How Cash May Be Stolen

By James Finlay

Cash is defined as a medium of exchange that a bank will accept at face value. It includes bank deposits, currency and checks. Cash fraud schemes, therefore include but not limited to schemes in which employees / volunteers steal currency, checks and other forms of negotiable instruments. In general most cash fraud schemes committed by employees / volunteers focus on either currency or checks.

Cash Theft

There are two ways a fraudster can steal cash from his or her employer. The first is to trick the organization into making a payment for a fraudulent purpose. A dishonest employee may produce an invoice from a non-existing company or submit a time record that he did not really work for. Based on the false information that the fraudster/employee provides, the organization issues a payment, e.g. by sending a check to the bogus company or by issuing an inflated paycheque to the employee. These schemes are known as Fraudulent Disbursements Schemes. In a fraudulent disbursement scheme, the organization willingly issues a payment because it thinks that the payment is for a legitimate purpose. The key to these schemes is to convince the organization that money is owed. We will look into Fraudulent Disbursement Schemes in a later article.

The second way to misappropriate cash is to physically remove it from the organization through a method other than the normal disbursement process. E.g., an employee / volunteer may take cash out of the cash register, put it in his pocket and walk out the door. Or, he might remove a portion of the cash from the bank deposit on his way to the bank. This type of misappropriation is what is referred to as a Cash Theft Scheme.

Types of Cash Theft Schemes

There are two categories of Cash theft schemes, Skimming and Larceny. The difference in the two categories depends on when the cash is stolen. Cash Larceny is the theft of money that has already appeared on a victim organization's books. Skimming is the theft of cash that has not yet been recorded in the accounting system. The way the employee extracts the cash may be exactly the same for a cash larceny or skimming scheme.

Skimming is the removal of cash from an organization before the cash has been recorded in the organization's books. Because the money is stolen before it appears on the books, skimming is known as an "off-book" fraud. The absence of any recorded entry for the missing money also means there is no direct audit trail left by the scheme. The fact that the funds are stolen before they are recorded means that the organization may not be aware that the cash was ever received. Consequently, it may be very difficult to detect that the money has been stolen but can be reduced by having good internal controls. Skimming can occur at any point where funds enter a business, so almost anyone who deals with the process of receiving cash may be in a position to skim money. This may include salespersons, tellers, volunteers, and others who receive cash directly from customers or donors. Many skimming schemes are perpetrated by employees / volunteers whose duties include receiving and recording customers' and donors' payments. Employees / volunteers may be able to slip checks out of the incoming mail rather than posting the checks to the proper revenue or customer accounts. Skimming variations may occur depending on whether the employee / volunteer skims Sales or Receivables (see lapping below).

The vast majority of skimming schemes involve the theft of incoming sales or donations, as opposed to receivables. The reason is that receivable skimming is harder to conceal. If a customer owes a certain amount on an account receivable, that customer's payments are expected. As a result, if an employee steals an incoming payment from the customer, the payment will be missed.

For an occupational fraudster, concealing the fraud is the most important part of the crime, even more important than obtaining the funds. Employee fraud has a different character than typical street crime. If a thief enters a shop, pulls out a gun and takes all the day's sales, this thief only concern would be getting away without being caught. But if an employee of that shop decides to steal money from the shop, he will not only keep from being caught, he will also try to conceal the fact that a theft has occurred. This employee needs to hide his identity and the crime itself. Occupational frauds are usually long-running schemes that consist of several thefts which get bigger and or/more frequent as time goes by. In order to be successful, the employee-fraudster must keep the scheme from being detected. As long as the organization is not aware that it is being victimized, the employee / volunteer can continue to steal. Once the scheme is detected, however, the employee / volunteer stands a good chance of losing his job, being prosecuted, being ostracized by his friends and family, etc...

Skimming tends to affect sales or cash / cheque donations more than receivables. Skimming can occur anywhere cash enters an organization, and non-profits should make extra effort to ensure all their cash receipting and handling procedures are secure. Knowing that sales or donor skimming is more likely, non-profits should take extra care to safeguard all points of sale and donations from employee / volunteer theft.

The method and impact of cash theft schemes can vary depending on the job responsibilities of the perpetrators and the level of supervision over the cash collection process.

Employees / Volunteers

Skimming particularly in non-profits who sell items to boost revenue occurs at the cash register – the spot where revenue enters the organization. Employees or volunteers who work at the register are usually not highly paid or work in kind. These people can be subject to a high degree of temptation as they spend their days handling sums of money. At some point the temptation for certain employees / volunteers becomes too much and they decide to pocket some extra cash on the side.

