Stockman Bank

BUSINESS FRAUD PREVENTION CHECKLIST

In the digital age, fraudulent activities are more common, and more severe, than they have ever been. It's imperative you take preventative measures to protect your business finances and sensitive information. The following best practices can help.

ESTABLISH INTERNAL CONTROLS & OPERATIONS

A strong fraud prevention strategy starts with creating and maintaining strong internal systems.

■ Create formal policies and procedures

- Create payment instructions for internal verification.
- Create a process for changing a vendor's address and/or banking information to ensure accurate invoicing.
- Never change payment or contact information from an e-mail or phone request until you have called the vendor at a known number to verify the change.

■ Understand unauthorized transaction recovery timeframes are time-sensitive

- Unauthorized ACH debit returns and check returns are time-sensitive.
- Monitor accounts daily for unauthorized or suspicious activity. Report any findings to your bank immediately.

■ Give employees the tools they need to:

- Follow established policies and procedures.
- Safely conduct business online by keeping systems up to date, utilizing antivirus software, and following strong cyber security practices.
- Protect user data by setting strong passwords and never leaving workstations unattended.
- Recognize fraud attempts, including phishing emails, and social engineering phone calls.
- If available, use authentication apps such as Google, Microsoft, or Duo. An authenticator helps improve your online security by adding two-factor logins to accounts connected to the authenticator. MFA, or multi-factor authentication increases security because, even if one credential becomes compromised, unauthorized users may not be able to access the second requirement.
- Teach your employees about the risk of business e-mail compromise, or BEC. Fraudsters use this sophisticated scam to request transfers or new payment methods which are then redirected to the fraudster. Always verify e-mail requests with a phone call to a known number to verify before making changes.

Manage system access

- Implement controls limiting access based on role or job function.
- Immediately remove access when an employee leaves the company.
- Conduct daily and monthly reconciliations, as well as regular account audits.
- Do not share or reuse passwords.

Segregate duties

- Consider separation of duties when processing accounts payable and receivables.
- Require different individuals to process collections, disbursements, and reconciliations.

Business Email Compromise - What does it look like?

Here is a real (and typical) example of how BEC (business e-mail compromise) can impact your business:

A business received an e-mail request from a vendor that they were changing banks. The vendor provided a new account number and asked to be paid by wire going forward instead of check. The business complied and, after three months, the business learned that their vendor had not received the last three months payments. The e-mail was fraudulent, and the fraudster successfully redirected the monthly payment.

A simple phone call to the phone number on file for the vendor may have prevented this disastrous mistake.

Stay vigilant

- Exercise additional due diligence for vendor payment request changes such as payment bank or account number, dollar amount changes, or type of payment method.
- Use secure check stock, limit access to check inventory, and implement an approval process on high dollar amounts.

TAKE ADVANTAGE OF STOCKMAN BANK SERVICES

Stockman Bank offers a variety of fraud prevention tools to protect your business.

- Monitor your accounts daily using online and mobile banking.
- Enroll in electronic statements for quicker access to review account activity.
- Set up account alerts to receive notification of:
  - Suspicious activity.
  - Large withdrawals.
  - Exceeded balance thresholds.
  - Processed payments or cleared transactions.

Sign up for Positive Pay:

(Only available with Cash Management services.)

- Check Positive Pay will verify your checks and notify you if any records do not match.
- ACH Positive Pay allows you to whitelist approved companies, and we'll let you know if an unapproved company debits your account.

To learn more about Stockman Bank prevention services including Positive Pay, contact your local Stockman Bank Branch