APEX
FORENSIC SERVICES
ACCOUNTING EXPERTS

Supply Chain Fraud

A Guide to Detection and Prevention

By

Jeffrey Harfenist

August 2022

Introduction

Supply chain fraud exposes companies to substantial losses and potential liability. In its 2020 annual Report to the Nations, the Association of Certified Fraud Examiners estimated that companies lose approximately 5% of their revenues to fraud each year. When applied to gross worldwide production in 2019 of $90.5 trillion, this amounts to roughly $4.5 trillion in annual fraud losses. Additionally, in instances where bribes are funneled through third parties, the losses are magnified by the liability and penalties associated with violating anti-corruption statutes.

Asset misappropriations are the most common tactic perpetrators use to defraud their employers, with fraudulent disbursement schemes comprising an overwhelming number of cases. Interestingly, the top 2 methods used to conceal these fraud schemes include:

- Creating fraudulent supporting documentation, and
- Altering actual third-party supporting documents.

This paper examines how companies can apply various forensic protocols and utilize specialized data mining tools to identify fraudulent disbursement schemes in their infancy. These tools allow mitigating steps to be taken promptly and halt the outflow of critical cash resources.

Supply Chain Fraud

Supply chain fraud is on the rise. Driven by various schemes, it is being perpetrated by employees, vendors, third-party facilitators, and service providers. Supply chain fraud occurs throughout the procurement lifecycle from the initial stages when new vendors are approved to purchasing decisions made by individuals with undisclosed conflicts of interest. The ways that supply chain fraud occurs are varied and may include:

- Kickbacks from vendors resulting from overpayments,
- Payments to Ghost Vendors and Employees,
- Transactions to fund bribes,
- Excessive rebates and discounts,
- Evading tariffs by concealing a product's country of origin, and
- Disbursement fraud, including transactions where commensurate value is not received for payments made.

The following section focuses on disbursement fraud, followed by several case studies involving sophisticated schemes conceived by company insiders to funnel millions of dollars into their pockets.

Fraudulent Disbursement Schemes

Fraud involving disbursement schemes are typically initiated by one or more internal personnel[1], and to a lesser extent, external parties. It is more common for the fraud to involve the purchase of services as opposed to goods; however, both pose the risk of significant losses. Services present a unique forensic challenge when analyzing their propriety after the fact. Unlike the purchase of hard assets, it may be difficult to verify their delivery.

Most procurement frauds that Delta's experts have investigated fall into one of the following categories:

- Purchases where no value is received in return for payments made; and
- Purchases where commensurate value is not received in return for payments made (i.e., overpayments).

Most companies employ a combination of policies and controls to mitigate the risk of the scenarios above from occurring. Performing due diligence during the vendor onboarding process is a widely used tactic; however, this approach fails to identify critical areas of significant risk including beneficial ownerships and conflicts of interest with company insiders.

The principal risks associated with undisclosed conflicts of interest arise primarily in cases where an employee influences the vendor selection, onboarding process, or purchasing decisions. While most companies have policies requiring that employees disclose conflicts of interest, those intent on defrauding their employers rarely make such disclosures.

Likewise, due diligence relies on a combination of disclosures by the prospective vendor, and searches of third-party databases that seek to identify high-risk attributes. While vendor due diligence provides value, it has its limitations. Disclosures can be manipulated by a party intending to defraud the company, and other relevant information may be incomplete and/or misleading.

The power of applying analytics rests on the fact that the data memorialized in the company's ERP systems are typically not easily manipulated. The information comprises payment amounts, payee names and dates, purchase order information, invoice information, and how the transaction was entered into the accounting system. Once entered, system controls prevent the data from being altered or manipulated.

Case Studies

To illustrate the application of analytics to identify supply chain fraud, two case studies based upon actual investigations are presented below[2].

Scheme #1

Assumed Facts

[1] Incidences of collusion are on the rise and typically result in substantially larger losses.

[2] Significant facts, such as the location of operations have been altered to protect client confidentiality.

- ***Company A***, a privately held mining company with operations in South America, received a whistleblower allegation claiming to have knowledge of an instance of procurement fraud with one of the Company's vendors.
- The Internal Audit group conducted a limited scope investigation into this vendor and determined that the allegation had merit.
- The loss from this one vendor approached $75,000.

