ONLINE BANKING SECURITY AND FRAUD PREVENTION BEST PRACTICES

Online fraud is on the rise, so here are some recommendations to help you protect yourself:

ONLINE BANKING USERS

- For clients on Cash Management Online with external transfer capabilities, it is highly suggested that a dual approval security is implemented as another layer of security.
- When logging into Private Banking or Cash Management Online, it is best practice not to use public computers or other unsecured computers.
- Avoid conducting online transactions in hot spots or on unknown network connections.
- Avoid using computer features where usernames and passwords are saved.
- Never share log-in information with anyone and/or third-party vendors.
- Users should always check their last log-in time whenever using their Online Banking system.
- Users should review account balances and transaction details on a daily basis to confirm the validity of account activities and immediately report any suspicious activities to the Bank.
- To limit account exposure and obtain better electronic record keeping, users should use the Online Bill Payment system instead of checks whenever possible.
- Users must take advantage of the alerts and notifications that the Bank offers, below are some examples:
    - Balance Alerts
    - Outgoing Wire Transfer Alerts
    - Debit Card Alerts
    - ACH Debit Alerts

COMPUTER SYSTEMS

- Never leave your computer unattended while using the Online Banking system.
- Never respond to suspicious e-mails or click on any hyperlink embedded in suspicious e-mails as they may contain a malware that can hijack your online session and conduct fraudulent transactions.
- Never conduct transactions while multiple browsers are open.
- All computer systems must have anti-virus or spyware detection software installed and scan the PC in real time. Free software may not provide sufficient protection against the latest threats in comparison to industry standard product.
- All computer systems must be updated regularly with the latest versions and patches of both anti-virus and spyware detection software.
- All operating systems and key applications must be patched regularly.
- If possible, refrain from conducting online banking transactions on the same computer used for internet surfing.

It is important to remember that the Bank will never ask you to provide your account number or other personal information via telephone calls, texts, or email. Please disregard such requests and report the incident to the Bank immediately.

IF YOU BECOME A VICTIM of Identity Theft or Phishing attempt, immediately contact the following bureaus:

- Equifax- 800.525.6285, Experian- 888.397.3742, and TransUnion- 800.680.7289.
- File a complaint with the Federal Trade Commission at ftc.gov or 877.382.4357, or the Anti-Phishing Working Group at antiphishing.org.
- Social Security Fraud Line 800.269.0271.
- File a police report locally at the police station in the community where the act was committed.

ALSO REFER TO these government entity sites for more information:

- The United States Department of Justice on Identity Theft and Identity Fraud

- Resources from the Government on Identity Theft
- State of California Department of Justice on Identity Theft

FOR MORE INFORMATION on Online Banking Security and Fraud Prevention Best Practices:
Please visit The Private Bank of California's website at http://www.tpboc.com and click on the "View Now" button, located in the middle of the website, which will take you to the Bank's Online Educational Center where you can select the various security online tutorials. Please call our Cash Management Group at 310.286.0710 for any concerns or questions regarding Online Banking Security.