



Fraud prevention checklist

Payment fraud isn't something that happens to other organizations. You can lessen your chance of being defrauded through established controls, periodic reviews and fraud-mitigation solutions.

Partner with U.S. Bank to regularly review the threat landscape, best practices and the latest tools that can help you maintain a strong fraud prevention program.



1. 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



2. 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, consider using 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



3. 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



4. U.S. Bank fraud prevention solutions

For SinglePoint® online access

Install IBM® Trusteer Rapport® to detect and eliminate malware (free to SinglePoint users)

Receive payment service alerts by email, text or fax: SinglePoint Alerts & Notifications

For paper check disbursements

Review exceptions daily and make payment decisions: SinglePoint Positive Pay

Review payee exceptions daily, make payment decisions: SinglePoint Positive Pay - Payee Option

View check images online, eliminate storing cancelled paper checks: SinglePoint Image Access and SinglePoint Image File Delivery

Reconcile accounts daily or monthly: U.S. Bank Account Reconciliation (ARP)

Outsource check processing to eliminate the storage of check supplies: SinglePoint Check Payables

For deposit-only

Place blocks on accounts to prevent unauthorized debits: U.S. Bank Check Filter Service

Reconcile deposits weekly or monthly: U.S. Bank Deposit Reconciliation Service

For ACH transactions

Use Account Validation to ensure the account you are being asked to send a payment is open and owned by the intended payee.

Ensure dual authorization is required: SinglePoint ACH Origination

Ensure approvers are vigilant in their final review and approval of all outbound monetary transfers

Set appropriate transaction limits for each initiator and approver of monetary transfers

Review exceptions online for incoming ACH (debits): SinglePoint ACH Positive Pay

Track ACH Positive Pay authorization status: ACH Filter Rejected Item report, ACH Filter Authorizations report: SinglePoint Information Reporting

Prevent ACH originators from debiting your account: ACH Block, Business Check Block

Control access to your account by customer ID and dollar amounts: ACH Filter

For wire transfers

Ensure dual authorization is required, especially for non-repetitive transfers: SinglePoint Wire Transfer

For regular review of your account information

Review your accounts online, at any time: SinglePoint Information Reporting

Next Steps

U.S. Bank is committed to helping you meet your treasury management needs including fraud prevention. To learn more, contact your U.S. Bank Relationship Manager or Treasury Management Consultant. To find a consultant near you, email a request to TreasuryManagementSolutions@usbank.com.

Disclosures

U.S. Bank and SinglePoint are registered trademarks of U.S. Bank National Association. IBM® and Trusteer Rapport™ are registered trademarks of the International Business Machines Corporation registered in many jurisdictions worldwide. U.S. Bank makes no warranty of any kind as to the effectiveness of the Trusteer Rapport software. U.S. Bank is not responsible for and does not guarantee the products, services, or performance of third parties. CR-53643114.

© 2024 U.S. Bank. Member FDIC. U.S. Bank National Association. Member FDIC. (x/24)