As a result of the whistleblower report mentioned above, the Board of ***Company A*** engaged forensics experts to assess whether this fraud was an isolated instance, or whether there were other comparable scenarios indicating a systemic issue. The primary challenge involved identifying the existence of potentially fraudulent vendors out of a pool of almost 10,000 vendors – a daunting process in the absence of data analytics. Key data sets were examined using various methods to score transactions and risk rank them as low, medium, or high risk. The first analysis of the data produced the results presented in ***Figure 1***. As expected, because the vast majority of transactions in any company are legitimate, the bulk of the results were clustered at the bottom left corner indicating very low risk. From a fraud perspective, the areas of primary interest involved the outliers which are highlighted in ***Figure 1*** with a red outline. Further analysis of the outliers revealed a number or similar attributes.

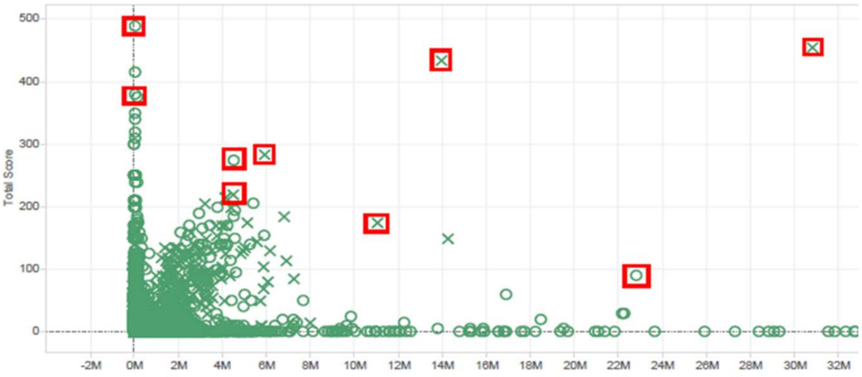
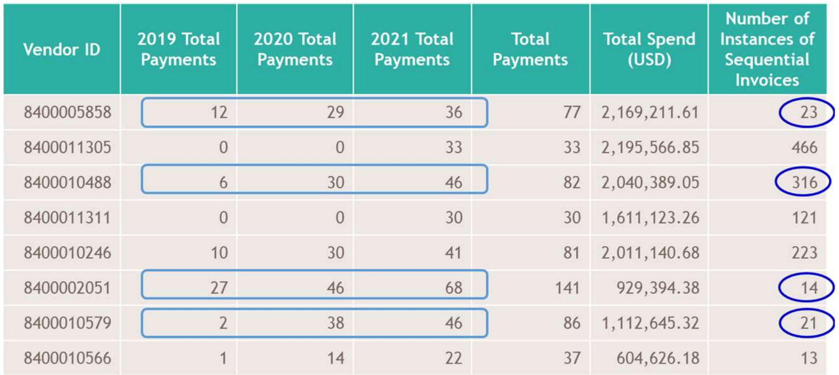


Figure 1



Vendor ID	2019 Total Payments	2020 Total Payments	2021 Total Payments	Total Payments	Total Spend (USD)	Number of Instances of Sequential Invoices
8400005858	12	29	36	77	2,169,211.61	23
8400011305	0	0	33	33	2,195,566.85	466
8400010488	6	30	46	82	2,040,389.05	316
8400011311	0	0	30	30	1,611,123.26	121
8400010246	10	30	41	81	2,011,140.68	223
8400002051	27	46	68	141	929,394.38	14
8400010579	2	38	46	86	1,112,645.32	21
8400010566	1	14	22	37	604,626.18	13

Figure 2

The output from this initial analysis enabled the forensic team to tighten the focus on a specific part of the Company's operations and target a smaller number of vendors. The data presented in ***Figure 2*** resulted from the next set of data queries, which produced a list of two hundred high risk vendors from the total population of 10,000 vendors – a substantially more manageable group. The ability to cull this sub-set of high-risk vendors would not have been possible without data analytics. This new list of vendors was probed using a series of analytics that focused on additional risk factors typically associated with fraud, including the frequency of transactions, the changes in the frequency of transactions over time, and the trends in overall spending. In addition, the forensic team identified a range of other properties that are typically associated with high indicia of fraudulent acts, including, but not limited to a high volume of sequentially numbered. As a result of these additional analyses, a significant number of fraudulent transactions were uncovered, including those with vendors 8400005858, 8400010488, 8400002051, and 840010579.

The forensic team determined that sixty-two vendors and individuals from the purchasing, maintenance, and accounting department were involved in fraudulent behaviors. Many of the Company's employees owned the fraudulent vendors in whole or in part. Ultimately, the forensic team identified losses that exceeded $12 million over a five-year period.

