

Broken Promises, Shattered Trust



By Melanie Lockwood Herman

Executive Director

Resource Type: Articles

Topic: Fraud and Financial Oversight

Preventing and Responding to Fraud and Misuse of Assets in a Nonprofit Organization

During the recent 39th annual Risk and Insurance Management Society (RIMS) annual conference held April 29-May 3rd in Atlanta, GA, a panel-style workshop on the topic of “Fraud” was held as part of the annual Nonprofits Industry Session. Attendees included risk managers from large secular and religious nonprofit umbrella organizations. The session was led by William Chapin, Director of Risk Management for the Roman Catholic Diocese of Rockville Centre.

In his introductory remarks, Chapin emphasized the importance of considering the legal, internal control, and resource-related aspects of fraud and fraud prevention. More than half of the session participants reported personal experience coping with the aftermath of fraud in their nonprofit organizations. Chapin characterized fraud as “pervasive” and often “accepted” in American society, noting that systems of control provide “reasonable assurances,” not absolute controls or protections against theft. Chapin added that since fraud risk, like other risks, cannot be eliminated altogether, effective risk management in this area requires a commitment to examining “what happened” in the aftermath of a fraud loss.

The second speaker on the panel was Charles J. Adams, an attorney from the firm of Patrick F. Adams, PC in Bayshore, New York. Adams explained that, in many cases, the person who commits fraud in a nonprofit is “someone that you know, like, and trust.” According to Adams, convincing a nonprofit to prosecute employees who commit fraud is often a difficult task for legal counsel. Several participants agreed that there is a general reluctance among nonprofits to prosecute employees, and this reluctance is perhaps most often found in religious nonprofits. Bill Chapin reminded participants that a nonprofit’s duty to its donors is significant, adding that when a nonprofit decides not to prosecute it is letting down these donors as well as the organization itself.

Adams described three general categories of workplace fraud and cautioned participants that nonprofits — like other businesses — are vulnerable to all categories of fraud.

- **Asset misappropriation** — This category includes everything from theft of cash to use of the nonprofit’s “corporate” credit card for personal items. Adams described a fraud case involving an employee who initially used the nonprofit’s credit card for an emergency. When this misuse was ignored

by the organization, the employee used the card over and over again, spending \$14,000 by the time she was caught. In another case, a bookkeeper forged checks totaling \$180,000. Her theft was detected after she left the organization. By that time she had stolen from her new employer. The subsequent investigation revealed that the bookkeeper had previously spent four years in prison for embezzlement.

- **Fraudulent statements** — When employees falsify their credentials, they have perpetrated a fraud against your organization. In one case a university staff member hacked into the institution's computer in order to award himself a degree.
- **Bribery and corruption** — In an example cited by attorney Charlie Adams, a manager with purchasing authority urged a consultant to submit fictitious bills, and the consultant agreed to share his "earnings" with the manager. Approximately \$300,000 was stolen by the pair before the scheme was detected. In another fraud case involving a New York-based nonprofit, a volunteer was responsible for counting cash receipts at the organization's annual fundraiser. The volunteer had performed this task for 30 years. One year, an accountant was assigned to assist the volunteer with the count. The volunteer offered the accountant a "cut" of the take in exchange for her silence about the theft.

Fascinating Fraud Facts

Source: [Association of Certified Fraud Examiners](#)

The following statistics about fraud and white-collar crime are featured in the Association of Certified Fraud Examiners' *Report to the Nation*. The Report contains a wealth of information about the causes of fraud, the direct and indirect costs of occupational fraud and abuse, and the methods by which employees and other insiders commit fraud. The Report is available at the ACFE web site: www.cfenet.com.

- Fraud and abuse costs U.S. organizations more than \$400 billion annually.
- The average organization loses more than \$9 per day per employee to fraud and abuse.
- The average organization loses about 6% of its total annual revenue to fraud and abuse committed by its own employees.
- The typical perpetrator is a college-educated white male.
- Men commit nearly 75% of the offenses.
- Losses caused by managers are four times those caused by employees.
- Median losses caused by executives are 16 times those of their employees.
- The most costly abuses occur in organizations with less than 100 employees.

During his presentation, Adams reminded attendees that while nonprofits often devote their greatest attention to protecting cash and checking accounts, other assets are at risk, such as inventory and contracts for services. Both inventory and information — such as the bids from other companies competing to provide services to the nonprofit — may be misappropriated.

Letting the Perpetrator Off the Hook

Four of the most commonly cited deterrents to reporting and prosecuting fraud in nonprofit organizations are:

- **Fear of notoriety** — many organizations fear the effects of negative publicity if they file an official report about insider theft;
- **Fear of legal action** — a nonprofit may be threatened with civil and criminal action by an offender. For example, someone caught with their hands in the till may threaten to sue for defamation, false arrest, violation of privacy, wrongful termination and more. These may be effective threats in some organizations and result in a decision not to prosecute;
- **Concern about personal safety** — as workplace violence takes up permanent residence on our "radar screens," employers are understandably wary of prosecuting thieves who threaten personnel with bodily injury; and
- **Compassion for the offender** — in many cases a nonprofit organization's leaders have a difficult time taking appropriate action when they have a sense of compassion for the circumstances facing the embezzler. For example, the bookkeeper or volunteer treasurer may claim that he stole from your nonprofit because he needed to purchase medication for a sick family member.

