

First Friday Fraud Facts+

December 6, 2013

The Idaho State Controller's Office 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

Inside this issue:

Welcome	1
Fraudulent Invoices	1
Red Flags	1
Best Practices	2
Fraud Case	2

Welcome to First Friday Fraud Facts+ (F4+). This edition will cover a type of procurement fraud which involves the fraudulent billing of invoices.

FRAUDULENT INVOICES

A contractor or supplier can commit fraud by knowingly submitting false, inflated, or duplicate invoices; whether acting alone or in collusion with contracting personnel. False invoices refer to invoices for goods or services not rendered. Duplicate invoices are fraudulent if issued *knowingly* with the intent to defraud. *Knowingly* is typically defined as an actual knowledge of being false, deliberate ignorance of truth ('willful blindness'), or reckless disregard of truth.

Duplicate, false, or inflated invoices are often used to generate funds for bribe payments.

RED FLAGS—GENERAL

- Weak controls over the review and payment of invoices
- Discrepancies between contract or purchase order, receiving documents, and invoices
- Discrepancies between contractor's billings and supporting documents
- Invoice is in a round dollar amount (if that is unusual)
- Total payments to a contractor exceed total contract or purchase order amounts

RED FLAGS—INFLATED INVOICES

Invoice prices, amounts, item descriptions, or terms exceed or do not match:

- Contract or purchase order terms
- Receiving records
- Inventory or usage records
- Discrepancies between invoice amounts and supporting documents



RED FLAGS—FALSE INVOICES

- No receiving report for invoiced goods or services
- Invoiced goods or services cannot be located in inventory or accounted for
- No purchase order for invoiced goods or services

RED FLAGS—DUPLICATE INVOICES

Multiple payments in the same time period:

- In the same or similar amount to the same or related vendors
- On the same invoice or purchase order
- For the same or similar goods or service

Multiple invoices with the same:

- Description of goods or services
- Amount
- Invoice number
- Purchase order number
- Date

BEST PRACTICES

- Perform due diligence background checks on a contractor to confirm it is a legitimate company capable of providing the invoiced goods or services, and whether the company has previously been investigated or sanctioned for fraud or for submitting fraudulent invoices
- Independently verify the correctness of the submitted invoices, (e.g., confirm that invoiced services were performed as claimed, the quantity and quality of invoiced goods were delivered as claimed)
- Note duplicate invoices and payments for the same or similar purchase order number, invoice number, amount, date, and item description
- Compare total invoiced amounts from the contractor to the total purchase order or contract amounts, noting any overpayments. Look for evidence of fraudulent knowledge and intent, (e.g., delivery, test, or inspection reports have been altered, discrepancies exist between internal time and invoiced expense records and invoiced amounts)¹

FRAUD CASE

This case involves a former hospital vice president at University Medical Center (UMC) in Lubbock, Texas, whose bogus billings and misuse of a corporate credit card for more than 4 years resulted in more than \$700,000 in financial losses for UMC.

According to the factual resume the defendant signed, he conspired with another man, Rudolph Reyes “Rudy” Mata to bilk the hospital between

June 2007 and December 2011, primarily using two businesses. One bogus business was B.R. Media Monitoring, which apparently was presented to UMC as a marketing firm. The other bogus business was a company called ATAM Technology Solutions.

The defendant submitted invoices to UMC on behalf of B.R. Media Monitoring. The hospital paid the bills, sending the checks to a mailbox the defendant had rented. The defendant also used a UMC credit card to make unauthorized payments and purchases. The defendant used these funds, in part, to pay Mata's travel, educational, entertainment, and personal living expenses.

The defendant resigned when UMC officials confronted him about the results of an internal audit that exposed the losses.

In a plea deal, the defendant pleaded guilty to one count of mail fraud against the hospital. The judge accepted the plea deal and ordered a presentence investigation. (A sentencing date will be set when that report is completed.) The maximum sentence for mail fraud is 20 years in prison, a fine of \$250,000, and a term of supervised release after the completed prison sentence. In addition, he may be ordered to pay restitution.²

¹Potential Scheme: False, Inflated and Duplicate Invoices. <http://guide.iacrc.org/potential-scheme-false-inflated-and-duplicate-invoices/>. Accessed June 11, 2013.

² Former Lubbock hospital VP pleads guilty to fraud. <http://amarillo.com/news/latest-news/2013-06-06/former-lubbock-hospital-vp-pleads-guilty-fraud>. Accessed June 12, 2013.

