Reprinted with permission — *Child Care Information Exchange*
PO Box 3249, Redmond, WA 98073 • (800) 221-2864 • www.ChildCareExchange.com

Who Can You Trust?

by Thomas Lukaszewski, CPA

Why Worry? — The Extent of Fraud

Like all of us, you want to believe your employees, co-workers, and partners have the best interests of the business at heart. But you have a "gut" feeling that something just isn't right:

- *Two or three clients have complained recently that they had already paid their bill when they received another statement for late payment from you.*
- *It seems odd that you have been paying so much more for reimbursing staff for their supplies or out of pocket expenses during the last four to six months.*
- *Your payroll checking account never runs this low over several months. Not to worry, because your payroll clerk is so dedicated she doesn't even take a vacation, especially near payday!*
- *Perhaps you need to change banks — they have been getting on your nerves lately, especially since they have been losing some of your canceled checks during the past few months!*

The above situations are not unusual in large or small businesses. They don't necessarily mean that fraud exists; but they should be warning signs to pay closer attention to what is going on in your business, because they do signal possibilities that foul play is occurring. A large company can often recover from the loss of assets; but for a small company, the consequences can be devastating.

An increase in the use of part time and temporary employees coupled with increased instability and competitiveness in the job market all contribute to an increase in employee fraud.

How big is this problem? Organizations such as the Bureau of National Affairs or the Association of Certified Fraud Examiners have estimated that *annual losses* from employee embezzlement may be as high as $20 *billion* to $40 billion, and that white collar crime, which includes several types of fraud, may be as much as $400 billion or more per year!

"But my business is small, and I am there every day. That is just a problem for big companies!" Not so! A major business magazine states that over 80% of all crimes against businesses are inflicted on small businesses.

Different Types of Fraud

First of all, what is *fraud*? The U.S. Supreme Court has defined fraud as a legal wrong, or "tort," which meets the following conditions:

Thomas E. Lukaszewski, CPA, heads an accounting firm in the Chicago-land area which focuses on business issues facing the child care industry as well as other not-for-profit organizations.

■ a misrepresentation of a material fact

■ the perpetrator knew was false and

■ made with the intention that the misrepresentation be relied on and that

■ the victim did rely on and, as a result, incurred a loss.

It is important to note that the misrepresentation must have been intentional. Misrepresentations made unintentionally or by mistake are not fraud.

The National Crime Information Center calls fraud "a nonviolent crime for financial gain, committed by deception."

There are two broad classifications of fraud:

■ **Employee fraud** — which involves the misappropriation of assets.

■ **Management fraud** (actually refers to any employee who can manipulate the financial records — not just management), sometimes called "cooking the books" — which involves fraudulent financial reporting.

Some common types of **employee fraud** involve:

■ Theft of cash by:

— Diverting cash receipts

— Manipulating accounts receivable by "lapping" (which involves stealing a customer's payment and concealing the theft by applying subsequent payments from other customers to the first customer's account)

— Altering bank deposits

— Stealing or forging checks

— Stealing petty cash

— Disguising thefts as cash payments for supplies

— "Less cash" schemes — This is where a deposit is made but cash is withdrawn on the deposit ticket and only the net amount is deposited

■ Abuse of travel or entertainment reimbursements by including personal items, or by submitting different documentation more than once for the same charge (e.g., first an airline ticket, later a credit card receipt)

■ Payroll schemes such as:

— "Ghost" employees — In this scheme, nonexistent employees are created, fake records are set up for them in the payroll system, and they are "paid" along with the regular employees

— Paying more hours than actually worked

— Employees writing extra checks to themselves (usually where one person prepares the payroll with little or no supervision)

— Keeping a terminated or retired employee on the payroll for one or two extra periods — Here the perpetrator then steals the extra checks, forges the endorsement, and cashes or deposits the checks

Note that the above are by no means a complete list as there are many ways in which fraud can be committed.

Management fraud involves the intentional misstatement or omission of financial statement amounts or disclosures to deceive users of the financial statements. Here, either fictitious transactions are recorded, valid transactions are omitted, or accounting rules are intentionally not applied properly. These schemes may involve falsifying, altering, or manipulating accounting records or source documents such as invoices.

Why would such a situation occur?

■ Perhaps the owners approved an unrealistic budget, and the staff needs to inflate the revenues or decrease the expenses to be rewarded with bonuses or to even meet these goals just to keep their jobs.

■ Perhaps the organization needs to borrow money to make improvements to their programs or to stay competitive. The incentive here might be to inflate their assets or reduce the liabilities on the books so the lender will be more likely to approve the needed funds.

■ In smaller businesses, there may be pressure to increase tax deductions to minimize taxes, perhaps by charging personal expenses to the business.

Again, there are many other reasons why management fraud might be committed. The above is just a partial list.

In all of the situations where fraud exists, research done in this field by criminologists, psychologists, and other business disciplines have determined that three key factors are usually necessary for fraud to result:

■ **Pressures facing the person**, whether stemming from financial hardship; personal habits such as drugs, alcohol, or gambling, which may result in financial pressures to commit fraud to support these habits; or work related pressures such as feelings of being overworked and underpaid, which may prompt a person to want to "get even" with the employer by committing fraud.

