BKR DUPUIS & RYDEN

Spring 2002

FOOTNOTES

A newsletter from an Independent Member of BKR International with Offices Throughout the World

HighNotes

Nonprofit Fraud 1

Reduce Your Losses from Errors and Fraud 3

Skimming Receivables 4

Security Policy 101 5

How to Prevent Common Internal Control Problems 5

Thought Leadership 6

Etc. Etc. 6

Services:

Accounting & Auditing
Business Valuation
Fraud
Litigation Support
Tax Planning & Complilance

Affilations:

BKR International

Ballard Accounting & Tax
Tom Bement
810.653.1930

Locations:

Flint 810.767.5350
Grand Blanc .810.695.3870
Fenton 810.750.6266
Ann Arbor 734.747.8863

www.bkrdupuisryden.com

Nonprofit Fraud

Continuing with our theme of fraud control, the issue of fraudulent activity in nonprofit organizations has become more evident because of the increased public perception that some are not properly handling their finances. Lax accounting policies, poor internal controls and autocratic directors have been the major contributors to fraud in these organizations and have resulted in millions of dollars of abuse.

A Few Examples from the Nonprofit Fraud File

Several recent nonprofit frauds have captured everyone's attention, and their stories have been openly discussed in the media.

For 10 years, the executive director embezzled an average of $100,000 a year. He had raised millions for the charity and had an impressive list of fundraisers.

A not-so temporary bank account used 10 years previously for a fundraising walkathon had been left open. The director deposited several checks from donors into that account for his personal use. He was the only one who knew the account existed. Feeling guilty about his actions, he was caught when he told a staff member about the bank account.

Why did he commit fraud? He stole because he felt he

- was underpaid (his salary was approximately $110,00 per year, while other directors of similar nonprofits had annual salaries of about $200,000)
- was overworked (he spent countless hours raising funds)
- needed to maintain a high standard of living, given his stature as director.

The former chief of an agency was convicted and sentenced to seven years for having spent over $600,000 to pay for romantic getaways with his teenage girlfriend. At the time he was caught, he was 77 years old.

One office of an organization lost $10 million to fraud and mismanagement that approximated 25% of its yearly budget. One million dollars was stolen and $9 million was wasted. Several employees padded expense accounts, falsified medical claims and channeled money to phony organizations.

The Fraud Triangle

Three elements are present in every fraud:

1. perceived pressures
2. rationalization and
3. perceived opportunity.

Everyone experiences pressures and everyone rationalizes. Thus, everyone is a walking-around two-thirds fraud triangle. Combining the right level of pressure and rationalization with the perceived opportunity is what allows a person to commit fraud. Therefore, an organization should follow several steps to lessen the chance of fraud. These include the following:

1. Pre-screen potential employees.
2. Talk often with current employees so you'll know when they're feeling pressured.
3. Tell employees the consequences of committing fraud.
4. Be sure management sets a good example by following the rules.
5. Establish a sound internal control system.

A System of Internal Control

It is vitally important to have a strong system of internal control. Recent studies confirm the following key facts:

- The top *detector* of fraud is *good* internal control.
- The top *cause* of fraud is *poor* internal control.

Controls may be good in theory but not in application. Many frauds occur when controls are in place but are being circumvented. Therefore, you should constantly monitor and evaluate your control system. You should also create written policies which spell out proper and improper employee behavior.

(continued on Page 2)

(continued from Page 1)

Separation of duties is a major factor in an internal control structure. Be sure to separate the following three duties:

- authorization of transactions
- custody of assets
- record-keeping related to those assets.

The cardinal principle concerning controls is simple: The more liquid the assets, the more controls are needed to protect the assets from fraud. Cash is, of course, the most liquid asset. If your organization ever receives cash, it's especially vital that you establish proper internal control. Ideally, the same individual should not be responsible for receiving cash, depositing it and handling the recordkeeping (that is, reconciling the bank account and recording the accounting entries). Under no circumstances should a director be personally handling the organization's cash donations.

