

First Friday Fraud Facts+

May 3, 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
Deception Detection	1
Deception Tactics	1
Fraud Case	2
Announcements	3

Welcome to First Friday Fraud Facts+ (F4+). This edition will cover deception detection and tactics.

DECEPTION DETECTION

Deception is a powerful form of information manipulation that occurs when an opportunistic person misrepresents the facts in order to negatively influence someone else. Left undetected, deception can cause decision makers to make assessments based on erroneous information. In order to detect deception, the elements of manipulation must be identified.

Why does deception work? Typically, the deceiver is intimately familiar with an organization's processes and procedures, which leads to two primary reasons for successful deception: 1) The deceiver works to exploit procedural weaknesses and 2) the deceiver understands the detection efforts that have been set in place and is able to employ a plan to circumvent those efforts. In essence, the deceiver uses the organization's own weaknesses and detection procedures against them.

DECEPTION TACTICS

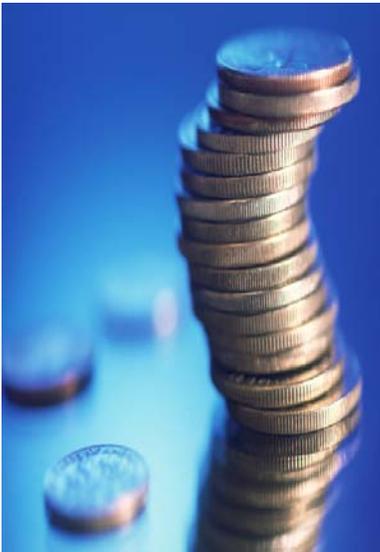
The deceiver will typically employ one or some combination of the following tactics:

Masking – Blocking or removing key pieces of information. (Example: Failing to record or disclose an expense or liability.)

Dazzling – Attempting to cause confusion. (Example: Disclosing information in the footnotes rather than in the body of the statements.)

Decoying – Focusing attention in the wrong direction. (Example: Emphasizing legal issues that turn out to be immaterial.)

Repackaging – Presenting information in such a way that it gets misclassified. (Example: Framing issues in such a way as to maliciously justify the use of favorable accounting procedures.)



Mimicking – Modifying the object or event so it looks like something else. (Example: Creating fictitious transactions.)

Double Play – Providing weak evidence so the object or event is dismissed. (Example: Improperly applying Generally Accepted Accounting Principles where an item is not individually material.)

Unfortunately, the deceiver understands how to bring failure into the process, making deception detection extremely difficult. However, learning more about the tactics these fraudsters use can help illuminate potential areas of weakness and improve internal control processes.¹

FRAUD CASE

See if you can identify the deception tactics used in this case.

In 2005, New York state auditors performed a forensic audit of the Roslyn School District near New York City and discovered that top district personnel had diverted more than \$11 million of district funds over a seven-year period. The district superintendent and chief financial officer were both arrested and charged according to their crimes.

District personnel concealed more than \$6 million in unauthorized disbursements by changing vendor names in the financial management system. When the auditors compared cancelled checks and system transactions they found the vendor names did not match. The checks had typically been written out to banks and credit card issuers while the accounting system reports showed the vendors for the same transactions as normal district suppliers.

Approximately 57,000 checks were written. Ledger entries, bank reconciliations, approved check warrants, and vendor files either didn't exist or were missing. District personnel bypassed the normal automated warrant process and issued hand-drawn warrants. The hand-drawn warrant process was meant to only be used for emergency circumstances. These warrants were processed outside the usual accounting office between normal semi-monthly payment cycles and did not go through any review by the Internal Claims Auditor. In addition, the state Treasurer had granted check-signing authority to the district secretary.

Senior district administrators had their salaries increased significantly to expand the salary base upon which their retirement benefits were calculated. Several senior officials received increased vacation accruals to enable larger cash payouts for unused vacation time upon retirement.

The audit revealed the following:

- \$5.9 million paid on at least 74 personal credit cards belonging to the district superintendent and his friends and family.

- \$1.25 million to related-party companies.
- \$1.1 million for private mortgages.
- \$600,000 to Home Depot; typical annual charges to Home Depot amounted to approximately \$4,000.
- \$580,000 in excess salaries and benefits to senior staff.
- \$200,000 in private automobile leases.
- \$130,000 in questionable travel reimbursements.²

¹Detecting deception: adversarial problem solving in a low base-rate world. <http://cse1.eng.ohio-state.edu/courses/ise818/papers/johnsonauditor.pdf>. Accessed March 11, 2013.

²The Forensic Audit: An Example from the Public Sector. <http://www.bus.lsu.edu/accounting/faculty/lcrumbley/jfia/Articles/FullText/2010v2n1a4.pdf>. Accessed March 11, 2013.

ANNOUNCEMENTS

Annual Closing Package Training held at the State Controller's Office:

Beginner

Wednesday, May 8, 2013, from 8:30 a.m. – 11:30 a.m.

Intermediate

Tuesday, May 7, 2013, from 1:00 p.m. – 3:00 p.m.

Thursday, May 9, 2013, from 8:30 a.m. – 10:30 a.m.

Beginning this year, attendees unable to participate in person can now participate in the training by connecting remotely from their computer using Adobe Connect. Please see the registration form for more details by visiting www.sco.idaho.gov, click Training, then Instructor-Led Courses, and then 2013 Closing Package Training Registration Form. If you plan on attending (whether in person or remotely), please fill out/select all of the required fields on the registration form, and submit by Friday, May 3, 2013.