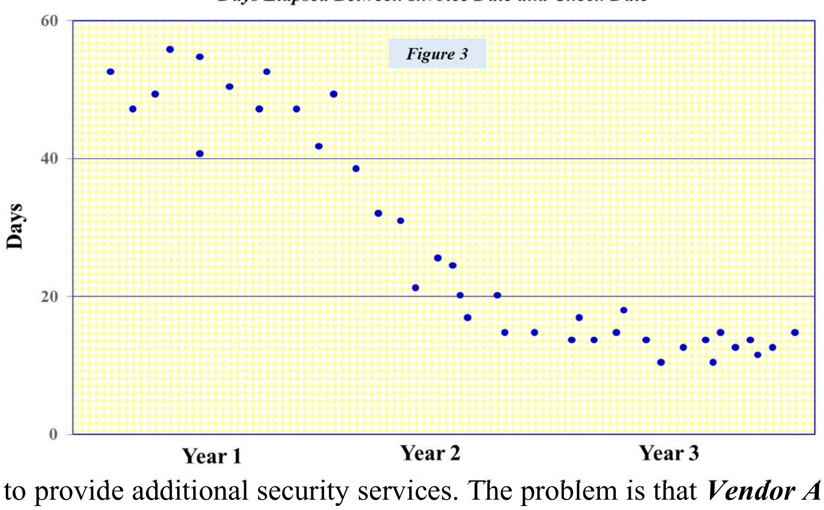
Scheme #2:

Assumed Facts

- A listed company secured a contract to provide engineering and project management services for a large-scale infrastructure project.
- To mitigate the risk of fraud, sub-contractors and/or vendors seeking to support the Company on this project needed to submit to a rigorous approval process.
- Once approval is granted, the Company typically paid vendor invoices within 55 days pursuant to its standard accounts payable policy.
- A payable cannot be established to a sub-contractor or vendor who is not in the vendor master file, and as a result, no payments can be made to unauthorized entities through the accounts payable process.

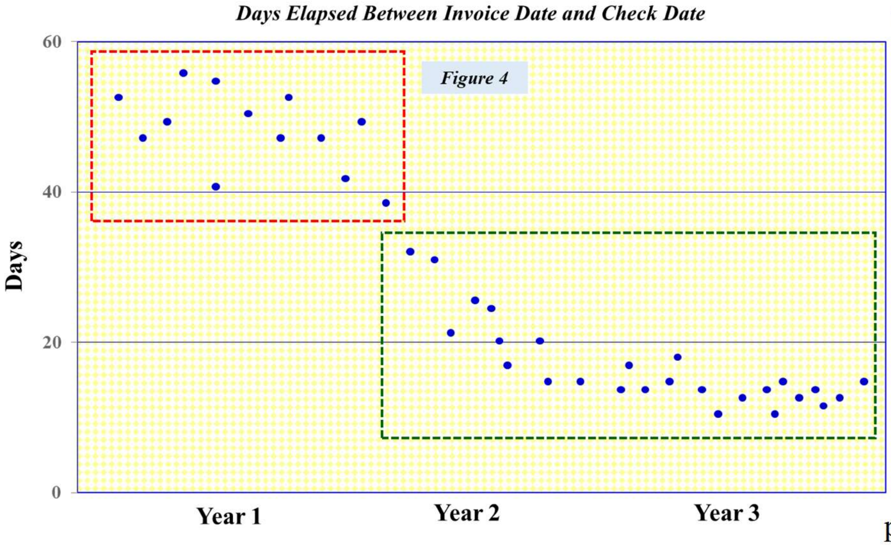
At the outset of the project, numerous vendors submitted proposals to provide security services to protect the machinery/equipment, inventory, supplies, and personnel involved in the project. During the due diligence phase, the Company determined that one such company seeking approval - ***Vendor A*** - was partially owned by a government official, and as a result, was not selected. However, twelve months into the project, invoices were submitted by ***Vendor A,*** approved, and subsequently paid. Each payment was recorded in the general ledger under the expense code "Security Services". The payments were made directly to the vendor via wire transfer and bypassed the A/P process. ***Vendor A*** was ostensibly added to provide additional security services. The problem is that ***Vendor A*** was a bogus vendor who failed to provide any discernable benefits to the project. ***Figure 3*** presents the results of a forensic test that compared the elapsed time between the date of an invoice and the payment associated with that invoice for a specific sub-classification of vendor expense data. Several conclusions are evident from the data presented in ***Figure 3***. First, a regression plotted through this data will generate a downward sloping

Days Elapsed Between Invoice Date and Check Date



trend line that approaches zero. This attribute is highly suspicious and would warrant further analysis on its own.

