

# First Friday Fraud Facts

February 6, 2009

## Share your stories

If you have a case you would like to see shared in *First Friday Fraud Facts*, please let us know.

## QUESTIONS OR COMMENTS:

Erin Haney, CIA

Statewide Financial Internal  
Controls Officer  
155 Cottage St NE, U50  
Salem, OR 97301

Phone: 503-378-3156 ext. 277

Fax: 503-378-3514

E-mail: [erin.d.haney@state.or.us](mailto:erin.d.haney@state.or.us)

## Inside this issue:

Welcome	1
Prevention vs. Detection	1
The Fraud Triangle	2
Payroll Fraud Tests	2
Fraud Case Overview	3
Payroll Fraud Uncovered	4
Q & A Contacts	4

Welcome to First Friday Fraud Facts. This new monthly communication will provide an opportunity to become more alert and better equipped to deal with the increasing potential for fraud. Information will be provided for both educational and actionable methods to address fraud risks. In addition, this publication will include announcements of training events as they become available. It will also cover some of the cases of fraud around the state and nation, both public and private sector. These case overviews will cover what happened, what controls could have prevented it, how the perpetrator was caught and the ramifications of the actions both on the perpetrator as well as the organization.

## PREVENTION VS. DETECTION

Prevention entails, but is not limited to: adequate systems of control, system edits and value ranges, approval paths, staff education, system and human monitoring, code of conduct, setting appropriate "tone at the top," hiring standards and background checks.

Detection includes, but is not limited to: analyzing reports, monitoring anomalies, data analysis and interrogation techniques, "fraud hot-lines" and websites, use of internal auditors, analytical software and Benford's Law, suspicious transaction flags, email monitoring for key phrases, and system access (and denial) logs.

A balanced approach can provide a better chance of mitigating fraud risk as well as catching honest errors. Crafting a strong message with education, prevention, and detection offers many possibilities at a low cost. In addition to mitigating against fraud, many of these techniques can often help find unintentional errors, omissions, misstatements, and other honest mistakes.

Fraud detection can come from many sources. According to a recent Association of Certified Fraud Examiners (ACFE) study, in the



government sector over 50% of fraud is detected through tips, followed by Internal Audits with over 26% and Internal Controls with almost 20%.

### THE FRAUD TRIANGLE... A Recipe for Disaster

#### One part **Motivation**:

This is the “what” of the equation. Internal pressures to perform, too much work, too much expectation. External pressures from family, expectations to succeed, financial expectations, family medical issues and financial needs, divorce, gambling, alcohol, and drugs. And sometimes just plain old greed.

#### One part **Opportunity**:

This is the “how” of the equation. Breakdowns, or sometimes just lacking, internal controls. Too much trust and not enough checks and balances.

#### One part **Rationalization**:

This is the “when” of the equation. Rationalization, justification, attitude, behavior, ethics; for some it starts with a loan, for others it is a sense of entitlement, it may be justified by the need to help their family or loved one, or sometimes it’s just driven by addiction.

### PAYROLL FRAUD TESTS:

This month we will cover some common fraud tests to help mitigate the risks of payroll fraud:

#### **Ghost Employees**

This term refers to a scenario when an individual is on the payroll for a company but does not actually work there. This is most commonly a recently departed employee, a made-up person, or a friend or family member of the perpetrator. Some test to check for this include:

- No taxes or benefits
- Invalid Social Security Number
- Frequent employee address changes
- P.O. Box, Drop Box Address, Organization’s Address, or no home address
- Unusual work location, no work phone or location
- No annual or sick leave used over a reasonable period
- No evaluations, raises, or promotion over an extended period
- Terminated employees still on the payroll
  - \* Paycheck issued after the termination/last worked date
  - \* Match paycheck file with active employee file

---

### Excessive Pay Rates

- Gross Pay Adjustments
- More than one pay increase/change without a position change in the last year
- Employees with the same address in the same unit (preferential hiring)
- Excess overtime or continual pattern of overtime
- Excessive comp-time accruals

### FRAUD CASE OVERVIEW

This case involves a ghost employee scheme in which a payroll specialist for a non-profit organization embezzled \$112,000 over a two year period to cover medical costs.

The employee's duties included posting time and attendance to the computer system and preparing payroll disbursements summaries. He was not responsible for adding or deleting employees from the master file, this was the responsibility of another employee. The organization also had a process in place for a supervisor to approve all payroll disbursements, and they used direct deposit for all payroll disbursements.

The perpetrator had to employ several techniques in order to circumvent the internal controls in place. He was able to obtain his co-workers user ID and password in order to obtain access to add employees to the master file. In addition, he knew that tax deductions were programmed for employees within a given range of employee numbers, he intentionally assigned the fictitious employees numbers higher than that range. This ensured that the "ghost" employees did not have deductions taken from their checks. At this point he was able to enter their false wage information into the system, and he arranged to have the checks direct deposited into his own account. Finally he prepared his own false payroll summary for the supervisor's signature. The perpetrator was a trusted and valued employee, and as such the supervisor did not check his work carefully and failed to notice the fraudulent documentation had been printed with a different typeface from the legitimate reports. The employee also created fake file copies of the ghosts' paychecks using white paper instead of the yellow that was used for the legitimate checks printed by the accounting department.



The scheme was discovered when an auditor noticed the white copy of one of the fraudulent checks during routine transaction-testing of the payroll account. The employee entered a plea bargain agreement and served no jail time but was sentenced to 15 years' probation and ordered to pay restitution.

### **PAYROLL FRAUD UNCOVERED:**

Some simple but effective techniques to prevent or detect ghost employee schemes include:

- Ensure the payroll preparation, disbursement and distribution functions are segregated.
- Look for paychecks without deductions for taxes or Social Security.
- Encourage direct deposit; although this is not foolproof (as can be noted by the above case) it can reduce the risks of payroll fraud.
- Check payroll records for the presence of duplicate names and social security numbers.
- Have managers hand deliver, when possible, paychecks/stubs to employees and require a positive identification.
- Be wary of budget variations in payroll expenses.

***FIRST FRIDAY FRAUD FACTS IS  
PUBLISHED BY THE STATE CON-  
TROLLER'S DIVISION***

Statewide Financial Services

155 Cottage Street NE

Salem, OR 97301

Phone: 503-378-3156

Fax: 503-378-3514

<http://www.oregon.gov/DAS/SCD/>

**WHO CAN YOU CALL FOR HELP?**

The State Controller's Division reminds state agencies that it is always available to answer internal control questions. If you have an internal control problem or an audit finding and need help in resolving it, please contact:

**Erin Haney**

**Statewide Financial Internal Control  
Officer**

[erin.d.haney@state.or.us](mailto:erin.d.haney@state.or.us)

**503-378-3156 x277**

**Internal control tools are on the Web!**

**[http://www.oregon.gov/DAS/SCD/internal\\_controls.shtml](http://www.oregon.gov/DAS/SCD/internal_controls.shtml)**