HOW TO PREVENT SMALL BUSINESS FRAUD

(Excerpt from Chapter II)

II. HOW EMPLOYEES STEAL — CASH FRAUD

Introduction

In discussing cash fraud schemes, it is important to understand exactly what the term *cash* means. Cash may be defined as any medium of exchange that a bank will accept at face value. It includes bank deposits, currency, checks, bank drafts and money orders. Cash fraud schemes, therefore, are not limited to schemes in which employees steal currency. They also involve checks, bank drafts, and other forms of negotiable instruments. In general most cash fraud schemes committed by employees focus on either currency or checks.

Cash Theft

The first categories of cash frauds that will be discussed are the cash theft schemes. It is important to remember that for purposes of this discussion, the term “theft” has been limited somewhat. *Black’s Law Dictionary* defines theft as “the act of taking property without the owner’s consent.” This definition is so broad it would encompass all forms of employee fraud because any time an employee steals from his company, this necessarily involves the taking of the company’s assets without consent. For our purposes, the term *cash theft* has been limited to mean schemes in which an employee physically removes cash from the company.

There are basically two ways a fraudster can steal cash from his or her employer. One is to trick the organization into making a payment for a fraudulent purpose. For instance, a fraudster might produce an invoice from a nonexistent company or submit a timecard claiming hours that he did not really work. Based on the false information that the fraudster provides, the organization issues a payment, e.g., by sending a check to the bogus company or by issuing an inflated paycheck to the employee. These schemes are known as *fraudulent disbursements* of cash. 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.

The second way to misappropriate cash is to physically remove it from the organization through a method other than the normal disbursement process. For example, an employee might take cash out of his 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*. These schemes reflect what most people think of when they hear the term "theft"; a person simply grabs the money and sneaks away with it. So please be aware that when we discuss cash theft schemes in the following pages, we are referring to a limited class of schemes; those in which the perpetrator physically sneaks money out of the company's control and into his own.

Types of Cash Theft Schemes

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

Skimming and Larceny

S*kimming* 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 a skimming 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.

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 includes salespersons, tellers, waitpersons, and others who receive cash directly from customers. In addition, many skimming schemes are perpetrated by employees whose duties include receiving and logging customers' mail payments. Employees may be able to slip checks out of the incoming mail rather than posting the checks to the proper revenue or customer accounts.

The basic structure of a skimming scheme is simple: Employee receives payment from a customer, employee pockets payment, employee does not record the payment. There are a number of variations on the basic plot; however, depending on the position of the perpetrator, the type of company that is victimized, and the type of payment that is skimmed. In addition, variations can occur depending on whether the employee skims *sales* or *receivables*.

Unrecorded Sales

The vast majority of skimming schemes involve the theft of incoming sales, as opposed to receivables. The reason is that receivables 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. It is important to remember that employee fraud has a different character than typical street crime. If a person walks into a convenience store, pulls out a pistol, and takes all the money from the cash register, this thief's only concern is getting away without getting caught. But if an employee of that convenience store decides to steal money from the cash register, he must not only keep from being caught, *he must also conceal the fact that a theft took place.* He not only needs to hide his identity, he needs to hide 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 on. Therefore, in order to be successful, the employee-fraudster must keep the scheme from being detected. As long as the company does not know it is being victimized, the employee can continue to steal, reaping more and more ill-gotten gains. Once the scheme is detected, however, the employee stands a good chance of losing his job, being prosecuted, being ostracized by his friends and family, etc.

The upshot of all this is that skimming tends to affect sales more often than receivables. Of course, skimming can occur anywhere cash enters an organization, and businesses should take pains to make sure all their cash receipting and handling procedures are secure. But knowing that sales skimming is more likely, small businesses should take extra care to safeguard all points of sale from employee theft.

The method and impact of these schemes can vary depending on the job responsibilities of the perpetrator and the level of supervision over the cash collection process. The following text will discuss how skimming works in some common scenarios.