Second, and more importantly, by segregating the data presented in ***Figure 3*** into two subsets based upon a "before and after" perspective (i.e., before and after the addition of ***Vendor A***) one arrives at what is depicted in ***Figure 4*** below. The first box outlined in red on the left side covers all the recorded transactions for security services in Year 1, each of which occurred prior to the addition of ***Vendor A***. This data presents a pattern that one would expect to observe based upon the expected frequency and payment policies for the services rendered. However, beginning in Year two and continuing into Year three, the data points in the green box of ***Figure 4***, present the data solely for ***Vendor A***, which exhibits both a different frequency profile and a steadily declining gap between payment dates and invoice dates. When compared to the data points contained in the red box, a substantially different pattern emerges. Both attributes are problematic when considered on their own. However, when occurring together there is a clear sign of serious problems warranting immediate investigation. A monitoring program would have identified these anomalies early on in Year two, saving the organization more than a million dollars in losses, and avoiding the occurrence of approximately forty "Books and Records" violations for non-compliance with the Foreign Corrupt Practices Act.



While the investigative procedures discussed above are illustrative of the broad spectrum of tests available to forensic professionals, the total pool of analytical tests is as varied as the nature of issues one is looking to uncover.

Prevention and Detection

- *Understand Risks and Vulnerabilities*

  A fundamental presumption for practitioners of fraud prevention and detection is that one cannot control risks that have not identified and understand. As a result, the first step one should undertake is the periodic preparation of a fraud risk assessment with a corresponding analysis of the policies, procedures, and controls in place to mitigate each of the identified risks. Fraud risk assessments should be performed annually, except for circumstances such as an acquisition that alters the company's risk profile, or adverse developments to other external factors that bring significant pressure to bear on the company's market or industry.

Secondly, to determine whether the policies, procedures, and controls in place are working as proscribed, periodic compliance audits of transactions should be performed. These audits will determine effectiveness of the control/policy environment, and the steps required to mitigate any compliance failures or gaps. These tests should seek to uncover undisclosed conflicts of interest, circumvention of controls, and transactions that lack an economic rationale.

Lastly, implement post-onboarding testing of vendors to identify problematic trends and other instances with high indicia of fraud.

- *Implementation of an Exception Management Program*

A continuous monitoring system produces the most significant benefits in organizations that approach the process in a structured manner. Consider the following when implementing a monitoring program:

- ***A clear vision of the program's goals:*** Is the organization solely looking to test for compliance with company policy, or is there a broader ambition of improving management oversight by detecting and eliminating accounting irregularities, as well as potentially fraudulent behaviors and transactions? These decisions will dictate the types of analytical tests to perform.

- ***Insight into the underlying data that will be analyzed***: For example, do the recorded cash disbursements represent transactions initiated through the ERP system, or are they recorded post issuance - producing underlying data that may lack integrity.

- ***Work-flow processes:*** This would include the full range of actions and responsibilities, including the assignment and management of exceptions. In the absence of timely follow-up, the benefits of a continuous monitoring system will be substantially diluted.

- ***Experienced professionals***: What are the backgrounds of the key individuals involved? It is important to have an experienced team design the front-end analytical tests that drive the system and a skilled team monitor the output, including separating the instances of real concern, from the range of false positives inherent in early warning systems.

Concluding Thoughts

Due to the global nature of today's supply chains, the risks associated with fraudulent billings schemes, kickbacks, corruption, and asset misappropriation continue to rise. In addition, the loss of precious capital associated with supply chain fraud can be substantial. Lastly, the observed trends in the sphere of forensic investigations are quite troubling. There is a growing sophistication and aggressiveness of the schemes being perpetrated, a rise in the prevalence of conspiratorial relationships inside companies, and a mounting awareness among those perpetrating frauds of the investigatory protocols being employed by forensic experts. Each of these conditions pose unique challenges that require thoughtful and reasoned responses that must continue to evolve. The unfortunate truth is that one cannot stop fraud from occurring; however, solutions can be implemented to detect prohibited behaviors and fraudulent transactions quickly, shut them down in their infancy, and implement additional controls to further enhance existing systems.

About the Author

Mr. Harfenist has over 30 years of investigative experience, having directed investigative teams on some of the most high-profile investigations in U.S. history, including the Tyco, Enron, and AIG matters. He possesses extensive, hands-on expertise leading multi-disciplinary forensic teams in government-initiated investigations, including matters implicating the FCPA, matters where allegations of asset misappropriation by insiders and financial statement manipulations are present.

He is an expert in the application of forensic tools used to identify anomalous transactions and high-risk relationships. His engagements have spanned the globe and have at times required the deployment of multiple forensic and document review teams in excess of 100 individuals lasting up to 3 years. He is a CPA and earned his MBA from the Jones School of Management at Rice University, where he was one of the top 5 graduates in his class. Mr. Harfenist can be reached at 713-417-9150 for any follow-up questions.