City of Springfield
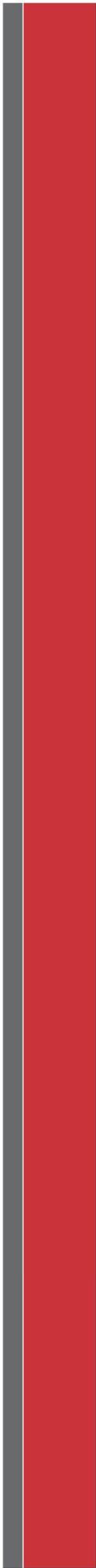
Report on Data Analytics Procedures – Analysis of Vendor and Accounts Payable Data

December 2, 2020

Contents

April 9, 2021

Mr. David Holtmann
Director of Finance
City of Springfield
218 E. Central
Springfield, MO 65801

We have performed data analytics procedures related to the employee, vendor, and accounts payable data of the City of Springfield (the City). Our work was limited in scope and not intended to be a complete review of all transactions, operations, and procedures. Therefore, our procedures would not necessarily disclose all improprieties or errors. The City's management is responsible for the design and implementation of programs and controls to prevent and detect fraud.

These procedures do not constitute an audit and, accordingly, we are not expressing an opinion on the City's financial statements. This report is limited solely to providing management with the results of the data analytics procedures for follow-up and makes no final representations as to conclusions of any potential improprieties, errors, or unusual transactions.

We have relied on information supplied to us in performing the analysis contained in this report. If additional information should come to our attention at a later date, our report could change. We reserve the right to modify this report if additional information is provided, but are not required to do so.

This report is solely for the use of the City's management and should not be used by any other party for any other purposes. This report is the property of **BKD, LLP**. If any party intends to publish or otherwise reproduce this report and make reference to our firm name, BKD must be provided with the printer's proofs or masters for our review and approval before printing or other reproduction and provided with a copy of the final reproduced material for our approval before it is distributed, including posting our report on any website.

We greatly appreciate the opportunity to assist with this project. Please let us know if you have any questions.

BKD, LLP

BKD, LLP

December 2, 2020

Data Mining Procedures

We are pleased to offer this report to the City of Springfield (the City), which outlines the data analytics services we performed related to your employee, vendor, and accounts payable data. The City provided us with employee master, vendor master, and accounts payable detail files (the "Files") in electronic format. A summary of these files is below:

Summary of Files

File	Applicable Date Range
Vendor master	As of June 30, 2020
Employee master – active	As of July 7, 2020
Employee master – terminated	As of July 7, 2020
Accounts payable detail	April 5, 2017 – March 27, 2020

The vendor master file contained 14,504 vendors. The employee master – active file contained 4,577 employees. The employee master – terminated file contained 998 employees who had been terminated between April 18, 2019 and June 25, 2020. Our analysis of accounts payable transactions encompassed 69,776 payment transactions with invoice level detail during the period April 5, 2017 through March 27, 2020.

We analyzed the Files to identify patterns potentially indicative of irregularities, errors, or fraud. We provided our results to management to review and research as necessary.

The procedures we performed, along with the risks assessed, are below:

	Procedure	Risks Assessed
Vendor and Accounts Payable Data	Identify employee/vendor matches and relationships	FV, CoI
	Identify vendor duplications and relationships	FV, DP
	Identify vendors with mailbox service addresses	FV
	Identify vendors with PO Box address	FV
	Identify vendors missing information	FV
	Identify employee/vendor proximity relationships	FV, CoI
	Digital frequency analysis of payments	IP
	Identify potential duplicate paid invoices	DP, IP
	Identify checks issued on a weekend or holiday	IP
	Identify unusual vendor payment trends	IP
	Identify gaps in the check sequence	UP
	Identify round-thousand dollar payments	IP

Risks Assessed Legend

FV = Fictitious vendor
CoI = Conflict of interest
IP = Inappropriate payments
DP = Duplicate payments
UP = Unrecorded payments

BKD
CPAs & Advisors

Analysis of Vendor and Accounts Payable Data

Our analysis of vendor and accounts payable data focused on identifying characteristics indicative of fictitious vendor, conflict of interest, inappropriate payment, duplicate payment, and unrecorded payment schemes. The remainder of this section summarizes the key results of our testing of vendor and accounts payable data and is not meant to be a comprehensive discussion of all procedures performed. We provided detail of our results to management for review.