This type of scheme is very simple. When a customer purchases merchandise, he or she pays a cashier and leaves the store with the goods purchased. Instead of placing the money in the cash register, the employee / volunteer puts the cash in their pocket without ever recoding the sale. This process is made much easier when employees / volunteers at cash collection points are left unsupervised. When an employee / volunteer knows that his or her conduct is not being monitored, this creates a perception that it will be easy to steal from the organization. The lack of supervision, in other words, increases the likelihood that fraud will occur.

However, when there is a supervisory presence at the point of cash collections, some employees / volunteers will still attempt to skim unrecorded sales. A common technique is to ring a "no sale" or some other non-cash transaction on the employee register. The false transaction is entered on the register so that it appears that the employee is recording the sale. The method of disguising the theft will vary depending on how the non-profit records sales transaction, the salesperson's location in relation to his or her supervisor and / or the customer, and the creativity of the particular culprit.

Reconciling till roles with cash each day and investigating void or no sale transactions and periodic inventory counts can help to avoid skimming schemes.

Lapping

Lapping is not a fraud itself. It is the method of using a new fraud to hide an old fraud - one fraud laps over another. If undiscovered, lapped frauds may continue indefinitely though they do require constant maintenance.

Lapping can be used when the fraudster steals a debtor or donor receipt. The receipt is not recorded against the debtor or donor (if it were, the banking records would not match the entries in the ledger). Before the next statement is sent to the debtor or a letter to the donor requesting a new donation, an entry must be made recording the receipt or the debtor / donor will ask questions and an investigation may begin.

How does lapping work?

Lapping is the committing of a new fraud to cover an initial fraud. Before the next statement is issued, an amount needs to be credited against the original debtor to hide the theft of their receipt. The money needed for debtor A's account is taken from a receipt from debtor B - usually a debtor who pays just before the issuance of these statements. That is, the monies from debtor B are recorded as being collected from debtor A. That hides the fraud with debtor A, but creates a new fraud with debtor B, and a new problem next month. At the end of that month money from debtor C is used to solve the discrepancy with debtor B, and so on.

As the first fraud is resolved by creating a second, the current fraud is usually fairly new and there is always potential to cover that with another 'lap' before it is discovered.

Internal Controls

As with many small businesses, non-profits are limited to their resources when it comes to employees and volunteers in the organization, therefore it is important that correct controls are in place to reduce fraudulent activity. If possible segregation of duties should be in place, e.g. employee “A” opens and records all incoming mail and receipt of funds. Employee “B” enters funds into the accounting system and employee “C” takes the funds to the bank. Those that record funds in the accounting system should not reconcile the bank account. Bank statements should be reviewed on a monthly basis by an independent person. Of course it is not possible for all non-profits to have this flexibility as resources are scarce. A good practice of hiring such as, background checks, reference checks and ensuring that the resume is reviewed for red flags will reduce the potential for fraud. A fraud policy should be in place and should indicate consequences. It can be possible that internal controls can be too tight and cause inefficiencies within the organization. Therefore **trust** becomes a big factor.

Case In Point – Volunteer charged with defrauding army cadets of $36k

In a recent newspaper article a popular volunteer and well-known former Burlington citizen of the year – **and a founder of Crime Stoppers of Halton** – was charged with fraud for allegedly taking $36,000 from local army cadets. The 75year old volunteer was charged with three counts of fraud over $5,000, breach of trust and making a false statement. The investigation began in April last year when the Army Cadet’s, noticed “inconsistencies” in their finances. The investigation included an audit of the corps’ finances and its funding from the City of Burlington as a non-profit organization, which receives support from the city. Charges cover the two-year period between September, 2006 and September, 2008, when the perpetrator was a volunteer chairperson of support in charge of finances with the cadet corps. It is allege the volunteer “fraudulently remunerated himself” with more than $36,000, belonging to the corps. Audits revealed the suspect had issued himself a salary of more $19,000 each year and there were also discrepancies regarding receipts. The volunteer was named Burlington’s citizen of the year in 1998 for his civic involvement, which has included everything from co-founding Crime Stoppers of Halton in 1978, to years of service with the St. Johns Ambulance, minor hockey associations and service on various city hall committees.

In the next article, we will look further from the fraud tree at schemes that could affect your organization.

James Finlay is a Certified Fraud Examiner; he can be contacted on 905 870-1832 or at info@finlay-associates.com or via www.finlay-associates.com.