FRAUD TRIANGLE ANALYTICS, 12 YEARS LATER

It's been over a decade since *Fraud Magazine* examined Fraud Triangle Analytics, a method of risk ranking individuals by applying keywords for pressure, opportunity and rationalization to electronic communications. Here we look at how advancements in technology have helped improve FTA in today's battles with tech-savvy fraudsters.

COLUMNIST
VINCENT M. WALDEN, CFE, CPA
CEO, KONA AI

Back in 2009 and 2010, I collaborated with two of my colleagues at EY, Dan Torpey and Mike Sherrod, along with ACFE Chief Training Officer John Gill, J.D., CFE, and several other talented individuals from EY and the ACFE to demonstrate that the behavior described in the Fraud Triangle, developed by Dr. Donald Cressy in the 1950s, could be observed in electronic communications such as email and online chats. In a *Fraud Magazine* three-part series, we outlined a methodology and a mathematical algorithm we termed "Fraud Triangle Analytics (FTA)." (See "Exposing the Iceberg," "Fraud Triangle Analytics" and "Breaking the Status Quo in E-mail Review," by Dan Torpey, CPA, CITP; Vince Walden, CPA, CFE; and Mike Sherrod CFE, CPA; *Fraud Magazine*, May/June 2009, July/August 2009, May/June 2010, tinyurl.com/3v2xeuba, tinyurl.com/23e6ab46 and tinyurl.com/bdf37spk.)

It's been well over a decade since we completed our research. At the time, we were in the throes of the global financial crisis, which was creating a perfect storm for fraud risks at organizations struggling amid a dire economic downturn. Massive layoffs and the broader uncertainty in the business environment put many executives under considerable pressure and heightened the temptation to rationalize fraudulent activity. While the current environment is not as dire as it was a decade ago, pressures are mounting and risks increasing. High energy prices stemming from the conflict in Ukraine, supply disruptions, a tight labor market and concerns about a recession in the U.S. as the Federal Reserve battles inflation with rate hikes all point to a new perfect storm. Against that backdrop, it's perhaps time to dust off that old FTA methodology and see how it applies amid the latest advancements in technology, more robust analytics and easier deployment models.

Revisiting FTA

FTA originally started as an idea I had while in the shower as I thought about keyword terms to use on an e-discovery matter at EY. I asked myself, what if we correlated words and phrases related to the three components of the Fraud Triangle: perceived unshareable financial need (often expanded to mean "pressure"), perceived opportunity and rationalization? (See ACFE.com/triangle.) That would be one way to find high-risk individuals by studying emails. It seemed logical that if a person was exhibiting more pressure, they'd use terms such as "meet the deadline," "under the gun" or "I'm stressed," in their communications with peers. The same logic would apply to the other two elements of the Fraud Triangle. Terms related to individuals spying opportunities to commit fraud would include "override," "write-off" or "figure out a way," while rationalization terms might be "that sounds reasonable," "therefore, let's do it" and "I deserve."

I'll never forget the first phone call I made to the ACFE as a recent new member. I connected with Gill, who was then the ACFE's vice president – education, and asked him if the ACFE maintained such a list of keywords. I'll never forget his simple, yet perfect, answer: "No, but that list sounds like a great idea. Let's build it." We've been good friends and collaborators ever since.

How it's improved

Over the past decade, I've either worked on or observed FTA being used in both proactive compliance and anti-fraud monitoring programs at a few leading organizations or in investigations by anti-fraud and e-discovery professionals. It's been used to uncover fake billing schemes, check-kiting schemes, bribery and corruption, and financial misstatement fraud. Having been a consultant

for the past 25 years and now CEO of an anti-fraud analytics company, I've used this methodology in developing my own anti-fraud solutions. I've also incorporated artificial intelligence (AI) — in particular, predictive modeling and other text mining and statistical anomaly detection techniques — to seek out potentially improper payments, rogue employees or third-party behaviors.

FTA and new technologies

NOFRAUD Latam LLC is one company that's successfully adopting these methods to prevent and detect fraud, corruption, corporate abuse, waste and other workplace issues that destroy organizations' value.

"The company takes a proactive approach by helping corporations determine the motives that highlight employees' decisions to commit fraud, opportunities that empower them to perpetrate the act and rationalizations as a good person living in a bad moment," says co-CEO Marta Cadavid.

NOFRAUD uses AI, data analytics, and a semantic library of over 90,000 pressure, opportunity and rationalization-related terms to capture typed information (such as an end-user's keyboard or cell phone keystrokes) and voice communications to find matched patterns related to the Fraud Triangle. With over 75,000 endpoints (i.e., end-user employee devices being monitored) across the U.S. and Latin America, the technology works in real time. It risk scores employees who are classified according to the Fraud Triangle vertices to generate a risk management dashboard. (See image below.)

Balancing data privacy and monitoring

Clearly, data privacy and protection are important considerations when deploying monitoring tools like FTA — especially when it comes to employee communication data. And NOFRAUD has implemented controls to address these issues.

"At NOFRAUD, our team conducts rigorous due diligence to ensure the organization has the policies in place regarding the consent to monitor," says Cadavid. "To avoid issues regarding corporate privacy, it is always best to consult with legal and compliance."

The company only captures the phrases related to the library of expressions and keystrokes, not the document or file itself. It doesn't view or access the companies' actual data, and the client has full control of the endpoint's implementation.

The right tool for the right job

As we build predictive models around identifying potentially improper payments or rogue transactions, we can also use FTA to analyze the text descriptions, purchase orders or invoice details, and other written text accompanying these payments.

While FTA can be a powerful methodology for detecting fraud, it's important to remember that it's just one of many tools at the fraud examiner's disposal. "As an investigative professional, it's important to consider the most relevant analytics or test for the allegations at hand," says Torpey, a partner in EY's Forensic & Integrity Services practice and one of the founding team members of FTA.

"With today's advancements in forensic accounting, data science and data visualization, CFEs have several technology-assisted audit and analysis techniques at their disposal to meet a variety of risk scenarios," he adds. "The FTA methodology we explored over a decade ago can be further advanced and automated using today's technology."

It's important that the fraud examiner uses sound judgment in developing an investigative work plan that includes interviews, walk-throughs and — after understanding the situation — selecting the most relevant analytics in combination with the proper technology platform, says Torpey. ■ FM

Vincent M. Walden, CFE, CPA, is the CEO of Kona.AI, an AI-driven anti-fraud and compliance technology company. He welcomes your feedback and ideas. Contact Walden at vwalden@konaai.com.