SLICING THE SALAMI: SMALL-DOLLAR RECURRING FRAUD

David Zweighaft CPA, CFE

While the major "eye-popping," headline-grabbing financial statement frauds have captured the attention of the investing public in recent years, little heed has been given to the smaller dollar, repetitive frauds that occur in organizations year in, year out. These unauthorized transactions can deplete the resources of an organization in much the same way that wind and water can reshape large boulders – gradually, unnoticeably over time, until the scheme is either discontinued or it is uncovered and brought into focus.

In the 2004 Report to the Nation on Occupational Fraud and Abuse, the Association of Certified Fraud Examiners estimates that six percent of revenues will be lost to fraud. When viewed in a vacuum, six percent may seem to be an immaterial amount to many larger entities, but when it is considered as a percentage of the total Gross Domestic Product of $11 trillion, this "immaterial percentage" now translates into $660 billion lost to fraud annually.[1]

According to a November 2003 fraud survey released by KPMG, financial reporting fraud cost the most per incident, however employee fraud was the most prevalent, occurring in 60% of the companies surveyed. Even more troubling are the trends behind that statistic – over the past five years, theft of assets and expense account abuse, already high in 1998 (the last time the survey was conducted) more than doubled in 2003.[2]

While the initial reaction is to blame the perpetrators in these cases of recurring, small dollar fraud, a more considered review of the situation may lead to a different conclusion. As we are all well aware from reading auditor's opinions, management certifications, and the seemingly endless Sarbanes-Oxley articles and special reports, *the design and implementation of internal controls is the responsibility of management*. As part of the stewardship of corporate resources and the fiduciary responsibility to stakeholders, management (and the Board of Directors and Audit Committee) is tasked with eliminating fraud. In order to meet the challenge and eliminate the opportunity for fraud to occur, management needs to recognize that fraud occurs at all levels of an organization and that effective internal controls and communication of management's anti-fraud stance throughout the organization are the basis for effectively reducing the incidence and impact of employee fraud.

It is worthwhile to review the historical precedents to the current legislated anti-fraud requirements placed on management. The National Commission on Fraudulent Financial Reporting (commonly known as the Treadway Commission) was established in 1987 with the purpose of defining the responsibility of the auditor in preventing and detecting fraud. The Committee of Sponsoring Organizations (COSO) was formed to support the implementation of the Treadway Commission. In 1992, the committee issued *Internal Control—Integrated Framework*. This report was a collaborative effort of the American Accounting Association, the American Institute of CPAs, the Financial Executives Institute, the Institute of Internal Auditors, and the Institute of Management Accountants. The report is meant to apply to all entities, public and private, regardless of size. The COSO report complements Treadway's recommendation to the SEC that public companies' management reports include an *acknowledgment for responsibility* for internal controls and an assessment of effectiveness in meeting those responsibilities.

In 1999, the Committee of Sponsoring Organizations for the Treadway Commission (COSO) published a follow-up study to its 1987 report. The new report, entitled *Fraudulent Financial Reporting: 1987-1997, An Analysis of U.S. Public Companies*, examined a random sample of 204 financial statement fraud cases that were the subject of SEC enforcement. Notably, the majority of companies that experienced fraud losses were

relatively small, with the typical size ranging well below $100 million in total assets. Seventy-eight percent were not listed on the New York or American Stock Exchanges. Also, most frauds were not isolated to a single period, with most overlapping at least two fiscal periods. The relatively small size of the companies suggests that they may be unwilling or unable to implement cost-effective internal controls. Management needs to be held accountable to ensure that a baseline of internal control is present.

The purpose of this article is to examine the factors that allow fraud to flourish at a low level, or "under the radar" of internal controls, describe some of the common schemes that occur; and propose responses that management can implement to prevent fraud from occurring in the future. The title of this article derives its name from the term "Salami Techniques," as defined in the Encyclopedia of Fraud as:

> "*The theft of small amounts of assets from a large number of sources without noticeably reducing the whole. In a banking system, the amount of interest to be credited to an account is rounded off. Instead of rounding off the number, that fraction of it is credited to a special account owned by the hacker"*(page 450).