On-Site Employees

Most skimming, particularly in the retail sector, occurs at the cash register—the spot where revenue enters the organization. Employees who work at the register are usually not highly paid. These people may be subject to a high degree of temptation as they spend their day handling large quantities of cash. At some point, the temptation for certain employees becomes too much and they decide to pocket some extra cash on the side.

This type of scheme is very simple. When the customer purchases merchandise, he or she pays a cashier and leaves the store with the newly purchased goods. Instead of placing the money in a cash register, the employee simply puts it in his or her pocket without ever recording the sale. The process is made much easier when employees at cash collection points are left unsupervised.

A lack of supervision plays directly into Cressey's second factor: opportunity. When an employee knows her conduct is not being monitored, this creates a perception (usually a justified one) that it will be easy to steal from the company. 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 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's register. The false transaction is entered on the register so that it appears that the employee is recording the sale. If a manager is nearby, it will look like the employee is following correct cash receipting procedures, when in fact the employee is stealing the customer's payment. Of course, the method for disguising the theft will vary depending on how the company records sales transactions, the salesperson's location in relation to her supervisor and/or the customer, and the creativity of the particular culprit.

Remote Salespersons

Salespersons who work off-site are in a particularly good position to skim funds. These employees often work with little or no supervision, making it easy for them to sell goods or services, pocket the proceeds, and never record the sale. With no supervisory authority around, it can be difficult for an organization to verify exactly how much revenue the remote salesperson is generating.

Skimming Off-Hours Sales

Another way employees sometimes skim unrecorded sales is by conducting sales during non-business hours. For instance, some employees have been caught selling company merchandise on weekends or after hours without the knowledge of the owners. In one case, a manager opened his store two hours early every day and ran it business-as-usual, pocketing all sales made during the "unofficial" store hours. As the real opening time approached, he would destroy all records from the off-hours transactions and start the day from scratch.

Theft in the Mail Room—Incoming Checks

Employees who are in charge of opening incoming mail are also in a good position to skim revenues. Instead of logging checks that are received, the perpetrators simply steal one or more incoming checks for their own benefit. This type of scheme usually occurs when a single employee is in charge of opening the mail and recording the receipt of payments.

Check-for-Cash Substitutions

Check-for-cash substitution schemes usually occur when a company receives some sort of unexpected revenue such as a rebate, a refund, etc. The employee who receives the incoming check sets it aside without recording it, and when an equal amount of currency has been received, the employee takes the currency and replaces it with the check. For example, suppose ACME Co. receives a $2,000 rebate on some computer equipment it purchased 3 months ago. David, the bookkeeper for ACME, receives the payment in the mail. Instead of recording the check, he places it in his desk drawer and waits till the end of the day when the daily deposit is prepared (by him). David removes $2,000 in currency from the deposit, and replaces it with the $2,000 rebate check. Assuming the rebate had not been booked, the loss of funds is completely off-book; the deposit balances. Of course, the composition of the deposit has changed currency has been replaced with a check and the deposit won't match the day's sales reports, but the totals match. As long as no one is too diligent in reconciling the daily deposit, David's fraud will go undetected. (In most cases, David will be the one reconciling the deposit anyway; another example of how the failure to separate duties can lead to fraud losses).

The Inventory Problem

Although sales skimming does not directly affect the books, it can show up on a company's records in indirect ways, usually as inventory *shrinkage*. Assume Jane is assigned the duty of opening the incoming mail for a mail order clothing company. One

day, she steals a check from Customer A, who had mailed the check to the company in order to purchase a new coat. If Jane simply cashes the check and does nothing more, Customer A will complain when the coat does not arrive. This could trigger a fraud investigation, something Jane (if she is intelligent) will want to avoid. The most direct way for Jane to avoid this problem is to take a coat from the company's inventory and mail it to Customer A. This eliminates Customer A as a potential whistleblower, but by stealing the coat, Jane has created inventory shrinkage: there is one less coat in inventory than there should be. Thus, we see how inventory shrinkage serves as a red flag of skimming schemes.

