Fraud prevention checklist

Check these boxes to help protect your organization against fraud.

Protect your organization through established controls and scheduled periodic reviews. Use this checklist to help maintain a strong fraud prevention program.

Internal procedures and controls

Establish fraud prevention best practices and responsibilities

☐ Educate personnel 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.

Ensure procedures are being followed

☐ Conduct surprise audits.

☐ Review transactions before they leave the company.

☐ Verify out-of-pattern payment instructions from internal employees.

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.

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.

Safeguard your communications and confidential data

- Avoid using email to send confidential information.
- 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.
- Require use of security tokens, with strong authentication, for payment applications.
- Review employee access privileges and limit system administrative rights.
- 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.