SunTrust
Live Solid. Bank Solid.

Online Fraud Protection: Best Practices Checklist

General

- ☐ Educate users to not share passwords or divulge account or login credential information such as Personal Identification Numbers (PINs) or user IDs to anyone.
- ☐ Create passwords that are memorable but would be difficult for others to guess. Do not write them down.
- ☐ Do not click links or otherwise respond to requests for information in unsolicited emails.
- ☐ Review user activity reports available in online cash management systems throughout the day to ensure appropriate usage.
- ☐ Ensure that all computers in your department have the most recent operating system updates and current virus protection software, and exist behind company firewalls.
- ☐ Conduct frequent audits of your payment processes.
- ☐ Use a dedicated computer not used for web surfing or email to perform online cash management activities.
- ☐ Avoid conducting online banking business activities on home computers or at publicly shared locations such as those at hotels, airports, coffee shops, or shared business centers.
- ☐ Report any suspicion of viruses or slow computers to the appropriate authority at your company.

Online System Administration

- ☐ When employees who have online user access leave, remove the access as part of your exit procedures.
- ☐ When employees go on vacation, temporarily disable their online access.
- ☐ Remove online services and accounts that are not needed to fulfill job functions from employees' user IDs. This includes limiting access to high-risk functions, including payment transactions and user entitlements.
- ☐ Implement dual system administration responsibilities by segregating the setup and verification of user ID maintenance tasks.
- ☐ Ask your banks for a payment transaction dual approval process that can't be disabled by your company security administrator(s).
- ☐ Set approval limits at the user level, account level, dollar amount level, and/or transaction type.
- ☐ Request monthly password updates and use strong password formats (e.g., alphanumeric with length greater than 5 characters).

Payments

- ☐ Set up alerts to notify multiple managers of payments initiated above an appropriate threshold amount that warrants management attention.
- ☐ Use Universal Payment Identification Code (UPIC) for accounts that you use to collect payments from your trading partners.
- ☐ Implement dual approval by segregating duties among employees for template maintenance, payment initiation and payment approval functions.
- ☐ Initiate and approve transactions from separate computers to help protect against malware.
- ☐ Use a repeat template for high-dollar, repetitive wire transactions to reduce the chance of misrouted funds.
- ☐ Use fraud blocking services offered by your banks to protect your accounts from unauthorized debit access.

For More Information

For additional resources and tips, please visit **suntrust.com/alert** or contact your SunTrust representative. If you suspect you have encountered a fraud attempt on your SunTrust account or accessed SunTrust services from an infected computer, report it by calling 800.447.8994.

SunTrust Client Commitment: SunTrust will never send unsolicited emails asking you to provide, update, or verify your personal or account information such as passwords, Social Security Numbers, PINs, credit or Check Card numbers, or other confidential information.