ARIZONA Auditor General
Making a Positive Difference

FRAUD PREVENTION ALERT

Data Analytics: Part 1
November 2017

Why are we issuing this alert?

Using data analysis techniques with risk-based assessments to identify trends, patterns, anomalies, and abnormal relationships in data can be an effective anti-fraud control. Regularly using these techniques on your organization's data and investigating findings can help your organization identify fraudulent activity before it becomes significant. This Fraud Prevention Alert, the first in a four-part series, describes the different data analysis techniques and outlines how public officials can help protect public monies by establishing proactive data monitoring and analysis programs to prevent and detect fraud. The three Fraud Prevention Alerts following this one will provide practical applications for using techniques from each of the three data analysis categories: basic, statistical, and advanced.

What are data analytics?

Data analytics are processes for examining quantitative or qualitative data to draw conclusions about the information contained therein. As applied to fraud detection, entities can use data analysis techniques with risk-based assessments to identify trends, patterns, anomalies, and abnormal relationships in data. Regularly performing these techniques on your organization's data can help identify fraudulent activity before it becomes significant.

Specific data analysis techniques that can be applied to data include, but are not limited to, basic techniques such as even-dollar amount, duplicate, and gap testing, and sequence validation; statistical techniques such as regression analysis and Benford's Law;[1] and other advanced techniques such as location and trend analysis. For example, using basic techniques, public officials could analyze accounts payable data for: adherence to financial limits; even-dollar amount transactions; and duplicate invoices or vendor numbers, and then investigate any findings by comparing data to source documents such as invoices, packing slips, and receiving reports.

The types of data analysis techniques include, but are not limited to:

- **Basic—**Even-dollar amount, duplicate, and gap testing, and sequence validation.
- **Statistical—**Regression and frequency distribution of data digits analysis.
- **Advanced—**Location and trend analysis.

Public officials could also employ statistical and advanced analysis techniques such as: comparing trends between current and prior year expenditures; matching data sets like employee and vendor files; performing location analysis on a patient's distance to a medical provider; performing statistical analysis such as regression tests; examining the frequency distribution of data digits such as Benford's Law; and other reasonableness testing.

After performing these techniques, initial findings could indicate fraudulent, improper, or erroneous activity. Therefore, knowledgeable and trained employees should perform timely investigations of findings and results should be communicated to management.

Proactive data monitoring and analysis can help prevent fraudulent activity

Public officials can establish data monitoring and analysis procedures to control how public monies are expended and thereby help protect against misspending and fraudulent activity. For example, our Office reported in June 2016

[1] Benford's Law describes the expectation that out of a collection of numbers, most will start with the number "1." The number "2" will be the next most common, then "3," and so forth at a predictable rate. Using a formula, $\log 10(1+{}^{1}/_{n})$, derived from this law to evaluate the first digit in a data set can indicate fraudulent, improper, or erroneous data.

that a state agency helped to prevent users from misspending public monies deposited in empowerment scholarship bank accounts intended for educational purposes.[2] Specifically, agency officials worked with the Arizona Office of the State Treasurer (Treasurer's Office) and the bank contracted to provide the empowerment scholarship bank accounts to deny the practice of making any cash withdrawals from these bank accounts, and took steps to automatically deny other transactions depending on the merchant category code (MCC).[3] Specifically, agency officials identified MCCs not generally related to education, such as fast food restaurants and lodging and hotels, and worked with the Treasurer's Office and bank to automatically deny transactions in these categories.

Additionally, our Office recommended that agency officials establish standard risk assessment criteria or factors to assess the misspending risk associated with empowerment scholarship bank accounts and expenditures. For example, the agency could use the criteria or factors to identify certain empowerment scholarship bank accounts, purchases, or merchants that are a higher risk for misspending and prioritize them for more timely review. Further, agency officials could use data analytics to compare empowerment scholarship account users' expense reports to the bank's system reports to identify amounts that do not reconcile and could be considered a high risk for fraudulent activity.

Proactive data monitoring and analysis can lead to the discovery of fraudulent activity and limit loss amounts

According to the Association of Certified Fraud Examiners' 2016 *Report to the Nations on Occupational Fraud and Abuse*, proactive data monitoring and analysis is among the most effective anti-fraud controls at limiting the duration and cost of fraud schemes.[4] Organizations that undertake proactive data analysis techniques experience frauds that are 54 percent less costly and are detected in half the time compared to organizations that do not monitor and analyze data for signs of fraud.

In fact, an Arizona university limited its losses when it undertook such proactive data monitoring, discovered an employee's fraudulent activity, and put a halt to it. In particular, during a university-wide review of purchasing card activity and MCCs, a university employee performed data analysis by comparing goods and services purchased with university purchasing cards to prior years' purchases. As a result, the university employee discovered $12,287 of unauthorized charges made in a 6-month period with an employee's university purchasing card that were associated with his personal business. Consequently, university officials terminated the employee and contacted our Office. We conducted an investigation and submitted our report to the Coconino County Attorney's Office, which took criminal action against the employee resulting in his indictment on six felony counts.[5]

Recommendations

To help protect public monies, public officials should establish proactive data monitoring and analysis programs designed to deter and detect fraud. Specifically, public officials should:

- Review all areas of operation and determine areas that may be susceptible to fraud, using a risk-based approach to prioritize the most vulnerable areas.
- Develop and regularly perform data analysis techniques to detect fraud in the identified areas.
- Investigate findings in a timely manner using knowledgeable and trained employees to interpret results.
- Communicate the results to management.

---

[2] See Office of the Auditor General, Performance Audit: *Arizona Department of Education—Department Oversees Empowerment Scholarship Accounts Program Spending, but Should Strengthen its Oversight and Continue to Improve Other Aspects of Program Administration*, June 2016, Report No. 16-107.

[3] National credit card companies developed a system that assigns a merchant category code such as 4900 utilities, 5311 department stores, and 5399 miscellaneous general merchandise based on the types of goods or services the merchant provides.

[4] Association of Certified Fraud Examiners, Inc., *Report to the Nations on Occupational Fraud and Abuse*, 2016.

[5] See Office of the Auditor General, Special Investigation: *Northern Arizona University—Theft and Misuse of Public Monies*, October 2016, Report 16-405.