If your organization is so small that you can't separate duties, you should require an independent check of work being done. You can have a board member or an independent auditor perform this check.

Another way to perform an independent check is to require employees to take vacations. While one employee is gone, have someone else take over the duties and verify that no fraud has taken place.

In one recent fraud, a bookkeeper stole in the simplest way possible. She wrote checks to herself and deposited them in her own bank account. She could do so because she had authorization over transactions, kept the records and had custody of the assets. These three duties should have been separated, but they weren't. That was the organization's first mistake. Its second mistake was that no one reviewed the bookkeeper's work. As the organization's director put it, "We trusted her completely."

Proper separation of duties will not stop all frauds. Employees and management may override the internal control system. But having such a system in place will dramatically cut your risk.

A True Independent Reviewer

No matter what the size of your organization, your board of directors should require an audit, not just a review of your financial statements. An audit can be expensive, but it's well worth it when you consider the devastating price of fraud.

Only a certified public accountant (CPA) can perform a financial audit and express an opinion on the organization's financial statements. A professional auditor is bound by special standards. These standards don't apply if someone simply reviews your financial records. In a professional audit, the following standards apply:

- The auditor is required to assess the risk of errors and irregularities which may cause your financial statements to be materially misstated.
- Based on the level of risk, the auditor is required to design the audit to assure that material errors and irregularities are detected.

So concerned is the auditing profession about fraud that the American Institute of Certified Public Accountants (AICPA) recently issued a new auditing standard. This standard, "Consideration of Fraud in a Financial Statement Audit," describes two types of fraud:

- intentional falsification of financial statements and
- theft of assets.

The standard requires auditors to assess the risk of material misstatement arising from fraud on every audit. It notes that if auditors discover fraud, they must tell the appropriate levels of management, the organization's audit committee and appropriate regulators.

What to Do if Fraud Occurs

When fraud does occur, you must punish the offender. You may be tempted to keep it quiet so that the public won't get wind of it. But if you hide what has happened or allow the guilty employee to resign, you send a lethal message to the rest of your employees: "Go ahead and commit fraud. The worst thing that can happen is that you will be let go."

A Fraud Response Plan

The best strategy is to have a plan in place *before* fraud occurs. In your plan, describe ways to prevent fraud and procedures to follow if fraud occurs. Answer such questions as these:

- What is the organization's policy on fraud?
- Who should be contacted first when fraud is detected or suspected?
- What approaches should employees take to secure the organization's assets?
- What key people outside the organization may be helpful in preventing, detecting or correcting fraud? (Examples include police, insurers, regulatory agencies and forensic accountants.)
- What steps should be taken if fraud is detected?
- Who will act as spokesperson for the organization if a major fraud occurs?

Remember, fraud can hurt more than your bank account. It can be devastating in terms of employee morale and community reputation. When fraud occurs, it may be impossible to recover if you don't have a plan in place.

Don't take the position that fraud occurs only in other organizations. In fact, all organizations are susceptible to fraud. Fraud can never be totally eliminated, but proper actions and some common-sense approaches can reduce your risk.

Our next two issues of *Footnotes* will contain further articles on fraud.

Peggy Haw Jury, CPA, CFA

"Whoever is careless with the truth in small matters cannot be trusted with important matters."

Albert Einstein

Reduce Your Losses from Errors and Fraud

A simple system of internal controls can save you money by decreasing risk.

1. Don't Depend on Trust Alone

Many leaders trust that people will "do the right thing." But errors and fraud do occur if proper controls aren't in place. Internal controls prevent and detect errors and fraud by providing a system of checks and balances.

Keep an Eye Out for Errors

Errors can be acts of commission (such as honest mistakes in cash handling) or omission (such as failing to get grant applications in on time and thereby losing out on funding). Monetary losses can mount up when there is no system of internal controls to catch and correct errors before they get out of hand.

Watch for Fraud

Damage from fraud can be even more disastrous than losses from errors, as these examples show:

The local police fraternal organization's treasurer, a 15-year police officer, embezzled $200,000 over six years. He was responsible for check authorization, check signing and bank reconciliations. He admitted writing checks to himself to pay off his credit cards, among other personal reasons.

