THE SEVEN WONDERS OF FRAUD DETECTION ANALYTICS

Fraud is constantly evolving. So too should our technologies for detecting and preventing it. Inspired by the Seven Wonders of the World, I present my seven favorite anti-fraud techniques. Some have been in use for over a decade, some are new and evolving – but all of them are "wonderful."

In 2000, a Swiss foundation thought it was time to name a New Seven Wonders of the World. After all, only one of the original seven that the Greeks compiled in the second century B.C. was still standing — the Pyramids of Giza. People around the world apparently agreed, casting more than 100 million votes in response to the foundation's campaign. The final results were announced in 2007, but not without some controversy as participants grumbled about various wonders that were omitted. (See "New Seven Wonders of the World," by Amy Tikkanen, Britannica, tinyurl.com/2p8c2ju2 and "Seven wonders stir up controversy," by Tom Robbins, The Guardian, June 3, 2007, tinyurl.com/yjfzj4h8.)

In this "Innovation Update," I take inspiration from the Seven Wonders of the World and compile my own top-seven list of the best ways to prevent, detect and investigate fraud using data analytics. Like the New Seven Wonders of the World, this isn't intended to be an all-inclusive list but serves to highlight some of the key techniques that fraud examiners can use in their investigations and proactive monitoring efforts.

Instead of reflecting on decisions made in the second century B.C., I've drawn a line in the sand in the early 1980s — when Microsoft first launched Excel — and focused on how we've found new ways since then to incorporate big data, statistical analysis, machine learning and advanced visualization techniques. Just as most people lack the time or money to visit all Seven Wonders of the World, most businesses don't have the resources or the need to incorporate all of the following seven "wonders" in anti-fraud analytics. But by incorporating at least one, or maybe a few, organizations can make game-changing improvements in fraud prevention and detection. Join me as we explore the seven wonders of analytics for detecting and preventing today's fraud schemes.

COLUMNIST
VINCENT M. WALDEN, CFE
ALVAREZ & MARSAL'S DISPUTES AND INVESTIGATIONS PRACTICE

Wonder No.1: Predictive modeling

The Gartner glossary of technical terms defines predictive modeling as "a form of data-mining technology that works by analyzing historical and current data and generating a model to help predict future outcomes." (See Gartner Glossary, "Predictive Modeling," tinyurl.com/45dwswhk.)

It's particularly effective when a fraud investigator has a sample set of known or suspect transactions, communications or events to help train the model. Predictive modeling uses a "more-like-this" algorithm to identify statistically similar transactions, and continuously improves based on human validation of results.

In one investigation I was involved in, the forensic accounting team needed to analyze 400,000 payments (I've changed the numbers for anonymity) to third parties in response to a regulatory subpoena alleging bribery under the Foreign Corrupt Practices Act (FCPA). The investigative team reviewed around 2,000 payments and concluded that about 400 of them appeared suspicious. The model then analyzed those 400 transactions, including their payment descriptions, dollar amounts, vendor names, countries of origin and expense categories. It also analyzed what wasn't suspicious about the remaining 1,600 payments. The team applied both results to the model to analyze the remaining 398,000 payments and generated an additional 14,000 transactions that statistically had a very high likelihood of being suspicious. The sum of those 14,000 payments was just over $8 million, far less than the $25 million alleged by the plaintiffs. This helped the client in settlement negotiations and saved them hundreds of thousands of dollars in investigative fees

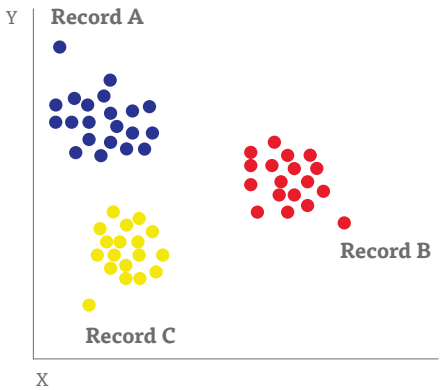
they would've spent to manually review all 400,000 payments.

Wonder No.2: Machine learning, text mining and natural-language processing

Machine learning comprises many technologies, but let's focus on one component called natural-language processing (NLP). NLP technology has the ability to turn text or audio speech into encoded, structured information, based on an appropriate ontology. In the context of the Fraud Triangle, an individual's rationalization is often found in the text descriptions of message chats, emails and free-text descriptions of journal entry transactions. Text-mining techniques, such as word clouds, text link analysis, sentiment analysis and concept clustering, are great ways to identify hidden code words or communications that demonstrate corrupt intent. As I always stress in my presentations, nobody calls it a bribe expense, but perpetrators often come up with code words to cover their tracks (like "friend fee" or "facilitation payment") or categories under generic expenses (such as miscellaneous, marketing or petty cash accounts). (See Gartner Glossary, "Machine Learning," tinyurl.com/3rxjuzdd.)

Wonder No.3: Anomaly detection using K-means clustering

K-means clustering is a popular statistical method for partitioning data into groups that share a common set of quantitative attributes, and identifying anomalous payments or transactions that don't seem to be common to anyone else. This method of organizing data, for example, might help



fraud examiners discover credit card fraud by discovering abnormal purchasing and payment patterns. The graph above shows how such patterns might appear using this method. (See "K-Means Clustering, What Does K-Means Clustering Mean?" techopedia.com, tinyurl.com/m8mmj8rx; "Credit Card Customer Clustering with K-means," by Luke Sun, Towards Data Science, Oct. 19, 2020, tinyurl.com/bb49u4su and "Genetic K-means Algorithm for Credit Card Fraud Detection," by Pooja Chougule, A.D. Thakare, Prajakta Kale, Madhura Gole and Priyanka Nanekar, International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 6 (2) 2015, 1724-1727, tinyurl.com/mryrhwx3.)

