BBVA
Creating Opportunities

Treasury Management Solutions

Fraud Awareness and Prevention Checklist

Protect your Organization by instituting fraud prevention and risk management controls.

Your organization is not immune from either internal or external fraud. Operational and systems practices need to be reviewed. Whether your company is using traditional forms of payment such as checks or you are fully electronic, you are susceptible because check fraud is still rampant and Electronic Funds Transfer (Wire and Automated Clearing House) fraud is on the rise. And critically, cyberfraud is a very real threat. Even the most secure systems are not invulnerable. Penetration testing frequently reveals that "helpful" personnel or employees deferring to "authority" are the weakest link.

BBVA strongly recommends that your company take preventative measures utilizing technology and instituting policies and procedures in the following areas:

- Account Structure
- Check Supply
- Transaction Controls
- Antivirus
- Spyware Software
- Anti-Malware
- Firewall
- Internal Controls
- Staff Training
- Banking Services

Review the checklist on a regular basis and make appropriate changes to your policies and procedures.

Account Structure

- ☐ Minimize the number of accounts where feasible
- ☐ Use unique serial number ranges for specific purposes
- ☐ Segregate accounts at greater risk
- ☐ Segregate accounts by intended application
- ☐ Secure accounts so that they are only capable of their intended purpose

---

Check Supply

- ☐ Use an established vendor
- ☐ Incorporate security features into check stock such as fluorescent fibers, watermarks, chemical resistance, bleach reactive stains, thermochromatic ink, microprinting warning, etc.
- ☐ Use an unique check style for each account type
- ☐ Use secured storage with controlled access for check stock, deposit slips, check printing equipment, endorsement stamps, and canceled checks

---

Fraud Prevention Checklist

Transaction Controls

- ☐ Review and reconcile accounts daily and monthly
- ☐ Review out-of-pattern transactions
- ☐ Validate vendor legitimacy and account information by performing a callback if the invoice is suspect or there is a change of address request
- ☐ Formalize procedures to securely retain then safely shred checks after remote deposit
- ☐ When possible convert paper payments to electronic formats
- ☐ Implement policies requiring employees to always log off and not wait for automated time-out
- ☐ Do not provide your EIN unless required for a validated need
- ☐ Secure your workplace by deterring nonemployees from accessing files, including trash bins
- ☐ Shred documents with sensitive content, voided or image converted checks as appropriate
- ☐ Maintain ACH and wire transfer limits as low as possible
- ☐ Segregate duties into create and review and approve roles

---

Antivirus Anti-Malware and System Controls

- ☐ Do not open attachments to an email if the subject line or email itself looks suspicious or unexpected
- ☐ Do not download from unfamiliar file-sharing sites
- ☐ Aggressively update your antivirus applications regularly
- ☐ Install a firewall as a first line of defense against hackers, with default-deny configuration
- ☐ Schedule antivirus software to update and run daily and automatically
- ☐ Utilize security certification verification software
- ☐ Employ intrusion analytics software
- ☐ Prepare, implement and practice an incident response plan
- ☐ Install perimeter spam and malicious-content filtering
- ☐ Secure USB ports to preclude compromise of critical data
- ☐ Never access bank, brokerage or other financial services information using public wi-fi
- ☐ Formally and regularly review internet security. Keep browsers and operating systems up-to-date.

Internal Controls

- ☐ Exercise extreme caution when confronted with any request to divulge account information or banking access credentials
- ☐ Immediately report any transactions in your accounts that you question
- ☐ Never leave a computer unattended while using any online banking or investing service
- ☐ Use dual authorization for all monetary transactions, including online ACH originations, ACH direct transmissions, wire transfers, and Remote Deposit

Fraud Prevention Checklist

- ☐ Set policies regarding passwords such that 1) same passwords are not used for different applications 2) they are not easy to guess e.g., pet or children's names, etc. 3) they contain special characters and not just alphanumeric 4) they are changed often 5) longer passwords are more secure
- ☐ Use two factor authentication where enabled
- ☐ Mask account numbers and EINs on correspondence
- ☐ Conduct surprise audits
- ☐ Never sign checks in advance
- ☐ Review and update signature cards annually
- ☐ Be sure that your financial services providers have the most current Corporate Resolutions and Certificates of Incumbency
- ☐ Use only dedicated, stand-alone computers for online banking where email and web browsing are not allowed
- ☐ Set policies to disable user IDs and passwords during leaves and to discourage pre-filling passwords and user names at log-in
- ☐ Establish call back procedures to verify the authenticity of transactions requesters

---

Staffing

- ☐ Limit authorizations to appropriate employees
- ☐ Segregate duties between staff that issue payments and those that reconcile
- ☐ Rotate banking duties to prevent collusion
- ☐ Review system access privileges for all employees regularly
- ☐ Proactively provide education on phishing and other cybercrimes
- ☐ Screen and log temporary help and vendors that come on site
- ☐ Review access credentials to preclude use by former employees or contractors
- ☐ Promptly deactivate employee access cards for temporary or laid-off staff

---

Banking Services

- ☐ Validate the legitimacy of checks presented by using Positive Pay
- ☐ Designate accounts for use in electronic transactions only and block checks from debiting
- ☐ Stop all ACH originators from debiting certain accounts by using ACH debit blocks with ACH Authorization
- ☐ Ensure only authorized ACH originators can access your accounts for predetermined amounts by using ACH debit filters using ACH Enhanced Authorization

---

Please note: The Fraud Awareness and Prevention Checklist is not all inclusive and does not guarantee protection from fraud.