Fraud Protection Checklist

Fraud is an unfortunate and permanent reality in business today. Check ACH fraud continues to threaten companies, and cyber-fraud has ramped up in the past few years, with cyber syndicates as serious about their business as you are about yours. While no organization is immune from either internal or external fraud, it is imperative that you take preventive measures through use of technology and procedures.

We recommend that you review this checklist on a regular basis and make appropriate changes to your policies and procedures.

Account Structure

- ☐ Minimize the number of accounts
- ☐ Segregate accounts at greater risk

Checking Supply

- ☐ Use an established vendor
- ☐ Use unique serial number ranges for specific purposes
- ☐ Incorporate security features into check stock such as fluorescent fibers, watermarks, chemical resistance, bleach reactive stains, thermochromatic ink, etc.
- ☐ Use a unique check style for each account type
- ☐ Secure your check stock and other negotiable documents and manage under dual control
- ☐ Secure check printing equipment and endorsement stamps and manage under dual control

Transaction Controls

- ☐ Review and reconcile accounts daily and monthly
- ☐ Validate vendor legitimacy and account information by calling back your known contact if an invoice is suspect or there is a change-of-address request
- ☐ Convert paper payments to electronic formats when possible
- ☐ Do not provide your EIN unless required for a validated need
- ☐ Secure your workplace by deterring nonemployees from accessing files, including trash bins
- ☐ Maintain ACH and wire transfer limits, and implement dual controls
- ☐ Formalize procedures to securely retain then safely shred checks after remote deposit

Antivirus and Spyware

- ☐ 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
- ☐ Install a firewall as a first line of defense against hackers, with default-deny configuration
- ☐ Update your antivirus applications regularly
- ☐ Schedule antivirus software to 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

**This Fraud Protection Checklist is not all-inclusive and does not guarantee protection from fraud.*

TEXAS CAPITAL BANK®

Fraud Protection Checklist

Social Engineering

- ☐ Validate, by phone or in person, all transaction requests from a co-worker's email
- ☐ Exercise extreme caution when confronted with any request to divulge account information or banking access credentials
- ☐ Never leave a computer unattended while using any online banking or investing service
- ☐ Implement policies requiring employees to always log off and not wait for automated time-out
- ☐ Never access bank, brokerage or other financial services information at internet cafes, public libraries, etc.
- ☐ Install Trusteer Rapport on all computers to supplement your anti-virus software and protect your online banking sessions

Internal Controls

- ☐ Reconcile your bank account regularly and notify us immediately at 1.800.839.2801 if you spot an unauthorized transaction
- ☐ Use dual authorization for all monetary transactions, including online ACH originations, ACH direct transmissions, wire transfers and Remote Deposit Capture (RDC)
- ☐ Formally and regularly review internet security
- ☐ Set policies regarding passwords such that:
  - *same passwords are not used for different applications*
  - *they are not easy to guess; e.g., pet or children's names, etc.*
  - *they contain special characters*
  - *they are changed often*
- ☐ Mask account numbers and EINs on correspondence
- ☐ Conduct third-party auditand intrusion testing
- ☐ Never sign checks in advance
- ☐ Review and update signature cards annually, and when employees change positions
- ☐ Use only dedicated, stand-alone computers for online banking where email and web browsing are not allowed
- ☐ Set policies to ensure user IDs and passwords are disabled during employee leaves of absence and to discourage pre-filling passwords and user names at login

Banking Services

- ☐ Validate the legitimacy of checks and ACH debits presented by using Positive Pay and ACH 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
- ☐ Ensure only authorized ACH originators can access your accounts for predetermined amounts by using ACH debit filters

ABOUT TEXAS CAPITAL BANK

Texas Capital Bank, N.A., is a commercial bank that delivers highly personalized financial services to businesses and entrepreneurs. We are headquartered in Texas and work with clients throughout the state and across the country. Texas Capital Bank is a wholly owned subsidiary of Texas Capital Bancshares, Inc. (NASDAQ®: TCBI) and is recognized as one of *Forbes*' Best Banks in America.

Our relationship managers are specialists, trained to provide you with personal, sophisticated services and creative business solutions that other banks simply cannot deliver.

Fraud protection is everyone's responsibility. *At Texas Capital Bank, N.A., we employ world-class systems to protect you from fraudulent activity, but they only work if you diligently keep your computers and networks up-to-date. Security measures are constantly evolving, and keeping the latest versions of software and upgrades installed can be the difference in protecting you from fraud. We encourage you to periodically ensure your computers and networks have the latest security protections available.*

**This Fraud Protection Checklist is not all-inclusive and does not guarantee protection from fraud.*