Similarly, the financial director of a state chapter wrote 58 checks to herself over a 13-month period and was charged with embezzling $85,000. Officials failed to investigate her background before entrusting her with their financial matters. If they had, they would have discovered that she was on probation for embezzling $800,000 while an accountant at a real estate firm.

A nonprofit organization's treasurer deposited members' checks but pocketed their cash payments. Many members were thus reported as having large balances due. The board asked the treasurer about these balances and was told that everything was "in hand". The board's finance committee failed to investigate the problem further.

In the aftermath of these frauds, board members explained that they trusted the person and had no reason to believe anything was wrong. In all cases, however, they could have avoided embarrassment and loss of public confidence by instituting a system of internal controls.

2. Remove the Opportunity

For even the most trustworthy person, the important thing is to eliminate the opportunity.

Segregate Duties

To reduce the opportunity for error and fraud, make sure you separate the duties of authorization, access and recordkeeping. Separating these duties ensures that one person doesn't have access to assets (such as cash), the ability to authorize transactions involving those assets *and* the ability to change records pertaining to the assets. Thus, no one has the opportunity to take assets and hide the loss by altering the records.

The treasurer in voluntary organizations typically has too many duties: The treasurer authorizes expenditures, has custody over cash receipts, makes deposits, signs checks, performs recordkeeping functions and reconciles the bank statements! It would be more appropriate to have the treasurer serve as a controller or recordkeeper. To prevent errors or fraud, other officers must have some involvement in the accounting process.

For example, the vice president—not the treasurer—should sign checks (separation of access from recordkeeping). The secretary or other third party not responsible for check signing should reconcile bank statements to verify that bank records agree with the organization's records (provision of oversight separate from recordkeeping and access). The president or executive director should approve reimbursement requests before the vice president writes checks (separation of authorization from recordkeeping).

Also be sure to separate the duties of people who are related to each other. Otherwise, one person can cover up for the other or pressure the other to do something unethical because of their special relationship.

For example, if the president is the treasurer's spouse, the organization doesn't have proper separation of duties. Furthermore, the president and treasurer shouldn't have a supervisor-supervisee work relationship.

Use Physical Controls

Another way to eliminate opportunity is with tangible controls. For example, require pre-numbered receipts or checks. It's easier to tell if funds have been misappropriated or misplaced if serially numbered documents are used. It's also important to limit access to assets—not only to cash but also to fundraising assets such as cookies or raffle tickets.

3. Reconcile Accounts

Reconciliation is important to check for errors and provide oversight of the recording function. Such tasks include reconciling fundraising assets, such as raffle tickets and cash receipts and performing a monthly reconciliation. A person who doesn't authorize transactions, have custody of assets or keep the records should perform the reconciliations.

4. Be Sure the Board Fulfills Its Duties

The board is responsible for ensuring that the organization is run in accordance with its charter and legal requirements. Board members also hold ultimate responsibility for managing the organization's financial risks. They must see to it that an internal control system is in place and that an annual audit is performed by an unbiased external consultant. They may either review the audit themselves or create an audit committee to do so.

5. Keep Good Records

Written procedures are essential in minimizing errors, exposing fraud, reducing risk and helping people carry out their duties effectively. Adequate records provide information on proper procedures as well as historical information on your organization's activities. In addition, employee and officer transactions will be efficient if you have good records.

6. Get Help

Professional accountants can help you tighten your internal control system. If you can't afford an accounting firm, look for free or inexpensive assistance.

(continued on Page 4)

Contact the local chapter of your state CPA society, which may provide pro bono services for charitable organizations. Also, call the accounting department of your local university. Many universities require students to provide accounting services to nonprofits as part of their course assignments. In their coursework at the University of New Orleans, for example, auditing students evaluate the internal controls of small voluntary and professional organizations.

No matter whom you get to advise you, don't leave your control system to chance. A system of internal controls need not be burdensome. But such a system is essential to improve the integrity of your organization's financial statements, reduce the potential for errors and fraud, maintain public confidence, control your activities and achieve your goals.

