ARBUTUS

Finding Fraud at a Fortune 500 Company

About Luminescent

Luminescent Inc. is a consulting firm based in Minneapolis, MN, focused on forensic accounting, governance and financial integrity. The firm has performed hundreds of forensic accounting engagements involving concerns of fraud, non-compliance, and business disputes. Their competitive advantage is an ability to analyze large, complex datasets.

Fraud or Oversight?

Recently, accountants at a Fortune 500 company* discovered a large variance in a General Ledger (GL) account. Evidence suggested a particular vendor had been overcharging the Company, possibly for years.

Faced with millions of transactions to sift through, the Company's legal team decided to bring in external forensic accounting firm Luminescent Inc. to assist with the investigation. Luminescent has differentiated itself from other forensic accounting firms with its expertise in analyzing transactions to detect anomalies and identify key risks in procurement and other business processes.

"When the Company contacted us, they admitted straight off that they weren't even sure if they were actually victims of an overcharge, and if so, whether it was intentional, human error or system error," said Mike Mumford, Managing Director, of Luminescent. "It was an incredibly complex case, spanning years of transactions of all sizes, and to make matters even more challenging, a third-party logistics company was involved in the procurement process."

"But this is quite typical of the vast majority of fraud cases we've seen. Rarely is there ever a smoking gun, like an email where someone spells out exactly what they're up to. It just doesn't happen like that in the real world."

Processes and Systems Invoived in Questioned Purchases

Luminescent's role in the investigation began with an examination of the daily processes and systems in place between the Company, Logistics and the vendors, which included no fewer than eight steps.

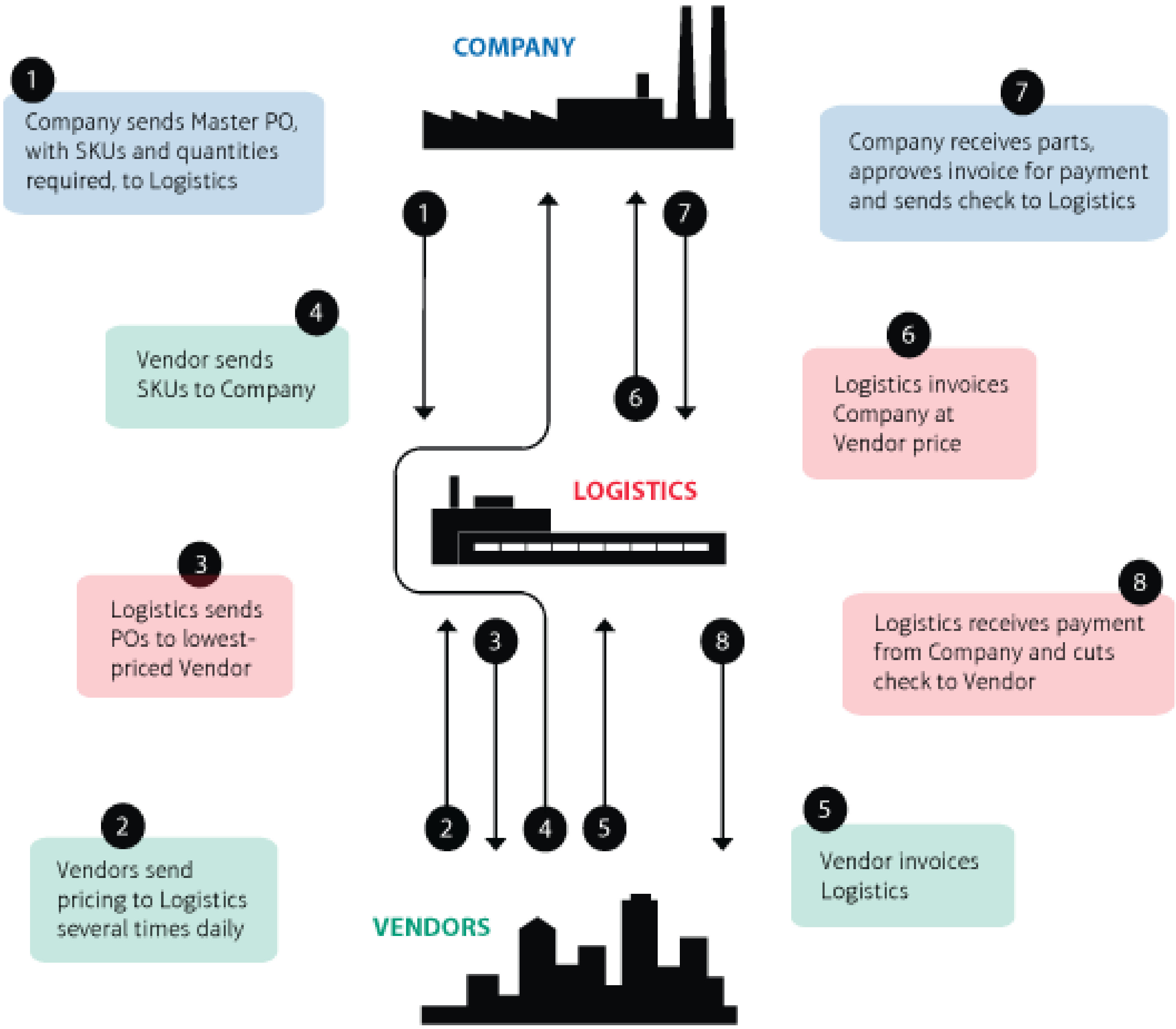
"We required a deep understanding of the processes and systems involved to understand what data was created each day," recalls Mumford, "from determination of need through ordering, receipt and payment."