For the sake of clarity, a few definitions are in order:

Occupational Fraud – the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets.[3]

Small-Dollar Recurring Fraud – misappropriation of an entity's assets, repeated during any given accounting period (e.g., month/year) in an amount insufficient to be detected by the entity's system of internal controls.

Quantifying the amount at issue is subjective; it may be relative to the size of the organization, but as a "rule of thumb" it can be amounts that, in the aggregate, indicate throughout the organization that management does not take fraud prevention seriously. What is notable about this interpretation is that it is expressed in terms of management's attitude and tolerance toward fraud. The more proactive an entity's management is at preventing fraud, the lower the resulting fraud losses will be. Likewise, an entity with more relaxed controls will most likely suffer greater fraud losses.

Common Characteristics

Occupational fraud schemes have several common characteristics, which can be attributed to either the perpetrator or to the entity. These characteristics are described below.

Characteristics of the perpetrator (the three elements of the "Fraud Triangle")[4]:

Need – a need (financial, emotional, real or imagined) that cannot be shared and drives the perpetrator to commit the fraud. Such needs or problems are subjective, and are often tied to the perpetrator's sense of self-worth. These include the inability to pay mounting bills, personal failures, business reversals, craving social status or resentment directed at one's employer.

Rationalization - attitude of entitlement or rationalization by the perpetrator that allows him/her to commit fraud with a free conscience. This is often coupled with the confidence and belief by the perpetrator that the amounts being stolen are so small that they will continue to go unnoticed. Individuals rationalize their crimes as non-criminal, justified, or as part of an environment over which the offender has no control.

Opportunity – the Operating Environment and lack of adequate Internal Controls allow the perpetrator to devise and execute the scheme (with or without assistance). These include being in a position of trust or responsibility, access to assets, ability to initiate, authorize or record transactions into the books and records of the entity.

Characteristics of the entity that enable fraud to occur:

Management Attitude - the attitude within the highest levels of organization is sufficiently lax that the fear of detection and prosecution is minimal. This is the so-called "tone at the top" described in the COSO Internal Control Integrated Framework Report. When management exhibits a casual attitude towards internal controls and fraud prevention, that transmits a powerful message throughout the organization that individuals will not be held responsible for any resultant breakdowns in internal controls, nor for any losses due to fraud.

Operating Environment – these are systemic factors that allow fraud to occur without detection. These factors may be economic, such as industry competition, rapid growth, recession, and employment cutbacks, or they may be the result of mergers, changes or failures in financial or management reporting systems, or management turnover. Other contributing factors are the lack of written policies and training, or outdated policies that do not reflect the day-to-day operations of the entity.

Lax Internal Controls - the internal controls in place are ineffective below a given threshold; no pre-employment background checks; inadequate supervision, no segregation of duties, no internal audit function.

A common occurrence in mid-size to large companies is the notion that good internal controls is a "one size fits all" concept. With so many companies rushing to comply with recent legislation, a proliferation of off-the-shelf risk assessment and control documentation packages have become available. Lured by the prospect of "scalable" and "customizable" controls, entities are purchasing hollow assurance and rolling it out across all of their operating units. This "cookie-cutter" approach can result in the same controls being used at a convenience food manufacturer and at a chain of gas stations, and management of both entities are under the delusion that they are employing customized controls that address the various risks specific to their industry.

A fundamental truth is that internal controls are merely processes that are only as effective and reliable as the people responsible for carrying them out. In order for these controls to be as effective as possible, management is responsible for communicating the importance of these controls and for continuously monitoring and assessing the results of the control procedures. "Control delusion" is management's complacency and the belief that controls are satisfactory without monitoring or communicating with the human elements in the control environment.

Common Recurring Small-Dollar Fraud Schemes

Since the easiest (and most common) type of fraud to commit is the misappropriation of an entity's assets, it should come as no surprise that the asset of choice for frauds is cash. Untraceable, fungible and highly liquid, cash can be siphoned out of an entity before or after it has been recorded in the entity's books and records. The distinction here is an important one – cash that has not yet been recorded is much easier to steal because there are no accounting entries to make, no ledgers to balance and fewer controls to circumvent. Cash that is already "in the system" (i.e., recorded by the entity) may be extracted through outright theft or through a fraudulent disbursements scheme. These schemes require a check to be written or cash to be wired for what appear to be a valid business expense, generally to the perpetrator or to a fictitious vendor.

