Deloitte.

Focus on 5
Insights into behavior patterns and fraud detection

Large or small, closely held or publicly traded, many companies continue to find themselves in the public spotlight reacting to discovered fraud. A long-trusted employee quietly embezzles millions of dollars over several years. Aggressive sales and compensation practices, combined with lax oversight, are found to be at the root of fraudulent activities across a wide swath of a company's sales force. A key question to be addressed is why organizations don't see it coming – especially in highly regulated industries or in companies that, on the surface, appear to have robust compliance programs.

The inability to sense, identify, and possibly fend off fraud earlier could be a matter of missing the patterns that would give it away. Everyone behaves in patterns, even when the pattern is no pattern at all. A change in someone's behavior pattern can be an early sign of a brewing fraud. Likewise, someone whose pattern deviates notably from that of peers could be a signal that something is amiss.

The signals can be faint, perhaps muffled by organizational and data silos. Yet sensing and acting on them is essential to uncovering emerging areas of risk. Rare events can point to ongoing activities, and connecting the dots between these activities can yield patterns that reveal previously undetected schemes.

Organizations that want to examine and monitor behavior patterns of employees and third parties as part of their fraud-fighting strategy can benefit from considering five insights that may influence their efforts.

Potential fraud red flags

Common behavioral indicators of potential fraudulent activity include:

- Living beyond one's means
- Financial difficulties
- Unusually close association with a vendor
- "Wheeler-dealer attitude" that the rules don't apply to them
- Control issues, unwillingness to share duties
- Recent divorce or family problems[1]

#1 Companies often wait too long

Complacency is the enemy of effective fraud fighting. Organizations that sail along doing business without encountering problems may believe that they have adequate controls in place and, crucially, can trust their people. But an out-of-the-blue revelation of missing funds, a customer accusation of malfeasance, or a sudden government investigation can blindside the organization and leave leaders scrambling to halt a fraud scheme and contain the damage.

Instead of waiting until trouble is at the door, enterprise leaders can take proactive steps in an effort to combat fraud. By addressing the data and technology requirements of an effective antifraud program, incorporating analytics, and implementing a system of ongoing fraud monitoring, an organization can be better prepared for the likely attempts to defraud it.

#2 Red flags are often missed

An organization may understand fraud drivers but overlook faint indicators or "traces" that hint something out of line could be happening (see ***Potential fraud red flags***). For example, advanced data analysis conducted by an insurance company investigating possible sales fraud identified potential employee red flags such as compliance violations, missed training, customer complaints, and expense report issues. Individually, the transgressions were viewed as minor offenses that didn't warrant further investigation. However, combined in the profile of a particular employee, these indicators reliably pointed to instances of sales fraud in the ensuing months.

Fraud schemes typically go on for some time before they're uncovered. Had the red flags been noted and acted on at the time of discovery, the organization potentially could have mitigated financial losses, reputational and litigation risks, and heightened regulatory interest in whether similar issues exist elsewhere in the business.

[1]Report to the Nations on Occupational Fraud and Abuse – 2018 Global Fraud Study, www.acfe.com.

#3 Effective fraud analytics rely on both technology and human dimensions

Many organizations increasingly recognize the value of being able to predictively identify current activities that could grow into future problems. They are using analytics to help uncover and address these risks.

Importantly, effective analytics involve more than summarizing and aggregating data. The value of the efforts hinges largely on whether the right indicators are being analyzed. A misdirected investigation can be of little use, yielding few insights and perhaps wasting limited resources in the pursuit of false positives.

In contrast, analytics can provide useful information and guidance when conducted by professionals who understand fraud and have access to reliable and wide-ranging data. Working together, experienced investigators, subject matter specialists, and the analytics team can identify key fraud indicators.

#4 Remember that fraud analytics are science and art, not science fiction

Data analytics are revolutionizing fraud investigation. Many organizations hesitate to make the leap, however, because they may believe such capabilities are not yet mature or they fear doing so could lead to privacy issues. For example, false positives can still be a very real concern, especially when the latest generation of analytics tools give investigators the ability to analyze 100 percent of data sets rather than sample just a small portion, as in the past. Having the skills and experience to reduce false positives yet still derive meaningful insights from the data is an important requirement.

