

MINIMIZING EXPOSURE TO FRAUD – PART 1: CHECKING ACCOUNT CONTROLS

Posted on January 9, 2013

Small businesses and nonprofit organizations may have more exposure to fraud since they often do not have the resources or systems available for fraud prevention. Fraud can occur when an employee is provided with the opportunity to handle cash or assets without a system of “checks and balances” in place. While there is no way to completely prevent fraud, there are ways to minimize the risk and increase the chance of detection.

When considering an organization’s vulnerability to fraud, it is important to keep the following in mind:

- **Financial statement audits do not detect fraud.** Audit reports specifically state that they are not intended to detect fraud. Fraud may be discovered during a financial statement audit, but an audit is not an effective means of protecting your organization from fraud.
- **Banks do not guarantee signature verification.** Although your bank may notice an unauthorized signature or missing signature(s) on a check, the volume of bank activity makes signature verification an unreliable method for protecting against fraud.

The following recommendations can help organizations minimize exposure:

Checking Account Controls

- Do not delegate responsibility for check signing. CEOs and Executive Directors are ultimately responsible for the finances of an organization and should retain check signing authority.
- Do not use signature stamps for checks.
- Have all checks printed from QuickBooks (or your accounting system). Computer generated checks provide a level of assurance that the payee on the check matches that recorded in the system and reduces the risk of alteration.
- Minimize handwritten checks. Although the bank reconciliation process verifies check amounts and numbers, it is not often possible to verify the payee.
- Request that the bank return cancelled checks (or electronic images) with your bank statements and verify that the payee on a cleared check matches the payee in the accounting system.
- Endorse checks for Deposit. Immediately upon receipt, use a stamp or endorse all checks received with “For Deposit Only” along with the company’s bank account number.

- Have bank statements mailed to a separate address.
- Open and review bank statements when received – before providing statements to accountant for reconciliation.
- Limit access to bank account PIN numbers and avoid the use of debit cards. Providing employees with codes or software that enables them to transfer money essentially provides them with check signing authority.
- Do not allow anyone to misrepresent themselves as you by giving them your password, or allowing them to sign your name. Allowing an employee to sign your name, even on credit card purchases, could compromise your legal recourse if fraud or embezzlement occurs.
- Provide only original documents for posting and payment processing. Using original documents can prevent fraudulent alteration of document copies.