

Top Ten Tips to Help Prevent Fraud (in Order of Effectiveness)

1. Send Bank and Credit Card Statements to a Separate Address. Do not send your bank statements to your business address. Have your bank statement sent to your home, PO Box, or lockbox address. Review each check both front and back for payee, signature, and endorsement. Even if you don't allow your employees to use your credit card, make sure those statements sent to an alternative address too. Examine each statement carefully. Review each and every line item of both payments and charges.

2. Do Not Let Anyone Misrepresent Themselves as You. Do not let them use your password, sign your name, or use your credit card, ever. Never let an employee sign your name, use your credit card, or misrepresent themselves to your bank or credit card company. Reimburse their expense. Don't reveal sensitive passwords. If you allow your employee to sign your name even on credit card purchases, it could compromise your legal recourse in case of fraud or embezzlement.

3. Reconcile Bank Accounts and Review Statements. Review every statement. Make sure all bank accounts and credit cards are reconciled. Afterwards, take time to review every reconciliation report. Notice stale checks or deposits that have not cleared the bank. Check for missing deposits. An increase in the number of reconciled items may also reveal mischief.

4. Assign Administrative Rights Effectively. Use the Administrative rights in QuickBooks to protect your data. The first person to set up QuickBooks is by default assigned as Administrator. This role has unique permissions. So the administrator should be designated to either an outside party, i.e., a CPA, a QuickBooks Certified Consultant, or the savvy owner. Make sure that every user is set up separately and that passwords are used. Lock down permissions to change or delete transactions. **Especially important:** Use passwords for closing dates.

5. Use the Audit Trail in QuickBooks. If you don't have the latest version of QuickBooks, make sure you turn on the **Audit Trail**. Go to **Preferences > Accounting** and click on the box **Audit Trail**. **Caution:** the **Audit Trail** won't tell you if a vendor name has been changed or merged. It is wise to maintain a strict paper trail. Supporting documents need to be readily accessible in your files and then archived according to the type of document.

6. Use the Voided/Deleted Transaction Report. After you have turned on the Audit Trail, and made its review part of your routine, periodically review the **Voided/Deleted Transaction Report** to see which entries which have been modified.

7. Establish Accounting Controls. The principle of countervailing power is the fundamental reason to use checks and balances in accounting. Split the responsibilities between staff members or outside accounting professionals. **Warning Sign:** If only one person writes the checks and reconciles the account, there is no double check. Separate the duties. Consider another person to

Ferry's Bookkeeping, Etc. LLC

do reconciliations so it is done by a person other than the staffer generating the checks. Perhaps a Certified QuickBooks ProAdvisor® or CPA can provide these services.

8. Adhere to a Numerical Sequence. Use a numerical sequence for all transactions. Invoice, bills, and checks which are numbered fall in a logical and chronological order. The reason: To identify missing documents. Look at the bank statement for large gaps. Secure paper checks. If you keep voided paper checks, remember to tear off the signature area to keep it from being misused. If your bank sends paper checks, sort them numerically.

9. Review Receivables and Payables. Look for adjustments to **Receivables** or **Payables**. Such adjustments could indicate subverted payments or vendor checks.

10. Back up Your Data. Repeat after me – Back up, back up, back up. Think redundant backups as a contingency plan for disasters of all sorts. Make scheduled copies. Rotate the media (tape drive or portable storage). If you use CDs, better buy the read-only variety. Store your backups at another location. Such diligence can come in especially handy if there is a disaster. In some fraud cases, the bookkeeper may delete all of the QuickBooks files to avoid detection. In such cases the business has to pay a large sum for data retrieval, in hopes of capturing any shred of evidence. Be smart; back up. It only takes a few minutes.

Let us know if you have any questions. You can contact us at (541)550-0465.