

Fraud Protection: Best Practices Checklist

General

- Conduct background checks on new hires and vendors
- Separate and rotate financial responsibilities such as payment initiation and account reconciliation to assist with preventing collusion.
- Safeguard systems and passwords, and do not share passwords or user IDs
- Keep bank authorization lists up to date with personnel changes
- Establish, enforce, document, and train security procedures and payment policies; review them annually
- Conduct surprise audits of your payment processes, and review activity reports
- Shred sensitive information such as financial reports and employee data
- Do not send confidential or personal information by email outside your company
- Know your business partners - fraud can occur when an organization believes the perpetrator is legitimate
- Mask or truncate account numbers and tax ID numbers in your correspondence

Check Fraud Protection

- Purchase check stock from known vendors
- Store check stock, deposit slips, bank statements and cancelled checks in a secure location
- Follow secure check and check stock destruction processes
- Implement dual controls over check stock, check issuance and account reconciliation
- Utilize available check fraud protection solutions such as positive pay with payee name verification, and reverse positive pay

ACH and Wire Fraud Protection

- Segregate accounts for better control: for instance, collection vs. disbursement activity, high-volume accounts vs. low-volume accounts, or ACH debits vs. ACH credits
- Monitor and reconcile your transactional accounts daily
- Protect your accounts against incoming unauthorized ACH transactions by taking advantage of ACH fraud control products to block all debits, authorize single transactions, or authorize recurring transactions (requests that do not meet your criteria are rejected)
- To protect your receivables accounts, use a UPIC (Universal Payment Identification Code) - a dummy account number you give to trading partners so they can pay you by ACH, with debits automatically blocked
- Separate wire and ACH initiation and approval responsibilities, and establish transaction limits for each employee
- Establish repetitive wire templates, and review the list on a regular basis
- Employ all available security features, including dual administration, dual approval, user entitlements, and authentication devices
- Consider using the reporting and monitoring capabilities of online services
- Review wire and ACH details - including advices and alerts - related to each transaction immediately

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.