*** Don't Depend on Trust Alone**

*** Remove the Opportunity**

*** Reconcile Accounts**

*** Be Sure the Board Fulfills Its Duties**

*** Keep Good Records**

*** Get Help**

Skimming Receivables

Employees sometimes skim from receivable payments by understating the amount owed on the books, then stealing the excess. For instance, if a customer owed $5,000, the perpetrator might post the receivable as $3,000 and skim the excess $2,000. The fraudster either enters the wrong amount owed, or adjusts the account that already has been posted.

Forum participants listed techniques to detect receivables skimming – particularly cases in which one employee is in charge of collecting and posting receivable payments as well as authorizing adjustments to those accounts:

- Send customers satisfaction surveys or account balance letters.
- Compare customer's copy of receipt to store's copy.
- Rotate job responsibilities without prior notice.
- Implement policy that separates receivable duties (i.e., employees who post payments cannot enter or adjust accounts receivable items).
- Monitor and follow up on customer complaints.
- Look for lifestyle changes in accounts receivable personnel.
- Enforce mandatory vacations and rotate assignments.
- Audit receivables randomly.
- Analyze trends for excessive discounts.
- Check supporting documentation for all adjustments to accounts receivable.
- Install hidden flags on accounting software to highlight changes/overrides to accounts receivable.
- Monitor gross profit margins on receivables.
- Spot-check credit sales to receivables accounts.
- Use three-part invoices – one to accounts receivable, one to independent staff, one to customer – and see if they match.
- Perform ratio analysis: compare each salesperson's profit margins for common products.
- Create exception report for alterations to accounts receivable.
- Review all general ledger adjustments.
- Compare "goods shipped" records to "payment received" records.
- Monitor employee desks and trash bins for notes indicating forced reconciliation.
- Intercept incoming mail, open and note amount of receivable. Re-seal the envelopes, have employees open them and then check the recorded receivables.

How to Prevent Common Internal Control Problems

Segreation of Duties

- Separate authorization, custody and recordkeeping functions.

Cash Receipts

- Give receipts for dues or donations of cash.
- Use pre-numbered cash receipts book.
- Keep membership application/dues remittance advice.
- Immediately place restrictive endorsements on checks.
- Make deposits daily.

Cash Disbursements

- Have authorization procedure for cash disbursements.
- Require documentation to support cash disbursements or petty cash payments.
- Do not write checks for an amount that exceeds supporting invoice.
- Pay from original invoices to prevent duplicate payments for items.
- Institute a policy prohibiting purchase of personal items with organization funds.
- Require two signatures on check over a pre-specified amount.
- Don't permit organization checks to be made out to "Cash."
- Have a designated check signer or signers.
- Be sure the payee is listed in check register for each check.
- Classify expenses for control purposes.
- Enter bank service charges in check register.

Procedures

- Provide written procedures for cash receipts or cash disbursements.
- Make sure current officers know about written procedures.
- Prepare periodic (annual, at least) financial statements.
- Put large checking balances into a short-term CD.
- Periodically analyze whether bank charges on the account are excessive.

Physical Controls

- Limit access to unused checks or unused cash receipts books.
- Limit access to petty cash.
- Have only specific people be responsible for cash box at fundraising events.
- Limit access to fundraising assets: raffle tickets, T-shirts, cookies, etc.

Reconciliations

- Reconcile cash deposited for dues to dues application/remittance advice.
- Reconcile raffle tickets, etc., with cash receipts.
- Perform bank reconciliation monthly.
- Keep the bank statements or canceled and voided checks.
- Trace (match) bank deposits to amounts in the checkbook.
- Reconcile money transferred to or from national organization/ organizational network.
- Have an audit performed by an external auditor.

Security Policy 101

One size doesn't fit all when setting a security policy. But for any business, the more detailed and specific the policy, the better the protection it will provide. Your policy should address these key areas.

