



Ten Ingredients of Effective Fraud Prevention

by Verne Hargrave, CPA

FINANCIAL “bad behavior” is becoming rampant in the church. You would have to be living in a cave not to recognize this. There is not a week that goes by without another headline appearing that tells the sad story of a “trusted” church employee “gone bad.”

The good part of this, if there is a good part, is that the news is getting to be so nerve-wracking that churches and church administrators are finally beginning to recognize that a problem exists. The two most common questions suddenly being asked are, “What can we do?” and “Where do we start?” Unfortunately, financial misbehavior in the church is very pervasive and the variety of methods of abuse seemingly unlimited, causing answers to these questions to be quite elusive to the average church administrator.

When faced with such a daunting task, one good practice is first to call a time out. Before doing anything rash, it may be best to take a step back and gain a more comprehensive view of the situation. Added perspective can result in an honest assessment of the situation. More importantly, challenges are more easily overcome when they are broken down into manageable pieces. The following ten ingredients can be viewed as tools to gain some per-

spective on effective fraud prevention. By addressing these factors deliberately, one at a time and preferably in order, churches can increase their effectiveness in protecting themselves from the danger of financial fraud.



A STRONG ORGANIZATIONAL STRUCTURE

Let me be blunt. The fact that a church has never had an incident of fraud is due to one of two things: **luck** or **planning**. Needless to say, the odds of successfully avoiding fraud are much higher with the latter approach. If a church has been relying on the first approach and has never had an incident, it should be congratulated for its good fortune. But, the church should also be reminded that its good fortune rests on the fact that either the crooks have not made it to their church yet, or they just have not been caught. In time, one or both of these things will probably occur.

To increase the chances of avoiding fraud, the best practice is to **plan and organize**. This is accomplished by implementing a strong organizational structure within the church. Evidence points to the fact that churches with little or no organizational structure are frequent targets of fraud. The reason is rather obvious; many fraud-

sters are much better students of management theory than the average church. They can spot an “easy mark” a mile away. Crooks can also spot a well-defended church and will avoid it. Greener pastures are very easy to find because well protected churches are significantly outnumbered by poorly managed congregations. A crook-resistant church usually develops a strong organization in three areas.

Tone at the top is the key to a church's entire fraud prevention structure. If integrity is missing at the top levels of management, all other controls will prove to be pointless. Every church needs to have senior level staff that respect and understand the need for accountability. Good leaders may not care much for expense reports and purchase orders, like most of us, but they do understand their necessity. It is crucial that leaders comply without visible complaint to those around them. Junior staff will follow their leaders and the direction they are led is of extreme importance.

An empowered leadership team is another essential ingredient, without which transparency is not possible. When making a point about the need for openness and transparency, Supreme Court Justice William Brandeis is credited with saying, “Sunlight is the greatest disinfectant.” One of the ways churches operate

in the sunlight is by appointing a formally designated leadership team to guide them. (Titles vary from church to church: deacons, elders, directors, leadership team, etc.) Members of the team must be adequately trained to understand the requirements and responsibilities of their jobs and allowed to ask difficult and uncomfortable questions.

Competent volunteers are essential to the church, the greatest volunteer organization in the history of the world, but volunteers should be given sufficient orientation and training in order to understand their roles. Also, a church should not just let anyone be a volunteer. Volunteers need to be checked out. Unfortunately, many volunteers have ulterior motives behind their willingness to help out.

2

A WRITTEN ORGANIZATION PLAN

Establishing an organizational structure is the first step in combating fraud; however, it is not enough.

In order to stay within reasonable boundaries, churches must take the time to document their management structure and practices carefully. Churches that fail to do this do so at great risk.

A written organizational plan serves several purposes. First, it serves as a compass providing direction for the church as it navigates through difficult decisions. Similarly, the organizational documents serve as a map, helping the church chart courses of action of a more long-range nature. Finally, and directly related to fraud prevention, documentation serves as an anchor, keeping the church from drifting into dangerous waters. For this discussion, I have grouped documentation into three categories.

