Fraud Awareness & Risk Management Checklist

WebsterBank
LIVING UP TO YOU™

61% of organizations experienced attempted or actual payments fraud.* You can't afford to have your organization disrupted or funds stolen by criminals and malicious software. To help make sure that you have secure fraud controls in place to protect your organization's finances, review this checklist on a regular basis.

PROTECT YOUR PASSWORD

- ❑ Do not share IDs, passwords or account or log-on credentials with anyone
- ❑ Use easy to remember, hard to guess passwords *(i.e., no words from the dictionary, pet names, SSNs, etc.)*
- ❑ Change passwords on a regular basis
- ❑ Disable user IDs/passwords during leave/vacation
- ❑ Ensure your password does not pre-fill at log-on
- ❑ Consider privacy overlays on computer screens, especially log-on credentials
- ❑ Never use the "save ID/password" option on websites where sensitive and/or financial data is accessed/stored
- ❑ Ensure passwords are stored securely *(i.e. not in desk drawer/under keyboard)*

PROTECT YOUR COMPUTER AND MOBILE

- ❑ Do not open attachments to an email unless you're expecting them or recognize the sender
- ❑ Do not click on imbedded links if the subject line looks suspicious or unexpected
- ❑ Review internet security regularly; validate best practices
- ❑ Do not download from unfamiliar file sharing sites
- ❑ Back-up files on a regular basis to disks or CDs
- ❑ Update anti-virus systems/applications regularly
- ❑ Install firewall for first line of defense against hackers
- ❑ Install security certificate verification software
- ❑ Employ intrusion analytics
- ❑ Turn off your computer at night
- ❑ Update your operating system regularly
- ❑ Add anti-spyware as an option
- ❑ Ensure routers on a network are protected

PROTECT AND CONTROL TRANSACTIONS

- ❑ Use Dual Control procedures for monetary transactions including, but not limited to, online ACH originations/ file transmissions, Fed wires and check processing including Remote Deposit
- ❑ Reconcile daily/monthly *(separate duties - staff that issue payments vs. those that reconcile)*
- ❑ Be aware/validate instructions to change beneficiary routing and account information
- ❑ Validate account information by a callback or other direct communication prior to paying a vendor invoice or processing a change of address request
- ❑ Create procedure to void/secure checks remotely deposited
- ❑ Shred deposited items after predetermined timeframe
- ❑ Convert paper-based payments to electronic payments
- ❑ Review and update signature cards annually
- ❑ Always log-off *(do not default to automated timeout)*
- ❑ Do not share, publish or provide your EIN unless absolutely required and validated
- ❑ Do not include sensitive information such as SSNs in payroll file transmissions
- ❑ Negotiable documents should have a control # that is managed under Dual Control
- ❑ Secure your workplace – beware of potential access to your files by non-employees *(i.e. trash)*

PROTECT YOUR CHECK SUPPLY

- ❑ Use trusted, established vendor
- ❑ Use a unique check style for each account for easy differentiation of payments
- ❑ Consider check stock with pre-printed numbers so missing checks are easily noticed
- ❑ Incorporate security features into your check design
- ❑ Monitor check orders and inform supplier if not delivered in a reasonable time
- ❑ Use secure storage with controlled access for your checks, printing, Remote Deposit equipment, endorsement stamp and cancelled checks
- ❑ Never sign checks in advance

PROTECT YOUR STAFF AND ORGANIZATION

- ❑ Limit authorization to employees who need it
- ❑ Segregate duties within accounting department
- ❑ Conduct surprise audits
- ❑ Introduce policies that require periodic risk assessments and controls evaluation
- ❑ Rotate banking duties among staff to prevent collusion
- ❑ Review system access privileges regularly
- ❑ Provide education on phishing and external dangers
- ❑ Screen temporary help and vendors that come on site
- ❑ Have a Disaster Recovery Plan that includes a Data Breach Response Plan
- ❑ Consider importance of liability insurance for 1st and 3rd party with indemnification protection
- ❑ Do not embed signatures in emails or put email addresses on your website

*2014 Annual Payments Fraud Control Survey, Associate Financial Professional and J.P. Morgan.

To help safeguard your information, Webster Treasury & Payment Solutions provides cash management services that can help you reduce risk:

ONLINE BANKING

- ❑ Event Notifications to be alerted about changes
- ❑ Internet banking to review account(s) daily

PAPER TRANSACTIONS

- ❑ Check Positive Pay, with default of return
- ❑ Establish Check safekeeping policies – truncate or shred/destroy cancelled checks
- ❑ Request images of paid/deposited checks on CD
- ❑ Set-up Check Block – stops all checks from debiting
- ❑ Lockbox Services – segregation of duties

MANDATORY EVENT NOTIFICATIONS

- ❑ Check Positive Pay Exception Item
- ❑ ACH Positive Pay Exception and Batch Release
- ❑ Wire Release
- ❑ Password Change or Reset
- ❑ Update Security Challenge Questions

WIRE TRANSACTIONS

- ❑ Adopt a Dual Control environment
- ❑ Ensure wire entitlements and transactional limits correspond to business need

ACH TRANSACTIONS

- ❑ ACH Positive Pay - ensure only authorized originators can debit your account up to a predetermined amount; or block all debits to your account
- ❑ Adopt a Dual Control environment
- ❑ Ensure ACH entitlements and transactional limits correspond to business need

ACCOUNT OPENING & MAINTENANCE

- ❑ Minimize number of accounts to reduce fraud risk
- ❑ Use unique serial number ranges for specific purposes within one account instead of additional accounts
- ❑ Segregate accounts at greater risk

INFORMATION SECURITY

Every organization should have a comprehensive Information Security Policy. IT experts can help upgrade an existing policy, or create a new one. Key components that should be considered:

- Clearly stated security objectives to preserve confidentiality, integrity and availability of information
- Reference to network access by employees, contractors or any other person
- Formal acknowledgement from all applicable parties
- Logical and physical access controls
- System and Network software updates and patches

RISK ASSESSMENTS

We also recommend you conduct periodic Risk Assessments. This creates an environment of discovery, correction and prevention of security problems. It should involve representatives from all applicable parties or lines of business and should include:

- A system inventory, listing all system components
- The system's policies/procedures, and details of its operation
- Risks *(i.e. reputation, operational or technology)*, severity of impact and likelihood of occurrence
- Safeguards for controlling threats/vulnerabilities, recommended changes, approximate effort/timeframe and level of residual risk remaining

NOTE YOUR NEXT STEPS:

_____

_____

_____

For more information visit WebsterBank.com/cashmanagement.com or call 1-888-932-2256.

If you feel that you have received a fraudulent or suspicious email from Webster Bank:

- Forward the email to reportfraud@websterbank.com
- Or, call Webster Bank's Security Hotline at 1.800.966.0256, 7:00 a.m. to 10:00 p.m., 7 days a week.