Theft of Cash Before it is Recorded: Skimming Schemes

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.*[5]

Skimming sales can occur when i) cash is collected but the sale is not recorded; ii) casual sales occur outside of regular business hours or away from normal business locations; iii) sales are recorded at less than their full amount and the full amount is collected from the customer, or iv) destroying or altering sales records to hide skimmed sales. A contributing factor common to each of these schemes is the lack of adequate supervision of the sales recording and cash receipt functions.

Aside from the point of sale, skimming can take place at the point of payment receipt. In most organizations, payment checks are received in the mailroom. Stealing checks is a simple, short-term form of skimming. The only complicating factor is if the checks are received against accounts receivable, in which case the customer's account will become past due. When the customer is notified of the delinquency and the cashed check is produced, the perpetrator may be identified.

Skimming receivables is accomplished by stealing the payments made against accounts receivable and then disguising the theft through a variety of means. On method is lapping the accounts of different customers, whereby a payment is stolen from one account, and a payment for another account is applied to the first account. A subsequent payment against a third account is applied against the second account, and the process continues 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.

Besides lapping, another way to prevent delinquency is to make false entries in the entity's accounting system. If a payment is made on a receivable, the proper entry is a debit to cash and a credit to the receivable. Instead of debiting cash, the perpetrator could debit an expense account. This transaction still keeps the company's books in balance, but the incoming cash is never recorded. In addition, the customer's receivable account is credited, so it will not become delinquent. Alternatively, the perpetrator could post a credit memo to the account, thereby reducing the receivable balance sot that the missing payment would go unnoticed.

These false debits can be made to fictitious accounts, or to existing accounts with very large balances where a small debit might go unnoticed. Another account that might be used in this type of concealment is the bad debts expense account.

A final method for skimming of receivables is posting entries to contra revenue accounts such as "discounts and allowances." If, for instance, an employee intercepts a $1,000 payment, he would create a $1,000 "discount" on the account to compensate for the missing money.

Theft of Cash After it has been Recorded: Fraudulent Disbursement Schemes

In order to extract cash from an entity, the perpetrator must create an appearance that a *bona fide* obligation exists and that the entity is supposed to make that payment as part of the normal course of business. There are so many different payments that businesses are required to make on any given day, hence the opportunities for frauds may seem overwhelming. Since the focus here is on *recurring fraud*, we can restrict this discussion to repetitive, regularly scheduled payments. These would include payments primarily to vendors and employees. Within an entity, a perpetrator who is in a position to approve, process or record disbursements can forge or manipulate documents to create the appearance of normal business transactions. The only difference is that the disbursement is being directed to the perpetrator, or an account controlled by him/her.

Payments to Vendors

The principal types of payments to vendor schemes are: false invoicing via fictitious vendors, and false invoicing via vendors.

A fictitious vendor scheme is made particularly easy if the perpetrator has unsupervised authority to approve invoices. Most fictitious vendor schemes involve the purchase of services, rather than goods, because intangible services are harder to verify. The perpetrator uses his fictitious company to purchase legitimate merchandise, and then resells the merchandise to his employer at an inflated price.

A real estate limited partnership that owned and operated a high-end commercial property was experiencing severe cash flow problems, and was not making the anticipated distributions to the Limited Partners. An investigation revealed that the property manager had entered into several duplicative contracts for property management and asset management. These contracts were with shell companies that had the same mailing address as the property management company. The result of these bogus contracts was that they charged between 2.5% - 7 % of total rental income <u>each</u> to perform the same functions, thereby depriving the partnership of distributable cash flow. In the litigation that ensued, the property management company was found to have diverted $1.3 million from the partnership over the course of 5 years.