The panelists concurred on the various downsides of "passing" on prosecuting insiders, which include:

- setting a precedent that could lead to additional fraud;
- creating an environment that spurs rather than deters fraud;
- loss of credibility and respect for the organization among employees and others; and
- lack of access to a crime policy — some, but not all crime policies, require that the insured prosecute employees and volunteers who steal.

Conditions That May Lead to Fraud

According to Bill Chapin, some of the conditions that may increase incidents of insider theft include:

- **Lack of checks and balances.** One participant described a fraud case involving a check signer at a nonprofit who used her check signing “authority” to write checks for personal expenses. Without an internal system of checks and balances, it took months for the nonprofit to detect the fraud.
- **Cozy relationships between staff and suppliers.** In one case described by a panelist, a nonprofit staff member authorized above market prices for goods and services. The organization’s history of “overpaying” was detected during the annual audit.

Adams advised workshop attendees to investigate all suspected cases of fraud, adding that it’s important to get outside or in-house legal counsel involved from the beginning. An attorney can help ensure that evidence of fraud is properly preserved, and can advise your organization about whether sufficient probable cause exists to successfully prosecute. He or she can also advise on the organization’s likely success in civil court, and can assist in handling employee terminations.

The CPA’s Perspective

Michael McNee, Principal in the Metro New York Higher Education/Not-for-Profit Practice of Arthur Andersen, LLP was the final speaker at the recent fraud workshop. During his presentation, McNee shared insights from a career that includes 18 years of experience working with nonprofit organizations. McNee is the former chairman of the Nonprofit Organizations Committee of New York Society of Certified Public Accountants.

During his presentation, McNee cautioned that too often, fraud occurs where “a trusted person takes higher or extra paychecks, writes or wire transfers funds/checks to him or herself or to cash, to personal creditors, to an accomplice, or to a bogus company that is actually the trusted person.”

McNee presented a range of suggested controls and strategies to deter would-be thieves and uncover fraud promptly when it occurs, despite your precautions. For example, to guard against theft by the trusted employee who has too much authority:

- **Open and review bank statements** — Make certain that someone independent of check processing receives unopened bank statements each month and reviews payees, amounts, signatures, and endorsements.
- **Review bank reconciliations** — Have a supervisor review bank reconciliations on a monthly basis.
- **Verify wire transfers** — Have someone independent of the request for a wire transfer verify all wire transfers.
- **Provide appropriate system access** — Ensure that the level of system access by an employee is consistent with the employee’s job function and responsibility.

To prevent theft of incoming receipts:

- **Verify cash logs** — Make certain that your cash receipts log matches the cash receipts entry in the ledger and the actual bank deposit.
- **Involve a second person in cash receipts processing** — Have a second employee involved in verifying incoming receipts.
- **Make bank deposits daily.**
- **Learn how to spot “lapping receivables”** where an incoming payments from a third party is misappropriated and a later payment is credited to the earlier invoice.

To guard against “kickbacks” or false vendors:

- **Run vendor addresses through an edit check** to see if any match each other and/or employee addresses.
- **Review the vendor list in your accounting system periodically.**

On the topic of bank reconciliations, McNee explained that the importance of bank reconciliations is often overlooked, and the review of bank recs may be assigned to a junior accountant during an annual financial statement audit. An experienced CPA can spot irregularities during a review of these crucial financial documents.

Bank reconciliations should be completed on a timely basis, reviewed by a third party, and initialed by the reviewer. McNee also recommends that while it's crucial to establish an initial system of internal control, equally important is the process of re-examining these controls on an ongoing basis and making changes as needed.

Before ending his presentation, McNee offer a few additional reminders about fraud prevention:

- Don't assume that your bank will catch things and adhere to the rules you've established, such as requiring dual signatures on large checks.
- Keep in mind the fact that sometimes fraud starts where an individual receives an inadvertent "overpayment" in the form of a paycheck or reimbursement. If an overpayment makes its way through your accounting system and into the pocket of an employee, he or she may believe that future overpayments will also go undetected.
- Many nonprofits go to great lengths to protect written checks and forget about controls with regard to wire transfers.

The Nonprofit Risk Management Center is grateful to the three individuals who participated in the workshop on Fraud that was part of this year's RIMS Nonprofits Industry Session. Contact information for each speaker is featured below. For general follow up and questions, contact the Nonprofit Risk Management Center at (202) 785-3891.

William Chapin is Director of Risk Management for the Diocese of Rockville Centre, NY. Bill can be reached at (516) 678-5800, ext 261 or wgchapin@drvc.org.

Charles J. Adams is an attorney with Patrick F. Adams in Bayshore, NY. Charlie can be reached at (631) 666-6200.

Michael L. McNee, CPA, is Principal, Metro New York Higher Education/Not-For-Profit Practice, Arthur Andersen LLP. Mike can be reached at (212) 708-6312 or Michael.L.McNee@us.andersen.com