CAMA Colorado Advanced Manufacturing Alliance

BEST PRACTICES

Best Practices for Businesses – Preventing Fraud Losses

By Cindy Grove and Curt Morgan

CoBiz Financial

Colorado Business Bank
CoBiz Financial

In their lifetime, 75% of businesses will experience fraud at least once. Small and mid-sized businesses are increasingly becoming targets as security controls may be more easily compromised. The number one reason for fraud losses is poor, circumvented or non-existent internal controls.

The good news? The majority of fraud schemes are preventable if you have sound internal controls and procedures. At Colorado Business Bank, we want to help you protect your business. Review the below best practices to learn what internal procedures you can put into place to defend your organization.

Perform Financial and Transactional Risk Assessments

- Review inflows and outflows for all deposit and credit accounts
- Determine volumes, dollars and types of transactions (wires, checks, debit/credit cards, electronic payroll/vendor payments)
- Determine who has access to review and initiate different types of transactions
- For larger volume businesses, establish thresholds that balance risk tolerance and workload
- Internal Accounting Controls
- Develop a cross training program and require rotation of duties—especially for accounting functions
- Require at least one full week of time off for each employee
- Balance and reconcile accounts frequently
- Separate transaction and reconciliation responsibilities
- Review payroll records including amounts and new hires
- Review account payables including new vendors
- Review accounts receivable aging reports and verify outstanding amounts
- Secure access and destruction of sensitive documents
- Develop and implement security procedures for cash and check stock

Technology Controls

- Ensure technology staff or vendor has background in current network and Internet security architecture
- Consider an independent review of network security and architecture
- Ensure the installation of regular updates of operating system, firewall, virus and spyware detection software

- Consider download restrictions from the Internet on network PCs
- Ensure protection of data on laptop/home/mobile devices
- Ensure network system administration includes strong password protocols and inactivity protections
- Isolate PCs used for financial transactions or have the highest levels of Internet security on these devices

Banking Controls

- Use online banking to review all transaction activity every day
- Implement Positive Pay and/or Check Blocks to protect against check fraud losses
- Implement ACH Filters and/or ACH Blocks to protect against ACH (electronic transaction) fraud
- Use a Universal Payment Identification Code (UPIC) to facilitate the acceptance of ACH payments from customers

Human Resource Controls

- Develop Code of Conduct and Ethics
- Perform background checks of new hire candidates
- Institute whistleblower programs
- Educate employees regarding appropriate use of technology
- Limit personal Web browsing
- Provide training on detecting suspicious emails, confidential information sharing and safe remote access to company data
- Develop reporting on employee computer usage

Cindy Grove
VP Relatioship Manager, Colorado Business Bank
Phone: 303-291-2974
cgrove@cobizbank.com

Curt Morgan
VP Treasury Management, Colorado Business Bank
Phone: 303-383-1241
cmorgan@cobizbank.com