Recommended Security Procedures

PC and Mobile Devices and Internet Connectivity

- Install a dedicated, actively managed firewall, especially if there is a broadband or dedicated connection to the Internet, such as DSL or cable.
- Access only trusted websites for business purposes.
- Restrict computers from accessing personal email accounts.
- Install commercial anti-virus, spyware detection programs on all computer systems and ensure they are updated regularly.
- Never leave a computer unattended while using any online banking or investing service.
- Avoid accessing bank, brokerage, or other financial services information using public or shared computers at cafes, public libraries, or any other unsecure locations.
- Develop internal procedures to identify and isolate computers from the network that become infected with malware, making certain infected computers are fully remediated prior to reintroducing them to the network.

Password and Username Management

- Do not use online portal passwords for another non-related website.
- Never share usernames and password information.
- Create strong, long, and unique passwords and usernames.
- Use a variety of characters when creating you password, such a mix of capital and lowercase letters, numbers, and special characters.
- Even if not required, update your password periodically.
- Avoid using personal information as component of your password.
- Store passwords in a secure and protected password management tool.

Email Practices

- Do not open file attachments or click on web links in suspicious emails or from unfamiliar email addresses.
- Be on the lookout for grammatical errors or other typos as red flags for fraudulent emails.
- Exercise caution from emails requesting sensitive information, as trusted sources will typically not request such information via email.
- Ensure accuracy of email addresses from seemingly trusted sources – criminals will sometimes create what appears to be a valid email address from a trusted source with slight typos in the username or extension of the email address.

Online Banking Fraud Mitigation Tools

- Enroll in Check Positive Pay to utilize HTLFs check verification system and combat check fraud.*
- Enroll in ACH Positive Pay to review and return unauthorized ACH transactions on deposit accounts.*
- Use notifications to alert you of transaction status changes.

Transaction Processing Best Practices

- Utilize dual control for electronic transaction origination on products including Bill Pay, ACH Origination, and Wire Origination.
- Send prenotes when using ACH Origination to verify recipient account information is correct to avoid returns or notifications of change on real dollar transactions.
- Periodically review and confirm recipient information.
- Leverage segregation of duties for payment approvals and entitlement changes.
- Set appropriate limits for individuals origination transactions that align with your business practices.
- Create templates to eliminate errors in manually keying account information.
- Do not accept payment information via unsecure electronic channels.

Remote Check Processing Security

- Properly disposal of checks no sooner than 30 days.
- Equipment and deposited items maintained in a secure location.
- Controls and segregation of staff duties involved with reconciling deposits.
- Proper upkeep and cleaning of equipment to ensure satisfactory image quality.
- Development of a contingency plan in the event you are unable to access your Remote Check Processing service.

***Contact your Sales Representative for additional details for these services. HTLF Bank recommends the use of these services. Your failure to use these services may result in greater liability to you.**