

The Village of Tinley Park

*Report on Fraud Risk Assessment
and Data Analytics Procedures*

March 5, 2018

Board of Trustees
Village of Tinley Park
16250 South Oak Park Avenue
Tinley Park, IL 60477

Thank you for the opportunity to provide consulting services to the Village of Tinley Park (the “Village”) in connection with the Board of Trustees’ (the “Board”) assessment of fraud risk. The procedures we performed were agreed to by the Board and were solely to assist the Board in assessing fraud risks.

Our services were provided in accordance with the Statement of Standards for Consulting Services promulgated by the American Institute of Certified Public Accountants and, accordingly, do not constitute a rendering by BKD or its partners or staff of any legal advice, nor do they include the compilation, review or audit of financial statements. We were not engaged to, and did not conduct an examination, the objective of which would be the expression of an opinion on the effectiveness of internal control over financial reporting. Accordingly, we do not express such an opinion. All procedures of the fraud assessment and data analytics were completed. Had we performed additional procedures, other matters might have come to our attention that would have been reported to you. Because our services were limited in nature and scope, they cannot be relied upon to discover all documents and other information or provide all analysis that may be of importance in this matter. The sufficiency of the procedures are solely the responsibility of the parties specified in the report. Consequently, we make no representation regarding the sufficiency of the procedures performed either for the purpose for which this report has been requested or for any other purpose.

This report is the property of **BKD, LLP**. This report is intended solely for the information and use of the Board and management of the Village and should not be used by any other party or for any other purpose without our prior consent. 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.

BKD, LLP

BKD, LLP

March 5, 2018

Project Summary

We are pleased to offer this report to the Village of Tinley Park (“Village”), which outlines the work we performed to assist the Board’s assessment of fraud risks. We performed forensic data mining services on the Village’s accounts payable, employee, payroll, vendor and general ledger files. The scope was expanded beyond the initial agreement to include current and former Trustees back to 2014 in our testing. We were then further requested to conduct testing of capital projects and the related requests for proposals/qualifications. Our services were for the period May 1, 2014, through October 31, 2017.

Overall, our procedures did not result in findings of inappropriate activity at the Village. The details of the procedures we performed and our results are discussed in the sections below.

Overview of Fraud in Government and Public Administration

Fraud committed by employees and other insiders poses a significant risk for organizations throughout the world, including government and public administration. Incidents of occupational fraud are so common, their occurrence is no longer remarkable. Results of a 2016 survey conducted by the Association of Certified Fraud Examiners (ACFE) published in the “Report to the Nations” estimates organizations lose as much as five percent of their yearly revenues to fraud, waste and abuse. This same survey also addresses the most common fraud in the government and public administration industries which are listed in the adjacent table.

As noted in the adjacent table, corruption and billing schemes comprise the majority of fraud in government and public administration. Corruption, as the term is used here by the ACFE, includes “A *scheme in which an employee misuses his or her influence in a business transaction in a way that violates his or her duty to the employer in order to gain a direct or indirect benefit (e.g., schemes involving bribery or conflicts of interest).*” In government and public administration, corruption includes an override of existing controls and overexertion of power by management of the Board. This project looked for instances of overridden controls and/or misuse of power. In conjunction with data analytics procedures, we conducted select testing of capital projects for adherence to bid budget and any potential conflicts of interest.

Industry/Scheme	Government and Public Administration
Cases	229
Billing	25.3%
Cash Larceny	7.9%
Cash on Hand	10.5%
Check Tampering	9.2%
Corruption	38.4%
Expense Reimbursements	15.7%
Financial Statement Fraud	7.9%
Non-Cash	14.8%
Payroll	13.5%
Register Disbursements	1.7%
Skimming	14.0%

Data Mining Procedures

The Village provided us with vendor master, accounts payable detail, employee master, payroll detail and general ledger 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 October 2, 2017
Employee master	As of October 2, 2017
Accounts payable detail	May 1, 2014 – September 22, 2017
Payroll detail	May 1, 2014 – September 29, 2017
General ledger detail	May 1, 2014 – October 31, 2017

The vendor master file contained 3,295 vendors. Of these, 3,291 vendors showed as active, and four were inactive. The employee master file contained 728 employees, which include part-time, full-time and retirees. Of these, 497 employees showed active status, 222 showed as inactive status, and 9 showed on leave status. Our analysis of accounts payable transactions encompassed 35,433 payment and invoice transactions during the period May 1, 2014, through September 22, 2017. In addition, the general ledger detail files, specific to revenue and expenditure accounts related to the General Fund, contained tens of thousands of lines of activity for the period May 1, 2014, through October 31, 2017.