Corporate records of the church are the first consideration. All churches should have in place a practice of insuring that their articles of incorporation, by-laws, and/or constitution are up-to-date and in compliance with federal, state, and local

law. This is best accomplished by engaging legal counsel familiar with church and exempt organization law to perform periodic reviews of the corporate documents.

An accounting and management policy and procedure manual is a must in the battle against fraud. Fraudsters do not like consistency because it forms a base-line upon which to make quick and simple comparisons. Having a central document, such as an accounting and management policy manual, provides a proper backdrop for church operations. Without creating a massive "code of regulation" the policy should be comprehensive. At a minimum, typical topics included should be organizational structure, budget development, cash receipts and disbursement procedures, financial reporting and personnel administration.

Documents specifically aimed to reduce fraud should also be included in a church's policy and procedure portfolio. Written policies should be created that address conflicts of interest, business expense reimbursements to employees and volunteers, credit card use, benevolence, and building and property use.

3

KEEPING UP WITH THE TIMES

Until the 1960s perhaps into the 1970s, churches were rather slow to pick up on new ideas, particularly in regard to technology. (If you have a hard time believing this, think back to the first time someone wanted to bring an electric guitar into your sanctuary!) But that is no longer the case, especially when it comes to information technology.

Churches have embraced the digital world and are becoming very proficient in the use of computers. A vast array of applications has been made available to the church including sophisticated financial accounting and reporting, child-care security, online purchasing, online tithing, phone trees and coffee bars with free Internet wireless. Without a doubt,

churches have become technologically savvy.

Unfortunately, there is a vast array of other things that most churches are not so savvy about: the numerous new portals computers provide through which fraudsters can gain entry into the church. Computer and online crime is drastically changing the face of fraud prevention. The best way to address this situation is simply to provide a list of questions each church should ask itself:

- Does our church have a formal Information Technology security plan?
- Do any individuals at our church have access to all modules of the church's software system?
- Does our church partition its computer applications so that employees and volunteers have access only to files necessary to perform their duties?
- Does computer access require passwords that are confidential and unique?
- Are our passwords changed periodically?
- Are passwords complex including alpha, numeric, and case sensitive characters?
- Do we have backup procedures that are performed regularly that include off-campus storage?
- Do we have measures in place to protect the church from malware?
- Do we train our employees to avoid accepting email from unknown locations?
- Do we have a download policy?
- Do we maintain separate public and private wireless networks?

4

FULL DISCLOSURE FINANCIAL STATEMENTS

Another practice of many churches plays right into one of a fraudster's strengths, the ability to withhold information. Perhaps in an attempt to avoid interminably long finance committee meetings brought on by micro-managing members, or more

The purpose of strong IRS compliance is not simply to stay out of trouble. Doing what the government asks will also close down some favorite targets of individuals committed to stealing from the church.

likely, fearful that the messenger is going to be killed, some church administrators tend to hold back on the financial facts. Failure to present full-disclosure financial statements is the most common way of holding back information.

Instead of traditional financial statements, a church may elect to present summary information in an attempt to control the facts. Making matters worse, they may also use electronic spreadsheets to do the work. Although spreadsheets are very powerful and useful, they have one major flaw: the preparer is in total control over what goes into the report. There are no balancing requirements as with a normal set of financial statements based on a double-entry accounting system. Some crooks have one word to describe this situation: Disneyland!

Financial statements are simply another form of communication used to convey the financial situation of the church. Their goal, in the church environment, is to answer a few basic questions:

- How much cash do we have on hand?
- Is any of it restricted?
- What kind of assets do we own?
- Who and how much do we owe?
- How did we do this year?
- Did we stay within budget?

To answer all of these questions adequately, a church must present a full set of financial statements. This includes at a minimum, both a balance sheet and an income statement. (These are business terms. The corresponding nonprofit titles are statement of financial position and statement of activities respectively.) In addition, if a church has a high volume

of restricted activity, a separate schedule of restricted gift activity should also be presented.

Not only does "summary reporting" result in an uninformed church. It can also result in a victimized church. A church with a history of being satisfied with summary reports combined with poor personnel decision-making may end up with an embezzler having the best of both worlds: being able to take what he wants from the church and covering up the evidence with his own reporting system.