Wonder No.4: Entity resolution

When it comes to anti-money laundering, third-party due diligence or vendor and customer matching, entity resolution tools can be powerful allies for helping uncover an entity's true identity. (An entity can be a person, company, location, vehicle or vessel, for example). Entity resolution and analysis (ER&A) — a process that gathers a complete body of data about one particular item or object — helps solve problems stemming from "data entry errors, aliases, information silos and other issues where redundant data may cause confusion," according to techopedia.com. Multiple references to the same name may result from data-entry errors, inconsistency due to multiple systems for entering data, intentional falsification of information or the creation of false identities. (See image, left.) Entity resolution helps resolve this challenge, even when similar entities don't share a unique primary key value, such as the same Social Security number. (See "What Does Entity Resolution and Analysis (ER&A) Mean?" techopedia, tinyurl.com/2vd44mnd.)

Wonder No.5: Pattern-and-link analysis

On TV, often a complex crime is solved in a 30-minute segment by an investigator who maps out the main suspect's social

network, with all their linkages and relationships to other people, assets or events. If only it were so easy in real life. However, pattern-and-link analysis can help in cyberfraud and other investigations. Technology tools that incorporate pattern-and-link analysis provide a great way to find hidden patterns and relationships across multiple, disparate data sources. Pattern-and-link analysis identifies relationships (connections) between a multitude of entities (nodes). Hidden patterns or relationships can be identified among various types of these nodes, including organizations, common addresses, phone numbers, people and transactions. For those who want to learn more, some great examples of free open-source link analysis and JavaScript utilities can be found at d3js.org.

In a recent case I worked on, a client wanted to proactively analyze their employees' gift and entertainment expenses across the globe to identify high-risk venues, gift recipients and meal attendees. This was a perfect use for pattern-and-link analysis, where recurring (most common) meal and gift recipients were linked to multiple employees (contributors).

Wonder No.6: Transaction-risk scoring

For years, I've been advocating for transaction-risk scoring as a way to increase precision and accuracy in your transaction testing. The concept isn't new. In the financial services industry, credit card companies use real-time transaction data for scoring credit risk by creating risk profiles that identify an individual's pattern of behavior as it happens. Pulling in multiple data sources about an individual, financial services, companies also use machine learning to increase the predictive accuracy of future transactions. By scoring each transaction according to its risk attributes (or triggers), one can create a descending risk-ranking report that allows an investigator to focus on higher-risk transactions first. These higher-risk transactions are then aggregated to the respective entities (vendors, customers and employees).

An example of risk triggers could be when a vendor payment 1) is made before the invoice date, 2) comes from a political or state-owned entity, 3) bypasses due diligence, 4) is a round-dollar amount (indicative of a cash payment) and 5) is expensed to a generic general ledger account such as "miscellaneous." We can reasonably assume this payment is riskier than other payments that only meet just one of the above criteria. Additionally, some risk attributes — such as a payment from a political entity — may carry more inherent risks than others. The model should be flexible enough to add additional weighting to those higher-risk variables.

> YOU MAY FEEL AS THOUGH YOU DON'T HAVE THE TIME, NOR THE NEED TO DO ANYTHING DIFFERENT AS YOUR CURRENT METHODS SEEM TO BE WORKING WELL.

Wonder No.7: Innovations in data visualization

If you haven't yet heard of data visualization, you'll find it's the easiest seventh wonder to witness. It's like having the Taj Mahal in your own town — just look and you'll see it. Many commercial tools like Tableau, Microsoft PowerBI, Qlik, Sisense, Spotfire and others offer relatively low-cost data visualization tools to help synthesize and make sense of large datasets. I like how Tableau describes data visualization on its home page:

"Data visualization is the graphical representation of information and data. By using visual elements like charts, graphs, and maps, data visualization tools provide an accessible way to see and understand trends, outliers, and patterns in data. In the world of big data, data visualization tools and technologies are essential to analyze massive amounts of information and make data-driven decisions." (See "What Is Data Visualization? Definition, Examples, And Learning Resources," Tableau, tinyurl.com/3rabtmav.)

As an alternative to displaying data in an MS Excel spreadsheet, taking the same data and loading it into a data visualization dashboard makes the data pop — you can observe trends, patterns or risk areas that would've have been difficult to identify in the rows and columns of a traditional spreadsheet.

Be adventurous

Naturally, the Seven Wonders of Fraud Prevention and Detection aren't absolute, nor are they all on the cutting edge. Innovations in artificial intelligence, prescriptive analytics and other advanced statistical techniques (such as Benford's Law) may also be on your favorites list, which I would love to hear about. I encourage you to get out of your comfort zone and think about how to do things differently. You may feel as though you don't have the time, nor the need to do anything different as your current methods seem to be working well ... until something slips through the cracks and the next fraud case lands at your front door. Keep innovating! ■ FM

Vincent M. Walden, CFE, CPA, is a managing director with Alvarez & Marsal's Disputes and Investigations Practice and assists companies with their anti-fraud, investigation and compliance monitoring programs. He welcomes your feedback and ideas. Contact Walden at vwalden@alvarezandmarsal.com.

