SAFEGUARDING AGAINST FRAUD

BY MARK A. KELLER, SR/WA, ASA

Trust is a strong bond within organizations. Unfortunately, it can be easily misplaced. When this happens, embezzlement, misappropriation of funds, cover-ups and inappropriate hiring practices may follow. These are only some of the growth areas of fraud that are draining the resources of organizations today. Non-profit organizations can be especially susceptible.

According to "Non-Profit Fraud," author Jan Miller notes that non-profit organizations had the second highest median loss ($100,000 per fraud occurrence) of all organizations studied. The culture of a non-profit is one of utmost trust, and the general perception is that all members, officers, and workers are ethical and trustworthy. This perception can lead to a false sense of security. As a result, there may be inadequate internal controls and separation of duties, creating an ideal environment for fostering dishonesty.

Stephanie Strom highlights this phenomenon in "Report Sketches Crime Costing Billions: Theft from Charities." The 2006 report indicated that roughly 13% of the annual funds given to charities were embezzled. With an average of $300 billion generated annually, that equates to nearly $40 billion. The report found that the most common theft was committed by female employees with no criminal record, who earned less than $50,000 per year. While the average amount stolen was less than $40,000, one case cited involved a volunteer treasurer of the Madison County Humane

“Someone who was always easy to work with suddenly became belligerent and hostile when questioned about money...”

Society in Indiana who was charged with using $65,000 of the charity's money to buy jewelry and makeup. The most grievous cases however, involved male executives earning $100,000 to $149,000.

TELL-TALE SIGNS

A lack of proper internal controls and separation of duties can result in disaster. In a case of one non-profit organization, an officer had willingly volunteered to take on a variety of roles. This individual maintained the website, published the newsletter, managed the PayPal account and handled the annual tax preparation. He had performed flawlessly, so the other officers felt confident that they could rely on him to conscientiously perform all of his duties as a trusted officer. Unconditional trust was bestowed upon him.

Problems started to surface when the officer's attitude took a sudden change. There were noticeable changes in his commitment, personality and behavior. Someone who was always easy to work with suddenly became belligerent and hostile if questioned about money during the monthly meetings. According to forensic accountants, this is a tell-tale sign of trouble, and indeed things were about to unravel.

On a hunch, another officer decided to review revenue and expenses over a period of several years. The officer immediately noticed some inconsistencies and a pattern of systematic deposits and withdrawals to an unauthorized account. Upon further analysis, it was discovered that all activity was either linked to specific events where funds were collected or when new officers were appointed.

Subsequently, a formal review was performed of all accounts, passwords, domain names and records. An outside team comprised of a CPA, attorney, website consultant and other officers were able to reconstruct the fraudulent scheme. After exhaustive research, it was determined that a significant amount of the funds had been embezzled.

Hard work and determination eventually resulted in a favorable ending to this unfortunate situation. The group was able to recover the embezzled funds, along with all associated fees. Furthermore, the troubled former officer was prosecuted criminally.

Since that incident, the group has initiated checks and balances for checking accounts and signing authority. They have updated all of their procedures, instituted a separation of duties and require that all officers take an active role. In addition, they utilize QuickBooks for monthly/annual reconciliation, process all credit card payments electronically and conduct an annual audit with an outside CPA.

TAKE A CLOSER LOOK

The statistics can be alarming. If you are an officer in your organization, ask yourself some basic questions. Are proper accounting procedures and internal controls in place? Who is overseeing the funds collected? Is someone else auditing the financial statements? Have you noticed any inconsistencies in revenue?

According to internal auditors and forensic accountants, some basic steps can go a long way in preventing fraud and other financial problems. This list can get you started:

- Background check of officers, committee members and vendors
- One bank account; signature card with limited signing authority
- Bonding of officers and committee members
- Clear separation of duties
- Website and domain name security measures
- QuickBooks or other recognized accounting program
- Security measures if using services like PayPal
- Records retention and safeguarding
- New officers succession plan
- Established bylaws and procedures
- Annual audit plan and review

It takes a team of officers to get the job done. Review the organizational structure and duties to avoid carte blanche trust in any one officer or member. Formulate and implement a system of internal controls with many checks and balances. As former President Ronald Reagan once said, “Trust, but verify!”

Mark Keller, SR/WA, ASA

Mark is an appraiser with Salt River Project, a water and electric utility provider in Phoenix, Arizona. An active IRWA member since 1995, he has served in chapter and regional positions and as a member of the Valuation and Membership Committees. Mark is also active in the local chapters of ASA and ASFMRA.