Business Fraud Checklist

Safeguard your financial data and processes to prevent and monitor business fraud. The best way to protect your company is to educate yourself and your employees, which is what our Business Fraud Checklist aims to do.

Policies & Procedures

Employees can be your business' first line of defense and your greatest risk. Establishing policies and procedures are an important first step in combating both internal and external fraud.

Implement separation of duties for employees:

- □ Limit access and resources for each job role.
- □ Provide cross-training and job rotation to reduce risk of collusion.
- □ Implement dual control procedures for following transactions:
  - □ Web & Mainframe ACH
  - □ Remote Deposit Capture
  - □ Wires
  - □ Tax Payments
  - □ Check Automation

Establish procedures to review transactions before they leave the company:

- □ Ensure proper authorization of transactions.
- □ Verify any changes in payment instructions.

Conduct control testing and audits:

- □ Audits should be scheduled and done at random.
- □ Review financial information.
- □ Evaluate computer network and firewall protection.
- □ Ensure "clean desk" policy (all sensitive internal and customer information filed away).

Review insurance coverage:

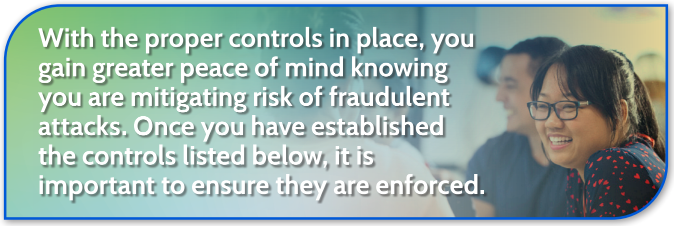
- □ Contact your insurance agent to better understand your options.
- □ Ask about specific coverage for data breaches, system failures and intellectual property rights.

Educate employees:

- □ Establish a training program that builds employee awareness of social engineering, phishing, acceptable use, identity theft and fraud education.
- □ Make information about fraud safety easily accessible.

premier bank

Internal Controls



With the proper controls in place, you gain greater peace of mind knowing you are mitigating risk of fraudulent attacks. Once you have established the controls listed below, it is important to ensure they are enforced.

Review access privilege:

- □ Give financial access only to employees who need it and review access privileges regularly, particularly when employees change roles.

Limit authorization:

- □ Implement dual control procedures for accounts receivable and accounts payable responsibilities.
- □ Preauthorize high value checks. Approve high dollar amounts before the checks are written.

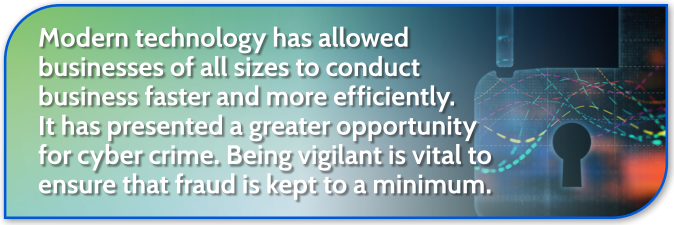
Safely store sensitive material:

- □ Ensure canceled checks, accounts receivable and payable records, payroll information and materials with bank account information are stored securely with limited employee access.

Have a plan B:

- □ Establish and regularly test a response plan for disaster recovery, business continuation and incident response that includes notification procedures and defined responsibilities.

Internet Safety



Modern technology has allowed businesses of all sizes to conduct business faster and more efficiently. It has presented a greater opportunity for cyber crime. Being vigilant is vital to ensure that fraud is kept to a minimum.

Keep systems updated and use a firewall:

- □ Attackers often look for faulty, outdated systems. Run vulnerability scans and monitor intrusion-detection and intrusion-prevention systems.

Monitor business bank accounts daily:

- □ Implement dual procedures for creating and approving online payments and report suspicious activity to your bank.

Business Fraud Checklist

Continued....

Limit administrator password use:

❒ Do not use the administrator password to initiate or approve transactions. Administrator passwords should only be used to manage user access.

Think before you click:

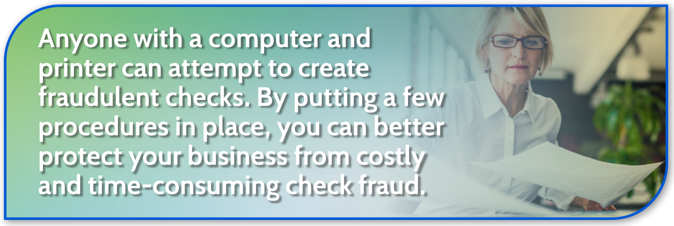
❒ Be cautious in clicking links and downloading attachments from unknown senders that may contain malware.

❒ Require unique usernames and strong passwords. Use unique ID's for each employee accompanied with complex passwords made up of letters, numbers, and special characters. Remind employees to log-off when leaving their work area.

Control access:

❒ Limit each employee's access to only applications needed to perform his or her duties. In addition, use a dedicated computer with limited internet use for online banking to reduce risk of viruses and malware.

Preventing Check Fraud



Anyone with a computer and printer can attempt to create fraudulent checks. By putting a few procedures in place, you can better protect your business from costly and time-consuming check fraud.

Be selective with check providers:

❒ Only use an established, respected provider. If check orders are not received within 10 days, notify the supplier.

❒ Use a unique check style for each account type to improve check identification.

❒ Select one style of checks for each account to allow for easy recognition. Look for check designs with security features such as watermarks, chemical resistance or micro-printing.

Store checks securely:

❒ Keep blank checks and check printing equipment in a secure area with controlled access.

❒ Conduct periodic inventory procedures, including accounting for the sequence of unused checks.

Stay in touch with your bank:

❒ Review and update authorized signature cards annually or when staff changes occur.

Fraud Prevention Solutions

When working with Premier Bank, you not only get an experienced business specialist to help guide your business but access to the latest digital banking solutions to keep your account and transactions protected.

Business Internet Banking:

❒ Stay connected with Business Internet Banking. Manage accounts, control cash flow and make payments in a secure, easy-to-use format.

Business Mobile Banking:

❒ View business accounts, transfer funds, pay bills, see check images, approve pending ACH and wire transactions and deposit checks go with Premier Bank's Business Banking App.

Check Positive Pay:*

❒ Streamline your account reconciliation process using Business Internet Banking with Check Positive Pay. Simply submit a list of checks that you plan to issue. When the checks are presented for payment, you are alerted of any discrepancies. Then approve, void, return or process stop payments* the same day or return suspect checks the next day.

Reverse Check Positive Pay:*

❒ Reduce risk with Reverse Check Positive Pay, an automated check fraud detection tool to help businesses feel secure about the money coming out of their accounts by identifying unauthorized transactions before final payment. It prevents criminals from using stolen account numbers and catches bad checks where the check amount has been altered or the check has an invalid date.

ACH Positive Pay:*

❒ Conveniently monitor authorized ACH debit transactions with ACH Positive Pay, which is based on originator information or transaction amount ranges through Business Internet Banking. Using ACH filters, you can block all ACH debit activity or only allow specific types of transactions to post.

ChecXchange:TM

❒ Premier Bank has partnered with ChecXchangeTM to offer a check recovery service that automatically collects your returned checks at no cost to you, reducing your staff time and expense on collection.

Questions? We're here to help.

premier bank

POWERED BY PEOPLE.

*Additional fees may apply.