

## **WHAT IS “FRAUD”**

Theft of funds belonging to the local or region

Outright misappropriation

Reimbursement for fictitious expenses

Diversion into a separate account, with reimbursement at a later date (stealing the temporary use of the money)

Theft of funds belonging to the IEA-NEA

Improper membership reporting

Failure to pay dues

Misleading financial reporting

Purchase of goods or services from related parties at an inflated cost

Use of local/region funds for purposes not intended by the governing body

## **WHAT ARE THE CONTRIBUTING FACTORS TO FRAUD?**

Many experts use the “fraud triangle” concept to assess the risk of fraud in any particular situation. They feel that fraud becomes more likely when:

Someone has the **opportunity** to commit fraud, due to poor controls and/or lack of oversight.

Someone has an **incentive** to commit fraud: trying to maintain an extravagant lifestyle, unexpected financial obligations, etc.

Someone can find ways to **rationalize** their fraud somehow (“they owe it to me,” “the last Treasurer did it,” “I’ll pay it back later,” etc.).

Some sides of the triangle can be stronger than others. If an “honest” person has opportunity and a strong incentive, it can become relatively easy to take the next step and rationalize a fraudulent act. However, if opportunity is prevented due to strong controls and oversight, even if a person has a strong incentive and rationalization it will be very difficult for him/her to commit fraud.

A fairly typical situation is the case of an honest and law-abiding individual who has performed a job for years without taking a dime. Everyone trusts him and because of this, over time the controls and oversight over him are gradually slackened and ignored.

Then the person gets hit with some unexpected medical bills. He recognizes that he can take \$100 to pay a doctor bill out of his employer’s funds, without getting caught. He rationalizes this by thinking of all of the extra hours he has worked without pay or recognition. He also tells himself that he will pay it back when his financial situation improves. He takes the \$100 and covers it up by adjusting the books. No one notices. The next doctor bill is \$500. He takes this out of the till and is not detected. This cycle continues, with the thefts getting larger and more frequent. His supervisor and co-workers are oblivious. He stops taking vacations because he is afraid that someone will find his thefts if they examine the books.

He is finally caught when he becomes ill and has to miss work for a week. The person who takes over his job accidentally discovers the fraudulent bookkeeping entries that were made to cover up the thefts. Everyone is shocked. They shouldn’t be. They let the fraud occur by providing the opportunity. The opportunity just lay dormant for years until the incentive presented itself. The two joined forces and easily overpowered the willpower of a person who under other circumstances would have never taken a dime.

## **WHY DOES FRAUD GO UNNOTICED?**

With occasional exceptions, there is nothing new under the sun in terms of fraudulent or inept business practices. Even schemes based on new technology are usually just variations of time-honored frauds from the past. There is a wealth of literature on this topic, including many theories as to why people commit fraud and the common warning signs of inappropriate business practices.

If this is the case, why aren't more frauds or accounting fiascos caught before they get out of control? Unfortunately, most people in a position to do something about a questionable business practice do not know to recognize it. Even if they do, and the signs are all around them, they usually refuse to believe or act on them. This is due to trust or friendship with the person involved, a Pollyanna-like view of human nature, or a refusal to get involved (the "ostrich" mentality).

In a volunteer organization in which the people you work with are your friends and colleagues, "trust" can become a barrier to effective business practices. A local President might be afraid to propose that two signatures be required on all checks, for fear that the Treasurer would be offended because "You don't trust me." A Treasurer might let the President get away with inadequate documentation of expenses because they went to school together and she trusts her.

To get past this, all of the local leaders should recognize that inadequate controls and business practices are in no one's best interest. If fraud or other losses occur, the people who allowed the poor system of checks and balances to exist may be seen as co-conspirators or at least as incompetent leaders. Even if it doesn't result in actual fraud, a poor control environment erodes the credibility of the local and its leaders. Conversely, a good system of controls is a kind of safety net for local leaders. If questions about business practices arise, they can use the control environment to demonstrate that they are taking good care of the local's resources.