The same is of course true of other skimming schemes, such as unrecorded sales made at the cash register. The perpetrator in these cases sells merchandise to customers but keeps the proceeds for themselves. Therefore, whatever merchandise the customer purchases and takes home ends up as unexplained shrinkage in the company's inventory system. This will be the case unless the fraudster is skimming the sale of services or intangible benefits (like insurance policies).

In some cases, fraudsters will pad inventory totals or write off inventory as missing or damaged in order to conceal the shrinkage that results from skimming. This is not very common, however. Unless skimming is being conducted on a very large scale, it is usually easier for the fraudster to ignore the shrinkage problem. From a practical standpoint, a few missing pieces of inventory are not usually going to trigger a fraud investigation. However, if a skimming scheme is large enough, it can have a marked effect on a small business' inventory. Small business owners should conduct regular inventory counts and make sure that all shortages are promptly investigated and accounted for.

Skimming Receivables

As was previously stated, an intelligent fraudster will generally prefer to skim sales, rather than receivables, if given the choice. Skimming receivables is much more complicated because a receivable represents an amount of money a customer owes to an organization. The payment from the customer is expected by the organization, and if the payment isn't received, its absence will be noticed. This makes it much more likely that an organization will detect the theft of a receivable.

If a payment on an account receivable is stolen, the receivable becomes past due and collection efforts will be made by the victim company. Of course, the customer in this scenario has already paid his bill. The only reason the payment has not been recorded is because an employee of the victim organization has stolen the payment. If questioned about the missing payment, the customer will presumably be able to produce a cancelled check verifying that payment was made. Once this happens, the company will know that one of its employees has stolen the payment. The fraudster is thus placed in the awkward position of having to hide the scheme from two victims: the company whose revenue is being stolen, and the customer whose account is not being credited.

The methods for physically misappropriating receivables payments are basically the same as those used to skim sales. The employee still pockets incoming funds before they have been recorded. The real difference between sales skimming and receivables skimming lies in the methods used to conceal the schemes. Because evidence of receivables skimming will appear in a company's records in the form of delinquent accounts, the real key to a successful receivables skimming scheme is the ability of the fraudster to keep the victim from spotting this red flag. In general there are six concealment techniques that are utilized by employees who skim receivables. They are:

- Forcing account balances
- Fraudulent write-offs
- Debits to aging or fictitious accounts
- Lapping
- Stealing account statements
- Destroying transaction records

Forcing Account Balances

Force balancing is generally done by employees who are in charge of both collecting and posting customer payments. Of course, a single employee should not be entrusted with both of these duties, but it is common in many businesses particularly small businesses where staffing may be limited to consolidate multiple accounting duties in a single employee.

The employee who has a hand in both ends of the receipting process is able to post the customer's payments to their receivables accounts, even though the payments will never be deposited. This keeps the receivable from aging, but it creates an imbalance in the cash account. The perpetrator hides the imbalance by overstating the total on the cash account (basically adding wrong), to match the total postings to accounts receivable. If the force balancing continues without being corrected, the company will eventually suffer

cash shortages and will see checks returned non-sufficient funds because its own records overstate the amount of cash in its bank accounts.

Write-Offs

It can be especially difficult to detect receivables skimming if the perpetrator has authority to make adjustments to receivables accounts. Fraudulent write-offs, discounts, and debits can all be used to create the appearance of balance in the victim's books while the perpetrator silently drains money from the company's coffers. This follows the general rule that the more authority a fraudster has, the more damage that can be done.

For example, a fraudster will sometimes use her authority to write off a targeted account as uncollectable. The idea is that once an account is written off, payments on the account are no longer expected. Of course, the customer has no idea that his account has been written off, so he continues to make payments on schedule. The fraudster steals these incoming payments as they arrive. Since the account has been taken off the books, there is no danger of it running delinquent and triggering an investigation. There will be no red flags to go up (other than the fact that the account was written off in the first place). On the books, the missing payments will no longer signal fraud.

