SIG Alert #8: Fraud Conducted by Executive Branch Employees in FY 2013-2014

Agency Heads,

Attached is the SIG's first "Annual Report of Fraud Conducted by Executive Branch State Employees--FY 2013-2014."

For a branch of government executing a $24 billion budget with 58,000 employees, the frequency and total fraud losses in the Executive Branch are indicative of a high integrity work force. However, given our fiduciary duties, any fraud undermines the public's confidence in State government, particularly in today's 24/7 news cycle. I hope each agency uses the report to pat your troops on the back, but also leverage the report's data into a fraud awareness training tool with real life examples and lessons learned. Our greatest tool to prevent frauds or corrupt activity is raising the awareness of 58,000 pairs of eyes and ears & setting the expectation to report suspicious activity.

Thanks

State Inspector General's Annual Report of Fraud Conducted by Executive Branch State Employees Fiscal Year 2013-2014

The State Inspector General (SIG) tracks fraud conducted by Executive Branch employees to assist State agencies in their investigations; serves as an indicator of integrity within the Executive Branch workforce; and transparently reports to the public to maintain its confidence in the integrity of State government. At this time, the SIG does not track frauds conducted by third parties against the State, such as tax, Medicaid, pharmaceutical diversion, SNAP, or contract fraud, most of which are investigated by sworn law enforcement personnel residing in the respective State agencies.

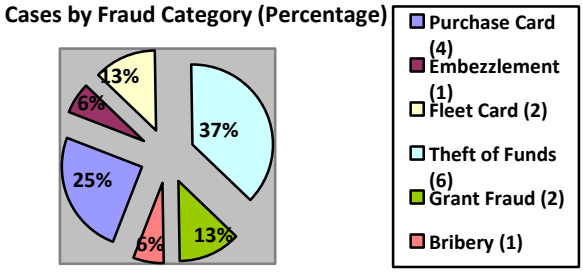
The SIG identifies this fraud through mandatory reporting by agencies to the SIG; reporting from SLED; agencies' annual reporting of fraud to the Comptroller General's Office; and open source reporting. In Fiscal Year (FY) 2013-2014, reporting identified 16 Executive Branch employee frauds from 12 agencies, which resulted in total losses of $543,590.34. The median loss was $326.33, with one fraud scheme causing a $414,976.68 loss.

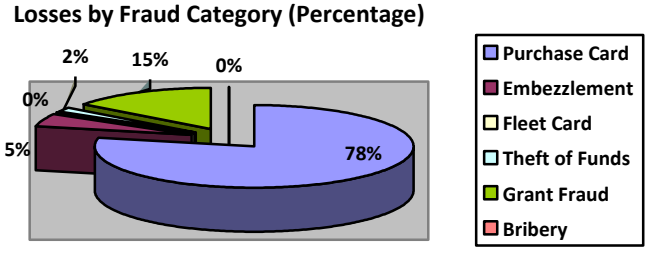
The breakdown of the fraud categories and associated losses is as follows:

Fraud Category	Number of Complaints	Fraud Losses by Category
Purchase Card Fraud	4	$425,669.86*
Embezzlement	1	$28,044.50
Fleet Card Fraud	2	$110.98
Theft of Funds	6	$9,765.00
Grant Fraud	2	$80,000.00
Bribery	1	$0.00**
TOTALS	**16**	**$543,590.34**

* One incident totaled $414,976.68

** State suffered no loss because scheme was disrupted by federal officials as a result of wiretap information.





Relevant observations from analyzing these frauds were:

- Purchase card (P-card) fraud, while accounting for only 25% of the reported fraud, contributed to 78% of the total fraud losses.
- Case subjects were 14 front line employees (88%), a supervisor (6%), and an executive (6%).
- The overriding primary internal control weakness identified in all six categories was ineffective supervisory oversight, often, where supervisors approved transactions involved in the fraud without being provided sufficient justification or asking logical questions about transaction irregularities.
- Secondary contributing internal control weaknesses included: (1) lack of inventory control; (2) failure to conduct timely reconciliation of P-card accounts by supervisors; (3) over-issuance of P-cards to end users, undermining the benefit of segregating the end user from the purchaser; and (4) failure to make timely deposit of funds.
- Frauds discovered by subject's work unit supervisor or co-workers (50%), external complaints (25%), internal audit department (19%), and law enforcement (6%).

