FRAUD PREVENTION & BEST PRACTICES CHECKLIST

At Frost, we want to partner with you to protect your company from fraudulent activity. Developing a layered approach focusing on education, technology, business rules, and procedures is the best way for you to achieve that protection. While not all inclusive, this checklist is a great way to get started.

USER SECURITY

- Restrict entitlements to all systems and review settings periodically
- Implement user limits for electronic payment originations
- Require dual control for all cash handling steps
- Require dual control for all payment initiation, payment file handling, and to set up profiles for payment initiation
- Use repetitive wire transfer profiles whenever possible
- Require documentation for all internal requests for payments
- Confirm vendor account changes with a known vendor contact
- Document all procedures, and train for them
- Audit user activities regularly
- Educate your employees about email, text and other scams
- Implement effective hiring practices, include background checks
- Lead a strong ethics policy by example

SEPARATION OF DUTIES

Employees who:

- Write checks or initiate electronic payments should not reconcile accounts
- Initiate electronic payments should not approve them
- Maintain profiles for electronic payment initiation should not initiate or approve payments
- Open the mail should not prepare or make deposits

COMPUTER SECURITY

- Require use of a segregated computer for banking activities only. No internet surfing or email use
- Protect your network using a properly configured firewall
- Keep your industry standard antivirus and malware software current
- Apply latest security updates from operating system supplier
- Restrict access to the computer's administrative privileges
- Disable CD/DVD/USB access when not in use
- Implement procedures to protect laptops when away from the office and before reconnecting them to the network
- Establish unique login and passwords for all systems and require periodic changes
- Impose strong password rules. Use special characters, without words or names
- Always log in through your corporate infrastructure, especially when using online banking
- Close pop up windows by clicking on the X, never click inside the window
- Support all security measures, such as security tokens or out-of-band authentication
- Never send sensitive information via unsecured email
- Implement procedures for employees to report computer infections
- Delete on-line users following employee terminations or resignations

ACCOUNT RECONCILIATION

- Reconcile all accounts immediately: checking, savings and credit cards
- Review account activity daily
- Review statements and internal reports, all account numbers should be masked
- Review cancelled checks for:
  - Checks to unknown suppliers/others
  - Checks written to cash
  - Forged signatures
  - Missing or out of order checks
  - Checks written to third parties, yet endorsed by others
  - Checks that do not match accounting records (payee, amount)

CHECK SECURITY

- Go paperless whenever possible
- Use a reputable vendor for check stock
- Use business checks and check stock with security features such as heat reactive ink and micro print
- Store blank check stock securely, under dual control
- Store mechanical signature plates securely, require dual control and store separately from check stock
- Perform periodic audits to account for all checks
- Securely store cancelled checks
- Control access to images of paid checks
- Control access to checks received for payment, and photocopy each check

BANK ACCOUNT MANAGEMENT

- Review agreements to ensure that internal procedures are aligned with signed documents
- Delete terminated employees or employees who have resigned from bank records and update signature cards
- Report fraud to the bank immediately

BUILDING SECURITY

- Identify employees, guests and suppliers
- Purchase a good shredder or use a document shredding service
- Do not leave sensitive information on desktops or printers
- Be wary of over-the-shoulder viewing
- Lock your computer screen when stepping away

WE'RE HERE TO HELP

Call a Treasury Management Representative at (888) 481-0336.