



PACT Webinar
**Protecting our Churches and Related Ministries
from Fidelity Theft**

Guidelines for Program Administrators

URL References – the power point presentation and the recording of the actual February 2007 webinar are posted as a videostream that you can listen to and view at your desktop via the internet:

1. <http://www.screencast.com/users/AJGRMS/collections/Default/media/c5c6540a-b06a-41e4-b7bc-d33a3f6154f6> (allows you to jump to various parts of the presentation)
2. <http://www.screencast.com/users/AJGRMS/collections/Default/media/08ba11aa-fa2a-4e53-9da4-66a5c71f0b0c>

Suggestions for Program Administrators:

1. Host a webcast and play back this presentation with an opportunity for discussion at the end. In order to host a webcast, you will need the support of the PACT Service Center to organize the webex delivery and toll-free conference call line (there is a charge for this);
2. Ask participants to watch the videostream and come to a teleconference prepared to talk about their policies, procedures and experiences. You could also go over the handouts as best practices or ask specific churches to feature their best practices.

Handouts (attached) :

1. MPM – Steps for Proper Money Handling
2. Segregation of Duties in Local Church
3. An Internal Controls Checklist for the local Church

PACT Service Center
800-UMC-PACT
Email: umcpact@ajg.com

MPM

Financial Stewardship Steps for Proper Money Handling

Time and time again we read of churches and charitable organizations becoming victims of theft and embezzlement. Why are we such easy targets? The simple answer is trust. While we are in a trusting business, sometimes we become blind to the possibility that someone we know and love would actually steal from us.

With this way of thinking, we seldom put measures in place to protect the assets that have been entrusted to us by our congregation. While we should be shocked people would want to harm the ministry and the congregation, the fact remains that rather normal people get caught up in something that gets out of hand.

Incidents of embezzlement and theft within religious organizations are on the rise. Not only are there more cases, but the amounts of money being taken is significant. We must recognize that this problem can and does exist in faithful congregations and your church could be the next target.

This problem is seldom obvious and hard to detect even when you are looking. Therefore a series of safeguards to protect church funds should be part of your overall policies and procedures. Here are a few very simple guidelines that when applied, can save your church from financial mishaps.

Collections

From the time the collection is received until it is deposited, it should never be left with just one person. Two unrelated people should always be present with the funds. Unlike the days when we left the collection on the altar throughout the service, the standard practice today is to take up the collection, and immediately lock up the money.

Keeping Funds Safe

All collections and other funds should be locked in a safe. If a safe is not available, then the “two-lock” concept should be practiced, meaning the collections are in a locked cabinet or closet, within a locked office. While some churches count the funds immediately after services, others may wait until the following day. Regardless, two unrelated adults should be with the funds from the time they are collected, until they are secured, and ultimately until they are deposited. No one should ever be alone with the funds or be allowed to take the funds home.

Counting

Churches count their funds in a variety of ways. However, it is unwise to advertise where the money is counted or how it is counted. Teams of three or more should be in a secure room when they count. All counting should be verified and documented. Ideally, one signed counter’s sheet should be kept with the money and another placed in a file. The only time the funds should be removed is when at least two people are present. It’s also a good practice to alternate the counters and their responsibilities on a regular basis as this is yet another form of checks and balances that can prevent theft.

Depositing

Regardless of when the deposit is made, two people should take it to the bank. It is recommended that the bank bag not be exposed and that alternate routes to the bank are taken. The idea is to keep others from knowing who is holding onto the bank deposit and being able to determine your patterns week after week.

Ministry Protection Memo

“MPM” is a regularly featured presentation on various topics relative to Church and safety. Send your comments and interests to PACT’s Director of Ministry Protection, Carol Alberts, at umcpact@ajg.com.

PACT Service Center

Hours of Operation
8 a.m. to 5 p.m. CST

Contact Information

Toll-Free: 1-877-UMC-PACT
1-877-862-7228
Fax: 1-866-221-4858

“Therefore a series of safeguards to protect church funds should be part of your overall policies and procedures.”



