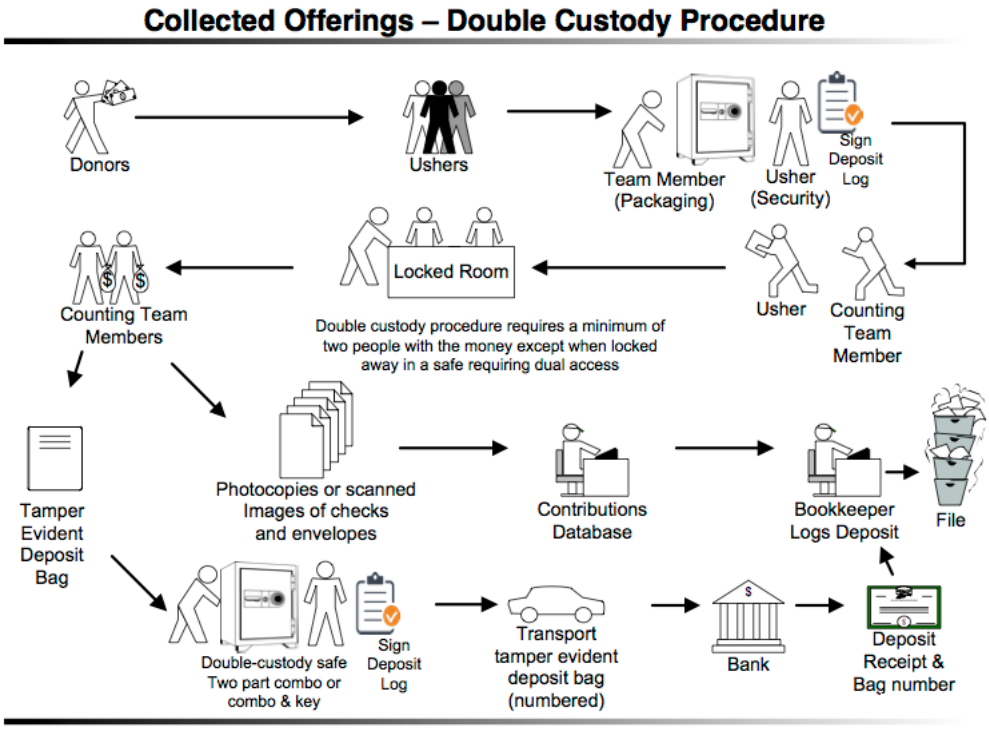
THE FOURSQUARE CHURCH

Collecting and depositing funds

During services:
Church congregations generally collect money during church services and often through other electronic methods. Strong internal controls will need to be in place, for both the physical receipt of funds and the electronic receipt of funds.



This diagram of the internal control structure for collecting and counting the offering illustrates at least two individuals handling unsecured money at all times. This process is referred to as a "double-custody procedure."

Important Note: If the church's meeting place does not have a church office where the offering can be secured in a permanent safe, it is recommended the church purchase a portable, double-custody safe to hold the offering until the offering can be counted. If this is not possible the offering should always be in the custody of two people at all times.

Modern safes come with new features such as hopper drawers and dual electronic/key combinations to provide better internal controls. The most important internal control principle is to have security measures in place to prevent any one person from accessing the safe on

their own. This can be accomplished by providing a safe combination to one person while a different person has a physical key (where both combo and key are required to open the safe). At no time should one person have unilateral access to the safe as this undermines the purpose of the internal control.

Important internal control considerations:

- Counted offerings should be kept in a **tamper evident bag.**
- These bags are numbered, and this number should recorded by the team on the deposit summary sheet prior to counting.
- The numbering system on tamper evident bags is a strong internal control, therefore the supply of bags should not be left available for easy access as this could undermine the strength of this internal control.
- The counted and secured offering can either be taken directly to the bank and placed in a secured depository (lock box) or placed back in the double-custody church safe until it can be taken into the branch.
- Deposits should be made within the first business day after collection to ensure timely detection if funds go missing.
- The deposit receipts and tamper-evident bag numbers should be provided to the bookkeeper as part of the deposit documentation. The bookkeeper should have noted the tamper evident bag number left for the counting team to use.
- The bookkeeper uses the copies of checks and envelopes, the deposit counting sheet to enter the deposit into the accounting software.
- After the deposit is entered, the documentation package should be assembled and verified that all totals agree. Then the deposit package should be filed.
- **Deposit documentation package** should consist of:
    - the offering summary spreadsheet signed and dated by all team members who counted the offering
    - photocopies of the checks and cash envelopes (also used by the individual entering this information in the contributions software).
    - a copy of the deposit slip
    - a printout or copy of the batch summary and transaction detail for all contributions entered into the contributions database (these reports should match deposit total and include an entry for "loose cash offerings").
    - the tamper evident bag number (or tear-off tag containing the number)
    - the deposit confirmation receipt provided by the bank listing the date, account number and amount deposited

Remember that the deposit and contribution reports contain sensitive information and must be kept secure with limited access.

