

# First Friday Fraud Facts

August 5, 2011

*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.*



## 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](mailto:mmcbride@sco.idaho.gov)

## Inside this issue:

Welcome	1
Assessing Fraud Risk	1
Fraud Risks and Controls	1
10-80-10 Rule	2
Fraud Case Overview	3

Welcome to First Friday Fraud Facts (F<sup>4</sup>). This edition will focus on some basic factors of fraud risk, control assessments, and things you can do to increase fraud awareness.

### ASSESSING FRAUD RISK

An effective fraud risk assessment program should be performed on a systematic basis. An important consideration is possible fraud schemes and scenarios, taking into account both internal and external factors. The process should assess risk at all levels of the organization, entity-wide, and significant business units. Another important factor is to evaluate the likelihood and significance of each risk. Think about the key controls in place; who could take advantage of them and why.

Knowing your data is also a key factor in maintaining fraud awareness. Knowing what the standard data within your organization looks like is important in identifying possible red flags in the data.

### FRAUD RISKS AND CONTROLS

Fraud risk exposure should be assessed regularly within an organization. This assessment will help identify potential schemes that could be perpetrated. Since these exposures may change over time as the organization changes, this assessment should be updated on a regular basis. Several items to consider when assessing fraud risk and the controls in place to mitigate against fraud include:

- Weigh the risks and associated costs
- Understand the controls in place and assess the weaknesses within those processes



- Identify who could potentially take advantage of the risks and weaknesses
- Be proactive in assessing the potential affect perpetrators of fraud could inflict in a fraud scheme
- Determine some of the potential signs and red flags of fraud
- Identify and access sources of information to detect fraud
- Based on knowledge of the processes, assess what you would expect to see from gathered data
- Run tests and review results – compare these results to your expected outcome
- Evaluate, follow-up, and revise processes as necessary

This process should be continuous and updated to adapt to changes within your organization.

This list is not intended to be all inclusive; many other processes and steps can be taken to protect against and detect fraud. Although these steps have the potential to alert you to fraud, waste, or abuse within your organization, implementation of these processes does not guarantee every occurrence of fraud will be caught or stopped. These steps are merely suggestions to mitigate against the occurrence of fraud, waste, or abuse.

### **10-80-10 “RULE”**

The 10-80-10 “rule” refers to a general assumption of the population and the likelihood of fraud occurrences.

- 10 percent of the population will NEVER commit fraud. This is the type of person that will go out of their way to return items to the correct party.
- 80 percent of the population might commit fraud given the right combination of opportunity, pressure, and rationalization. This is increasingly important given the current economic environment and emerging technologies that allow for new opportunities to commit fraud.
- 10 percent of the population are actively looking at systems and trying to find a way to commit fraud.

A good fraud awareness campaign can help deter many potential instances of fraud. If you assume the 10-80-10 rule is accurate, then roughly 80 percent of the population could be deterred if they thought they would be caught. Therefore, creating a climate of fraud awareness and an active prevention and detection campaign could protect staff from making a terrible mistake.

### FRAUD CASE OVERVIEW

This case involves an identity theft scheme in which a mortgage company employee was able to steal the identity of several individuals, including several in conjunction with a disaster relief program.

Over a four-year period, the perpetrator was able to steal the identity of over 200 individuals. The theft started when the perpetrator was an employee at a mortgage company and continued into subsequent employment with a government entity. The individual was able to steal the victims' information without the knowledge of the employer by copying their personal information from loan applications and applications for government assistance programs. Approximately 30 of the identity theft victims were applicants to government programs.

At least 74 of the stolen identities were used to open accounts with various retailers and fraudulently obtain credit in excess of \$156,000. The perpetrator used the credit to go on shopping sprees that included purchasing various items including jewelry, electronics, gourmet dinners, clothing, and various other items. The items were either kept for personal use or pawned at local pawn shops. During the four-year period, dozens of items were pawned and the perpetrator was able to obtain over \$24,000 in cash.

The perpetrator blamed a drug problem and abuse as a child for his crimes. However, the judge in the case noted that drug addicts do not typically order gourmet food, such as steak and lobster, and that simple restitution would not undo the damage he had done to the victims' credit and livelihoods.

The perpetrator faced a mandatory-minimum of two years in prison and a maximum of 32 years and a \$1,000,000 fine. Ultimately, the individual pleaded guilty to one count of wire fraud and one count of aggravated identity theft and was sentenced to 64 months in prison and ordered to pay over \$48,700 in restitution.