Internal Controls

There should be clear lines of separation among those who collect, count and make the deposit; one person should never be responsible for all of the steps involved. It is not that they are not to be trusted, but by giving each individual an individual task, you provide a more solid defense should an accusation ever be made. Often in the case of embezzlement, it is found that the person in charge of all aspects of the finances is the one in the best position to cover their tracks and remain undetected.

Special Event Funds and Petty Cash Purchases

These funds come from events such as concerts, meals, craft shows, etc. Secure the money; have at least two people count and verify the figures, and make the deposit using at least two people. Again, these funds should not be taken home.

Sometimes these events, as well as other activities, require purchasing of small items. Cash should never be handed out to cover these costs, persons should be required to complete the purchase and complete a reimbursement voucher. This will allow for a paper trail when reconciling petty cash accounts.

Audits

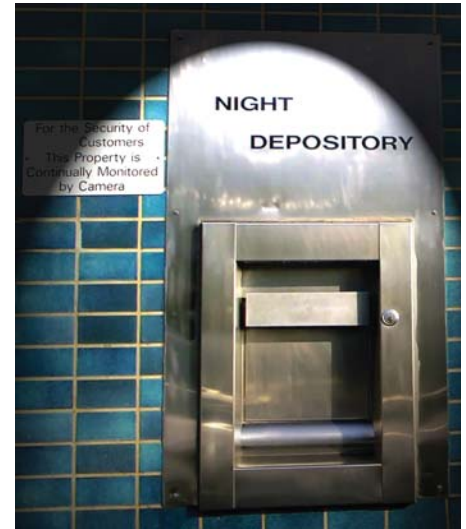
Some churches conduct their own internal audits; however, it is suggested an outside person or firm conduct an audit every 2-3 years. This will raise the accountability level and keep potential illegal activity from going on over an extended period of time.

Detecting Problems and Responding to Suspicion

We all hope theft and embezzlement does not happen within our congregation, but it does. More times than not, it is done by a person least suspected. Review your financial records, look for unusual behavioral patterns and instill these simple guidelines to protect the assets of your congregation.

If there is a suspected incident, quickly have your books audited by an outside firm; keep leadership informed, and like all incidents that happen within the church, consider both the victim and the offender. Seek to balance compassion and justice. If possible, seek restoration and get help for the people who need it.

Remember, no one in the church is perfect, but providing sound practices and procedures will protect your assets and keep those who may be tempted from robbing



your congregation of your finances and church members' faith.



PACT is an all-lines Property & Casualty (including Workers' Compensation) nonprofit captive and reinsurer domiciled in the District of Columbia and owned by its member annual conferences and agency insureds. GCFA continues its Book of Discipline fiduciary oversight through its membership on the Board of Directors of PACT. For more information, contact the PACT Service Center or go to the website at www.umcpact.org.



SEGREGATION OF DUTIES IN A LOCAL CHURCH

Two-Person Church Office

Church Bookkeeper	Church Treasurer/Senior Pastor
<ul style="list-style-type: none"> Record accounts receivable entries Mail checks Write checks Record general ledger entries Reconcile bank statements Record credits/debits in accounting record Approve payroll Receive cash Disburse petty cash Authorize purchase orders Authorize check requests Authorize invoices for payment 	<ul style="list-style-type: none"> Sign checks Sign employee/vendor contracts Complete deposit slips Perform inter-bank transfer Distribute payroll Reconcile petty cash Approve employee time sheet Process vendor invoices

Three-Person Church Office

Church Bookkeeper	Business Manager	Church Treasurer/Senior Pastor
<ul style="list-style-type: none"> Record accounts receivable entries Reconcile petty cash Write checks Record general ledger entries Reconcile bank statements Record credits/debits in accounting records 	<ul style="list-style-type: none"> Process vendor invoices Receive cash Mail checks Approve invoices for payment Distribute payroll Authorize purchase orders Authorize employee timesheets Approve payroll Disburse petty cash 	<ul style="list-style-type: none"> Sign checks Sign employee/vendor contracts Complete deposit slips Perform inter-bank transfers

Four-Person Church Office

Bookkeeper	Church Secretary/Clerk	Business Manager	Church Treasurer/Senior Pastor
<ul style="list-style-type: none"> Record accounts receivable entries Reconcile petty cash Write checks Record general ledger entries Reconcile bank statements Record credits/debits in accounting records 	<ul style="list-style-type: none"> Distribute payroll Receive cash Disburse petty cash Authorize purchase orders Authorize check requests Mail checks 	<ul style="list-style-type: none"> Complete deposit slips Process vendor invoices Approve payroll Approve invoices for pay 	<ul style="list-style-type: none"> Sign checks Sign employee/vendor contracts Approve employee timesheets Perform inter-bank transfers



FIDELITY INTERNAL CONTROL CHECKLIST FOR THE LOCAL CHURCH

Recognizing Warning Signs of Fidelity Theft and Preventing Problem Situations

Why are consistent internal controls important?

