MOUNTAIN AMERICA
CREDIT UNION

BUSINESS FRAUD PREVENTION CHECKLIST

In the digital age, fraudulent activities are more common, and often 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 you do that.

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.
- 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.

❑ Understand unauthorized transaction recovery timeframes:

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

❑ 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.
- Enable and enforce Multi-Factor Authentication (MFA) on all internet-accessible accounts. Authentication apps like Google Authenticator or Duo provide the strongest security, while emailed codes can be a good alternative. Avoid phone- or SMS-based codes for important accounts unless it is the only MFA option.

❑ 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.

❑ Segregate duties:

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

❑ **Stay vigilant:**

- For ACH, always have dual initiation approval 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.

Take advantage of external services

Mountain America offers a variety of fraud prevention tools to protect your business.

❑ **Monitor your accounts regularly using online and mobile banking.**

❑ **Have paper or electronic statements sent to multiple employees for review.**

❑ **Set up account alerts:**

- Be notified of suspicious activity.
- Receive notifications about balance thresholds, processed payments and 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 we'll let you know if an unapproved company debits your account.

To learn more about Mountain America's fraud prevention services, including Positive Pay, contact a business advisor at 1-888-845-1850.