

# **Business Security Guidelines**

As part of S&T Bank's continued commitment to maintaining your security and privacy, the following checklist of controls regarding Business Online Banking, ACH Origination and Checking Account Management are strongly advised for implementation for your protection.

1. ***Anti-virus and anti-spyware protections are critical to maintaining a secure and trouble-free computing environment.*** Key-logging, the process of stealing password and user information, is a well known practice with respect to cyber crime. In this case, software is unknowingly downloaded to a user PC when visiting some websites or receiving malicious e-mails. Once it is loaded onto your PC, sensitive personal and financial information can be captured and sent back through the Internet to potential hackers without your knowledge.

The best way to prevent this type of information theft and potential financial loss is to protect your network with software designed to eliminate potential spyware downloads. There are various viable solutions on the market today that combine anti-virus and spyware applications for your protection. Please note: it is critical to update your software frequently to capture new variations of virus and spyware releases.

2. ***Dual control over the approval and origination of financial transactions is an inexpensive, simple and effective control.*** This can be set-up within Business Online Banking and requires two individuals to approve and send financial transactions electronically. This practice helps protect your company from internal theft as well as external fraud by requiring more than one individual to execute any electronic financial transaction such as ACH origination.
3. ***Review your account transactions daily and reconcile frequently.*** This will help you to quickly identify any financial discrepancies and react quickly to potential fraud or financial irregularities. The reconciliation process should be entirely separate from those with check signing authority.
4. ***Passwords should be changed frequently, never written down, or shared with co-workers.*** Password protection is one of the most effective deterrents against electronic fraud. Administrator passwords have the most significant risk and exposure to fraud, as they can be used to create any kind of financial transaction. Passwords should be difficult to guess and should be composed of both alpha and numeric characters. Computers should be turned off every evening and logged out for any extended period of time that employees are away from their desk.
5. ***Implement physical and logical security controls over Business Online Banking.*** Having reasonable but effective controls within your business can help ensure you are not unnecessarily exposed to potential fraud or loss as a result of the origination of

unauthorized transactions. ACH limits should be set at the lowest possible levels and alternative products such as wire transfers should be utilized for larger financial transactions when necessary. Wire Transfers add additional controls in the set-up and validation processes, which is strongly recommended for your financial protection.

6. **Consider purchasing business insurance such as cyber insurance.** This insurance is designed to protect your company from fraud losses in the event access to Business Online Banking is compromised and unauthorized transactions are originated leading to financial loss. To learn more, please refer to the *Insurance Services* section on the [stbank.com](http://stbank.com) website.
7. S&T Bank offers two in-house fraud solutions to our business customers to reduce both check fraud and ACH fraud. **ACH Debit Filter** blocks any unauthorized ACH debit transaction attempting to post to your account. **Positive Pay** quickly identifies unauthorized checks in a similar manner and provides daily reports directly through Business Online Banking of unusual activity.

*If you would like additional information on either of these fraud solutions, please call one of our Business Banking Specialists at 1.888.935.2274.*