1. Local church decisions and financial reporting rely on the accuracy of figures recorded
2. Gives local stewards control of dollars in and out
3. Standardizes good management practices and procedures

Advantages of improved internal control:

1. Can reveal errors and omissions
2. Discourages employee theft
3. Protects assets

How to use the checklist:

1. Review the concept for each internal control area and answer the questions following each section
2. Each answer identifies an area that needs stronger internal controls

Segregation of Duties

CONCEPTS:

- Certain accounting /bookkeeping functions are designed to cross-reference each other for accuracy. If the same person is responsible for multiple duties, the natural check and balance of the system is removed.
- Trust is not the issue; verifying business transactions is. Giving a single person unquestioned authority of your finances is not a wise business practice.

CHECKLIST (each "yes" answer identifies a potential problem area):

- Is the person who handles your cash also responsible for recording the cash?
- Does the person who pays or orders inventory also receive the materials?
- Are two or fewer people responsible for the accounting function?
- Is only one person responsible for reviewing financial statements each month?
- In your review of financial journals sporadic?

Bank Reconciliations

CONCEPTS:

- Bank statements can only flag discrepancies if they are reconciled on a timely basis. Reconciliations should be done once a month. Bank adjustments need to be tracked carefully from one month to another.
- Segregating duties is also important in this area. Reconciliations should be performed by one person and reviewed by another. Also, the person who writes the checks should not have the authority to sign checks.

CHECKLIST (each "no" answer identifies a potential problem area):

- Do you review canceled checks and endorsements on a monthly basis?
- Do you compare payroll checks with your current employee records?
- Do you question funds transferred between bank accounts?
- Do you track the number of credit card bills you sign per month?
- Are bank reconciliations performed on a timely basis?
- Is someone responsible for reviewing reconciliations each month?
- Do you verify reconciled items?
- Does the owner receive and open the bank statement prior to turning it over to the person who performs the bank reconciliation?

Supporting Documentation

CONCEPT:

- Enhances communications and serves as a final checkpoint.

CHECKLIST (each "yes" answer identifies a potential problem area):

- Do you ever sign blank checks?
- Do you ever sign blank checks without original supporting documentation?
- Do you ever sign checks without canceling supporting documentation?
- Have funds ever been transferred between accounts without review or verification?
- Do you ever sign checks for new business vendors without knowing or verifying their name and association with your company?

Employees/Personnel

CONCEPT:

- Know your employees and be aware of changes in behavior.

CHECKLIST (each "yes" answer identifies a potential problem area):

- Are any of your employees extremely possessive of their work records and reluctant to share their tasks?
- Are any of your employees apprehensive about vacation and time off while always being the first in the office and last out?
- Have you noticed a substantial change of lifestyle in any of your employees?
- Do any of your employees have a possible substance abuse problem?
- Are any of your employees living beyond their means?
- Have you ever hired an employee before checking references?
- Do you permit your accounting personnel to work longer than a year without taking a vacation?
- Do you have any accounting staff or key personnel who have not been secured with a fidelity bond?

Safeguarding Assets

CONCEPT:

- Limit and monitor access to important documents and supplies.

CHECKLIST (each "yes" answer identifies a potential problem area):

- Are blank check stocks and signature stamps safely secured?
- Do you restrictively endorse all checks when received?
- Do you deposit cash and checks daily?
- Do you maintain a list of office furniture, equipment and company vehicles?
- Do you have adequate insurance coverage for assets?
- Are all systems backed up on a daily basis and is backup stored off-site?
- Is there password protection and security for all computer systems and programs?
- Are passwords changed at least every six months?