Vendor accounts are also a favorite target of in-house perpetrators. Some employees generate false invoices in the names of legitimate third party vendors—the vendors may be unaware of the scheme, they may be participants, or they may agree to keep silent. In "pay-and- return schemes," employees intentionally mishandle vendor payments. For instance, a clerk might intentionally pay an invoice twice, then request that the vendor return one of the checks. The clerk intercepts the returned check and converts it to cash, perhaps by depositing it into an account established in a name similar to that of the legitimate vendor.[6]

How does an entity prevent fraudulent disbursements to vendors? The answer once again, is a system of internal controls and management oversight and accountability. Depending on the organizational structure of the entity, there should be:

- A purchasing department (or at the very least a prescribed set of procedures for making purchases);
- A list of approved vendors that is reviewed at least annually;
- pre-printed, pre-numbered purchase orders for which a tracking log is maintained;

- A procedure for reviewing all purchase documentation (purchase order, requisition, proposal/invoice for vendor, etc) prior to preparing a check request for a purchase, ensuring that all required authorizations and signatures have been obtained; and
- Separate functions for purchasing, receiving, invoice processing, accounts payable, and general ledger/accounting.

Note that this is not a comprehensive list, but it is intended to illustrate the types of controls that can prevent vendor disbursements fraud schemes.

Payments to Employees

In the normal course of business operations, an entity makes payments to, or on behalf of employees for generally two bona fide reasons: compensation (salary, wages or commissions) and expense reimbursements. At issue with these types of payments are the amounts paid (are they correctly calculated and commensurate with the salary/wage rate and number of hours actually worked?), the propriety of the payments (are the payees actually employed by the entity and entitled to receive these payments?) and the accurate characterization of the expense being submitted (were the expenses actually incurred in connection with the individual's employment and accurately presented?).

Compensation Schemes

In compensation schemes the perpetrator may be an hourly employee boosting his/her hours in order to receive additional overtime pay, or a shift supervisor or payroll clerk collecting paychecks for "ghost employees" who were either terminated or never were employed by the company. In either case, funds are being disbursed in excess of the amounts that the payees are authorized to receive.

In the case of the hourly employee, the fraud is committed through either time cards or a handwritten timesheet, which is forwarded to a supervisor or payroll clerk for review. As is oftentimes the case, the review is cursory at best, and the inflated hours are forwarded to payroll accounting. Alternatively, the hourly employee may be submitting accurate time records, and then altering them after they have been approved.

An hourly employee at a warehouse had to "punch in" and "punch out" at the beginning and end of his shift, using a time card and a punch clock. He developed the habit of leaving an hour or two early and "forgetting" to punch out twice a week. On the mornings following his early departures, he would get the night shift supervisor to initial that that he left work at the appropriate time. The obviousness of this scheme led to its rapid discovery and the employee's termination.

In the case of "ghost employees," an information gap occurs between the human resources and the payroll accounting functions. Whenever an employee is deleted from the entity's labor force, the processing of that employee's records should include a final paycheck. Properly functioning internal controls (e.g. an employee termination checklist) should provide for notifying payroll accounting that no additional payments to that employee be allowed through the payroll system.

At the very minimum, the following general controls should be in place to detect and prevent payroll and ghost employee schemes[7]:

- Have someone other than the payroll department distribute checks;
- Require positive identification of each payee;
- Look for duplicate names, addresses, or deposit accounts;
- Require supervisors to authorize overtime and to refer timecards directly to payroll;

- Verify that each employee's Social Security Number matches the valid combination listed by the Social Security Agency;
- Determine whether any employees have failed to execute the tax withholding forms, or have not elected to receive any health benefits or other optional withdrawals, such as enforced savings plans;
- Review excessive overtime or overtime worked by a single employee in a department; and
- Compare the personnel list and the payroll list.

As stated previously, it is up to management to communicate that overtime and payroll are monitored and that management has taken a "zero tolerance" position on payroll fraud.

Expense Reimbursement Schemes

Employees often incur out-of pocket expenses in the course of discharging their obligations to their employers. Depending on the nature of the entity and the type of expenses incurred, these expenses may be reimbursed to the employees. The general reporting model for expense reimbursement is that the employee submits documentation for expenses incurred, and it is the job of the accounting department to determine if the expenses are correct, appropriate and reimbursable. The motivation to commit fraud under this reporting model can be very tempting, and an employee with a financial need may see an opportunity to take advantage by letting some personal expenses "slip into" the reimbursement submission. If expense report submissions are verified by the accounting on a sample basis, the perpetrator has a calculable chance of successfully committing this type of fraud on a recurring basis. In general, reimbursable expenses are subject to mischaracterization and overstatement.