COMPLIANCE WITH THE TAX LAWS

Churches tend to have only one motivation for staying in compliance with the tax laws. And that is staying out of

trouble. Churches practice compliance with the Internal Revenue Code primarily to avoid unnecessary penalties and interest, protect their tax-exempt status and stay out of the news.

The prevailing attitude is, "We do these things because we have to; the government is making us." Most churches see no benefit in compliance other than staying in the government's good graces. The resulting tendency is many do just enough to get by. By having this attitude, however, they are missing another very good reason why compliance is helpful: being serious about government compliance also provides another level of fraud resistance.

Knowing where many of these laws came from makes the same point. Our governments are not really very proactive. Contrary to popular opinion, they do not

dream up rules and laws just to be belligerent, they are more reactionary. Many of the rules churches must comply with were implemented in reaction to some type of bad practices or abuse of existing regulations. A very good example is the charitable contribution substantiation rules. One of the reasons for their coming into existence was the tendency of some people to deduct tuition payments to the church school as contributions. Also, "accountable reimbursement plans" are the result of abusive employee business expense deductions during the 1980s. Although it may come off sounding harsh, the fact is both of these practices, mischaracterizing payments as contributions and inflating expense reports, are forms of fraud the government wishes to eliminate.

The purpose of strong IRS compliance is not simply to stay out of trouble. Doing what the government asks will also close down some favorite targets of individuals committed to stealing from the church. A fraud-resistant church should take steps to be in compliance with IRS regulations regarding ministerial taxation, personnel benefits, business expense reimbursements, credit cards, and benevolence and contribution substantiation.



AWARENESS OF ALL SOURCES OF REVENUE

Any discussion of church tithes and offerings practices usually includes both a pat on the back and a criticism. First, in regard to the normal Sunday offerings I can say to most churches, "Way to go!" In fact, when I ask a client if they have taken any fraud prevention steps, the first thing usually mentioned is how much the church has done to protect the offering plate. Seldom do I encounter a church that does not have multi-member count teams, rotating terms of service, locking bank bags, dual-access safes, and in an increasing number, the use of an armored car service. I would venture an educated guess that the majority of churches have more than adequate controls over Sunday receipts. For some, Fort Knox would be an easier target.

But in regard to the rest of the money, the funds that come in during the rest of the week, I often have to say, "What were you thinking?" While being diligent to a fault on Sunday morning, almost anything and everything goes the rest of the week. Here are two in my hall of fame:

Offerings, fees, and other receipts arriving in the mail or dropped off by members are simply dumped on the financial secretary's desk. I have entered offices with large piles of unguarded cash on the accountant's desk more times than I can remember.

Special events funds sometimes are "managed" by a volunteer. The funds are kept off campus and are not turned over to the business office until the event is over. No accounting or reconciliation of goods sold is required.

Needless to say, some of our more interesting and sometimes humorous fraud stories occur in these two areas.

This is no laughing matter, however, because a significant "event" could cause irreparable damage. That being the case, definite steps should be taken. First, a brainstorming session could be held, the purpose of which is to determine all sources of income. Once identified, all sources should be included in the church's normal collection policies and procedures. For example, with weekday drop-offs and mail-ins, a lock box could be kept in the church's safe in which all of these receipts would be placed unopened. A separate log or register should be maintained to keep a record that the amounts were received. On Sunday, the box could then be opened and counted by the teller team on duty.



A WELL-DEFINED PURCHASE APPROVAL AND PAYMENT SYSTEM

There is a great difference in attitude in the church environment between receipts and disbursements.

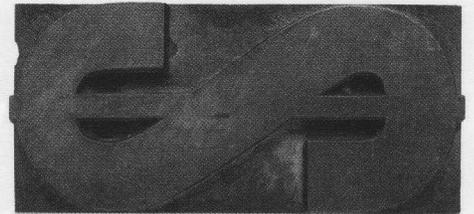
While churches exercise extreme vigilance over the "inflow" of funds into the church, many have a rather cavalier attitude towards the "outflow."