** Company names withheld by request.*

ARBUTUS

Finding Fraud at a Fortune 500 Company

PROCESSES & SYSTEMS INVOLVED IN QUESTIONED PURCHASES



1 Company sends Master PO, with SKUs and quantities required, to Logistics

2 Vendors send pricing to Logistics several times daily

3 Logistics sends POs to lowest-priced Vendor

4 Vendor sends SKUs to Company

5 Vendor invoices Logistics

6 Logistics invoices Company at Vendor price

7 Company receives parts, approves invoice for payment and sends check to Logistics

8 Logistics receives payment from Company and cuts check to Vendor

Finding Fraud at a Fortune 500 Company

Data Acquistion Challenges

Next, Luminescent obtained data layouts and data definitions for each of the systems, then identified the tables containing the data fields that might provide insight into the transactions. In cases like this, Mumford and his team prefer to obtain all data fields in a relevant table, if possible.

Although there are generally more data fields than they will have an immediate specified use for, obtaining all fields eliminates the need to go back for additional fields if unanticipated analysis is later required.

Acquisition of the data had challenges:

- The data resided on three systems, including Oracle, plus two that were proprietary. Joining the Oracle data required creating a new key field.
- Luminescent could not take the data from the data warehouse because of potential evidentiary issues, so data had to be taken from the live system. In one case, they had to reload data from tapes.
- Size and format of the data tables: one system included lengthy fields, that, if exported in a flat file format, would be huge, so they used pipe delimited.
- Finally, they had to make sure the data wasn't corrupted in the process.

The data acquired was extensive. It included data tables from Logistics containing vendor price lists, POs and invoices of various kinds, as well as A/P and payment data. They also acquired similar data from the Company, as well as GL data related to the variance account.

"We then entered all this data into Arbutus Analyzer," said Mumford. "The flexibility of the technology allowed us to import multiple data files in multiple formats from multiple sources and then normalize it for further analysis."

"From an evidentiary perspective, Analyzer is ideal," added Matt Storlie, Data Analytics Practice Leader. "Because it operates in read-only format, the original data cannot be corrupted. Since you can add virtual columns at any time, you don't have to worry about physically altering the data, as you do in Microsoft Excel or other spreadsheet software."

"In this particular case," explained Mumford, "the command and result tracking in the Log was also key in helping us document every step of the analysis. And if, later on, you couldn't recall how you created a particular analysis, you could just go back and look at the Log, making that feature a real time-saver."

Procedures & Analysis

The next step for Luminescent was to design procedures. First, they analyzed the data trail back from the GL account which held the original variance, a process which identified one particular vendor as the source of the majority of the variance. Next, they analyzed every one of the suspected vendor's transactions to understand how the variances occurred. Finally, they analyzed all the other vendors' transactions to detect other irregularities, if any.

"We used Analyzer to analyze things such as the number of transactions, including dollar amounts, by vendor, in total, over time, first by year, then by month," said Mumford. "We then looked at the different SKUs by vendor and by price range. Analyzer simplified the process and shortened the time needed to complete this stage of the investigation."

"From an evidentiary perspective, Analyzer is ideal. Because it operates in read-only format, the original data cannot be corrupted. Since you can add virtual columns at any time, you don't have to worry about physically altering the data, as you do in Microsoft Excel or other spreadsheet software."

Matt Storlie,
Luminescent Inc.

Finding Fraud at a Fortune 500 Company

"Joining and comparing different datasets at a transaction level was a breeze. By identifying which transactions were matched and which ones in each system weren't matched, we could compare the attributes of each transaction. "

By joining the General Ledger data to the Company's PO data, they were able to identify how the variance had occurred and which transactions caused the variance. Once the variance transactions were identified, they sought to understand which vendors were affected; how the variance transactions differed from the non-variance transactions; and what caused them to be recorded as a variance.

"With this information, we were able to identify where in the process the anomaly occurred. This would be the initial focus of the analysis of how the variance occurred and whether it appeared to result from fraud or had some other explanation."

Proving Intent

"Since we were working just with data at this point, we would only be able to find circumstantial, or indirect, evidence of intent," said Mumford. "We have never yet had a case where there is direct evidence, such as an email mentioning the fraud by name."

