

Fraud Awareness & Risk Management Checklist

73% of organizations experienced attempted or actual payments fraud.* Your organization can't afford to be disrupted or funds stolen by criminals and malicious software. To help make sure 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, account or log-on credentials with anyone
- Use smart, easy to remember, hard to guess passwords with upper and lower case, special characters and numbers i.e. \$GoAway2manyHackers! Something that cannot be socially engineered (*children birthdates, favorite food*)
- Disable user IDs/passwords during leave/vacation
- Never use the "save ID/password" option on websites where sensitive and/or financial data is accessed/stored
- Consider privacy overlays on computer screens, especially log-on credentials
- Ensure passwords are stored securely (*not in desk drawer/under keyboard*)

PROTECT YOUR COMPUTER AND MOBILE

- Do not open attachments or click on links in an email unless you're expecting them or recognize the sender
- Review internet security regularly; validate best practices
- Do not download from unfamiliar file sharing sites
- Back-up files on a regular basis to off-site, non-networked file

(See reverse side for additional information)

PROTECT YOUR STAFF AND ORGANIZATION

- Secure your workplace and access to your paper files by non-employees (*i.e. trash*)
- 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
- Regularly educate employees, vendors, temps, and customers on cyber security issues, external dangers, internal controls, and to protect information and systems. Put it in writing – ensure understanding and compliance
- Ensure your board and senior management are aware of cyber security activities and management
- Do not embed signatures in emails or put executive email addresses on your website

PROTECT AND CONTROL FINANCIAL TRANSACTIONS

- Use dedicated and protected computers. One for each user, following Dual Control procedures, including, but not limited to, online ACH originations/file transmissions, Fed wires, check processing and Remote Deposit**
- Reconcile daily/monthly (*separate duties - staff that issue payments vs. those that reconcile*)
- Validate email instructions, by phone or in person, to place a wire or to change any recipient, address or account information - before processing any wire or account change 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 turn off your computer at night (*do not default to automated timeout*)
- Do not share, publish or provide your Employer ID number 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

PROTECT YOUR CHECK SUPPLY

- Use a trusted, established vendor. Choose a unique check style for each account for easy differentiation of payments
- Use check stock with pre-printed numbers to easily identify missing checks
- 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 and Remote Deposited checks, endorsement stamp and cancelled checks
- Never sign checks in advance

Note: There is a difference between when checks are deposited drawn on other banks, when funds are made available (per regulations) and when funds are "good" funds, and therefore collected.

INFORMATION SECURITY

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

- Clear security objectives to preserve confidentiality, integrity and availability of information
- Detail network access by employees, contractors or any other persons
- Obtain formal acknowledgement from all applicable parties agreeing to your IT security policy
- Document logical and physical access controls
- Deploy operating system network software, anti-virus and security certification verification updates and patches regularly
- Consider implementing a comprehensive Unified Threat Management System (UTM), inclusive of Intrusion Protective Software (IPS)
- Ensure network routers are protected

RISK ASSESSMENTS

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 components, 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 actions, approximate effort/timeframe and level of residual risk remaining
- A scheduled proactive program of vulnerability testing
- Resources for incident response, separate from those involved in vulnerability analysis and security controls. Ensure your emergency response teams have a contact list, including back-ups and day and evening information
- Evaluation and adoption of cyber liability, privacy liability and/or network security to mitigate IT fraud related expenses
- Disaster recovery (testing) plans: what would your organization do if the internet was not available, if applications, files and other enabled web-based programs were impacted, destroyed or otherwise not available. Challenge your partners and service providers to be aware of services to your organization that are web-enabled

For more information contact your Client Support Specialist. If you do not know who that is, call 1.888.932.2256 or email us at cashmgt@websterbank.com.

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

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

ONLINE BANKING

- Security authentication at log-in
- Internet banking to review account(s) daily
- Mandatory event notifications to be alerted of any changes:
 - Check Positive Pay Exception Item
 - ACH Positive Pay Exception and Batch Release
 - Wire Release
 - Password Change or Reset
 - Update Security Challenge Questions

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 to stop all checks from debiting
- Lockbox Services – segregation of duties

WIRE TRANSACTIONS

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

ACH TRANSACTIONS

- Adopt a Dual Control environment
- ACH Positive Pay - ensure only authorized originators can debit your account up to a predetermined amount; or block all debits to your account
- 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 that are at greater risk