CHAPTER ONE

The Schematics of Fraud and Fraud Analytics

FRAUD ANALYTICS has become the emerging tool of the twenty-first century for detecting anomalies, red flags, and patterns within voluminous amounts of data that is sometimes quite challenging to analyze. The use of fraud analytic tools does not have to be complex to be effective. The techniques of criminals and fraudsters and their shenanigans are savvier due to technology and the means they use to hide fraudulent activities. While technology has played a role in increasing the opportunities to commit fraud, the good news is that it can also play a key role in developing new methods to detect and prevent fraud. In the past, a spreadsheet was the master of fraud analytics. However, a new revolution has taken us by force—new strategies, data mining techniques, and powerful new software are constantly evolving.

The term "fraud" is commonly used for many forms of misconduct even though the legal definition of fraud is very specific. In the broadest sense, fraud can encompass any crime for gain that uses deception as a principal modus operandi. More specifically, "fraud" is defined by *Black's Law Dictionary* as "a knowing representation of truth or concealment of a material fact to induce another to act to his or her detriment."[1] Consequently, fraud includes any intentional or deliberate act to deprive another of property or money by guile, deception, or other unfair means.

According to the American Association of Fraud Examiners (ACFE):

> Health care fraud, identity theft, padded expense reports, mortgage fraud, theft of inventory by employees, manipulated financial statements, insider trading, Ponzi schemes—the range of possible fraud schemes is large, but at the core, all of these acts involve a violation of trust. It is this violation, perhaps even more than the resulting financial loss, that makes such crimes so harmful.[2]

Because fraud inherently involves efforts at concealment, many frauds go undetected and the criminals get away with them. For these cases, it is impossible to know the impact of the fraud.

HOW DO WE DEFINE FRAUD ANALYTICS?

Fraud analytics is when analysis relies on "critical thinking" skills to integrate the output of diverse methodologies into a cohesive actionable analysis product. Analysis is used for various approaches, depending upon the type of data/information that is available and the type of analysis that is being performed. The analysis process requires the development and correlation of knowledge, skills, and abilities.

As we embark on the efforts to incorporate more fraud analytics within our organizations it is my hope that many develop a clear understanding of how imperative it is to start using the various tools that are available. There should be no excuse. A few years ago we were baffled after hearing that Bear Stearns had a liquidity problem and that perhaps it was one of the greatest financial scandals in history. The troubles deepened with Fannie Mae, Freddie Mac, AIG, Lehman Brothers, Bernie Madoff, WAMU and countless others. In my white-collar crime mind I often wonder if any fraud analytic tools were used and if so what might they have been? Up until now, the greatest financial debacle in history was perpetrated—believe it or not—in the 1700s. "The South Sea Bubble" scandal in 1720 caused the loss of over $500 billion translated to today's dollars. It took over 300 years to beat that record but is quite obvious that the 21st century has made its mark with fraud and the collapse of major companies that have for decades graced the pages of business magazines. Again, I'm curious to know what kind of fraud analytic tool those uncovered "The South Sea Bubble" scandal used. One would hope that it was a precursor to one of the tools mentioned in the chapters set forth.

Fraud analytics has aligned itself with more than one way to detect and deter, there are more definitions on fraud analytics than in the past and more

organizations that are depending upon the most effective and efficient tools that can get the job done.

Report to the Nations on Occupational Fraud and Abuse

In 2012 the ACFE released its annual *Report to the Nations on Occupational Fraud and Abuse*. The international expansion allows the ACFE to more fully explore the truly global nature of occupational fraud and provides an enhanced view into the severity and impact of these crimes. Additionally, the ACFE compared the anti-fraud measures taken by organizations worldwide in order to give fraud fighters everywhere the most applicable and useful information to help them in their fraud prevention and detection efforts.

