Park View FEDERAL CREDIT UNION

Business Fraud Prevention Checklist

Protect your business from fraud by safeguarding financial data and processes by implementing proactive measures and procedures to ensure the safety of finances and sensitive information. The following best practices help maintain a strong fraud prevention program.

Park View Fraud Prevention Solutions

Park View offers a variety of fraud prevention tools to protect your business.

- ❑ Monitor accounts regularly using online banking and Park View's mobile app
- ❑ View electronic statements as soon as Park View notifies that they have become available
- ❑ Set up online banking account alerts to get emails and text messages about balance thresholds, processed payments, transfers and more
- ❑ For Park View Business credit cards, register on myaccountaccess.com to receive account alerts, security alerts, and fraud notifications

If You Suspect Fraud

Debit Card Fraud:
(888) 918-7313

Credit Card Fraud:
(800) 558-3424

Business Account Fraud:
Contact a Member Business Advisor
(540) 236-5761

Technology and Internet Safety

There are a number of things you can do that will help protect your information when you are using the internet.

Keep Systems Updated

- ❑ Keep devices up-to-date, including operating system, anti-virus software, applications, security patches, and browser versions
- ❑ Consider using malware protection software as well as a firewall

Safeguard Confidential Data and Communications

- ❑ Protect user data by setting strong passwords that do not include personal information
- ❑ Lock computer when it is not in use
- ❑ Implement multi-factor authentication when possible
- ❑ Do not share passwords, verification codes, PINs, or answers to security questions

Preventing Paper Check Fraud

Ensuring the security of paper checks is essential for protecting your business against fraudulent activities. By implementing a few procedures, you can minimize the risk of unauthorized payments and protect your business from costly and time-consuming check fraud.

Protect Checks Against Fraudulent Use

- ❑ Preauthorize high dollar checks before the checks are written
- ❑ Require that checks are to be signed only when all required information is entered on them and the documents to support them (invoices, approval) are attached
- ❑ Choose a black gel pen when writing checks, as its ink is harder to tamper with, providing added security against alteration or fraud

Be Selective With Check Providers

- ❑ Select a highly established, qualified check vendor
- ❑ Use a different style of checks for each account to allow for easy recognition
- ❑ Select check designs that incorporate security features into check design such as watermarks, chemical resistance, or micro-printing

Store Checks Securely

- ❑ Ensure canceled checks, blank checks, and bank account information is stored in a secured area securely with limited employee access in a secured area
- ❑ Limit the working supply of checks

Check Processing Controls

- ❑ Monitor check orders to ensure receipt of exact quantity is delivered
- ❑ Consider creating a calendar reminder when new checks should arrive

Internal Procedures and Controls

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

Implement Clear Separation of Duties and Access for Employees

- ❑ Limit financial data access only to employees if there's a business need; follow the need-to-know principle
- ❑ Separate account receivable and accounts payable functions and processes

Implement dual control procedures or a secondary communication channel to validate payment related requests for the following:

- ❑ ACH payments, remote deposit, wires, tax payments, and check automation
- ❑ Payment requests from customers and vendors
- ❑ Vendors request change of payment

Bank Account Management

- ❑ Review bank accounts daily by logging into your online banking or Park View's mobile app
- ❑ Carefully review electronic transactions (ACH, debit card transactions) posted to your account
- ❑ Notify Park View of any staffing changes to help ensure the signature cards are updated to reflect current information

Establish Procedures to Review Transactions

- ❑ Implement dual initiation approval for ACH and wire transfers
- ❑ Reconcile expenses daily
- ❑ Verify changes in payment instructions
- ❑ Ensure proper authorization on transactions

Conduct Control Testing and Audits

- ❑ Schedule and conduct random audits
- ❑ Establish a clean desk policy (all sensitive internal and customer information filed away)
- ❑ Review employee financial access privileges and processes regularly, restricting access to financial information only to employees who require it for their roles

Educate Employees

- ❑ Educate employees on recognizing fraud attempts, including phishing emails and social engineering phone calls
- ❑ Follow established policies and procedures and fraud prevention strategies, ensuring that they recognize they play a key role in preventing fraud losses

Review and update signing authority

- ❑ Update authorized signature cards annually
- ❑ Remove executive signatures from annual reports to prevent illegal scanning and use