neewee
DATA » ANALYTICS » INSIGHTS

www.neewee.in

Procurement Fraud Identification & Role of Data Mining

Suyog Joshi, Neewee Analytics

The paper describes the known boundaries of Procurement Fraud and outlines the scope of data mining within the same. The paper also highlights some of the basic steps to be taken care of before the application of Data Mining algorithms on the identified procurement data sets

Introduction

Some of the most impacted business functions due to fraud are Banking, Payroll and Procurement. The Institute of Internal Auditors (IIA)[1] defined fraud as follows

"[a]ny illegal act characterized by deceit, concealment, or violation of trust. These acts are not dependent upon the threat of violence or physical force. Frauds are perpetrated by parties and organizations to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage" .

The above is an industry standard definition and serve as guidance for the entire auditor community auditing the frauds. The specific definition of procurement fraud defined by CPA Handbook and underlined by Paul Zikmund [2] is as follows

"Unlawful manipulation of the process to acquire goods or services to obtain and unfair advantage" (CPA Handbook on Fraud) [2]

Whereas, Wikipedia defines procurement fraud in following terms
"Dishonestly obtaining an advantage, avoiding an obligation, or causing a loss to public property or various means during procurement process by
Public servants, contractors, or any other person involved in the procurement" [2]

Fraud is a known phenomenon in the industry and causes substantial losses to the organizations.
2014 ACFE Fraud Survey [3] shows

- Typical organization loses 5% of the revenue to Fraud
- Estimated $3.7 trillion in fraud losses
- Median loss = $145K; 22% cases involved Fraud more than $1 Million
- Median Duration of 18 months before detection
- 23% reported fraud = billing schemes
- Risk areas - Processing transactions, Purchasing and non-cash misappropriations
- Vulnerable Industries — banking, government and manufacturing

Leonard W.Vona [4] identifies following fraud categories for the procurement function.

- Employee in collusion with a vendor
- Vendors in collusion amongst themselves
- Vendor alone
- Employee alone
- Directed by the customer of a cost-reimbursable contract.
- Foreign corrupt practice issues

This subject is very vast and covers lot of aspects which are not possible to be covered in this paper. We will provide only a high level overview so that the reader gets a picture of the various schemes which are considered as frauds under the procurement audit. Some of the common schemes are listed as follows

Conflict of Interest – This involves using of the authorized position to award a contract in return of the personal gain for self or family

Favored Vendor – Repeatedly favoring a vendor by awarding contract in return for some personal gain by rejecting the other bids

Phantom vendor - Employee establishes a fictitious vendor and submits false invoices for payment (or invoice may not exist to support payment)[5]

Split POs – Putting up multiple Pos below the control thresholds to avoid the bidding or approval

Personal purchases – Employee ordering the commodity for personal use or for resale

Duplicate payments – Issuance of duplicate payments with minor tweaking in Invoice numbers dates etc.

Defective products – Compromise in the quality of the product stated in the contract

Product substitution – Substitution of a product by equivalent product but not stated in the contract

Fictitious invoices – Fake Invoices with valid PO numbers

Bribery, Kickbacks and Extortions – All these measures to get the contract awarded

FCPA - Foreign Corruption Practices Act

Bid rigging (Bid Avoidance, Sole Vendor etc.) – Ways to avoid the bidding process for awarding the contract

Vendor Selection – Corrupt practices to allow certain vendors to be part of the vendor panels

Management Override – Intervention by management to award a contract to a vendor overlooking all the set processes

Progress Payment Frauds – This scheme involves invoicing by showing false progress card for a particular deliverable

Cost Mischarging – This is a vast area and involves various use cases. Some of the common are a) Charging expenses not mentioned in the contract b) Over charging expenses mentioned in the contract c) Overcharge to due unintentional/intentional interpretation of the contact.

These are some of the schemes which auditors have found most common amongst the procurement frauds. This list is by no way exhaustive. In the next section, we will see where the data mining routines can be applied.

Role of Data Mining in Fraud Detection

As you can see in the earlier sections, the scope of Fraud detection is quite vast and it is not possible to have data footprint for each of the transactions. The probability of the identification of frauds increase if we have the data available but in some of the case like corruption, vendor selection which are out of purview of data capture it is not possible to employ the data mining algorithms. There are some limitations where data mining is rendered ineffective in spite having the data elements. Such cases are contracts or documentation where you need insight into the business to identify the frauds. The data mining is very effective when you have missing data elements, unusual patterns etc.

The data mining is extensively used by auditors to locate or red flag the suspicious transactions. The auditors need to have a closer look at these red flagged transactions to determine if it is a fraud or not. Leonard W. Vona has specified some of the basics fundamentals group rules for the data mining algorithms to locate fraud

Understanding the ‘‘what,’’ ‘‘where,’’ and ‘‘how much’’ of data

This happens to be the first step where identification of data sources, data volume and data elements is done. This is the first basic step before we start building the routines.

Mapping the data fields to the fraud scenario

This is the next logical steps where all the data elements once identified, we identify the fields to be looked closely, calculations to be done and identify the derived fields.

Understanding the integrity of the data.

This step can be clubbed together with Step 1 and 2 where we understand the granularity of each data set and identify the normalization to be done to ensure all the data elements are integrated at correct grain.

Applying inclusion/exclusion theory

This step is about identification of logical groups which needs to be included or excluded. For example, for certain set of use cases you would want only data from North America to be included. Such inclusions/exclusion based on the logical grouping needs to be done.

Understanding false positives

Not every red flag transaction is a fraud. Hence it is important to get to know the known exceptions and exclude them from the routines so that auditor can save time.

Understanding the ‘‘norm’’ of the data

For anomaly detection algorithms, it is important to understand what is normal to come out with an analysis of abnormality and make changes in the configurations. This needs to be done before you start the run of your anomaly detection algorithms

Data correlations

Data correlation is an important aspect to developing effective search routines and analyzing the results of those routines. It is the process of making a connection between the fraud data profile and either an entity or an individual. While there are no absolutes, the key in data mining is correlating the data pattern to an entity structure and the related dollars.

Entity structures and search routines

Before start of the run, it is important to make a decision if we want to run the algorithms on all the entities or only for the active entities. In that case there is a need to filter out the entities which are no longer active for last predetermined time frame.

Typical Data Mining Algorithms Red Flags

- Unauthorized vendors or created by Employees
- Payments under control level
- Anomalous pattern in vendor spending
- Duplicate payments
- Outlier payments
- Phantom addresses
- Invoices paid with same date or range
- Duplicate or variants of vendor names, ids

These are some of the important outputs which Data mining algorithms will throw out. All these red flags need to be scrutinized closely before a decision is made if any of these transactions are indeed fraudulent.

Summary

The paper examines the boundaries of the procurement fraud area and highlights the areas of applicability of data mining algorithms. The fundamental steps in the applicability of the data mining routines is explained at high level and some of the important red flag areas of the data mining routines are provided. The reader can do a deep dive in each of these areas for further expertise in order to build the routines.

References

[1] www.theiia.org

[2] Definitions provided by Paul Zikumd, Leading Procurement Fraud Auditor

[3] http:// www.acfe.com

[4] Leonard W.Vona, Leading auditor in Frauds area

www.neewee.in
+91 804 202 4519
Contact@neewee.in