Fraud prevention best practices

Build your foundation on best practices

Establishing consistent fraud prevention practices is the first step in creating a fraud prevention program. It's an essential part of demonstrating your organization's commitment to providing ordinary care under the Uniform Commercial Code.

Best practices will help you identify the components of a fraud prevention program.

Use our U.S. Bank Fraud Prevention Checklist to further assist you in developing your fraud prevention program.

Define your fraud prevention program	Assess your payment fraud risk, segregate payments by account and apply appropriate bank solutions. • Consider an integrated treasury management system with built-in fraud prevention. • Convert from paper checks to electronic payments where possible. • Regularly review fraud prevention best practices and solutions for effectiveness.
Manage employees and organize tasks	Educate employees to recognize fraud and separate account management and cash management tasks. • Separate tasks by function and vary procedures by day and individual. • Enforce mandatory vacation policies. • Contact your local chamber of commerce or police department for sources of fraud prevention training.
Conduct timely account reconciliation	Monitor and reconcile accounts promptly to ensure timely and efficient account reconciliation. • Utilize bank account reconciliation tools. • Examine signatures on paid checks. • Verify sequence in serial or check numbers.

Maintain secure electronic environment	Maintain up-to-date systems and software, and establish policies and procedures that maintain secure passwords and security tokens. • Establish dual controls by separating tasks of issuing and approving online payments. • Use security tokens and secondary authorization from a separate workstation. • Limit Internet use on computers used for online banking.
Issue secure checks	Ensure your accounts are set up properly and notify your bank when changes occur relating to your check authorization. • Notify your bank when a checking account should be closed. • Only sign checks once the recipient and amount information is completed.
Secure check storage	Separately maintain check supplies and check producing equipment in a secure, locked facility. • Use secure check stock with a minimum of eight security features. • Limit access to check supplies and equipment and conduct frequent surprise audits. • Frequently change procedures and rotate responsibilities of personnel.
Accept authorized checks	Ask for appropriate identification and use check verification services to ensure checks are authorized. • Vary deposit procedures by day and individual, and review daily reports. • Use bonded couriers to make deposits.

Case file:

An organization initiated ACH transactions over the Internet for vendor payments and direct deposit of payroll. A virus-infected workstation detected ACH payments by capturing keystrokes, enabling a criminal to send an ACH payment resulting in loss of tens of thousands of dollars.

Solution: Dual controls for payment initiation and payment approval would have prevented loss.

Help protect your organization with the Fraud Prevention checklist.

Fraud Prevention Checklist

To ensure you have controls in place to protect your organization, use this checklist to assist with your periodic fraud prevention procedures review.

Review and update internal procedures and controls

	Train personnel on fraud prevention best practices
	Establish dual control procedures for ACH, remote deposit capture and wires
	Review employee access privileges and limit administrative rights on company computers
	Establish clear division of duties within accounting departments Separate account receivables and account payables functions and processes
	Only provide employees with access to financial data if there's a business need
	Conduct surprise audits to ensure appropriate procedures are being followed
	Preauthorize high dollar value checks before the checks are written
	Do not sign checks without the recipient and amount information completed
	Verify out-of-pattern payment instructions from internal employees
	Validate all payment requests from customers and company personnel, including senior officials
	Validate requests from vendors to change payment instructions; don't simply reply to email
	Review transactions before they leave the company
	Review and update bank signature cards routinely
	Remove executive signatures from your annual report to prevent illegal scanning and use

Fraud Prevention Checklist (continued)

Ensure online fraud protection

	Keep workstations current with security updates Confirm all anti-virus software is up to date Respond to software and security update alerts promptly Ensure protection on all computers and schedule routine updates
	Apply operating system updates promptly; beware of download requests from pop-ups or advertisement
	Avoid using email to send confidential information; truncate all but last four digits of account numbers
	Prevent malware infection Use caution when downloading applications or documents, installing software and opening email attachments Limit Internet use on computers used for online banking activities
	Limit personal email and Web surfing access on computers used for monetary transactions
	Use dual authorization for adding users and changing user profiles
	Require use of security tokens, with strong authentication, for payment applications
	Use dual authorization when initiating ACH or wire payments
	Establish separate controls for your business online banking application Use one computer to create online payments and a different computer for secondary approvals
	Monitor account balances and activity daily Report any suspicious activity immediately to your bank
	Consider the use of an anti-malware application, as well as a firewall
	Schedule updates frequently
	Check your operating system on a regular basis
	Install all the latest patches and updates
	Activate all the notification features available in the bank's online banking application Ensure proactive notification to all users of any suspicious activity
	Ensure users of financial applications are familiar with system screens and functionality, so suspicious screens are easier to spot and reported quickly to the bank
	Ensure user access and entitlements are up to date and accurate

Evaluate your paper check supply

	Select a highly qualified, established check vendor
	Use one style of checks for each account for easy recognition
	Incorporate security features into check design
	Monitor check orders to ensure receipt of exact quantity
	Store blank checks and check printing equipment securely
	Limit the working supply of checks removed from the secure area