■ **Perceived opportunity to commit fraud.** This situation usually occurs where conditions such as the following exist:

— Poor internal controls such as weak segregation of duties

— A rapid turnover of employees

— Constantly working under crisis conditions

— Absence of mandatory vacations

— Failure to consistently enforce standards and policies or to punish violators

Some conditions under which such opportunities exist include the use of many banks, inexperienced accounting staff, frequent change of auditors or legal counsel, or transactions between related parties.

■ **The person's integrity.** Even if the worker is under severe financial pressures, and is in a position to have the opportunity to commit fraud, the person will not do so if their personal integrity is high — it will prevent them from committing the fraud.

How to Protect Your Organization from Fraud

Establish an effective internal control system. This is perhaps the most important deterrent to fraud. Two of the most important aspects of an effective internal control systems involve:

■ Setting a tone, or developing a policy which lets employees know that the unauthorized use of the organization's assets will not be tolerated.

This policy should be communicated in a serious but non threatening manner. Most importantly, management must be prepared to follow through in implementing this policy; it will not be effective if violators are not dismissed or prosecuted. Effective managers can accomplish this while fostering a positive atmosphere of teamwork. A workforce developed in such a manner can contribute substantially to an organization's success.

Center leaders play a key role not only in enforcing this policy but as importantly in modeling compliance with it. If staff members perceive that the center director is using a staff vehicle for personal use, making personal phone calls on the center line, or being loose about work hours, they will get the message that it is okay to bend the rules.

■ Segregation of duties — that is, making sure that the responsibility for authorizing transactions, recording transactions in the books, and having access to assets should be performed by different people in the organization. In many small businesses, this becomes difficult as there are often not enough employees available to accomplish this. Where this is not possible, adequate control can be accomplished by the direct involvement of the owner/manager.

In the areas dealing with cash, for example, the owner can sign checks, review and make the bank deposits, review all bank statements and reconciliations, and monitor duties. In general, if the employees know you are actively involved in the security of your business, they are less likely to attempt fraud.

Pay attention to unusual behavior by employees. Psychology research indicates that when a person commits a crime, he or she often becomes overcome by emotions of fear and guilt. This usually displays itself in unusual behavior such as increased drinking, smoking, defensiveness, suspiciousness, etc. These types of behavior do not indicate that fraud exists; rather, it is the unexplained changes in behavior that arouse concerns, such as angry people suddenly become nice and vice versa. Caution should be used regarding probing employees' behavior without sufficient cause, as this may lead to charges of harassment.

Frequent tips or complaints. Often fraud is detected when customers, employees, friends, or managers complain that something is wrong. Customers complain because they feel they have in some way been taken advantage of. Fellow employees may feel jealous or angry when they see a sudden extravagant lifestyle change, or a soured friendship can be acted out in anger or blackmail.

Although the motives of the person complaining may be suspect, the allegations usually have merit that warrant further investigation.

Review bank reconciliations for old, reconciling items. Thefts of cash often cause reconciling items on bank reconciliations. For example, where receipts on the books do not appear as bank deposits on the same day, it could mean that the funds were diverted. Missing checks could indicate they were made out to unauthorized payees. Transfers between bank accounts should be reconciled on the same dates. A deposit in transit on one account might be listed as a reconciling item but never actually be deposited.

Excessive "void" transactions. Perhaps cash is received for extra services such as late fees, the receipts are diverted, and the office copy of the client's receipt for payment is marked "void." Here, observations

of unusual transactions occurring during particular employee's shifts are coupled with interviews with staff as to names of children who stayed late, followed up with a comparison of cash receipts records indicating whether those parents paid the required fee.

Many thefts of cash deposits can be discovered by comparing the entries in the cash receipts register for the day with that day's bank deposit ticket.

Periodic *surprise* cash counts of imprest petty cash funds is an effective way of determining cash shortages in the fund.

***Confirmations* of accounts receivable** is another effective detection method used in discovering fraud involving cash. Periodic statements should be sent to parents showing all billings and payments on your records asking them to indicate whether the record is correct.

Reviewing *write offs* of customer receivables as uncollectible may lead to information indicating the employee diverted customer payments for their own use.

Many types of payroll fraud can be detected by **examining the organization's payroll records, payroll checks, employees' lists, and personnel files**.

For example:

- If fictitious employees are suspected, determine whether the same social security number may exist for the same employee or whether two different employees have the same address. Further, examine canceled checks for unusual or second endorsements. Note any checks that were *cashed* rather than deposited (generally a bank adds a code marking indicating that the check was cashed rather than deposited). Have a high ranking officer physically distribute paychecks to each worker and follow up on any unclaimed checks.

- To determine if too many hours are being paid, trace the hours to time cards or other internal records used to track hours worked. Recalculate the gross pay if the worker is paid on an hourly basis. Trace gross pay rates to proper authorizations and employee contracts.

Expense account reports should be reviewed for reasonableness, and dates and details of the charges should be compared to other company records indicating the employee should have been on business for the organization during those time periods.

Establishing a positive and effective internal control system, creating an attitude that management is involved and aware of what is happening on an ongoing basis, maintaining an accounting system with built in audit trails, and following up when questionable situations arise — all of these will go a long way to protecting your organization from becoming a fraud victim.