The most illustrative "lessons learned" were gleaned from examining the largest fraud of $414,976.68 which involved multiple fraud schemes using a P-card. While this scheme occurred over a period of six years, the front-line employee exploited two significant gaps in the agency's financial control environment. First, the supervisor was insufficiently engaged in the work of his/her subordinate to understand the basis for the fraudulent purchases or just not paying attention when approving the subject's monthly P-card bills. Second, the best practice of separating the end user, the subject, from the actual purchaser was not followed. The subject was issued a P-card for convenience rather than need. Assigning a P-card to an end user operating independently in a remote location or making frequent low dollar amount purchases in the field is reasonable; but in this case, the subject was buying expensive computer components while stationed at the agency's headquarters. Failure of both of these basic financial controls provided the subject the opportunity to develop multiple fraud schemes, to include submitting fraudulent invoices for fictitious companies; over-purchasing items and selling the excess inventory; and the theft and resale of existing inventory.

Internal controls on finances are primarily designed to deter/prevent fraud, rather than detect fraud after the fact. Using the $414,976.68 P-card fraud case example, the subject was a long-term employee who was "trusted" by his co-workers and supervisors, yet the reality was he/she was blinking "red" as a fraud risk. Fraud risk has traditionally been assessed by looking at opportunity, pressure on employee, and employee's ability to rationalize the fraud. In this case, the opportunity was high as described by the missing controls; supervisory oversight and segregation of duties controls. The subject had enormous economic and family pressures. The subject resented that he/she was substantially underpaid. The point is employers are not good at discerning, much less predicting employees with high fraud risk, which underscores the need to diligently execute basic financial controls and avoid the temptation to solely rely on "trust" as a management control.

Another fraud committed by an executive during the FY pertained to a series of schemes conspired between an agency board member and multiple vendors, where the board member used influence corruptly to benefit his/her self-interest. This was only discovered through a federal wiretap, with the point of emphasis being corruption is incredibly difficult to identify with certainty in the normal course of business. There were no missing state funds; the benefits were "off-book" through kickbacks from vendors, which never leaves an audit trail. However, in this case, which is typical of government corruption, the corruption scheme in its entirety was not detectible, but snippets of the scheme were observed by co-workers that should have been reported, but were not, as highly suspicious or ethical issues. A common integrity control to address corruption is for an agency to place an affirmative duty on all employees to report suspected ethical or criminal conduct. This serves both as a deterrent and identification tool for corruption. Subjects know their actions, observable by co-workers create at least administrative liability for co-workers; which, in turn, increases the likelihood of co-workers reporting suspicious activity. Although this requirement is not contained in the State's ethical "Rules of Conduct," it can be added to an agency's code of conduct because the law allows agencies to promulgate policies that are more restrictive than the State statute's rules of conduct.

Fifty percent of the fraud cases were initiated based on co-worker or supervisory concerns. This is consistent with fraud research. This serves as a reminder that the best defense against fraud is providing employees with fraud awareness

training, which then creates eyes and ears throughout an agency to better discern potential suspicious activity that should be reported, as well as to deter those contemplating fraud opportunities.

In summary, with two exceptions, the residual 14 frauds reported during FY 2013-2014 were nominal in nature and indicative of Executive Branch employees operating in a high integrity environment given its $24 billion budget and 58,000 employees. However, the two exceptions should remind every Agency Head that even though the frequency of major frauds potentially damaging an agency's reputation and undermining the public's confidence are low in the Executive Branch, it happened twice during the past FY. State government agencies are essentially a part of a large partnership, where a negative event caused by one agency has the tendency to undermine the public's confidence in all State agencies. Given State agencies' position of trust and fiduciary responsibility to the public, any fraud, regardless of dollar loss, impacts the public's confidence in State government; and therefore, Agency Heads should be proactive in measures to reinforce financial controls. Ben Franklin's advice of "an ounce of prevention is worth a pound of cure" applies to following basic financial controls and fiduciary prudence.

ADMINISTRATIVE NOTE: The Vignettes describing the 16 frauds during FY 2013-2014 can be found at the following link: http://oig.sc.gov/Documents/Vignettes-Fraud%202013-2014.pdf