs, keep all your operating system, browser, anti-virus and other software up to date. Set these systems to automatically update on a daily basis. Scan your PC with your anti-virus software on a regular basis to check for new viruses of spyware that may have been missed initially.
- **Dedicated PC:** If possible, dedicate a PC to use ONLY for eTreasury+ and other critical business functions to mitigate against the risk of PC and user credentials being compromised. This PC should not be used for email, social media, or common web browsing. A compromised PC is the most common avenue for fraudsters to conduct fraud. The PCs used for the purpose of eTreasury+ need to be secure and free of viruses.
    - If you will be using the eTreasury+ PC(s) for other functions, be sure to use only known commercial software and visit only known and trusted websites when browsing the internet. Avoid downloading “free” software or clicking on links in e-mails; downloads, e-mail attachments, and malicious websites are a common source of virus infections.
- **Email Alerts:** eTreasury+ offers enhanced alert functionality, which notifies end users via email of account activity. All eTreasury+ users should review the available alerts and configure them for use to monitor for suspicious activity. If you receive an alert for a change or transaction that you did not make, contact our Commercial Client Support team at (866) 831-5717 for assistance.
- **Transaction Review:** Check your account balances and transaction activity daily and promptly report any suspicious activity to your account manager or call our Commercial Client Support team at (866) 831-5717.
- **Administrative Dual Control:** Prevents new users from being added and activated without a secondary approval. Prevents changes to existing users entitlements without a secondary approval.
- **Transaction Dual Approval:** Prevents a single user from creating and approving transfers, ACH and Wire transmissions. This is an important fraud control. Companies should have procedures in place to segregate duties and require a second set of eyes prior to transmission of these transactions.
- **Daily Limits Assigned:** eTreasury+ allows Admin users or the bank to set daily limits based on ACH and Wire types of transactions, accounts and by user. These limits should be based on need but restricted to where unusually high activity would require an override.

eTreasury+ End User Awareness:

- **Awareness:** People's United Bank encrypts all traffic between your PC and our online banking systems. When accessing the site look for security certificates, locked padlock symbols, and a URL that begins with "https". If the appearance of eTreasury+ screens looks different, new fields appear, or if you are asked to enter/verify sensitive information, report the issue to the bank for validation.
- **Internal Training:** Review entitlements and internal procedures to ensure access best practices are followed for PC and Online usage. Be sure employees using eTreasury+ are adequately trained on security best practices and practice safe computing habits.
- **Fraud Awareness:** Fraudsters use official-looking e-mails (Phishing) and websites to lure you into revealing confidential personal or financial information. The messages appear to be from trusted banks, retailers or other companies. Companies would never ask for sensitive information or passwords via e-mail. Be suspicious of any e-mail with urgent requests to "verify account information." When in doubt, call the sender directly and validate the message. The safest measure is not to click on links received via email from anyone, even those that appear to be trustworthy.
- **Security Center:** Peoples United Bank provides updated warnings, fraud education, recommendations for protecting your accounts, and links to other resources on the Security Center found at www.peoples.com/security.

eTreasury+ Support Contact Info:

Quick response to potential fraud incidents is key to minimizing losses and other disruptions. If you suspect there is fraud on your account, have general security concerns, or need assistance configuring the eTreasury+ security controls, please contact our Commercial Client Support team at (866) 831- 5717.