Important Note: There should be a separation of duties between (1) individuals who collect the money (including checks received by mail), (2) individuals who do data entry into the accounting and contribution software and (3) individuals who reconcile the bank account. When

cash or checks are received by mail, they should immediately be placed in a drop safe for later processing counting by two or more team members.

Collecting and depositing funds - electronic

Electronic Donations

For many congregations around the country, electronic donation systems have become the primary mechanism for receiving church funds. These systems offer a number of benefits over the processing of tangible monetary instruments, such as:

- Mitigated security concerns and eliminated risk of theft or robbery associated with processing cash
- Reduced potential for human error through data entry
- Stronger audit trail for the source, classification and destination of funds
- Streamlined processing of contribution records
- Eliminated time constraints for collection of funds
- Opportunities to normalize church income by through scheduled, recurring donations

Studies have shown that providing electronic giving options through website, kiosk and smartphone applications significantly increases the total contributions to churches and charities. The success of online giving platforms in a church can be greatly impacted by how clearly it is promoted and explained within the church.

While electronic giving can significantly reduce the risk of misappropriation or fraud; good internal controls are still necessary to ensure this doesn't become an area of weakness.

Setting up an electronic donation system

Electronic donation gateways utilize a financial intermediary known as a "merchant service or merchant gateway" for which the church must establish an account. These gateways interface with a web portal to collect and process the individual donation transactions and then work with the church's bank to deposit these transactions in batches into a checking account.

The importance of batching electronic deposits

It is recommended that churches adopt a merchant service provider that offers integrated services for online donations (ACH and credit card) and smartphone applications. Many church management systems (member databases) have contribution modules that integrate these features.

Regardless of which software solution the church uses, it is important to ensure the merchant gateway assigns a batch number to each contribution transaction and that these batch numbers directly correlate to the deposit batches that are made to the associated bank account. This is VERY important! Without this feature it is nearly

impossible to reconcile the bank account to the contribution records and may weaken your internal controls.

Choosing the right merchant service provider

It is recommended the church use a merchant service that maintains integrated internal controls. This can be assessed my asking the merchant service provider for a copy of their SOC 1 report.

There are two types of SOC reports:

- **Type 1**- does not state the effectiveness of the firm's internal controls.
- **Type 2** - provides an assessment of the adequacy of the firm's internal control, thus we recommend only using merchant services that can provide a type 2 SOC report.

When shopping for a merchant service provider, compare all the fees that are charged to be sure you incur the lowest fees: the process rate, the monthly rate, the per transaction fee and any other charges. Ask your merchant service provider for the nonprofit rate.

Other important considerations:

- The service provider will require information about the church bank account that will receive electronic deposits, and therefore will only correspond with an authorized banking contact from the sponsor organization.
- Good internal controls require this individual to be someone other than the bookkeeper and/or person managing the contribution software. Separating these responsibilities reduces the risk that an individual making bookkeeping or contribution entries could divert funds into a different account (not in the name of the church) without detection.
- The bookkeeper should receive notifications of an electronic deposits directly from the merchant service provider.

Process of booking batched electronic deposits in the church accounting software

1. The bookkeeper should reconcile the batch report sent by the merchant service provider with a corresponding transaction detail report from the church's contribution software.
2. The bookkeeper should use this reconciliation to record a summarized deposit entry (for the batch) into the accounting system.
3. The bookkeeper should print a copy of the deposit report from the accounting software and match this with the batch summaries from the merchant service provider and contribution software; this packet should be stored in a secure location and organized for easy retrieval.

Reconciling the bank account for electronic donations

The bank reconciliation performed (monthly):

- Verify the electronic deposit batches in the bank statement match the batches recorded in the churches ledger to ensure that all electronic deposits were deposited in the church bank account for the correct amount.
- Remember there are scenarios when an electronic refund may need to be issued to an individual. The issuance of a refund should be handled with adequate segregation of duties.
- Require that refunds be approved by a senior (authorized) team member with budgetary authority (other than the bookkeeper). This individual should verify the refund is legitimate and returned to the same debit/credit card or bank account that was originally charged.
- If the refund is processed in a batch, the documentation should be reviewed and included with the affected batch and recorded by the bookkeeper in the accounting software.
- These refunds will reduce the recorded tithe/offering income and should be verified as appropriate during the reconciliation process substantiated with proper documentation.