

Use these best practices to help you maintain a strong fraud prevention program.

## **Internal Procedures and Controls**

### Establish fraud prevention best practices and responsibilities

- Educate personnel regularly on the importance of safeguarding sensitive information, following established procedures and preventing fraud losses
- Ensure your staff understands they have the most important role in preventing fraud losses
- Refresh training regularly

### Establish clear division of duties and access

- Separate account receivables and account payables functions and processes
- Limit financial data access only to employees if there's a business need; follow the need-to-know principle

### Ensure procedures are being followed

- Conduct surprise audits
- Review transactions before they leave the company
- Verify out-of-pattern payment instructions from internal employees
- Review downstream processes for cyber security and fraud mitigation

### Use a second communication channel to validate payment related requests, including:

- Payment requests from customers and company personnel, including senior officials
- Requests from vendors to change payment instructions

### Update signing authority

- Review and update bank signature cards routinely
- Remove executive signatures from your annual report to prevent illegal scanning and use

## **Online Fraud Protection and Controls**

### Protect your workstations

- Update operating system, software, anti-virus, and malware protection
- Limit personal email and Internet use on computers used for online banking activities
- Back up data on separate servers regularly as this helps mitigate ransomware attacks

### Prevent malware infection

- Use caution when downloading applications, documents, installing software, opening email attachments
- Beware of download requests from pop-ups or advertisements
- Consider using an anti-malware application, as well as a firewall
- If you believe that your cyber environment was compromised, engage an outside cyber forensics firm to complete a comprehensive review

### Safeguard your communications and confidential data

- Avoid using email to send confidential information but if you must, utilize encryption software
- Truncate all but last four digits of account numbers in communications

### Establish separate controls for your business online banking application

- Require approvals to authorize ACH, wires, remote deposits and adding users or changing user profiles
- Ensure initiators and approvers use different workstations and require DUAL approvals
- Require use of security tokens, with strong authentication, for payment applications
- Review employee access privileges and limit system administrative rights
- Remove privileges for terminated employees
- Ensure user access and entitlements are up to date and accurate
- Ensure users know their system webpages and functionality, so suspicious content is easier to spot and is reported quickly to the bank

Monitor account balances and activity daily

- Report any suspicious activity immediately to your bank and alert your users
- Activate notification features in online banking applications

### **Paper Check Controls**

Check approval practices

- Preauthorize high dollar value checks before the checks are written
- Do not sign checks without the recipient and amount information completed

Review your check stock controls

- Select a highly qualified, established check vendor
- Use a different style of checks for each account for easy recognition
- Incorporate security features into check design
- Store blank checks and check printing equipment securely
- Limit the working supply of checks removed from the secure area

Check processing controls

- Monitor check orders to ensure receipt of exact quantity

### **Bank Fraud Prevention Solutions**

For online access

- Receive payment service alerts by email notification

For paper check disbursements

- Review exceptions daily and make payment decisions: Positive Pay
- Review payee exceptions daily, make payment decisions: Positive Pay - Payee Match Option
- View check images online, eliminate storing cancelled paper checks
- Outsource check processing to eliminate the storage of check supplies

For deposit-only

- Reconcile deposits weekly or more frequently

For ACH transactions

- Ensure dual authorization is required
- Ensure approvers are vigilant in their final review and approval of all outbound monetary transfers
- Set appropriate transaction limits
- Review exceptions online for incoming ACH (debits): ACH Positive Pay
- Control access to your account by customer ID and dollar amounts: ACH Positive Pay

For wire transfers

- Ensure dual authorization is required for all transfers, and verify instructions by phone, not email

For regular review of your account information

- Review your accounts online on a daily basis
-