Instead of writing off accounts as bad debts, some employees cover their skimming by posting entries to contra revenue accounts such as "discounts and allowances." If, for instance, an employee intercepts a $100 payment, he would create a $100 "discount" on the account to compensate for the missing money. The perpetrator will generally keep the false discounts small enough to avoid review.

Debits to Aging or Fictitious Accounts

Another way to conceal receivables skimming is by improperly debiting the accounts of other customers. If Customer A's payment is skimmed, the payment is still posted to A's account, but a corresponding debit is posted to the account of Customer B. The employees who use this method generally add the skimmed balances to accounts that are either very large or that are aging and about to be written off. Once the old accounts are written off, the stolen funds are written off along with them.

Instead of debiting existing accounts, some fraudsters opt to set up completely fictitious accounts and debit them for the cost of skimmed receivables. The perpetrator then simply waits for the fictitious receivables to age and be written off.

Lapping

Lapping customer payments is one of the most common methods of concealing receivables skimming. Lapping is the crediting of one account through the abstraction of money from another account. For example, suppose a company has three customers, A, B, and C. When A's payment is received, the fraudster takes it for himself instead of posting it to A's account. Customer A expects that his account will be credited with the payment he has made, but this payment has actually been stolen. When A's next statement arrives, he will see that his check was not applied to his account and will complain. This complaint could trigger an investigation, something the fraudster must avoid. The solution is to make it appear that the payment was posted.

When Customer B's check arrives, the fraudster posts these funds to A's account. Payments now appear to be up-to-date on A's account, but now B's account is short. When C's payment is received, the perpetrator applies it to B's account. This process continues indefinitely until one of three things happens: 1) someone discovers the scheme, 2) restitution is made to the accounts, or 3) some concealing entry is made to adjust the accounts receivable balances.

Because lapping schemes can become very intricate, fraudsters sometimes keep a second set of books on hand detailing the true nature of the payments received. In many skimming cases, a search of the fraudster's work area will reveal a set of records tracking the actual payments and how they have been misapplied to conceal the theft. While it may seem odd that people would keep records of their illegal activity on hand, many lapping schemes become extremely complicated as more and more payments are misapplied. The second set of records helps the perpetrator keep track of the funds that were stolen and which accounts need to be credited to conceal the fraud. Uncovering these records, if they exist, will greatly facilitate the investigation of a lapping scheme. Once again, however, business owners must be cautioned about searching an employee's work area without first consulting an attorney. Some employee workspaces are considered private, and a search of these areas without the proper justification and/or notice could result in exclusion of the evidence or even an invasion of privacy suit against the company.

Stolen Statements

When employees skim receivables, they often let the targeted accounts age instead of attempting to force the balances. In other words, they steal an incoming check intended as payment on a receivable, and they simply act as if the check never arrived. This method

keeps the victim organization's cash account in balance, because the stolen payment is never posted.

One way fraudsters attempt to conceal the fact that they have skimmed a payment from a customer is to intercept the customer's account statement and/or late notices. In some cases, the perpetrator intercepts the account statement by changing the customer's address in the billing system so that statements are sent directly to the perpetrator's home or to an address where he or she can retrieve them. In other instances, the perpetrator physically intercepts the statements before they are mailed.

Once the real statement has been intercepted, the fraudster usually alters the statement or produces a counterfeit. The false statements indicate that the customer's payment was properly posted. This leads the customer to believe that his account is up-to-date and keeps the customer from complaining about stolen payments.

Destroying Transaction Records

Some fraudsters conceal receivables skimming by simply destroying all records that might prove that they have been stealing. This is a very crude technique and one that is not well thought-out from the fraudster's perspective. Recall that there are two keys to concealing a fraud scheme. The first, as with any crime, is to conceal the identity of the perpetrator. The second, which sets occupational fraud apart from other crimes, is to conceal *the fact that a crime has been committed.* It is this second level of concealment that enables the perpetrator to continue the scheme over an extended period of time.

