February 2015

How a Congregation Can Avoid Theft or Embezzlement

In the last year, several of the congregations in the Grand Canyon Synod have experienced significant financial losses due to the illegal actions of bookkeepers, counters, or office staff. In some cases, the losses have been in the tens of thousands of dollars. In addition to the financial loss, it is an embarrassing situation for the stewards of the congregation's financial resources. It is also easily avoidable.

There are three common methods of theft or embezzlement used in these situations:

Loose/cash offerings: This method usually involves a "counter" who takes the money from the loose offering and turns the cash into the office. This type of loss is easily avoidable by having two counters, not related to one another, to independently count the loose offering and sign off on the amount being sent to the office. Thefts from the office can be easily avoided by having two people in the church office responsible for counting the cash and verifying the actual amount of the deposits.

Forged signature: This type of loss involves the forgery on the signature line of the check. In the typical case, an employee has access to blank checks, usually kept in the office, and frequently not kept under lock and key. This type of loss can go undetected for some time, particularly in situations where the employee is also responsible for the monthly bank reconciliation. Banks process so many items per day that they cannot possibly check signatures on every item. There are two ways to prevent this loss. The first is to keep blank checks not in active use under lock and key. The law in Arizona provides that the customer has 30 days after receipt of a bank statement to examine all of the items that were processed and report any forged signatures. If nothing is reported during that period of time, it is difficult if not impossible to go back and recover losses that occurred because the bank statements were not regularly examined.

Forged payee/endorsement: This type of loss involves two variations. The first is if the check is made out to a person or vendor that is real enough (such as the crook's family member or business partner) but who has provided no goods or services. The bookkeeper creates a fictitious account payable, usually in the name of some entity that would not be likely to raise any red flags (office supplies or landscaping are prime examples). Whenever the bookkeeper wants to steal some money, they simply make out a check to the recipient and put it together with a number of other checks that the authorized signer will see all at once. The bookkeeper then takes the properly signed check and deposits it to the account of the fictitious payee.

This type of loss takes a little more work to discover but is fairly easily avoided. On the books, there would a check payable to a vendor who is on the payables list, so even an "audit" by an accountant would probably not discover that the payee was fraudulent. The first safeguard is to lock or prevent access to the accounts payable list once an approved list is established. Most congregations should have a single list of accounts payable. Any change to the authorized Accounts Payable should have at least two people

involved other than the bookkeeper. The second safeguard is to never allow the same person to have responsibility for reconciling the bank account as the person who has responsibility for writing or handling the checks for the congregation. Sometimes this is difficult in the smaller congregation where there is only one person who really has any financial experience. In view of the potential losses, however, hiring an outside vendor to do the bank reconciliations would be a good method to protect the assets of the congregation.

Fraud Insurance: A commercial insurance policy usually has coverage for fraud losses. Be sure to read and understand what is covered or excluded from the coverage, especially the limits on what the insurance company will pay in the event of a loss. In addition, most insurers will have free resources for recommended policies and procedures to help prevent these kinds of losses from happening.