James D. Ratley, president of the ACFE, stated in the 2012 *Report*:

> As in previous years, what is perhaps most striking about the data we gathered is how consistent the patterns of fraud are around the globe and over time. We believe this consistency reaffirms the value of our research efforts and the reliability of our findings as truly representative of the characteristics of occupational fraudsters and their schemes.[3]

Key Findings and Highlights of the 2012 *Report to the Nations*

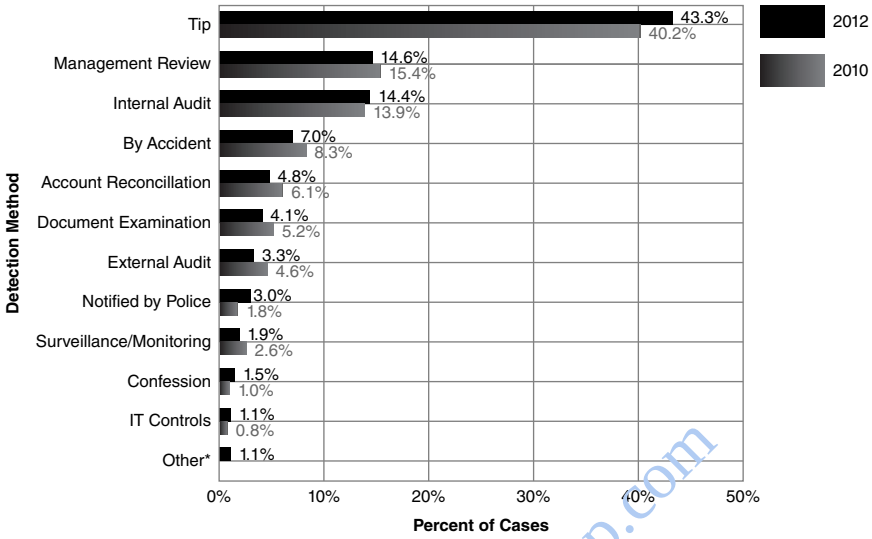
Here are some key findings and statistics provided by the 2012 *Report to the Nations*:

Impact of Occupational Fraud

- Survey participants estimated that the typical organization loses 5 percent of its revenues to fraud each year. Applied to the estimated 2011 Gross World Product, this figure translates to a potential projected global fraud loss of more than $3.5 trillion.
- The median loss caused by the occupational fraud cases in our study was $140,000. More than one-fifth of these cases caused losses of at least $1 million.[4]

Fraud Detection

- The frauds reported to us lasted a median of 18 months before being detected. . . .



**"Other" category was not included in the 2010 Report.

FIGURE 1.1 Initial Detection of Occupational Frauds
Source: Association of Certified Fraud Examiners, *Report to the Nations on Occupational Fraud and* Abuse (Austin, TX: Author, 2012). Reprinted with permission of the Association of Certified Fraud Examiners.

- Occupational fraud is more likely to be detected by a tip than by any other method. The majority of tips reporting fraud come from employees of the victim organization.[5]

Figure 1.1 are results provided in order to "identify patterns and other interesting data regarding fraud detection methods,"[6] the ACFE asked respondents to indicate how the frauds were uncovered. The results are shown in Figure 1.1.

Victims of Fraud

- Occupational fraud is a significant threat to small businesses. The smallest organizations in our study suffered the largest median losses. These organizations typically employ fewer anti-fraud controls than their larger counterparts, which increases their vulnerability to fraud.
- [T]he industries most commonly victimized in our current study were the banking and financial services, government and public administration, and manufacturing sectors.

- The presence of anti-fraud controls is notably correlated with significant decreases in the cost and duration of occupational fraud schemes. Victim organizations that had implemented any of 16 common anti-fraud controls experienced considerably lower losses and time-to-detection than organizations lacking these controls.

  . . .

