CARROLL and COMPANY

CERTIFIED PUBLIC ACCOUNTANTS

2640-A Mitcham Drive
Tallahassee, FL 32308-5400

FREDERICK CARROLL III, CPA
ABBY F. DUPREE, CPA
KATHLEEN E. BROTHERS, CPA
STEPHANIE G. ZOTTOLI, CPA

LAUREE M. ELLIOTT, CPA

(850) 877-1099
Fax (850) 878-7000
E-Mail: cpas@ccrcpa.com
Website address: www.ccrcpa.com

MEMBERS
AMERICAN INSTITUTE OF
CERTIFIED PUBLIC ACCOUNTANTS
FLORIDA INSTITUTE OF
CERTIFIED PUBLIC ACCOUNTANTS
GEORGIA SOCIETY OF
CERTIFIED PUBLIC ACCOUNTANTS

RE: BEST PRACTICES FOR AVOIDING FRAUD

During these difficult economic times, many business owners are discovering that their assets are not as well protected as they thought. This is especially true in small business environments. The potential risk is compounded for small businesses where a single employee manages all the finances and there are inadequate "checks and balances" to verify that transactions are accurate. Trust is not the issue, verifying the transaction is.

When proper, consistent procedures are not in place, employees can learn to manipulate the accounting system to their benefit. Whether they take money from the company or their mistakes are undiscovered, the end result can greatly impact the company's management discussions, financial reports, and tax filings.

Unfortunately, once your financial records have been altered, discovering problems is extremely difficult. Most standard accounting practices are not designed to uncover internal problems such as embezzlement.

We have compiled a list of basic fraud prevention best practices from a variety of sources that we believe every business owner or manager should implement to the extent possible in their organization.

EMPLOYMENT CONDITIONS

- Institute background checks on all new employees, and notify job applicants that their backgrounds will be checked.
- Clearly communicate to employees the behavior that is expected of them, and set a positive example for appropriate employee behavior. Conduct your own activities on a high ethical level, and take strong action against employees who commit fraud.
- Adopt a tip hotline or complaint-reporting mechanism that will enable employees, vendors, customers, or outside sources to report suspected fraud anonymously or without fear of reprisal.
- Provide regular and recurring training on the detrimental effects of fraud, and what to do if they suspect fraud or inappropriate behavior.

- Require uninterrupted vacations for all employees, and establish a schedule of rotation of certain employee responsibilities. Rotation of duties provides a strong disincentive to commit fraud.

- Be alert to changes in employee attitudes, behavior, and lifestyles. Pay attention to attitudes that are hostile or defensive toward management or the organization in general, changes in behavior that are inconsistent with employee's normal disposition, or lifestyles that are not reasonable based on the employee's level of compensation.

- Obtain reasonable fidelity bond coverage. The amount of coverage should be reviewed periodically for adequacy.

INTERNAL CONTROLS

By implementing some simple internal controls, you can reveal potential errors or discrepancies while safeguarding company assets and financial records.

- Develop a procedures manual. While providing a resource for activities, procedures manuals also serve two additional purposes: 1) examining and documenting often uncovers potential internal control weaknesses; and 2) serves as a benchmark for determining employee performance.

- To the extent possible, assign related duties to different people. Certain accounting functions are designed to cross-reference each other for accuracy, writing/signing checks, ordering/paying/receiving materials, handling cash/recording cash, etc. The procedures can reveal inconsistencies in your records in a timely manner.

- Control the mail. Receive the mail personally, or have the mail received by an employee who has no responsibilities related to the handling or recording of deposits, accounts receivable records, or revenues. All remittances from customers should be directed to a post office box. Limiting access to the organization's mail is essential in preventing unauthorized negotiation of cash receipts.

- Limit the number of authorized check signers. Consider requiring two signatures on checks over a specified amount. The use of facsimile signatures or signature stamps should be avoided if at all possible. <u>Never</u> sign blank checks.

- Always ask for proof before you sign a check or authorize a transaction. When you insist on reviewing original documentation, your employees become more accurate and communicate their needs more clearly. And remember to cancel supporting materials after signing a check.

- Establish an operating budget, and monitor actual results monthly. Investigate any significant variances.

- Review reports timely and thoroughly. Financial statements and other management reports should be prepared timely. Sloppy or delayed bookkeeping practices make decision making more difficult. In addition, timely review of the reports, especially comparative and trend statements can be the most efficient way to discover internal control problems.

- Scrutinize your bank statements each month. The owner/management should receive the bank statements personally unopened each month. Specific items that management should be alert to include:
  - Missing checks
  - Checks issued out of sequence
  - Unknown payees or payees that do not match the name in the check register
  - Checks that appear to have been altered or signatures or endorsements that look forged
  - Checks not signed by authorized signatories
  - Miscellaneous debits that are not recognizable
  - Other unusual or unexpected items

  After careful review of the bank statements, forward them to the bookkeeper for reconciling. Review the reconciliations for completeness and accuracy, paying attention to any "unreconciled differences" or other unusual items.

- Control the accounts receivable. Limit access to accounts receivable records, and in particular, the ability to issue credit memos, discounts, and refunds. Accounts receivable detail ledgers should be balanced with the general ledger control account on a regular basis, and differences should be investigated promptly. Only the owner/management should be authorized to write-off accounts deemed uncollectible. Any discrepancies reported by customers should be investigated promptly. Aged accounts should be reviewed monthly, and past due accounts investigated.

- Control the accounts payable. Establish and monitor approved vendor lists, and periodically review the list of approved vendors, being alert to:
  - Unknown vendors
  - Vendors with names similar to other known vendors
  - Vendors with no physical address or telephone number
  - Vendors whose addresses match employee addresses

  Changes to vendor master files should require supporting documentation, management approval, and independent review.

- Limit and monitor access to important documents and supplies – keep blank checks and signature stamps secured, and deposit cash and checks daily.

- Account for sequences, including checks, invoices, credit memos, and all other prenumbered items. Voided documents should be defaced to prevent unauthorized use, and retained to complete sequences.

- Control general journal entries by personally reviewing and approving all "non-standard" journal entries made. Review supporting documentation before approving journal entries, and investigate the following:
  - Entries made to unrelated accounts
  - Entries made to receivables or revenues at or near the close of a period
  - Entries made by persons whose responsibilities are not consistent with the accounts being adjusted

- Take advantage of computer controls provided in most accounting software packages, including QuickBooks, such as:
  - Use the password feature effectively, including limiting access to closed periods and changing passwords regularly.
  - Turn on and use the audit trail report for reviewing transactional detail and history, including an identification of those making changes.
  - Update the closing date monthly.
  - Back-up often and keep back-ups off site.

We would appreciate the opportunity to review these recommendations with you at your convenience, and/or assist with any implementation questions or issues you may have. Please call with any questions you have in the meantime.

Sincerely,

CARROLL and COMPANY