First Friday Fraud Facts+

October 2, 2015

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:

Chris Floyd, CPA
Financial Specialist
P.O. Box 83720
Boise, ID 83720-0011

Phone: (208) 332-8814
Fax: (208) 334-3415
E-mail: cfloyd@sco.idaho.gov

Inside this issue:

Welcome	1
Billing Schemes	1
Red Flags	1
What You Can Do	2
Fraud Case	2

Welcome to First Friday Fraud Facts+ (F4+). This edition will discuss billing schemes.

Billing Schemes

Billing schemes are designed by dishonest employees to convince and manipulate their employer to approve an illegitimate invoice. The resulting payment is then recorded as an actual business expense and pocketed by the employee.

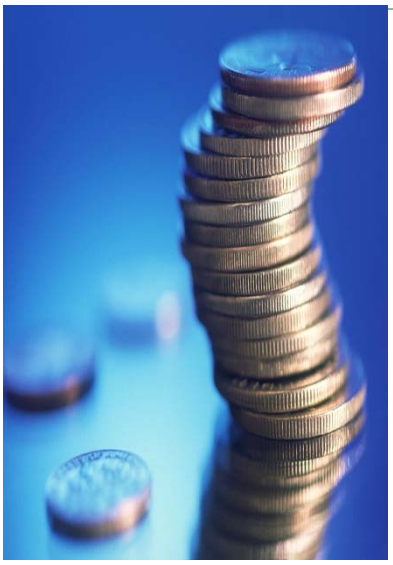
Four variables typically exist in a billing scheme:

- A new bank account is opened specifically for cashing fraudulent payments received (although a fraudster may use another cashing mechanism to avoid detection)
- A fictitious vendor name is created (often times similar to an existing, legitimate vendor)
- A false invoice is submitted to the employer (under the name of the fictitious vendor)
- The payment approval process is manipulated in some form (depending on the dishonest employee's specific responsibilities and/or influence)[1]

An employer can also fall victim to a billing scheme if a dishonest employee deliberately overpays an actual vendor invoice, and when the vendor returns the overpayment portion, the employee steals the refund. Another example of a billing scheme is when a dishonest employee intentionally processes a legitimate invoice twice. A couple of days after the original invoice is paid, the employee submits a copy of the original invoice for payment, and then manipulates the approval process. Once the vendor receives the duplicate payment, a refund check is subsequently sent back to the employer. The employee intercepts the refund check, forges the employer's endorsement, and cashes the check.[2]

Red Flags

Warning signs that could potentially raise suspicions, and possible alarm, include:



- Unknown vendors or vendor names with initials
- Invoices with ambiguous or significant consulting expenses above the norm
- Identical employee and vendor addresses
- Vendor bills received more often than what is considered normal
- Post office boxes used for vendor invoice payments[2]

What You Can Do

The following can help thwart billing schemes from occurring:

- Segregate the duties between agency personnel who order goods or services, approve purchases, and pay invoices
- Use pre-numbered purchase orders
- Verify post office box addresses used by vendors are legitimate
- Analyze vendor list for similar names[1]

Fraud Case

This fraud case involves a former IRS revenue officer in the collections division, convicted of embezzling almost $80,000 from taxpayers who thought they were paying their federal tax liabilities. As an experienced officer, the fraudster understood how the system worked and knew how to circumvent the system.

Jack Regan Stevens forged 13 taxpayer checks by altering the payee line made out to the 'IRS' and writing his name, 'JR Stevens'.

JR Stevens would then modify the IRS system, indicating the taxes, penalties, and interest owed by the taxpayer were satisfied. However, the government never actually received the money (his bank account did). After the checks were deposited into his personal bank account he used the embezzled money to pay off his large credit card debts.

His embezzling went unnoticed not only by banks cashing the altered checks but also by local IRS officials. The scheme unraveled when JR Stevens forgot to cover his tracks on one of the checks and didn't update the IRS system to show that the taxpayer's bill had been paid in full. Suspicions arose when the taxpayer's wife started having her wages garnished by the IRS for the 'unsatisfied' tax bill. The taxpayer contacted the IRS and learned that his $6,600 check was never applied to his tax liability. The taxpayer then contacted his bank, which discovered that the check had been altered and negotiated by someone other than the IRS.[3]

JR Stevens was ultimately sentenced to 7 months at a halfway house, 7 subsequent months of home detention, and ordered to pay full restitution.[4]

In other, similar cases, one IRS officer changed "IRS" to his initials of "ARS"; while another IRS officer changed "IRS" to "MRS" followed by her

last name. When writing checks to the IRS, taxpayers are encouraged to write "Internal Revenue Service" as the payee rather than the abbreviated "IRS".[3]

[1] Brisbane Chapter ACFE, "Billing Schemes—Cash Frauds" <http://brisbaneacfe.org/library/occupational-fraud/billing-schemes-cash-frauds/> Accessed May 12, 2015.
[2] GL Howard and Company CPAs, LLP, "Killing billing fraud schemes" <http://www.glhoward andcompanycpas.com/killing-billing-fraud-schemes/> Accessed May 12, 2015.
[3] Michael James, "Taxpayer checks paid IRS officer's credit-card bills 13 payments altered before forgery trick is discovered by bank", February 21, 1998, <http://articles.baltimoresun.com/1998-02-21/news/1998052078_1_ stevens-treasurer- check-cashier-checks> Accessed May 13, 2015.
[4] The Wall Street Journal, "Tax Report", June 3, 1998, <http://www.wsj.com/articles/SB896756512997880500> Accessed May 14, 2015.