

First Friday Fraud Facts

June 3, 2011



QUESTIONS OR COMMENTS:

Matt McBride, CGFM
Financial Specialist
P.O. Box 83720
Boise, ID 83720-0011

Phone: (208) 332-8805
Fax: (208) 334-3415

E-mail: mmcbride@sco.idaho.gov

Inside this issue:

Welcome	1
Asset Misappropriation	1
What You Can Do	2
Fraud Case Overview	2

The Oregon State Controller's Office created this newsletter. With their permission, the Idaho State Controller's Office edits and distributes this newsletter as a cost-effective method of increasing awareness about ways to detect and prevent fraud, waste, and abuse in government.

Approximately 90 percent of all occupational fraud schemes involve asset misappropriation. This issue of the First Friday Fraud Facts (F⁴) will cover some of the various types of asset misappropriation and what you can do to help protect your organization.

ASSET MISAPPROPRIATION

The Association of Certified Fraud Examiners (ACFE) places asset misappropriation schemes into nine different categories.

- **Skimming** is any scheme that involves cash stolen from an organization before it is recorded in the organization's records.
- **Cash larceny** includes any scheme that involves cash stolen from the organization after it has been recorded in the organization's records.
- **Billing schemes** occur when a person causes his/her employer to issue a payment by submitting invoices for fictitious goods or services, inflated invoices, or invoices for personal expenses.
- **Check tampering** schemes involve a person stealing from an organization by forging or altering a check or by stealing a check intended for another payee.
- **Expense reimbursements** is any scheme in which an employee claims a reimbursement of false or inflated business expenses.
- **Payroll schemes** occur when an employee causes his/her employer to issue a payment by making a false claim for compensation (i.e. ghost employees or excess overtime).



- **Cash register disbursements** schemes involve an employee making false entries on a cash register to hide the fraudulent removal of funds.
- **Cash on hand misappropriations** involve theft or misuse of cash that is held within the organization.
- **Non-cash misappropriations** are the result of employees stealing or misusing physical assets belonging to the organization.

Skimming and cash larceny are schemes that target incoming receipts; while billing, check tampering, expense reimbursements, payroll, and cash register disbursements all target outgoing disbursements.

WHAT YOU CAN DO

As has been noted in previous issues of the F⁴, billing schemes are the most common asset misappropriation scheme within the government sector. Some examples of billing schemes commonly take the form of fictitious vendors and invoices, shell companies, and personal purchases. In a recent ACFE study of 479 fraud cases, billing schemes were found in 26 percent of the cases (125 occurrences) and resulted in an average loss of approximately \$128,000.

Key controls in limiting the potential for fraudulent billing schemes is establishing adequate segregation of duties and proper checks and balances to ensure red flags do not go undetected. In addition, independent reviews of expenditures can be an important part of an internal control system. However, these controls only work if managers/reviewers understand the purpose behind the review and follow-up on all questionable transactions.

FRAUD CASE OVERVIEW

This case outlines a billing scheme involving both illegitimate payments resulting from fictitious invoices and inflated employee reimbursements. The perpetrator worked for the organization for over 12 years and was primarily responsible for assessing and coordinating the training needs of staff. In this capacity he would often work with outside consultants to aid in training development and implementation.

The perpetrator was able to submit fictitious invoices for a legitimate vendor. The payments were diverted directly to the perpetrator, and the checks were

deposited into an account established with false identification. Over a two year period he submitted 26 false invoices totaling over \$490,000.

He was caught when the bank flagged the account for suspicion during routine testing. They turned it over to law enforcement for an investigation. Law enforcement was able to work with the company's internal auditors to uncover the fraud.

Once they uncovered the fictitious invoices, the internal audit department expanded their investigation to review expense reimbursements submitted by the perpetrator. They discovered he had been submitting legitimate reimbursements to his supervisor and then, when the supervisor was out, he would submit duplicate reimbursements to the second in command. He would use original receipts for the first reimbursement and would use credit card receipts for the second. In addition, he would always ensure the amounts and dates were slightly different to enable the duplication to go undetected. He was able to obtain an additional \$32,923 over a three-year period for the inflated reimbursement claims.

The company later discovered, as part of the investigation with law enforcement, that the perpetrator, whose annual salary was \$85,000, had been living a very lavish lifestyle. This included a yearly membership to a private club totaling \$25,000 per year, vacations to exotic locations, and the purchase of a \$350,000 cottage in a very exclusive neighborhood. The perpetrator was tried and convicted for the fraud.

The company had a process in place in which the financial department would send out monthly budget-versus-actual reports for all expenses incurred during the month. In this case, the reports went to the perpetrator's direct supervisor for review and sign-off. This report could have helped in detecting the fraud scheme. The department was consistently over budget and later it was discovered that the supervisor, despite signing each of the monthly reports, was simply signing the reports without conducting the necessary review. As a result of this negligence the supervisor was discharged from the organization.
