Internal Controls Best Practices

Reduce the risk of payments fraud in your business through communication, awareness and controlling the opportunity with strong internal controls. These best practices have been collected from various industry sources. Park Bank makes no recommendation as to which best practices are appropriate for your business. Since every business is unique, Park Bank strongly recommends that you contact your accounting professional to evaluate your system and suggest best practices for your business.

- Segregate responsibilities among different employees for payments, template maintenance, bank deposits, payment entry and payments approval to ensure access is restricted to authorized personnel.
- Use multi-factor authentication tools such as tokens and digital certificates.
- Initiate ACH and wire payments under dual control using two separate PCs.
- Use robust and different passwords for different applications. Keep passwords confidential.
- Choose electronic delivery of statements and account information. If paper is necessary, shred account statements and documentation, or secure in locked storage.
- Ensure that blank check stock, signature stamps, facsimile signatures and card stock are stored in a secure environment with inventory control.
- Use check stock with security features.
- Segregate duties for creating, approving and releasing wires.
- Prevent users from sharing login credentials for accountability and security reasons.
- Monitor and reconcile accounts at least daily, including outbound ACH and wire transfers.
- Establish and review controls and limits for all payments and wire transfers.
- Return unauthorized ACH debits no later than the opening of business on the second banking day following the settlement date of the original entry.
- Require two signatures on checks or payments exceeding a pre-determined level.
- Make sure your ACH payment procedures comply with ACH rules:
  - Verify routing numbers
  - Secure Internet session (minimum 128-bit SSL encryption technology)
  - Conduct annual security audit
- Separate supplier/vendor creation and payment approval functions. Mask account and tax ID numbers in emails and use an encrypted email service.
- Purchase orders allow you to review the transaction before finalizing payment. Develop and follow a purchase order process: Who is able to initiate and issue?
- Review supplier lists. Do you run a credit report on new suppliers and have guidelines for entering a new supplier? Review changes to the supplier master file.
- Never share any confidential information, especially Social Security numbers, tax IDs, or account numbers via email. Park Bank will never ask for confidential information via email.
- Limit access to the Internet. Install only business-related programs.

PARK BANK
first IN LASTING RELATIONSHIPS®

Implement policies and procedures:

- Manage user access and passwords; promptly delete online user IDs as changes warrant (reassignments, terminations, etc.).
- Develop standards for when and how Social Security and account numbers should be used, displayed and printed.
- Conduct thorough background checks on new employees, possible periodic checks.
- Complete a fraud risk assessment and review it regularly.

Employee education:

- All employees on the business's shared network need to be educated on online fraud, regardless of job duties.
- If one computer on a shared network becomes infected, it can infect the entire business's network.
- Conduct surprise audits on financials, employee activity, and accounts. The Administrator in Business Online Banking can access a report of all activity performed and the user who made the changes. This is located within the Administrator tab and titled, "View User Activity Report". Share results with employees.
- "Does this make sense?" Think critically of each phone call and/or email received, especially if they are requesting personal information or asking you to access information from a link or attached file.
- Strongly encourage the use of complex passwords and proper storage of login credentials. Discourage sharing login information.
- Have employees sign a security agreement, acknowledging that they will properly use the company computer, systems and Internet.

Tips from leading experts:

- Designate a principal individual or unit responsible for fraud.
- Based on potential negative financial impact, approach fraud exposure and mitigation as a vital part of your business versus a function.
- Ask questions to understand your risk exposure.
- Identify and stay current on the threats to your assets.
- Enforce mandatory vacations or job rotation. Many internal frauds require manual intervention and are discovered when the employee is away on vacation.

Fraud protection services and features to consider:

- Positive Pay/Payee Positive Pay
- ACH Positive Pay, ACH Debit Block and Debit Filters
- Account Reconciliation
- Direct Deposit
- Alerts, limits and approvals
- E-Statements