Fraud Awareness & Risk Management Checklist

TREASURY & PAYMENT SOLUTIONS

81% of organizations experienced attempted or actual payments fraud.* Your organization can't afford to be disrupted by having funds stolen by criminals or by downloading malicious software. To help make sure you have secure fraud controls in place to protect your organization's data and finances, review this checklist on a regular basis with your business partners.

Protect your credentials

- ❑ Do not share account or log-on credentials
- ❑ Use easy to remember, hard to guess passwords: mix of upper and lower case, special characters and numbers i.e. $GoAway2manyHackers! Something that can't be socially engineered (children birthdates)
- ❑ Disable user IDs/passwords during leave/vacation
- ❑ Never use "save ID/password" on websites where sensitive and/or financial data is accessed/stored
- ❑ Consider privacy overlays on computer screens, especially log-on credentials
- ❑ Store passwords securely (not under keyboard)

Protect your computer and mobile devices

- ❑ Do not download/open attachments from file sharing sites or click on links in an email unless you're expecting them or recognize sender
- ❑ Review internet security regularly; validate best practices
- ❑ Back-up files to off-site, non-networked storage
- ❑ Do not use power sources with USB cable connector

Protect your staff and organization

- ❑ Secure your workplace and access to paper trash
- ❑ Limit authorization to employees who need it
- ❑ Segregate duties within accounting department
- ❑ Conduct surprise audits
- ❑ Rotate staff duties to prevent collusion
- ❑ Review system access privileges regularly
- ❑ Educate everyone on cyber security issues, external dangers, internal controls, protection of information and systems. Test understanding and compliance
- ❑ Keep your senior leaders aware of cyber security activities and management
- ❑ Do not embed signatures in emails or put executive email addresses on your website
- ❑ Never give personal information on an incoming call from a number you don't recognize
- ❑ Establish a clear fraud escalation process

Protect and control financial transactions

- ❑ Use dedicated and protected computers. One per user, follow Dual Control procedures, including 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 to place a wire or to change any recipient, address or account information with a call to a known phone number on file or in person, before processing**
- ❑ Scan email addresses for correctness (2 n's form m)
- ❑ Void/secure checks remotely deposited
- ❑ Shred deposited items after predetermined timeframe
- ❑ Convert paper-based payments to electronic payments
- ❑ Review and update signature cards annually
- ❑ Physically turn off your computer (not automated timeout)
- ❑ Do not share, publish or provide your Employer or Employee ID numbers unless absolutely required and validated
- ❑ Do not include sensitive information such as SSNs in payroll file transmissions
- ❑ Ensure negotiable documents have a control # managed under Dual Control

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.*

Protect your check supply

- ❑ Use an established vendor. Use a unique check style per account for easy differentiation
- ❑ Use stock with pre-printed numbers to identify missing checks
- ❑ Incorporate security features into your check design
- ❑ Monitor orders and inform supplier if not delivered in a reasonable time
- ❑ Use secure storage with controlled access for printing and Remote Deposited checks, endorsement stamp and cancelled checks
- ❑ Never sign checks in advance

*2020 Annual Payment Fraud and Control Survey, Association for Financial Professionals.
**Restrict access to these computers and specific access sites. Ideally with no email or general internet access.

Webster Bank®

Have a comprehensive information security policy

Consult IT experts to create or upgrade policy:

- Provide clear security objectives to preserve confidentiality, integrity and availability of information
- Detail network access for employees/contractors
- Get agreement from all applicable parties on IT controls
- Detail logical and physical access controls
- Deploy network anti-virus software, security verifications and patches regularly
- Implement a comprehensive Unified Threat Management System (UTM), inclusive of Intrusion Protective Software (IPS)
- Ensure network routers are protected

Conduct periodic risk assessments

Discover, correct and prevent security problems. Involve representatives from all applicable parties. Include:

- System inventory, list 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
- Proactive vulnerability testing
- Resources for incident response, separate from those in vulnerability analysis and security controls. Ensure emergency response teams have a contact list, including back-ups and day/evening info
- Evaluation and adoption of cyber liability, privacy liability and/or network security to mitigate IT fraud-related expenses
- Disaster recovery (testing) plans: What if the internet was down, if applications, files and other web-based programs were impacted, destroyed or not available? Be aware of third-party services to your organization that are web-enabled
- Create an Incident Response Plan for a DDOS, ransomware or any other cyber attack
- Regularly review insurance coverage for losses due to cyber attacks, employee dishonesty, account takeover, etc

Webster Treasury & Payment Solutions provides cash management services that can help you reduce risk:

Online and mobile banking

- ❑ Make sure you have access to a mobile app
- ❑ 3-point security authentication at log-in
- ❑ Review account(s), daily reconciliation
- ❑ **Set alerts to be notified 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
  - ❑ Out of Band Authentication via SureKey

Paper transactions

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

ACH and wire transactions

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

Account opening and 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 access to accounts that are at greater risk
- ❑ Ask for our Security in Layers account setup recommendation

Questions and answers

Q. Experienced a malware attack?

A. Do not turn off your device. Disconnect from network.
A. Contact your IT or Fraud Department

Q. Experienced actual or attempted Business Email Compromise (BEC) or ransomware?

A. Please file an internet-based fraud complaint with the FBI, visit: https://www.ic3.gov/default.aspx
A. Call your Webster Representative to report the fraud and fill out the Fraud Notification Form

Q. Received a fraudulent or suspicious email from Webster Bank?

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

FN00119 02/2021

WebsterBank®