Employee/Vendor Matching

Matches between the employee and vendor master files are common in fictitious vendor schemes. While it is normal for certain employees to receive payment as a vendor, *e.g.*, expense reimbursements, not all employees should necessarily be receiving these types of payments. Further, it is unusual for a corporate vendor to share attributes with an employee. These shared attributes may indicate a potential conflict of interest or fictitious vendor. For instance, an employee may find a way to add a fictitious company to the vendor master file and may use their home address as the vendor address. We identified employee/vendor matches and relationships based on the following attributes:

Attribute(s)	Description
Name or Tax ID, among others	Employee set up as a vendor
Any other than name or Tax ID	Employee related to a vendor

We identified 2,437 instances of an employee set up as a vendor. Further, we identified 343 instances of an employee potentially related to a vendor. This means there are a total of 2,780 potential employee vendor matches. Of these matches, we noted 14 vendors received total payments of at least $10,000.

Management Response

Finance Department staff reviewed all matches identified as high, medium, or low risk with payments totaling $10,000 or greater. Many of the matches were related to former employees who then performed contract work or contract vendors who then became employees. Employees are also being paid through the accounts payable process for reimbursements, travel, or settlements, which caused some of the matches identified.

Two potential policy violations were identified and referred to the City Attorney's office.

Vendor/Vendor Matching

Vendors related based on attributes such as name, address, and/or phone number are common in fictitious vendor schemes. They can also be indicative of internal control weaknesses resulting in the same vendor being included in the vendor master file multiple times, which can lead to accidental duplicate payments. We analyzed the vendor master to identify potentially duplicated or related vendors based on these, and other, attributes.

Attribute(s)	Description
Name, among others	Potential Duplicate
Any other than name	Potential Relationship

We identified 250 potential duplicated vendors. We identified 2,008 potential related vendors. This leads to a total of 2,258 potential duplicated or related vendors in the vendor master file. Of these matches, we noted 217 vendors received at least $10,000 in payments. We excluded address matches where the addresses matched on 840 Boonville, which is the Busch Municipal Building.

Management Response

Finance Department staff reviewed all high risk matches identified. No concerns were noted with the vendor matches reviewed.

Before a vendor is set up in the City's financial system, the business name and tax identification number (TIN) are checked with the IRS system. The payment address associated with a vendor must match the address on the invoice for accounts payable to pay it. An address is not changed in the system without a department request approved by a supervisor and proper verification from the vendor. In addition, employees who process accounts payable are not able to make changes to the vendor master file.

Vendors with Mailbox Service Addresses

When creating fictitious vendors, mailbox service addresses such as the UPS Store or FedEx office give the appearance of an established company at a legitimate business address. Although these services may be legitimately used by many businesses, mailbox services are frequently utilized in fraud schemes; therefore, we consider them to be worthy of additional attention. We compared the City's vendor master file to a database of over 36,000 mailbox service companies to identify vendors with an address matching one of these companies. We identified 77 unique vendors with an address matching a mailbox service. Sixteen vendors have an exact address and suite match or a vendor address including 'PMB' indicating a higher likelihood of the vendor utilizing the mailbox service.

Management Response

Finance Department staff reviewed vendors with exact address matches and a spend of greater than $100 as well as all medium risk vendors with the exception of the United States Postal Service, the top three low risk vendors, and the vendors identified by BKD as most notable. No concerns were noted with the vendors reviewed.

Vendors with PO Box Addresses

When creating fictitious vendors, addresses with only a PO Box give the appearance of an established company at a legitimate business address. Although these addresses may be legitimately used by many businesses, PO Boxes are frequently utilized in fraud schemes; therefore, we consider them to be worthy of additional attention. We identified 1,366 vendors with an address containing only a PO Box. We noted 36 vendors who received at least $500,000 in payments.