In addition, BKD performed a search of social media and other internet sites for any potential matches/relationships between Trustees (including former Trustees) and Village employees or vendors. This search included a list of 20 current and former Trustees and mayors.

We analyzed the Files to identify patterns potentially indicative of irregularities (*e.g.*, conflicts of interest), errors or fraud. We provided our results to Ruth Gibson, Senior Accountant, for distribution amongst Village management for review and research as necessary.

The Village of Tinley Park // Report on Fraud Risk Assessment and Data Analytics Procedures

March 5, 2018

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

Vendor and Accounts Payable Data	Procedure	Risks Assessed
	Identify employee/vendor matches	FV, CoI
	Identify employee/vendor proximity relationships	FV, CoI
	Identify vendors missing information	FV
	Identify vendors with mailbox service addresses	FV
	Identify vendors with other unusual characteristics	FV, IP
	Identify payments to vendors not in the vendor master file	FV, IP
	Identify unusual vendor payment trends	IP
	Identify check and invoice sequence errors	IP, DP, UP
	Identify potential duplicate paid invoices	DP, IP

Risks Assessed Legend

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

Employee and Payroll Data	Procedure	Risks Assessed
	Identify potential duplicate employees	GE
	Identify employee relationships	GE
	Identify employees with mailbox service addresses	GE
	Identify employees with irregular fluctuations in hourly rate	GE, HM
	Identify employees with unusual/excessive hours	HM
	Identify employees receiving checks on nonpayroll dates	GE, IP

Risks Assessed Legend

GE = Ghost employees
 HM = Hours manipulation
 IP = Inappropriate payments

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, improper 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 an employee 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 relationships based on the following attributes:

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

We identified 97 instances of an employee set up as a vendor where the vendor received at least \$1,000 in payments on or after May 1, 2014. Further, we identified 17 instances of an employee potentially related to an individual set up as a vendor where the vendor received at least \$1,000 in payments on or after May 1, 2014. We identified three instances where the vendor was a business entity and the vendor received some form of payment on or after May 1, 2014.

Management Response

Management reviewed all matches provided and confirmed the reasons for employees being set up as vendors and the reasons for any employee/vendor relationships. The following summarizes the results of the review for the new instances:

- Vendor type of “O” indicates typically a reimbursement vendor or a refund vendor.
- For many years, the Village has issued reimbursements for conferences, travel, etc. to employees and for a time reimbursed employees for charges above a certain dollar limit for prescription reimbursements. This plan ended a year ago, but existed for many years as it was bargained in the police contract.

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 business entities located within one-tenth of a mile of an employee. We identified 370 vendors representing 627 payments to a business entity located near an employee residing in a residential neighborhood.

Management Response

Based on review of payments to the vendors, it does not appear that employees identified were related to the identified vendors.

Vendors with Mailbox Service Addresses

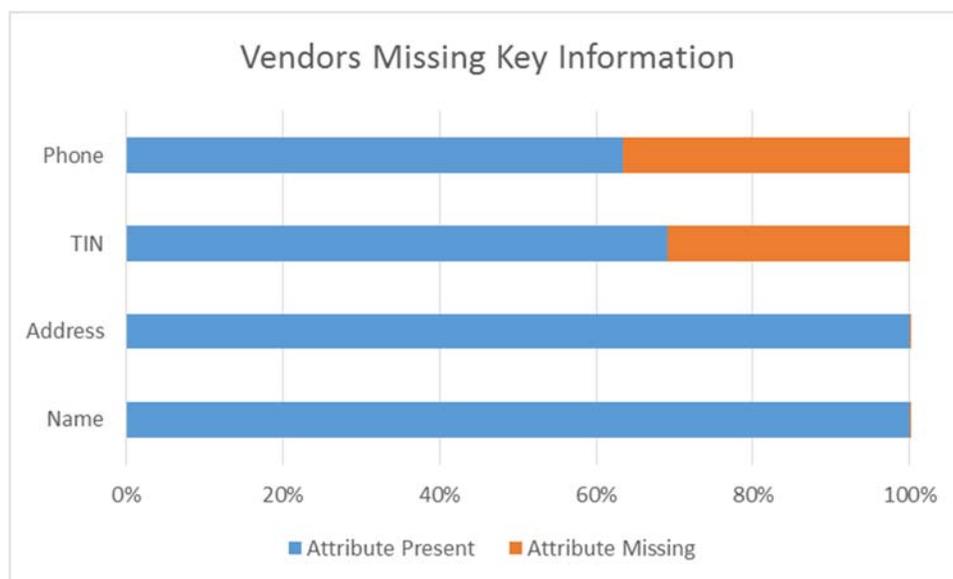
When creating fictitious vendors, mailbox service addresses give the appearance of an established company at a legitimate business address. Although these services may be legitimately used by many businesses, mailbox services are so frequently utilized in fraud schemes we consider them to be worthy of additional attention. We compared the Village's vendor master file to a database of over 11,000 mailbox service companies to identify vendors with an address matching one of these companies. We also searched the vendor file for addresses with an indication of "personal mailbox," another characteristic of a vendor using a mailbox service address. We identified 17 vendors with an address matching a mailbox service and receiving payments on or after May 1, 2014.

