230 West Street
Suite 700
Columbus, OH 43215

tel 614.221.1120
fax 614.227.6999

www.gbq.com

GBQ Partners

Fraud Exposure and Your Non-Profit Organization – Part III

In our first two articles, we discussed the general internal control environment, including documenting and assessing the internal controls at your organization, followed by a discussion of vendor/trade payable cash disbursements. This article will focus on internal controls around cash receipts.

Cash receipts may be related to several different transaction streams, including billing for services provided, grants received for programs, solicited pledges (already recorded as pledges receivable), and unexpected contributions (probably your most favorite type of cash receipt!). Each type of cash receipt creates a risk depending on the type of controls that your organization has implemented and how these controls are monitored. Some key considerations are presented below.

Consistent with our previous articles, segregation of duties is the most important control to implement with any transaction stream. Regardless whether actual cash is collected, cash and the more commonly used checks are the most liquid and easily transferrable assets which make them most susceptible to fraud. Ideally, the person who receives payments should not have access to post the payments to the general ledger or the fundraising tracking system, record accounts/pledges receivable write-offs, or make the deposit to the bank. Combining any of these duties presents the opportunity for theft and concealing of the theft, especially if your organization receives actual cash and not just checks or credit card payments. A lack of segregation of duties may result in untimely deposits, inaccurate cutoff of revenue/receivables, misreporting of revenue or contribution levels, and theft of cash.

- *Intake of Cash* – A very effective control that is easy to implement is to have the receptionist or someone outside of accounting record all cash/check receipts at the point of intake. When the mail is received each day, have that individual prepare a list of all cash receipts (cash, check, or credit cards). Whether the list is a written form or logged in a software spreadsheet, only a copy or read-only access of the listing should be made available to the accounting department and/or individual responsible for handling the checks/cash through the remaining duties of the deposit process. The key control is that the person depositing the checks or posting payments does not have access to make changes to the initial receipts log. Once all checks are logged (and stamped with restrictive endorsement), the individual should prepare the deposit slip and make a copy of the receipts log to provide to the person responsible for bank reconciliations and other accounting. ***To make this control most effective, accounting personnel preparing the bank reconciliation should compare the receipts log to the actual cash deposited (per the bank statement and deposit receipts) to verify all cash received was taken to the bank. This simple structure establishes both a deterrence and detection control.***

Author:
Jen Osburn, CPA

- *Deposit of Cash* – A lockbox arrangement is a great control to implement because most cash receipts would go right to your bank and would not be handled by your employees. The bank would provide you a report of cash receipts each day for posting to your general ledger. Alternatively, if you don't receive a high volume of checks or cash, consider the risk related to the frequency of bank deposits. While the most controlled environment would have cash deposited on a daily basis, you may find that it can be locked in a safe until deposited every other day or semi-weekly. Many banks also offer electronic deposit options where the checks can be scanned at your office and are automatically deposited, requiring bank deposits only be made for actual cash bills and change collected. There is a higher risk with keeping actual cash on hand. While the timing of your deposit may vary, it is important to keep the money together in the safe. It is not recommended to have the payments go to the fundraising department or membership department because this can provide for more difficult monitoring and less assurance that deposits are made timely with proper cutoff at month- or year-end; and if you also have the same people in those departments updating donations and membership information used in accounting reporting, an opportunity for a misappropriation of those funds and concealment of the misappropriation is present (otherwise known as fraud).

- *Posting Payments* – An individual separate from the intake of cash should be responsible for posting payments in the general ledger, whether they are posted against receivables or if they are new grants recording cash receipts and revenue. Likewise, a separate individual should be responsible for posting all donor activity if you have separate fundraising software. Activity can be posted from details on a copy of the receipts log or from copies of the checks made at the point of intake. On a monthly basis, the fundraising software activity should be compared to the general ledger to ensure complete recording of all contributions.

- *Posting Write-Offs* – Proper authorization should be required for writing off receivable balances. History should be reviewed by the approver and documentation maintained for why the write-off is considered necessary. This is a key control if you do not have segregation of duties related to the cash intake and posting payments. There is a risk of the individual not depositing payments received and then writing off the receivable account as uncollectible. Thus, the approval of the write-off should be considered with documentation of collection efforts and follow-up from separate personnel. Another simple control to implement is for a separate individual to make the collection calls or to prepare monthly statements to send to the customers, who would then question an outstanding balance if the payment has been made.

- *Review of the Accounts Receivable Sub-ledger* – Monitoring and review by someone outside of the collection and posting process is a strong control to reduce the opportunity for theft. Specifically, management should look for unusual postings, such as large credit balances or posting of payments to accounts that have been inactive for a longer period or that management does not expect current payments. These types of postings may be covering up a fraud scheme called lapping or skimming (see below).

- *Required Vacation* – A strong control for any type of transaction processing is to require all accounting personnel to take mandatory vacation for at least one week, with a substitute performing their duties. This control can easily identify a fraud scheme if the fraudulent individual is not there to keep up with the scheme and the cover-up. A common fraud scheme is lapping or skimming where, as payments come in, the first payment on an account is stolen and then subsequent payments on different accounts are applied to the prior account in a staggered manner. This prevents any questioning from the customers since payments are being posted to their accounts; however, the postings are delayed in that the fraud perpetrator must wait until the next payment is received to cover-up the prior intentional posting. If someone else fills in that role for a longer period of time, depending on the size of the fraud scheme, it will be identified when customers start questioning payments not applied to their account. Again, we cannot stress enough that the same person handling the intake of cash/checks and being responsible for the primary record keeping of that activity creates a high level of risk.

Our next, and last, article will address controls and considerations in preventing improper payroll transactions.

If you have any questions relating to assessing your internal controls, please contact Bob Stillman or Jennifer Osburn at 614.221.1120.