Business Fraud Mitigation Checklist

In today's digital world, it's no longer a question of "if" a business will be targeted with fraud, but rather "when" it will get targeted. It's more important than ever to arm yourself with the best tools and practices to protect your business' sensitive financial information. Use this checklist as a foundation for your company's plan to protect itself against fraud.

Establish Internal Controls and Operations

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

Create Formal Policies and Procedures

- Determine how payment instructions are verified internally (including payroll changes).
- Create a process for changing a vendor's address and/or banking information to ensure accurate invoicing.
- Verify emailed payment information directly with the payee through a known good channel – for example, over the phone with a known good number.
- Review your policies and procedures on a regular basis (at least annually).
- Review with new hire onboarding

Understand Unauthorized Transaction Recovery Timeframes

- 48 hours for unauthorized ACH debits
- 24-48 hours for suspicious or fraudulent checks clearing

Divide Duties

- Have separate accounts payable and accounts receivable departments.
- Require different individuals to process collections, disbursements and reconciliations.
- Have employees work at different stations with different login credentials.

Manage System Access

- Limit access to a need-to-know basis.
- Remove access when an employee leaves the company.
- Conduct daily and monthly reconciliations, as well as regular account audits.
- Do not share or reshare passwords.

Stay Vigilant

- For ACH, always have dual control and reconcile expenses daily.
- For wire transfers, utilize dual authorization, and be wary of high amounts, international requests and new or non-approved partners.
- For checks, preapprove high amounts before issuance, use a secure check stock and limit access to check stock.

Landmark CREDIT UNION

Banking Made Easy

Empower Employees with Resources and Information

- 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.
- Enable and enforce Multifactor Authentication (MFA) on all internet accessible accounts. Landmark allows for the following multifactor methods:
  - SMS Text
  - Voice Call
  - Soft Token
  - Hard Token
  - Authenticator Apps (i.e. Google Authenticator)

Take Advantage of External Services

Landmark offers a variety of fraud prevention tools to assist in mitigating fraud against your business.

Monitor your accounts regularly using Digital Banking

- Have electronic statements reviewed by multiple employees.
- Set up account alerts for:
  - Balance thresholds
  - Processed payments
  - Cleared transactions

Sign up for Positive Pay

- 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 get notified if an unapproved company debits your account.

To Learn More about Landmark Credit Union's fraud mitigation services, including Check and ACH Positive Pay, visit Landmarkcu.com/cash-management or contact our Cash Management team at 262-780-7137.