By destroying records en masse, an employee might conceal his identity, but he will not hide the fact that a crime has been committed; in fact, he will probably alert the company to the fraud by this very act. Destruction of records is usually an effort of last resort by a fraudster who has lost control of his scheme as it escalated past the point where it could reasonably be hidden on the books.

Cash Larceny from the Deposit

Although skimming is much more common and costly than cash larceny (the physical theft of on-book cash), small business owners should be aware that larceny is still a threat. Most commonly, cash larceny occurs when an employee steals cash from the daily deposit. At some point in every revenue-generating business, someone must physically take the company's currency and checks to the bank. This person or persons, left alone literally holding the bag, will have an opportunity to take a portion of the money prior to depositing it into the company's accounts.

Typically, when a company receives cash, someone is assigned to tabulate the receipts, list the form of payment (currency or check), and prepare a deposit slip for the bank. Then another employee takes the cash to the bank and deposits it. The person who made out the deposit generally retains one copy of the slip. This copy is matched to a receipted deposit slip, which is issued by the bank when the deposit is made.

This procedure is designed to prevent the theft of funds from the deposit, but thefts still occur, often because the process is not adhered to. In many small businesses, a single person is in charge of preparing the deposit slips, making the deposit, and reconciling the bank statement. That person can easily pilfer money from the day's receipts and conceal it by falsifying the deposit slips. If the day's receipts are $1,000, the perpetrator might fill out a deposit slip for $500 and steal the other $500. The employee then makes correspondingly false entries in the books, understating the day's receipts. This process creates a false balance in the victim organization's records. The best way to deter this kind of fraud is to separate the functions of tabulating receipts, preparing the deposit, and making the deposit.

Deposit Lapping

As with all cash larceny schemes, stealing from the company deposit can be rather difficult to conceal. In most cases these schemes are only successful in the long term when there is no separation of duties (i.e., the person who counts the cash also makes the deposit). In any other circumstance the scheme can really only succeed if those charged with preparing and reconciling the deposit are inattentive and fail to do their jobs properly. Nevertheless, there are some techniques that employees sometimes use to conceal cash larceny from the daily deposit; these can often be successful in the short term, allowing an employee to get away with multiple thefts before the crime is discovered.

Lapping is a fairly common method of concealment. Lapping occurs when an employee steals the deposit from day one, and then replaces it with day two's deposit. Day two is replaced with day three, and so on. The perpetrator is always one day behind, but as long as no one demands an up-to-the minute reconciliation of the bank statement — and if daily receipts do not drop precipitously — the perpetrator may be able to avoid detection for a period of time.

In order to prevent losses that are concealed by deposit lapping, small business owners should require that a bank deposit be made *every business day*, and an independent

person must verify the dates and amounts of each deposit from the receipted deposit slip and the bank statement to confirm that the deposit was properly made.

Deposits in Transit

Another strategy that is sometimes used to conceal stolen deposits is to carry the missing money as *deposits in transit*, which are a way of accounting for discrepancies between the company's records and the bank statement due to deposits that were not yet made at the time the bank statement was issued. For instance, suppose Company A's bank statement cuts off on the 20th of the month, and the statement typically arrives at Company A's offices on the 22nd. If a deposit is made on the 21st, this deposit will show up in the company's records, but it will not appear on the bank statement, because it was made a day after the end of the period. In order to reconcile the statement, the deposit for the 21st must be listed as a *deposit in transit*, meaning it has been made but will not show up on the bank's statement until next month.

These schemes can be very easily prevented and/or detected by separating the functions of making the deposit and reconciling the bank statement. Independent employees who perform the reconciliation should be instructed to trace all deposits in transit to subsequent statements. Any deposits in transit should be the first deposits to clear on the next month's statement.

(Next Section: Deterring and Detecting Skimming and Cash Larceny)