As fraudulent activities become more and more sophisticated, it's imperative that preventative measures are in place to protect business finances and sensitive information. The following best practices can help.

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.
- 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.
- Recognize fraud attempts, including phishing emails and social engineering phone calls or text messages.
- Store documents in a secure location.

☐ **Understand unauthorized transaction recovery timeframes:**
(excludes weekends + federal holidays)

- 48 hours for unauthorized ACH debits.
- 24 hours for any forged, altered, unauthorized, or fraudulent checks clearing on your account.

☐ **Conduct daily and monthly reconciliations, as well as regular account audits.**

- *Note: You have 33 days from the day Verve sends your statement to notify Verve of payments, transaction, or discrepancies that you find to be suspicious, unauthorized, or fraudulent.*

☐ **Enforce strict system security:**

- Appoint an employee to manage the protection of sensitive information and provide them training in that area.
- Keep all systems up to date with supported and patched software versions.
- Utilize well-known and up-to-date antivirus software.
- Require use of strong passwords including both upper and lower-case letters, numbers, and symbols and at least 15 characters in length. Disallow the use of common or known-breached passwords.
- Utilize 2-factor authentication (2FA) on all systems that support it. App-based 2FA like Google Authenticator or Duo can often provide stronger security than SMS-based 2FA.
- Utilize a URL filter and/or firewall to block access to websites that are not known to be business-related.
- Promptly remove access when an employee leaves the company.
- Utilize an external firm to perform a cybersecurity assessment at least annually.

☐ **Manage system access:**

- Do not share passwords.
- Limit access to a need-to-know basis on accounts.
- Remove access when an employee leaves a company.

☐ **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 checks, preapprove high amounts before issuance, use a secure check stock, and limit access to check stock.
- Consider taking mailed checks directly to the post office.
- 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.

Take advantage of external services

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

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

- Review options for alerts that you can configure and set up as desired.

☐ **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.

To learn more about Verve's business fraud prevention services, please call 800.448.9228.