

Detecting Fraud by Integrating E-mail Analytics with the Fraud Triangle

EXPOSING THE ICEBERG

Part 1 of 2

The audit committee chairman of a Fortune 500 company asked Bonnie Parker, the new internal audit director, to enhance the company's fraud detection procedures. The request reminded her that it was time to move past traditional fraud prevention efforts such as journal-entry tests and basic questionnaires and evolve the company's fraud detection program into something more robust and effective.

Parker recognized that the existing programs were only analyzing apparent situations with minimal consideration to potential submerged fraud "icebergs." She didn't realize that her quest to improve her fraud detection plans would lead her to instituting cutting-edge analytics involving the venerable Fraud Triangle and company e-mails. (Our fictitious Bonnie Parker represents all fraud examiners looking for the truth.)

ECONOMIC DOWNTURN CHANGES EVERYTHING

Due to recent company layoffs, the economic downturn, and increased pressure to meet analysts' expectations, Parker knew traditional fraud awareness programs and automated tests wouldn't suffice to weed out significant fraud at its earliest stages. Under normal circumstances, her company would seek to identify fraud-risk areas and develop high-level mitigating factors. However, in these uncertain times, additional efforts are required, which include the assessment of the controls that address each risk factor as well as substantive testing using data analytics.

Parker wondered where she should begin to develop a thrifty but creative program. She had only dealt with minor employee-related fraud schemes in the past, but she knew she needed to broaden her prevention and detection plans and look beyond the obvious. She began by outlining an approach to assess her fraud risk:

- Who within the company should assist and ultimately own the process?
- Upon what areas of the company should she focus her attention during the initial fraud-risk assessment?
- How should she structure the assessment?
- What tools or processes could she use to conduct the assessment?

The question that would hopefully lead her to her ultimate goal was: "How do I transform the results of the fraud-risk assessments into actionable components of the annual internal audit plan?"

By Dan Torpey, CPA; Vince Walden, CPA, CFE; and Mike Sherrod CPA, CFE

PERFECT STORM FOR CORPORATE FRAUD?

Companies and organizations around the world, concerned about becoming the subjects of cable news network programs, need to identify creative ways to proactively deal with fraud.

The Bernard Madoff Ponzi scheme, the consequent “mini-Madoffs,” and the recent alleged billion-dollar Satyam fraud have grabbed us by the throats, but we still can’t forget the infamous debacles of Enron, WorldCom, Tyco, Parmalat, Adelphia, and Société Générale.

The irony is that many companies still believe they’re not at significant risk. However, as the “2008 ACFE Report to the Nation on Occupational Fraud & Abuse” mentions, all organizations are susceptible to fraud. The report estimates that 7 percent of corporate revenues are lost each year to fraud, which certainly seems to prove investment in anti-fraud programs is worthwhile.

The three sides of the Fraud Triangle are still very much in play today. (See Figure 1.) The Fraud Triangle illustrates some of the fundamental concepts of fraud deterrence and detection. In the 1950s, criminologist Dr. Donald R. Cressey (one of the co-founders of The Institute for Financial Crime Prevention, the precursor to the ACFE) developed it to explain why people commit fraud. His premise was that all three components – incentive/pressure, opportunity, and rationalization – are present where fraud exists. [The Fraud Triangle is widely referenced in ACFE literature and examinations and in the American Institute of CPAs’ (AICPA) literature including Statement on Auditing Standards No. 99 (SAS 99), “Consideration of Fraud in a Financial Statement Audit.”]

As *pressure* mounts for executives to make the numbers, some might resort to unusual or unconventional accounting to maintain their jobs or make their numbers. The problem is magnified because many companies continue to downsize and reduce spending on objectives that aren’t critical to the mission. That can create tremendous strain on internal controls and advance the *opportunity* for fraud. Finally, as many companies eliminate bonus programs and employee benefits, and in some cases reduce pay, the *rationalization* for fraud increases.



Figure 1

This two-part article focuses on how established anti-fraud programs can be incorporated with an advanced analytics technique to chisel away at submerged fraud icebergs. We’ll present an innovative way to calculate a fraud-risk score by applying the Fraud Triangle theory to e-mails.