Management Response

Finance Department staff reviewed all high risk vendors and the vendors identified by BKD as the most notable. No concerns were noted with the vendors reviewed.

Vendors Missing Key Information

A name, address, taxpayer identification number, and telephone number are four basic pieces of information that should be required for each vendor set-up in the vendor master file. This information can help the City verify the existence of each vendor. Our procedures identified vendors missing these key attributes, as summarized below.
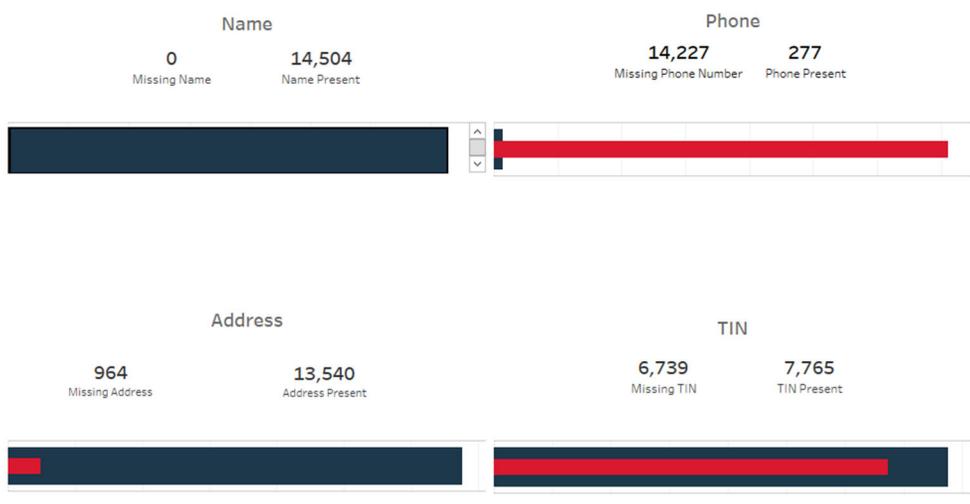
BKD observed that the missing addresses noted above are typically related to employees that are set up in the vendor master file for expense reimbursement purposes. While addresses for these employees are not contained in the vendor master file, there are addresses for these individuals in the employee master file.

BKD researched all vendors without a TIN receiving more than $20,000 in payments, noting that these vendors are typically employees (whose TIN is captured in payroll) or vendors that don't require a TIN.

Management Response

The vendor name, tax identification number (TIN), and vendor address are required for a regular supplier to be set up in the financial system. Additional information such as phone number, fax number, and email address are not required but are added if available. Purchasing cardholders are set up in the financial system as vendors to allow them to process their expense reports. These records do not have addresses or TINs associated with them. Employees set up as vendors for reimbursements or travel advances also do not have TINs associated with their records in the financial system.

Employee/Vendor Proximity Relationships

We analyzed the employee and vendor files to identify relationships based on geographic proximity. Proximity relationships are instances of a vendor's address located within a specified distance of an employee's address. Specifically, we focused on vendors located within one-tenth of a mile, approximately 500 feet, of an employee. We identified 3,391 vendors located near an employee. Of these 3,391 vendors, 43 vendors received at least 20 payments and had total payments of at least $30,000.

Management Response

Finance Department staff reviewed the vendors highlighted by BKD as the most notable. Many of the vendors highlighted were part of real estate transactions with the City. No concerns were noted with the vendors reviewed.

Digital Frequency Analysis of Payments

Benford's Law provides guidance regarding the expected frequency of leading digits in a set of numbers. In general, the lower digits should occur much more frequently than higher digits. In analyzing the accounts payable payment detail, we found the leading digits of three, five, and seven occurred slightly more frequently than expected. The detail of these payments were presented to management for review.

Management Response

Finance Department staff reviewed all high and medium risk vendors identified. No concerns were noted with the vendors reviewed.

Duplicate Paid Invoice Analysis

We analyzed the accounts payable detail file to identify instances of potential duplicate invoice payments. This analysis focused on the identification of duplicates based on key attributes related to the invoices: vendor, invoice number, description, amount, and invoice date.