"Fraud also requires proving the acts were intentional," explained Storlie. "Intent is in a person's mind, and since you can't read a person's mind, you have to illustrate through their actions what they were intending to do. Illustrating something that happened only once won't provide a lot of insight into a person's intent. Most one-time acts can be explained away as unintentional mistakes, but if you can demonstrate that the same thing happened, say, 20 times, it suggests the parties may have intended to do it this way."

However, even if something occurs 20 or 100 or 1,000 times, an experienced fraud investigator will not, with that evidence alone, end their analysis at that point. Other possible explanations include such things as a glitch in the computer system; an honest mistake repeated over time; a failure of controls; or a change in systems. This is why investigators of financial integrity like those at Luminescent dig a little deeper to see if anything else stands out with the possibly fraudulent transactions, such as comparing them with a large dataset of non-fraudulent transactions. This requires examination of the complete universe of data, and this, again, is where Analyzer helps.

Luminescent's analysis focused first on the vendor whose transactions were the cause of the variance. This helped determine that the variance was caused by a difference between the vendor price list and the invoice price from the vendor; a difference that did not occur at Logistics or at the Company.

Identifying Patterns in Data

Patterns within data can be used to illustrate intent. Some of the patterns identified in this case included:

- Growth over time, from a few hundred transactions in the first year, to thousands each successive year
- Growth in the percentage of variance transactions
- Short-term alterations in the pattern, including a week here or there, where there were no anomalous transactions - suggesting the perpetrator could be on holiday or out of office
- Transactions using the same SKU at the same time but different invoice prices
- Orders of large quantities of a SKU invoiced at inflated prices, while orders placed at the same time for single or small quantities of the same SKU were invoiced at prices from the price list

"The flexibility of the technology allowed us to import multiple data files in multiple formats from multiple sources and then normalize it for further analysis."
Mike Mumford,
Luminescent Inc.

Finding Fraud at a Fortune 500 Company

Luminescent's experience with cases like this taught them that when analyzing patterns, it is important to analyze the entire dataset. The scripting of the analysis is the same, whether it's for a long or short period, but it generally takes a little extra time to run it against the entire dataset. However, because Arbutus technology can analyze data of limitless size, this wasn't a stumbling block for Mumford's team.

Looking at the entire dataset also assists in determining when the fraudulent activity began. By comparing what was normal prior to the suspect activity, and looking for other explanations or changes over time, evidence like this can also help prove if the suspect acts were intentional or not.

The scope and dollar amounts of fraudulent activity are also important, but in ways that may seem counter-intuitive: For one, many frauds are focused on frequent smaller transactions, since they are generally subject to less scrutiny. And second, since frauds generally start small, then grow, you cannot exclude smaller dollar transactions, as you'll risk missing the development of the pattern.

Legitimate vs. Suspicious Transactions

A best practice that Luminescent employs in a fraud investigation is to compare data or transactions from trustworthy vendors with data from the suspect vendor, looking for 'normal' patterns in those vendors' transactions.

It can also be extremely beneficial to compare transactions within the suspect vendor's dataset to root out anomalous invoicing activity. For example, Luminescent learned from an email that the subject vendor CEO was generally absent on Fridays. Analysis revealed that anomalous transactions rarely occurred on Fridays, further cementing the criminal case against the accused.

Reporting & Presentation

"When it came time to determine the financial impact of the fraud, it wasn't sufficient to extrapolate the total amount; we calculated it precisely, transaction by transaction," explained Mumford. "We then used Analyzer to produce the data results, then exported them seamlessly into Excel for presentation."

Summary

Recoveries to the Company resulting from the investigation were in the multi-millions of dollars. Further, evidence developed using Arbutus Analyzer was presented in court, where the CEO was convicted and sentenced to federal prison.

"Analyzer offered the capabilities and speed necessary to define and analyze each and every transactional record from various data sources, encompassing millions of records," said Mumford. "Because Analyzer operates in read-only format, and therefore maintains the integrity of the source data, we were able to create virtual columns, so we could normalize data for deeper analysis into complex data relationships."

With built-in commands designed to quickly and easily provide profiling, counts, totals, and categorizations of relevant data, and the ability to compare and join every record to identify and measure key variances, Analyzer was key in helping Luminescent provide answers in this case.

Contact Arbutus to request your free 30-day evaluation of Arbutus Analyzer.

> "Analyzer offered the capabilities and speed necessary to define and analyze each and every transactional record from various data sources, encompassing millions of records."
> *Mike Mumford,*
> *Luminescent Inc.*

Based on 25 years of innovation excellence, Arbutus delivers the very best in purpose-built audit analytics technology to meet the exacting demands of today's business environment. Auditors, business analysts, and fraud investigators rely on Arbutus to enhance their testing, analysis and compliance capabilities.

ARBUTUS SOFTWARE INC.
#270-6450 Roberts Street,
Burnaby, BC V5G 4E1 Canada

Toll Free: 1.877.333.6336
T: 604.437.7873 | **F:** 604.437.7872

General Inquiries:
info@ArbutusSoftware.com
Technical Support:
support@ArbutusSoftware.com

ArbutusSoftware.com