Churches also tend to rely on a few "fraud prevention" methods which in my opinion provide little more protection than a security blanket. They may give a warm and fuzzy feeling but are no help in a real crisis. The two I hear most often are the requirement of dual signatures for checks over a predetermined amount and the requirement that a check request form be filled out before anyone gets paid. It is not uncommon for these to be the only two "fraud prevention" controls exercised over cash disbursements.

Churches that rely on methods this simple are unaware of two basic facts. First, dual signatures and homemade check requests are absolutely no match for an ethically challenged employee with the courage to forge. Second, and this may be the most surprising, many of the larger and more spectacular embezzlements involve tampering with the church's cash outflow, not the inflow.

While no system is foolproof (especially if collusion is involved) the best fraud prevention practice in regard to disbursements, is to segregate the bill paying tasks among as many people as possible. Some of the more important tasks to distribute are payment approval, receiving of goods, check preparation, check signing, bill mailing, and general ledger recording. Unfortunately, very few churches have enough employees to split all of these tasks up. So what can be done?

Just as with cash receipts a good place to start is by holding another brain storming session in which the church's procurement processes are analyzed. Flow charting is a very useful tool in this exercise. Then, to the best of the church's capabilities, the tasks should be distributed among several employees and volunteers. But even after this process, most churches will have more tasks than people to give them to.



Summary

- Churches and church administrators are finally beginning to recognize that a fraud problem exists. Financial misbehavior in the church is very pervasive and the variety of methods of abuse seemingly unlimited.
- Challenges are more easily overcome when they are broken down into manageable pieces. This article provides ten tools to gain some perspective on effective fraud prevention

1. A strong organizational structure
2. A written organization plan
3. Keeping up with the times
4. Full disclosure financial statements
5. A well-defined purchase approval and payment system
6. Compliance with the tax laws
7. Awareness of ALL sources of revenue
8. A well-defined purchase approval and payment system
9. A guard over fixed assets
10. A commitment to the future

Author

Verne Hargrave is a CPA with Pickens Snodgrass Koch, LLP, in Arlington, Texas. He can be reached at verne@pskcpa.com.



But, there are other steps that can be taken. Although they take place after-the-fact, these practices still provide strong measures of fraud prevention. First, someone outside the business office could be assigned the task of reconciling the bank account monthly. This could be another employee, the business administrator, or a competent volunteer. The reconciliation should not solely be a “balancing” of the checkbook but should also include a close inspection of the cancelled checks for endorsements and signatures and an analysis of outstanding items. Online banking and remote access has made this practice even more efficient and practical, as volunteers do not have to come to the church office to do the work.

Another step is to perform an analysis of the church’s check register by exporting it to an electronic spreadsheet and sorting by vendor. It is surprising how quickly check writing “anomalies” can be detected using this procedure. This practice should also be performed periodically.

Although not foolproof or guaranteed to catch everything, these two practices serve a bigger purpose. They are loud and clear advertising to any and all, that someone is looking. This will force a potential thief to at least stop and ask himself, “Do I feel lucky today?”



COMPREHENSIVE HUMAN RESOURCES PLANNING

Except in the rarest of cases, personnel costs are the single largest expenditure of a church.

Because churches are in the “service industry,” it should come as no surprise that forty-five to fifty percent of the typical church budget will be dedicated to employee related costs.

This highlights a basic principle in the behavior of an embezzler. For obvious reasons, people committing fraud prefer to remain anonymous. In order to enjoy the fruits of their labor they must remain

To prevent becoming the victim of fraud successfully, a church must assess its current condition, develop a fraud protection plan and implement the plan, but, it cannot stop there. The church must live by the plan from that point forward. It must make a commitment to the future.

hidden. It is much easier to hide fraud among the bigger numbers, like payroll.

As a result, personnel costs are a favorite target of fraudsters. Usually, fraud in this area is small-time with one employee falsifying his own time card or submitting phony expense reports; however, some payroll frauds can be quite extensive and creative. The more spectacular (and costly) may involve “phantom” employees, fraudulent insurance claims or bogus tax refunds. These scams can easily run into the tens of thousands of dollars.