Management Response

Management reviewed all mailbox service matches provided, finding no exceptions.

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 setup in the vendor master file. This information can help the Village verify the existence of each vendor. Our procedures identified vendors missing these key attributes, as summarized below.



Management Response

Management reviewed and identified the reason for the missing information, noting no exceptions. “Every effort has been made in recent years to include all information and we will continue to stress this with our accounts payable staff. We make every attempt to obtain all EINs. Our normal process is not to release a check unless we have this information. Many of the vendors in this listing are “O” type vendors, which means they are reimbursement or refund vendors. If we issue a utility refund, we do not have the customer’s social security number. We also do not require this if we are issuing a documented expense reimbursement with all receipts attached. In the case of employees, in recent years Eden has created a field to link the AP vendor to the employee profile which contains all information, including social security number.” The Village has been obtaining all four attributes for vendors for the past year.

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. In addition, our procedures identified one check issued on October 13, 2014, (Columbus Day) for \$24,000, and 144 checks issued on November 11, 2016, (Veterans Day) totaling \$429,022.26. We provided the details of these payments to Village management for review.

Management Response

Management reviewed the schedule of checks issued on a holiday noting all checks were issued on Veterans Day or Columbus Day, which are scheduled workdays at the Village.

Other Accounts Payable Analysis

Other accounts payable procedures included:

- **Duplicate payment numbers:** Of great concern are payment numbers issued on more than one occasion, which can indicate duplicate payments. Each payment number, whether check, EFT, wire or ACH payment, should be used only once. We identified two 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 not record the payment in the accounts payable detail. Therefore, it is important to record all checks in the accounts payable detail. We analyzed the check sequence to identify any check numbers not contained in the files, finding numerous instances.
- **Round \$1,000 payments:** We also analyzed the payment files for vendors with at least one payment in \$1,000 increments and identified 143 such vendors.

Management Response

Duplicate payment numbers

“For check 167408, this check had three different invoices that combined for one check. As such, not a true duplicate, just the check number noted on all invoices. Similar situation for check 171757.”

Check gaps

Management reviewed the activity for each of the vendors identified and did not identify any unusual activity. The Village has multiple bank codes. In addition, some of the numbers related to credit card refunds where the Village utilized the gateway transaction number as the check number. Check numbers are all six digits, and the different bank codes have different check number ranges. All numbers are assigned by the software when checks are printed and posted. The Village has only blank check stock with no imprinted information. All checks are printed by the system as part of a check process and the computer does not skip check numbers. In some cases, the missing number is a voided check.

Round \$1,000 payments

Management reviewed all payment matches provided, finding no exceptions.

Duplicate Paid Invoice Analysis

We reviewed 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, amount and date.

BKD’s analysis did not identify any potential duplicates sharing all four key attributes.

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 reviewed the activity for all vendors, identifying vendors with these types of patterns. We identified 27 vendors with patterns of activity we considered unusual. We provided graphs of these vendors' activity to management for review.

Management Response

Management reviewed the activity of each of the vendors identified and did not find any unusual activity.

Analysis of Employee and Payroll Data

Our analysis of employee and payroll data focused on identifying characteristics indicative of ghost employees, hours manipulation and improper payment schemes. The remainder of this section summarizes the key results of our testing of employee and payroll data. We provided detail of our results to management for review.

Employees with Multiple IDs

Having employees with more than one ID in the payroll system increases the risk of ghost employees. For this reason, it is important to have strong controls around employee setup. We identified 10 potential instances of an employee with multiple IDs in the employee master.