## **WHAT ARE SOME SIGNS THAT FRAUD MAY BE TAKING PLACE?**

Here are some signs that can indicate problems with the control environment. These are grouped in a manner that we're all familiar with.



### **RED Signals**

One person does all of the work related to financial and membership matters. Worst case is someone who serves as President, Membership Chair and Treasurer.

No oversight over the person with the checkbook (controls such as dual signatures are missing, there is no monthly financial reporting, etc.).

Deficiencies in documentation for disbursements:

- No documentation
- Use of copies instead of originals
- Multiple erasures/whiteouts on any kinds of financial records (checks, deposit slips, invoices, etc.)

Commingling of funds (general fund and PAC, etc.).

People with access to financial resources exhibit a “wheeler-dealer” personality, with little regard for financial responsibility. Sample comment: “Well, if I can’t pay my credit card bills, I’ll just declare bankruptcy.”

People who display an acceptance of dishonest behavior, as long as the consequences are avoided. Sample comment: "I made \$5,000 from my Avon business last year, and I didn't declare it as income because there's no way that I'll get caught."

Checks written to "Cash."

Cash withdrawals from the local's bank account.

Cash deducted from bank deposits.

### **ORANGE Signals**

The local is consistently behind in paying its IEA/NEA dues.

No annual review of the books/records by an outside body.

Signing of blank checks.

No budget, or no comparison of actual results to the budget.

Checks written payable to the check signer, without a second signature.

Bank statements are not reviewed by someone other than the Treasurer.

People in positions of authority appear to be living beyond their means.

No written, enforced guidelines on:

- Conflict of interest

- Ethics

- Documentation requirements/retention

- Reimbursement of expenses

- Check signing

- Training for treasurer on his/her duties

- Training for officers on financial matters such as controls and oversight over the bookkeeping function

- Annual Board approval of banking arrangements and approved signatures

- Strict controls over credit card use (or hopefully no use at all)

### **YELLOW Signals**

Delays in depositing checks/cash received.

Unexplained increases or decreases to the cash balance.

Treasurers, Membership Chairs and other officers do not attend IEA training sessions when they are offered in nearby locations, and/or are not aware of other IEA resources available to help them with their job duties.

Large petty cash funds with many transactions.

A local credit card is used for transactions that could be handled by check or reimbursement to an officer. In today's world most people have credit cards that provide rebates or airline miles for purchases. Therefore, it is not a financial burden to ask an officer to charge an expense to his/her credit card and then be promptly reimbursed by the local. This eliminates all of the control issues that come into play with the use of a local association credit card.

Use of an ATM or debit card for a local or region- unless there is a specific business purpose for such cards, they are usually just an invitation for misuse.

### **WHAT TO DO WHEN SIGNS ARE DETECTED**

In most cases, the signs listed above are not indications of anything other than poor controls. Do not jump to conclusions and assume otherwise. Even the presence of several of the "RED" or "ORANGE" circumstances does not prove that fraud or inept practices are occurring. However, these signs should generate questions and, in many cases, corrective action.

If the situation warrants, there should be an investigation to determine whether past transactions have been handled inappropriately. Resistance to this should be recognized as possibly another "RED" sign. Don't let "trust" be a barrier here. However, **your UniServ Director should be consulted before any sort of investigation begins.** He or she can discuss the situation with the appropriate staff in the IEA's Legal, Business Services, and Field Services Departments in order to determine the best course of action.

Even when the evidence seems solid, it is important not to accuse anyone of wrongdoing without the concurrence and involvement of the Legal, Business Services and Field Services Departments. Inappropriate or premature accusations can result in serious financial consequences and may also cause serious problems with member relations.

**PROACTIVE ENCOURAGEMENT OF PROPER CONTROLS AT EVERY OPPORTUNITY WILL LESSEN THE PROBABILITY THAT INVESTIGATIONS AND ACCUSATIONS WILL EVER HAVE TO BE MADE.**