In this light, analytics are quite ready for primetime, and many organizations are already using them widely and effectively to fight fraud. Consider the case of a financial institution that had worked with a law firm for almost a year to uncover sales practice issues but continued to struggle with large data volumes and formulating insightful questions. Using analytics, the institution identified eight people who were highly likely to engage in fraud. Ultimately, half of them were terminated and the rest faced strong disciplinary action. The discoveries did not require a year-long comprehensive investigation. Instead, by focusing on the specifically targeted questions, collecting carefully selected data, and developing a workable roadmap, the institution was able to complete the work in eight weeks.

#5 Two recent examples further illustrate the point

The experiences of two companies in different industries demonstrate the value of investigating behavior patterns to uncover fraud:

Major US utility company. A recent fraud event involving senior employees prompted the company to find ways to strengthen its fraud-detection analytics capabilities. With assistance from Deloitte, the company developed an analytics pilot within its customer operations center to test the capabilities of forensic analytics.

The process began with interviews and workshops with in-house counsel, customer operations staff, and technology personnel to identify nuances of specialized data and legacy systems. A 12-week pilot project explored anomalies in a particular type of transaction that was subject to unique risks. Analytics and forensics practitioners collaborated to develop a list of risk indicators that were modeled using semi-supervised methods and visualized in a dashboard.

In addition to the pilot, the initiative included an analytics maturity assessment and strategy workshops with the company's customer operations group. These activities provided the foundation to build a roadmap for the future state of analytics.

The analytics models identified fewer than 50 high-risk customers of interest out of a population of 70,000. The customer operations group reviewed the behaviors of these customers and developed and executed a roadmap to strengthen its analytics capabilities.

Major investment manager. Increasing regulatory pressure and a desire to develop more proactive testing prompted this firm's chief compliance officer to gather advice and recommendations on development of an advanced analytics program. A dozen interviews and workshops with the firm's compliance, technology, and internal audit departments produced valuable results.

Activities included the design of 75 potential analytics pilots to address regulatory and forensic priorities including Securities and Exchange Commission, Financial Industry Regulatory Authority, Foreign Corrupt Practices Act, and anti-money laundering requirements. Workshops explored both open-source and commercial analytics and case management tools. High-value data items were identified, including feeds from existing tools, and a flexible technology approach was designed to facilitate more agile analytics.

The development of a technology and information roadmap provided the basis for the compliance department to hire predictive analytics specialists and develop learning materials for existing staff. Case management and visualization tools, already in use elsewhere in the business, were leveraged to reduce redundancy in investigations and highlight faint signals by consolidating alerts and their dispositions. A framework to fine-tune rule thresholds further trimmed false positives, potentially reducing manual labor involved in reviews.

Potential fraud red flags

Analytics are quite ready for primetime, and many organizations are already using them widely and effectively to fight fraud.

Our take

Organizations operate using familiar and comfortable patterns of behavior. However, rapid advances in technology and processes now offer extraordinary new avenues to enhance the sensing, analysis, and ongoing monitoring of fraud threats.

The involvement of specific and focused people within the organization, including professionals from the lines of business and the compliance organization, is critical to capitalizing on these developments and uncovering unknown and emerging risks. It is also important to not become disheartened by a few false positives, or to neglect to follow up on leads.

Proactive monitoring that leverages advanced analytics can help identify trends, as well as fresh schemes not based on known fraud instances. Keeping track of anomalies and routinely attempting to reconnect the dots can help determine if new patterns are emerging.

Finally, there is no reason to wait for red flags before taking action. As fraud threats are increasing, so are the power and flexibility of tools to combat them. Being proactive instead of reactive and embracing new technologies can help uncover troubling patterns of behavior before they produce real problems.

Satish Lalchand

Principal

Forensic

Deloitte Transactions and Business Analytics LLP

slalchand@deloitte.com

+1 202 220 2738

Martin Biegelman

Managing Director

Forensic

Deloitte Financial Advisory Services LLP

mbiegelman@deloitte.com

+1 602 631 4621

Deloitte.