- Nearly half of victim organizations do not recover any losses that they suffer due to fraud. As of the time of our survey, 49 percent of victims had not recovered any of the perpetrator's takings; this finding is consistent with our previous research, which indicates that 40 to 50 percent of victim organizations do not recover any of their fraud-related losses.[7]

Perpetrators of Fraud

- Perpetrators with higher levels of authority tend to cause much larger losses. The median loss among frauds committed by owner/executives was $573,000, the median loss caused by managers was $180,000 and the median loss caused by employees was $60,000. . . .
- The vast majority (77 percent) of all frauds in our study were committed by individuals working in one of six departments: accounting, operations, sales, executive/upper management, customer service, and purchasing. This distribution was very similar to what we found in our 2010 study.
- Most occupational fraudsters are first-time offenders with clean employment histories. Approximately 87 percent of occupational fraudsters had never been charged or convicted of a fraud-related offense, and 84 percent had never been punished or terminated by an employer for fraud-related conduct.
- In 81 percent of cases, the fraudster displayed one or more behavioral red flags associated with fraudulent conduct. Living beyond means (36 percent of cases), financial difficulties (27 percent), unusually close association with vendors or customers (19 percent) and excessive control issues (18 percent) were the most commonly observed behavioral warning signs.[8]

The 2012 *Report to the Nations* research:

continues to show that small businesses are particularly vulnerable to fraud. These organizations typically have fewer resources than their larger counterparts, which often translates to fewer and less effective

anti-fraud controls. In addition, because they have fewer resources, the losses experienced by small businesses tend to have a greater impact than they would in larger organizations. Managers and owners of small businesses should focus their anti-fraud efforts on the most cost-effective control mechanisms, such as hotlines, employee education and setting a proper ethical tone within the organization. Additionally, assessing the specific fraud schemes that pose the greatest threat to the business can help identify those areas that merit additional investment in targeted anti-fraud controls.[9]

MINING THE FIELD: FRAUD ANALYTICS IN ITS NEW PHASE

In this book you will be introduced to seven fraud analytic (data mining) products that have offered many private companies, law enforcement, and financial institutions a broader scope in how to detect and prevent fraud in its truest form.

1. **ACL Analytics 10.** ACL Analytics 10 is one of the most domineering analytic tools on the market globally. It is highly regarded by many professionals in varying industries of the public, private and government sectors. ACL Analytics 10 is expedient in processing a plethora of data of all sorts. It allows for detection and monitoring of illicit transactions, allows for importing and exporting data into reports that are firmly clear and concise. ACL Analytics 10 has the capability to query scripts, looks for gaps, creates the capability of sampling different kinds of data, monitors control systems, and serves a positive approach of fraud detection. ACL Analytics 10 provides several useful techniques that will assist in the reduction of mitigation costs to any organization in deciphering fraud. ACL Analytics 10 is powerful and faster than any of the previous versions. It gets the job done in an expedient manner and remains to be a force to be reckoned with.
2. **CaseWare IDEA.** IDEA is ACL's primary competitor. IDEA is perhaps one of the most notable analytic tools used in the private sector and academia. It uses a Windows interface and is quite user friendly. IDEA is a primary audit/analytics tool used by accountants, investigators and auditors to detect red flags in financial transactions. IDEA is useful for detecting duplicate transactions, extracting unusual items of transactions, analyzing complex data, and creating samples of audit transactions. IDEA is an exceptional tool and one that needs no introduction to its high level of capability.

3. **Raytheon's VisuaLinks**. Raytheon's VisuaLinks is an analytical software solution designed to depict data graphically by linking entities and associations to uncover suspicious transactions. VisuaLinks provides exposure of hidden anomalies in fraud. It has the power to expose criminal organizations tactics by capturing complex fields of data. It has networking capability so various users can interchange information in a secure environment. VisuaLinks analyzes money laundering patterns, exposes the nuances of financial crimes, enhances the capabilities of counterintelligence that lends itself to terrorist financing, and supports all strategic and tactical auspices. VisuaLinks has supported investigations including not only money laundering and financial crimes, but also telephone toll analysis, insurance fraud, and healthcare fraud.[10]
4. **IBM'si2 Analyst's Notebook.** This application is a visual powerful investigative analysis tool that allows voluminous amounts of information to be analyzed quickly. The information can be attributed to people, places, events, financial transactions, and telephone numbers. In addition, it adds clarity to complex investigations, detects patterns, and verifies trends. In the data collection process, i2 Analyst's Notebook allows for a range of different sources to be utilized to confirm entities with using public records, propriety sources, existing databases, and human intelligence. To further enhance the analysis, i2 Analyst's Notebook is used to find connections that are hidden and meaningful to the investigation, helps one to understand complex associations/relationships through voluminous amounts of disparate data, and reveals the nature and the scope of the investigation.