BKD's analysis identified four potential duplicates sharing all five key attributes totaling $6,701.31. In addition, BKD found potential duplicates sharing four of the key attributes. We noted four instances of potential duplicates sharing vendor, invoice number, description, and invoice date totaling $19,635.32. We noted 17 instances of potential duplicates sharing vendor, invoice date, description, and amount totaling $62,905.55. We noted three instances of potential duplicates sharing vendor, invoice number, description, and amount totaling $3,000. We noted 38 instances of potential duplicates sharing invoice number, invoice date, description, and amount totaling $160,218.02.

Management Response

Finance Department staff reviewed a sample of the potential duplicates identified. One payment identified for the Art Museum was in fact a duplicate payment. The duplicate payment was made in September 2019 and corrected on a subsequent invoice in October 2019. No other duplicates were noted in the sample reviewed.

Checks Issued on a Weekend or Holiday

A payment issued on a weekend or holiday, if not consistent with normal business operations, can be an indication of fraudulent activity. We identified five checks issued on a weekend day totaling $86,902.88 during the period. Four of these checks were written on the same day: Sunday, June 1, 2019 totaling $86,717.58. Our procedures identified 91 payments on holidays totaling $1,167,090.24. Of these, 90 checks were written on New Year's Day totaling $1,161,820.24. Eighty-nine of the checks written on New Year's Day occurred in 2020.

Management Response

Finance Department staff reviewed all payments noted. The payments noted as being issued on a weekend day or holiday were actually issued on normal working days; however, the payment dates

associated with them in the financial system were a weekend day or holiday occurring on the first of the month due to how payments are posted.

Vendor Trend Analysis

Analysis of vendor payment trends can help identify unusual patterns of activity, such as an acceleration pattern. An acceleration pattern is one in which the vendor receives increasing payments across multiple periods (monthly, quarterly, etc.). We analyzed the activity for vendors to identifying these types of patterns. We identified nine vendors who received at least 10 payments totaling at least $10,000 exhibiting a 66 percent monthly and 66 percent quarterly acceleration pattern. We provided graphs of these vendors' activity to management for review.

Management Response

Finance Department staff reviewed the vendors identified by BKD as being most notable. Many of the vendors identified were contract labor for Parks facilities that have seasonal variances. A vendor used for Public Works and Environmental Services projects was also identified. The vendor worked on a project in 2017 and worked on additional projects in 2019 and 2020 explaining the increasing payments. No concerns were noted with the vendors reviewed.

Duplicate payment numbers

Of great concern are payment numbers issued on more than one occasion can indicate an attempt to obfuscate a fraudulent payment. Each payment number, whether check, EFT, wire, or ACH payment, should be used only once. We identified no duplicate payment numbers in the accounts payable detail.

Check gaps

A common fraud scheme is to issue a check to oneself, or a fictitious vendor, and either not record the payment in the accounts payable detail or delete it. Therefore, it is important to record all checks in the accounts payable detail and verify completeness. We analyzed the check sequences to identify any check numbers not contained in the files. We noted three check sequences for US Bank and identified 56 unique check gaps. Of these gaps, all but three had a gap of one check number, consistent with a single deleted payment. We identified three check sequences for Central Bank and noted 30 unique check gaps. Of these gaps, all but two had a gap of one check number.

Management Response

The check gaps of one number are related to overflow checks. The invoice numbers being paid are printed on the check stubs. If there are too many invoice numbers to fit on one stub, they are carried over to the next check stub and the next check number is not assigned. The other gaps identified are related to the bank change that occurred in 2019 and spoiled checks caused by printing errors. No concerns were noted with the gaps identified.

Round Thousands Payments

We analyzed the payment files for vendors with at least one payment in $1,000 increments and identified 363 such vendors. Fourteen vendors received at least 10 such payments totaling at least $10,000.

<u>**Management Response**</u>

Finance Department staff reviewed the 14 vendors with at least 10 payments in increments of $1,000 totaling at least $10,000. This group included the vendors identified by BKD as being most notable. No concerns were noted with the vendors reviewed.

Thank you for the opportunity to assist you with vendor analytics. We are happy to answer any questions you may have.