FINDING RATIONALIZATION VIA E-MAILS

We can evaluate pressures or incentives by looking at employee surveys, conducting interviews, or reviewing the code of conduct. We might identify opportunity by evaluating existing controls and policies. But how do we evaluate someone’s rationalization? Ask any fraud examiner, and he or she will tell you that the answer often lies within e-mails.

E-mail or text analytics provide valuable insight into the *who, what, and when* of fraud. Michael Cuff, a supervisory special agent with the FBI’s Financial Crimes Section, said that when the FBI is investigating a case, it considers a host of factors including a person’s position within the organization and one’s possible motivation for committing the alleged fraud.

“E-mail communications often play an important part when understanding the facts of a case,” Cuff said. “By reviewing e-mail communications an investigator can often gain an understanding of the actual corporate reporting structure, the types of access or actions taken, as well as the rationale or intent for proceeding with certain decisions.”

Parker was eager to use advanced analytics when ferreting out fraud motivation in e-mails, but she knew she first needed to devise an anti-fraud program.

WHAT IS AN ANTI-FRAUD PROGRAM?

The ACFE, the Institute of Internal Auditors (IIA), and AICPA collaborated in 2008 with national accounting firms and others in the industry to create “Managing the Business Risks of Fraud: A Practical Guide.” (See www.ACFE.com/documents/managing-business-risk.pdf.)

The guide identifies the key principles of fraud-risk management and provides a baseline understanding of an overall anti-fraud program with the objective of preventing, detecting, reporting, and investigating internal and external fraud.

Of course, a strong anti-fraud program supplies management and employees:

- Opportunity, guidance, and support needed to understand the company’s expectations
- Types of unacceptable behavior
- Relevant, company-specific examples of fraud risk
- Procedures that should be followed if fraud is suspected
- Actions to be taken if fraud is detected

As an integral first step to developing an effective anti-fraud program, management must understand and conduct a fraud-risk assessment. Management at some companies might believe they’ve conducted true assessments, but they might only be skimming the surface. They could be missing the hidden icebergs lurking beneath.

Parker and her team first sent a 40-question survey to 500 randomly selected employees. Then they interviewed 25 top business executives from various departments and business units to get a sense of where they perceived fraud risk within the organization.

CONDUCTING FRAUD-RISK ASSESSMENTS

Using the fraud-risk guide, Parker began to develop an approach that included surveys, interviews, and facilitated sessions with key executives to assist in the design and implementation of a cost-effective, creative, and comprehensive fraud-risk assessment.

She and her team first sent a 40-question survey to 500 randomly selected employees. The survey provided insight into the employees' perception of the corporate tone at the top, fraud risks, knowledge of ongoing fraud, and understanding of the ways in which fraud was handled internally.

At the same time, the team interviewed 25 top business executives from various departments and business units to get a sense of where they perceived fraud risk within the organization. Subsequent to these interviews, Parker's team conducted a facilitated question-and-answer session to assist in validating and prioritizing these fraud risks.

They then combined and summarized the interview, questionnaire, and facilitated session data into varying categories of risk so they could plot the results on a "heat map," one of the most critical elements of the assessment (Figure 2).

Each of the numbered boxes in the graph represented possible

Heat map

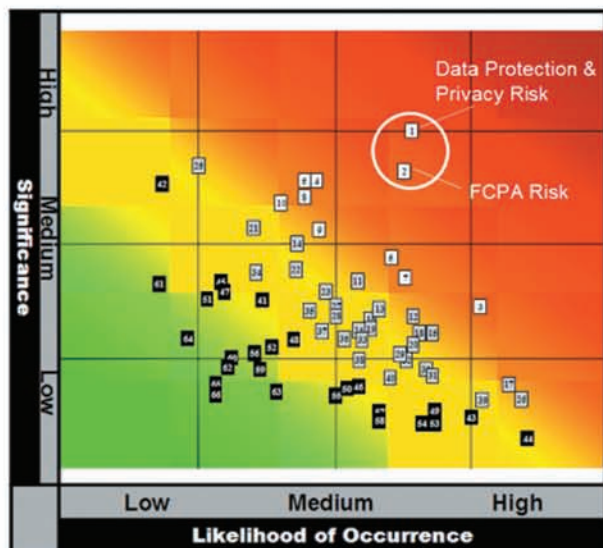


Figure 2

fraud risks. The map showed each fraud risk ranging from a cool green – no likelihood of occurrence of fraud – to hot red – very likely occurrence with severe impact. The numbers were also colored by white (hot), grey (medium), and black (cool) risks to demonstrate severity.