Computing Resources

This is a broad topic, and there are a wide range of abuses related to it, but your policy should identify and address what is tolerable and what the consequences are for violating the policy, including: Are your employees day-trading at work? Or running a small business, say, building web sites on company time? What about Quake tournaments in the office? Even seemingly harmless actions can cause serious security problems.

E-Mail

Determine what comes in and what goes out. Sophisticated attackers might be able to penetrate your network via e-mail and e-mail attachments regardless of what barriers you erect, but a good policy goes a long way toward reducing e-mail associated risks. For instance, simply blocking all incoming mail that has executable file attachments can greatly reduce vulnerabilities.

Virtual Private Networks

You've gone to great lengths and expense to create a virtual private network. But if home users – telecommuters, go-getters working late from home – connecting to the network aren't secure, then they can unknowingly escort attackers right in. Set up a system of checks and balances in which home users can't have remote access unless their connections are secured.

Passwords

One-quarter of respondents to the 2000 Information Security Industry Survey reported breaches from attacks using insecure passwords. Passwords need to be turned on in the first place. Then they need to be changed often. Of course, they also need to be protected. That means no sticky notes bearing passwords attached to computer monitors.

Fraud

A firewall can't protect you from everything. Focusing on technology issues at the expense of other threats is a mistake. Losses to fraud last year were greater than those due to sabotage, insider Internet abuse and viruses.

Physical Theft

Does your policy account for all the laptops that have been issued to employees? Ask the same question for any item of value that employees might be walking out with (inadvertently or not).

"It takes a great man to be a good listener."

Calvin Coolidge

Thought Leadership

Bethany Hearn achieved her ABV (Accredited in Business Valuations) designation. There are only 60 CPAs with this designation in Michigan and three in Genesee County.

Dave Gibbons facilitated a workshop for the University of Michigan Benefits Office on "Asset Allocation and Investment Strategies."

Jeanette Bateman was elected President of the American Society of Women Accountants for 2002-2003.

For many years BKR Dupuis & Ryden has been a strong supporter of Junior Achievement. Recently Marilyn Holmes, Michael Roeper, Nick Zuhlke and Barbara Bachman participated in JA's Accounting Blitz at elementary schools in the Carman-Ainsworth and Swartz Creek School Districts.

Janette Sullivant, JoAnn Smith, Kelly Visser, Tom Beaton, Tonya Roper, Jennifer Swank and Angel Davis instructed students at elementary schools in Flint, Flushing and Grand Blanc.

Etc. Etc.

Congratulations to Tonya Roper who was awarded an International Poet of Merit Award by the International Society of Poets for her poem "Climax".

Annual Scholarship Awards Presented

On April 23, 2002, Sarah Frost presented the BKR Dupuis & Ryden University of Michigan-Flint Accounting Scholarship Award to Laura Ottewell. At that time Elizabeth Ackley, Cameron Cassidy, Robert Lipset, and Adam Standen received the BKR Dupuis & Ryden's Accounting Achievement Awards.

Tonya Roper presented our annual four-year scholarship to Jordan Munerlyn from Southwestern Academy at the May 29, 2002 Urban League of Flint's Salute to Black Scholars Tribute.

If you're interested in a specific area of fraud and would like us to post a related article . . please contact Pat Smythe, psmythe@bkrdupuisryden.com or 810.766.6051.

Summer Hours

Our summer hours are now in effect.
Monday – Thursday
8:00 a.m. – 5:00 p.m.
Friday
8:00 am. - Noon

We now have a new feature on our web site under "What's New". It contains a complete array of financial calculators for home financing, investments, leases, personal financing and retirement.

Please visit our website,
www.bkrdupuisryden.com
regularly for important tax tips!

Your thoughts are important to us. If you recently received a client survey, please complete and return to us. We appreciate your cooperation.

BKR DUPUIS & RYDEN
Financial Services

PRSRT STD
U.S. Postage
PAID
Flint, MI
Permit No. 157

BKR Dupuis & Ryden
111 East Court Street, Suite 1A, Flint, Michigan 48502
810.767.5350 FAX 810.767.8150