Management Response

Management reviewed the identified ID numbers and confirmed that they are not duplicate employees. The Village payroll system processes payrolls for Tinley Park Public Library, Village of Tinley Park and Tinley Park Police Pension Fund. “When a police officer retires and then receives police pension, the Village does create a duplicate employee in order to process for the organization code of ‘Police Pension’.” All names appear to be valid employees at some point for the Village.

Employee/Employee Relationships

Employees related based on attributes such as address and/or phone number, are common in ghost employee schemes. We analyzed the employee master to identify potentially related employees, based on common address and/or phone number. We identified 60 pairs of employees related in some way, other than a common name, to another employee. We presented the list of these employees to management.

Management Response

All labeled with “Retiree” will be duplicates based on the reason stated in previous response above. “All others appear to have been or are employed by the Village.”

Employees with Mailbox Service Addresses

When creating fictitious employees, mailbox service addresses give the appearance of a legitimate address. Although these services may be legitimately used by individuals, mailbox services are so frequently utilized in fraud schemes we consider them to be worthy of additional attention. We compared the Village’s employee master file to a database of over 11,000 mailbox service companies to identify employees with an address matching one of these companies. We did not identify any employee with an address matching a mailbox service.

Employees with High Hours

In addition to analyzing the amount of pay by type, we also analyzed the hours recorded by type for unusual items. Specifically, we focused on regular, overtime and vacation hours. While these types of hours may vary, there should be consistency.

Based on the analysis of standard monthly employees, the expected regular hours are 7,978 for the period May 2014 through October 2017. We identified 11 employees with more than 7,978 hours and presented them to management.

Our analysis of overtime hours indicated a high-end expectation of 880 overtime hours during the Period. We identified seven employees with more than 880 overtime hours during the period and presented them to management.

Finally, we analyzed vacation hours based on an accrual of 20 days at eight hours per day, per year. This resulted in an expected maximum vacation hours of 540 hours during the Period. We identified 86 employees with more than 540 vacation hours during the period and provided them to management for review.

Management Response

Employees with high regular hours

“All meter readers are paid per meter. What appears as their hours is actually the number of meters they have read. The rate per meter is \$0.40 per meter read. This is also compared to their hours worked to make certain that the Village has complied with FLSA overtime standards.”

Employees with high overtime hours

Management reviewed, noting all listed were police officers and appeared reasonable.

Employees with high vacation hours

Management reviewed and all appear to be long-time employees. “Vacation for all non-police employees award on their anniversary date and, per Village ordinance, increases with number of years worked.”

Employees Receiving Checks on Nonpayroll Dates

One of the benchmarks of payroll processing is a routine schedule. This sets a firm expectation of the dates of payroll check issuance. We analyzed the payroll detail file to identify any checks issued “off-cycle.” In total, we identified 21 instances of checks being issued on nonpayroll type days, totaling 29 checks. We provided detail of these checks to management for review.

Management Response

Management reviewed the identified payroll checks, finding no exceptions. “These off-cycle payroll checks were issued primarily for severance and final checks to terminated employees.”

Capital Projects

As part of our procedures, we performed transaction testing related to various departments, selecting a total of 12 capital projects. We then evaluated the projects for adherence to bid budget and indication of potential conflicts of interest.

We were able to obtain all relevant supporting documentation for each tested project, including bid packet and recommendation documentation (to the extent relevant) related to these projects. As a result of the testing, we noted four projects for which the actual costs exceeded the known bid amount. The actual costs did not significantly exceed the known bid amount for these instances. The largest variance was approximately \$4,000, or five percent, over bid.

In addition, as part of our data analytics procedures, we noted Robinson Engineering and Airy's Inc. had historically provided contributions to mayoral/trustee campaigns. Robinson Engineering was the bid consultant for most of the selected projects in our capital project testing for which bid packet information was available. However, in assessing Robinson Engineering's invoices, we did not note any instances of excessive billings related to these projects. Airy's Inc. was the vendor involved in two of the projects (both lift station projects) in our testing. In each, Airy's Inc. was selected as the bid winner as they were the lowest bidder. Further, we noted in both instances the final projects costs were under the bid amounts. In fact, in one of the projects, the final cost was under the winning bid amount even though it involved a significant, authorized change order. In none of these instances did we note an indication of personal, economic or financial interest to the Mayor or members of the Board of Trustees for the period tested (2014–2017).

Conclusion

As previously mentioned, based on these procedures, we did not find indications of inappropriate or unauthorized activity. Further, we did not find indications that Trustees or the Mayor misused their influence in business transactions in a way that violated their duty to the Village in order to gain a direct or indirect benefit during the period tested (2014–2017).