Parker's next step was to focus resources on evaluating and monitoring internal controls to mitigate the hottest risks. She appointed members of her internal audit team to identify, document, and test the controls, and then others to review the results of their work.

Parker used the heat map to prioritize fraud risk and present her findings to upper management and the audit committee. However, those tools only point out the *tip* of the iceberg. Now she was ready to conduct substantive testing including selected data analytics of those high-risk items.

AN ADVANCED APPROACH TO DATA ANALYTICS

Sixty-six percent of occupational fraud is detected by tips or by accident, according to the Report to the Nation. It seems counterintuitive that we *still* detect most fraud via tips or by accident even with technology advancements and the increased regulatory climate. Now, more than ever, we need to apply advanced analytics to fraud detection.

Eighty percent of "enterprise data" (for example, company documents, presentations, Web, e-mail, etc.) is unstructured in nature, according to Gartner Research, yet, most of today's automated, anti-fraud detection tools and audit techniques focus on the 20 percent of structured data.

An advanced fraud detection program should consider a variety of relevant sources of data. Text-based information, when analyzed rather than read, can provide valuable insight into the *who*, *what*, and *when* of fraud especially as it relates to the third element of the Fraud Triangle – rationalization.

According to a 2003 Meta Research (now Gartner) survey, 80 percent of businesspeople surveyed believed e-mails to be more valuable than phone conversations for business communication. E-mail is one of the first data sources investigators, including U.S. Department of Justice attorneys, request during investigations.

What if we could gauge a person's level of incentive/pressure, rationalization, and opportunity by analyzing their communication patterns in the same way we use, say, Benford's Law to objectively analyze the numbers with algorithms? (Benford's Law, named after physicist Frank Benford, states that leading data in lists of numbers from many real-life sources of data is distributed

in a specific, non-uniform way. According to this law, the first digit is 1 almost one-third of the time, and larger digits occur as the leading digit with lower and lower frequency, to the point at which 9 as first digit occurs less than one time in 20.)

KEY WORDS

A team of Ernst & Young (EY) fraud investigation professionals, led by the authors of this article, and an ACFE research team, led by John Gill, ACFE’s director of research, are developing an objective list of key words that are specific to each Fraud Triangle component.

So far, we’ve accumulated and organized more than 3,000 words by each of the major fraud categories (such as financial statement fraud, asset misappropriation fraud, and corruption fraud) because the incentive/pressures, rationalization, and opportunity words often vary by fraud type.

Then we accumulated vast databases and reference materi-

als from EY and the ACFE to derive a master list of terms and phrases that relate to each component of the Fraud Triangle.

We included phrases like “under the gun” and “meet the deadline” to look for the presence of the pressure component and also included phrases like “sounds reasonable” and “I deserve” to search for the presence of the opportunity component. Finally, we used such terms such as “override” or “write-off” to identify areas of potential opportunities. (See Figure 3.)

In the July/August issue, we’ll explore this objective fraud-scoring methodology in further detail in the context of Parker’s fraud-risk assessment program. We’ll also provide details about the testing of the application based on actual fraud examinations.

We’ll provide you a framework for applying this model in your organization so you can approach anti-fraud programs with the most advanced techniques and technologies. 🔍

Dan Torpey, CPA, partner; Vince Walden, CPA, CFE, senior manager; and Mike Sherrod, CPA, CFE, senior manager, are members of Ernst & Young’s Fraud Investigation & Dispute Services Practice. Their e-mail addresses are: daniel.torpey@ey.com, vincent.walden@ey.com, and mike.sherrod@ey.com.

The authors recognize these individuals for their assistance with the research supporting this article:

- John Gill, J.D., CFE, research director, ACFE
- Dawn Taylor, CFE, accounting editor, ACFE
- Andi McNeal, CFE, CPA, research program manager, ACFE
- Pavan Jankiraman, CFE, Ernst & Young
- Anil Markose, CISSP, Ernst & Young
- Matt McCartney, EnCE, Ernst & Young

The views expressed in this article are those of the authors and don’t necessarily reflect the views of Ernst & Young LLP.

Fraud Triangle analytics



Figure 3



Reprinted from the May/June 2009 issue of

FRAUD
MAGAZINE