   i2 Analyst's Notebook is used in a variety of criminal investigations to include money laundering, counterroism, counterfeiting, organized crime and other fraud related cases. i2 Analyst's Notebook continues to remain at the forefront of fraud analytical tools.[11]
5. **Centrifuge Visual Network Analytics.** Centrifuge Systems company is a leading provider of data visualization. It has become one of the top ten analytical softwares for fraud analysis and is widely used in many organizations. Centrifuge VNA includes tools to assist in discovering relationships and patterns of specific entities and identifying statistical approaches to uncover hidden red flags. Centrifuge VNA can calculate data within seconds.

   Its highly effective approach covers the masses of discovery within any set of complex data fields. Centrifuge VNA is user friendly. It's an interactive tool that clearly feeds on its sole purpose of detecting hidden associations, coupled with investigating suspicious transactions.[12]

6. **SAS Analytics.** SAS Analytics provides an integrated environment for predictive and descriptive modeling, data mining, text analytics, forecasting, optimization, simulation, experimental design, and more. From dynamic visualization to predictive modeling, model deployment and process optimization, SAS provides a range of techniques and processes for the collection, classification, analysis, and interpretation of data to reveal patterns, anomalies, key variables, and relationships, leading ultimately to new insights and better answers faster.[13]
7. **Actionable Intelligence Technologies' Financial Investigative Software.** This is one of the newest tools to assist users as they follow the money in all profit-driven crimes. FIS assists in identifying the higher echelon of the criminal enterprise and bringing them to justice. . . . With FIS, fraud examiners, forensic accountants, and agents and agencies will track and seize more assets, identify the key players, and make bigger and better cases in a fraction of the time. FIS has the unique capability to scan and link bank statements, checks, deposited items, and other financial transactions. Once transactions are linked, FIS algorithms and formulas on the transactions and immediately produces tables, charts, and graphs with sources and destination of funds, debit items, credit items, items by payee, or in almost any fashion the fraud examiner, forensic accountant, or investigator wants at the touch of a button.[14]

Fraud analysis is used for various approaches, depending upon the type of data/information that is available and the type of analysis that is being performed. The analysis process requires three developmental broad skill sets; knowledge, skills, and abilities that must correlate with critical thinking skills coupled with the ability to think outside of the box.

Before delving into the main ingredients of fraud analytics, allow me to set the stage for three factors that contribute to analysis:

1. Accuracy of the information is essential. Wrong or biased information will inherently affect the quality of the analysis. As the volume of high-quality *accurate* information increases, the more precise the analysis will become. The key is to ensure that the quantity of information is accurate and relevant. The more detailed the raw data, the greater the likelihood of identifying subtle factors.
2. The details must be transparent and provided in a manner in which the information can be processed effectively for successful results.

3. The data itself cannot be convoluted or misinterpreted; the data must provide relevant factors.

An inference is the principal product of the fraud analysis process. It is an explanation of what the collected information means. The objective of fraud analysis is to develop the most precise and valid inference possible from whatever information is available. The advantage of fraud analytics relies on anomalies. Within fraud analytics, anomalies are unintentional and will be found throughout the data set; fraud itself, however, is intentional.

Since the inception of fraud analytics, several methods have been used to assist in fraud detection and prevention. The first concerns accounting anomalies, internal control weaknesses, analytical anomalies, extravagant lifestyles, unusual behaviors, and complaints via ethics hotlines. Keep in mind that it is the examination and processing of information that results in the development of recognizable trends and patterns. Fraud analytics is an entity of its own. It covers a multitude of industries and can be used from the most complex and complicated to the simplest of fraud examinations, financial investigations, and audits. No one technique is better than the other; they are all useful and much-needed tools.

The discussions and information in this book revolve around tools that are used in fraud analytics. As stated earlier, fraud analytics is an entity of its own, and several tools must be mentioned. Excel spreadsheets have been used throughout and still remain a standard component of fraud analytics. Relational databases have perhaps been some of the most widely recognized tools; they enable users to associate one entity with another by syncing two or three different databases. This allows users to review the source data from various viewpoints. In addition, relational databases provide a broader look at what users have attained, researched, and discovered.