Mischaracterized Expenses

The majority of reimbursable expenses fall into the broad categories of "travel, meals, entertainment and miscellaneous." While only business-related activities are reimbursable, employees frequently submit personal expenses as reimbursable. These relate primarily to restaurant meals, office supplies purchased for the employee's personal use, and entertainment expenses.

At a large insurance company, the Assistant Vice President of Investment Accounting had a reputation for gladly joining anyone for a drink. He was often wined and dined by banks and trust companies eager to get their hands on some of the insurance company's investments. If nobody was around to take him out, he would gather a group of six or eight employees from his department and go out for dinner and drinks. As "departmental outings," these were charged through on his expense reports. These outings caught the attention of someone in the internal audit department, who added up almost $25,000 in inappropriate expenses over the course of nine months, resulting in his termination.

In order to detect mischaracterized expenses, a detailed review of the submitted documentation is required. Scrutinizing dates, times and numbers of persons served and comparing these with a calendar and the employee's explanation of the reimbursable activities should reveal fraudulent expense. For example, when the reimbursement is for "dinner with client" and the restaurant receipt shows a time stamp of one o'clock in the afternoon on a Saturday, this is a mischaracterized expense.

Overstated Expenses

There are three ways to overstate expenses: overstating the actual costs incurred, submitting fictitious expenses and submitting the same expenses for reimbursement multiple times. While the financial impact of any of these

methods may be immaterial in a single instance, the impact of multiple employees committing expense reimbursement fraud over many periods can become substantial.

Overstating actual costs incurred is accomplished by either not providing any documentation to substantiate reimbursable expenses, or by providing altered documentation. In a manner similar to mischaracterization described above, the employee may purchase excess goods and keep a portion for him/herself, while submitting the cost for the entire amount for reimbursement.

Fictitious expenses are instances where the employee "creates" documents to submit in support of an expense reimbursement claim. There never were any expenses incurred, however old credit card receipts and forged documents are often used in these schemes.

Multiple reimbursement schemes occur when documentation for the same expense is submitted repeatedly. The documents may take different forms (e.g. invoice, receipt, online confirmation, etc.) but they all serve to substantiate the same expense.

As with mischaracterized expenses, in order to detect overstated expenses, a detailed review of the submitted documentation is required. It should be noted that perpetrators view reimbursable expense fraud as "tax-free income," since expense reimbursements are not subject to income or Social Security taxes. This serves as an additional incentive for management to develop, implement and maintain internal controls over reimbursable expenses.

Conclusion

Small dollar recurring fraud of one kind or another occurs in almost every organization. The most comprehensive controls will not prevent it from happening unless management adopts the mindset that they will not allow fraud to occur. This mindset has to be communicated to all employees and they need to become empowered to assist in preventing and detecting fraud. While the organization cannot address the unshareable **needs** or the ability to **rationalize** the actions of the fraud perpetrator, eliminating the **opportunity** for fraud to take place will significantly reduce the fraud losses that the organization experiences. A heightened sense of fraud awareness throughout the organization, and an understanding of how fraud affects not only the organization itself, but employees, customers, lenders and other stakeholders will reinforce the notion that the human element can be either the strongest or the weakest part of the control environment. This can only be achieved by management through anti-fraud communication and continually educating employees to report fraud and abuse within the organization.

---

[1] Association of Certified Fraud Examiners, 2004 Report to the Nation, pg. 8.
[2] KPMG Fraud Survey 2003, pg 4.
[3] 2004 Report to the Nation, pg. 1.
[4] Wells, Joseph T. Occupational Fraud and Abuse, Obsidian Publishing Co.1997
[5] How to Prevent Small Business Fraud, ACFE: Obsidian Publishing Co., 2002, pg 18.
[6] Wells, Joseph T. Encyclopedia of Business Fraud, Obsidian Publishing Co., 2002, pg 83.
[7] Wells, Joseph T. Encyclopedia of Business Fraud, Obsidian Publishing Co., 2002, pg 705.