Churches should not be naïve about payroll fraud. Because churches are as vulnerable to personnel fraud as businesses they should do two things. First, repeating the theme of a previous section, churches must follow the IRS compliance guidelines. This means designating an independent compensation committee to set compensation amounts, based on market comparison information, and documenting all decisions made. At a minimum, this process should be followed for executive level staff but is also a good practice to follow for the entire church staff.

Second, churches should also follow a “best practices” approach in human resources administration. In addition to contributing to a healthy workforce these best practices also contribute to eliminating the possibility of fraud. A few of these practices are the establishment of formal job descriptions, performing background checks, performing performance evaluations, and obtaining written termination letters from departing employees.



POSTING A GUARD OVER FIXED ASSETS

I do not mean this literally of course. Few churches have the resources to have full-time security guards, but churches

need to do more than they currently do. Because churches “obsess” over watching over their bank accounts, they have very little time left to watch over their “stuff.” That is why I can safely say that every church with non-cash assets will testify that if you do not watch your fixed assets, they may just “walk off.”

I am also fairly certain that this inattention is very costly. Most churches would be shocked if they totaled up their annual replacement costs for computers, televisions, recorders, and sound equipment. It would also be interesting to know how much of the purchases were to replace items stolen or “misplaced.” Churches would save money in the long-run if they practiced as much stewardship over “stuff” as they do over cash.

The starting point in gaining control over fixed assets is to maintain better records of fixed assets: what is owned, when it was purchased, how much it cost, and where it is supposed to be located. The list should be referred to often, re-evaluated each year, and adjusted for disposals and additions.

Periodically, a physical inventory should be taken, if for no other reason, to establish insurance values in the case of fire or natural disaster. This does not have to be a complex process, and simpler really is

better. A video inventory would be more than sufficient.

Finally, some assets need special consideration. These are assets that the IRS is most concerned with and are also most appealing to thieves, assets that can easily be used for personal purposes. Cars, trucks, computers, and video and recording equipment are the most popular types. Churches would be wise to establish a few policies to monitor the use of these assets.

CONCLUSION— A COMMITMENT TO THE FUTURE

To prevent becoming the victim of fraud successfully, a church must assess

its current condition, develop a fraud protection plan and implement the plan, but, it cannot stop there. The church must live by the plan from that point forward.

It must make a commitment to the future. The plan must be on-going. Here are a few key elements in an on-going fraud prevention program:

- Establishment of a formal, written program for managing fraud risk.
- Assigning ownership of the task to an anti-fraud taskforce made up of key employees and officers.
- Educating staff and members of the risks of fraud.
- Periodically (annually is preferred) assessing the church's systems in regard to fraud susceptibility.
- Implementing a periodic review of transactions. (often referred to as internal audit)

Several years ago the Auditing Standards Board of the American Institute of Certified Public Accountants issued a new auditing standard addressing the auditor's response to fraud. Since that time audi-

tors have been including in their management letters suggestions that their clients perform fraud risk assessments of their organizations. To date, very few have done so. The main reason given for not doing so is a result of something I mentioned at the beginning of this chapter. Because the challenge of fraud prevention is so vast, many just do not know where to begin. The purpose of these ten characteristics is to do just that, provide a starting point to achieving strong fraud resistance. 

Third Annual Event
October 20, 2011

Human Resources—Your Church's Valued Assets

National Church Administration Day (NCAD) is a service event of local chapters to share their knowledge of accurate, current information and resources to assist ministers and laity in congregations with the administration of their churches.

The theme for this year's event is human resources. Come prepared to learn!

NCAD through the local NACBA chapters seeks to offer answers to issues in church administration, on topics including building and grounds, financial, human resources, legal, insurance, worker's compensation, risk management, security, 501 (c)3, unrelated business income tax, and more.

All NACBA members who wish to share their knowledge and experience with the communities they serve should plan to participate through their local chapter.

If you do not have a chapter, contact Ruth in the national office to receive the provided program resources or for more information.

NATIONAL CHURCH
ADMINISTRATION DAY

OCTOBER 20, 2011