A proactive approach to fraud analytics is the only way to stifle and to lessen the effect of fraudulent activities, which are at an all-time high in numbers and schemes. Aside from the security provided to customers, the amount of money saved by organizations is large considering the financial payoff of implementing a fraud analytics solution. Fraud analytics is not only used in law enforcement; the private sector has taken hold of its reins and may have surpassed law enforcement in using the technique. The book discusses various methods and techniques that can be readily used in fraud analytics and provides an overview of their successes.

As professionals in the private and public sector, academia, intelligence analysis and law enforcement, we spend most of our efforts evaluating

analysis in some form. How does fraud analytics differ from other widely used methodologies?

HOW DO WE USE FRAUD ANALYTICS?

More law enforcement and private companies are finding and integrating fraud analytics within their everyday regime when working on investigations or merely conducting forensic accounting techniques. Fraud analytics is no different from any other source of analytics used in previous forms. A plethora of analysis strategies can be applied to detect the same anomalies; fraud analytics is an innovative and forceful tool kit that is packaged in many formats, which will be discussed in detail.

Fraud analytics offers a sophisticated and savvy way to detect potential fraudulent activities before they occur. Data warehouses collect financial-based information and create what-if scenarios to identify how external factors and market changes affect sales, product mix, and operations. These same technologies can be used to gather information and use predictive analytics techniques to identify suspicious patterns. The tools available today enable us to analyze and collect information in a methodical, calculated manner.

Fraud analytics has the capability to identify subsets of raw data and clean data, and to gather and decipher all potentially relevant information. When one seeks to decipher the trends in the data and find patterns of usage and discrepancies to classify potential fraudulent activity, this capability becomes important. This requires the collection of information related to people's interactions and associations with one another, commonalities among submitted claims information or address, and name data on financial statement documents to identify suspicious activities and overlaps of submitted data. Instead of developing predictive analytics models based on uncertainties, flags are created due to statistical probabilities to identify overlaps of information or patterned analysis that indicates when statistical probabilities have been reached or exceeded. This allows organizations to manage potential threats before they occur as well as to identify patterns within data that may not have been discovered beforehand.

FRAUD DETECTION

It has been said that the responsibility to combat fraud lies with the organization. Although fraud examiners and many other professionals can take the

necessary precautions to protect themselves against fraud, we need to make a concerted effort to educate the masses on what they can and should do to protect themselves from such nefarious acts. The costs of fraud can be astronomical in terms of financial loss and security breaches. With varied uses of fraud analytics, organizations can identify suspicious behavior and patterns before fraudulent activities occur. Financial and intelligence analytics are designed to find patterns, associations, and trends within data that people don't easily recognize. The same is true of fraud analytics; the recognition of the patterns identifying potential fraudulent behavior represents the inception, not the end, of the analytical process.

The main difference between the use of fraud analytics and other applications of analytics is methodology. By implementing a solution to combat fraud, organizations are taking the first step toward a proactive approach. A methodology includes how persons in positions within the fraud industry are able to detect fraud in its early stages and stop the fraudulent activities either before they occur or during the process, which lessens the opportunity for potential threats in the future of fraud monitoring.

The application of fraud analytics requires the knowledge, skills, and abilities to identify whether there is a basis to pursue a recognized pattern. Fraud analytics can determine if a vendor is submitting a suspicious invoice regarding amount of payables or if ghost employees remain on payroll. It can most certainly identify those mentioned in forthcoming chapters and several others that are critical in determining fraudulent spending, duplicate transactions, and duplicate billing schemes. Employees have a fiduciary responsibility to the company to relinquish all their invoices and information pertaining to the organization's financial ledgers. Without employee participation and ethical understanding on how fraudulent transactions can decrease the revenue of an organization, there may be no effective fraud detection solution.

We will discuss in greater detail some of the most notable fraud analytics tools. ACL Analytics 10, CaseWare IDEA, and the SAS Fraud Framework Tool are included in the chapters that cover fraud analytics, particularly in the areas of defining financial analysis, fraud detection resolutions, and identifying financial statement fraud in the auspices of financial investigations. Data visualization software has been at the forefront for quite some time (e.g., i2 Analyst's Notebook, Centrifuge Visual Network Analytics, VisuaLink Analytics). All have made great strides in depicting the associations and links in a visual manner, which assists users in deciphering and understanding the information.

One of the less discussed characteristics is the Portable Document Format (PDF), a file format essential to fraud analytics. It protects the analytical report and the findings that are represented in a written format. Essentially, it is used most effectively when one cannot manipulate the information provided. The format is an essential characteristic of fraud analytics.

When fraud analytics is used properly, the two elements that are valued as mere information prior to determining if the data is clean and/or user friendly: Raw data that becomes information when it is effectively analyzed, and information when it becomes knowledge when it is effectively communicated.

HOW DO WE DEFINE FRAUD ANALYTICS?

The term "fraud analytics" can be defined as analysis that relies on critical thinking skills to integrate the output of diverse methodologies into a cohesive actionable analysis product. Herein lies various approaches, depending upon the type of data/information available and the type of methodology being performed. The analysis process requires the development and correlation of knowledge, skills, and abilities.

FRAUD ANALYTICS REFINED

The refinement of fraud analytics is well centered on the various application processes that are set forth in establishing the patterns, trends, and tools which allow the most complex and sophisticated fraudulent transactions to become transparent as the fraud is unraveled. Under no circumstances can one be sure that only one process and/or tool will detect fraud; neither can we be certain that one will uncover the masses of unscrupulous data. It is all the more important that as you begin your assessments of the initial indications of fraud that the fraud toolkits be used in a manner that will allow you to determine the needs of your investigation.

Fraud analytics should be viewed as the ammunition to improve the performance and the process while embracing the ultimate factor of results that are solution driven. The approach is assessing the complex entities and providing a data-driven solution to understand and identify the challenges as well as the weaknesses. This can only be accomplished with a plan to strategically convey the nuances of the information attained. Clearly, in

reviewing the data it must make sense for the processes of analysis to have the capability of leveraging more than one resolution.

Fraud analytics does not surpass the ability of anyone; neither is its fact-finding approach diluted in any form. It provides results of hidden transactions, sets the tone for advanced analytics, and allows users to determine their own variables to analyze. Refined fraud analytics provides a means to the "big-data" solution. It is an approach that we can embrace for the future as it becomes more sophisticated; more savvy, and more effective in our efforts to capitalize on this ever-resurging evolution of fraud.

NOTES

1. Bryan A. Garner, editor in chief, *Black's Law Dictionary*, 8th ed. (Eagan, MN: West Group, 2004).
2. Association of Certified Fraud Examiners, *Report to the Nations on Occupational Fraud and Abuse* (Austin, TX: Author, 2012), p.6.
3. Ibid., p.2.
4. Ibid., p.4.
5. Ibid.
6. Ibid.
7. Ibid.
8. Ibid.
9. Ibid.
10. Raytheon Visual Analytics Inc., "VisuaLinks® Product Summary: Overview." www.visualanalytics.com/products/visualinks/summary/index.cfm
11. IBM Software, "i2 Analyst's Notebook: Data Analysis and Visualization for Effective Intelligence Analysis." www-03.ibm.com/software/products/dk/en/analysts-notebook/
12. Press release, "CENTRIFUGE Showcases Big Data Analytics and Visualization Solutions for Fraud and Risk," June 12, 2012. www.centrifugesystems.com/resources/press-releases/centrifuge-showcases-big-data.php
13. "SAS® Analytics: Analytics Delivering Greater Insight." www.sas.com/technologies/analytics/
14. Nelson J. Chen, "Beyond the Next Generation: Technology for Financial Crimes and Asset Forfeiture Investigations," *The Eighteen Eleven: Professional Journal of the Federal Law Enforcement Officers Association.* 133, no. 1 (Spring 2011): pp. 6–7. www.aitfis.com/AIT_1811ArticleWeb.pdf.