Deloitte.

Focus on 5:
Five insights into fraud risk analytics

Fraud volume and the cost per dollar of fraud loss—both of which are persistent and growing business risks—are rising.[1] In fact, just last year, the rate of fraud attacks rose by nearly 40-percent in just one quarter, and that was on top of a 62-percent rate increase the year before.[2] Many businesses are vulnerable to fraud—particularly those that have sales channels exposed to electronic payment portals and systems, account-driven customer bases, complex global supply chains, significant presence in emerging markets, and so on. Recently issued guidelines,[3] combined with leading practices for fraud risk management, can provide a catalyst for organizations to strengthen their fraud risk management program activities, particularly the application and enhanced use of data analytics to identify, validate, and monitor the risks of fraud as part of the fraud risk assessment. Following are five insights for executives to consider in using fraud risk analytics.

[1] "LexisNexis 2016 True Cost of Fraud℠," LexisNexis, http://www.lexisnexis.com/risk/insights/true-cost-fraud.aspx
[2] "Global Fraud Attack Index—Q4 2016," PYMNTS.com, http://www.pymnts.com/global-fraud-attack-index/
[3] In late 2016, COSO released its Fraud Risk Management Guide (the "2016 Guide"), which was a follow on to the COSO Internal Control-Integrated Framework issued in 2013 (the "2013 Framework").

Case study: Analytics were instrumental in curbing airline loyalty fraud

Airline travel miles are a coveted loyalty benefit, a gateway for customers to visit places new and old. To an unscrupulous ticket agent, travel rewards present a good-as-gold opportunity to fraudulently issue miles and then redeem them to book flights for personal and friends' use. One major airline recently introduced data analytics into its fraud risk management processes to identify anomalies, patterns, and trends signaling the potential for fraudulent activity. The analysis honed in on a variety of data elements, such as number of air miles awarded to customers and agents, flights booked using air miles, dates of awards, dates of travel, and more.

Analysis of these data elements can produce key indicators of potential fraud, such as:

- Anomaly detection – Were excessive air miles awarded by a single agent or to a single rewards account?
- Predictive classification – Are fraudulently awarded air miles being used to book particular flights?
- Clustering – Are there commonalities in the miles accruing to a rewards account, i.e., the same number of miles every Wednesday, or the same approving manager sanctioning the awards?

By leveraging a variety of analytics models and by testing hypotheses through analysis of combined datasets, the airline detected fraudulent activity earlier. Further, by carefully considering the requirements to operationalize fraud risk analytics, and inventorying current tools and technologies, the company determined that much of what it needed to perform the analytics was already in place, thereby substantially reducing upfront technology investments.

The latest guidance is evolving with technology

Technology has continued to become a more integrated component of virtually every business process over time, so it is not surprising that its use was a point of reference rather than a point of emphasis in this guidance. This is changing. COSO's 2016 Guide (the 2016 Guide) draws from and updates guidance for establishing a fraud risk management program as first published in 2008's *"Managing the Business Risk of Fraud."*[4] Among its elements, the 2016 Guide provides insights and considerations for addressing Principle 8 of COSO's 2013 Framework (the 2013 Framework), which is focused on an organization's consideration of the risk of fraud. Of particular note, the 2016 Guide explicitly discusses recent technology developments, specifically the role of data analytics in addressing an organization's risk of fraud as part of a comprehensive fraud risk management program.

Risk assessment is an essential tool in fighting fraud

A fraud risk assessment is an essential element of an organization's fight against fraud. Leveraging guidelines in the 2013 Framework, development of the fraud risk assessment often begins by identifying business and financial processes to be included in its scope. From there, various ways that fraud and misconduct can occur by and against the organization are identified, including potential schemes to circumvent existing internal controls or for management to override controls. At this point, though, the risks identified are purely heuristic—or based on what an organization's professionals think could occur, those fraud risks that have occurred, and schemes and risks that may be developed and included based upon industry.

From here, there is an opportunity to use one of an organization's most important assets, its data, to build upon the initial fraud risk assessment. With fraud schemes and the sophistication of fraud perpetrators constantly evolving, analytics tools provide the ability to discern anomalies, patterns, and trends—including in real time—across available data that might otherwise go unnoticed, whether within a business unit, in a particular region, or across the enterprise.

Three ways data analytics support the fraud risk assessment

The specific inclusion of data analytics and its benefits in the context of fraud risk assessment in the 2016 Guide recognizes the expanding role of analytics in three key stages of fraud risk assessment:

Identification. Data analytics can be used to look for anomalies or red flags that indicate potential fraud risk schemes and identify high risk areas for inclusion in the fraud risk assessment.

Validation. Analytics can validate the identification of high-risk schemes, evaluate the accuracy of risk assessment process findings, and indicate the need for additional procedures.

Monitoring. Tests and tools can be developed to continuously monitor high-risk schemes and behaviors, aid in assessing the effectiveness of the fraud action plan, and provide proactive alerts for possible exceptions and violations on an ongoing basis.

[4] "Managing the Business Risk of Fraud," the American Institute of CPAs (AICPA), Institute of Internal Auditors (IIA), and Association of Certified Fraud Examiners (ACFE).

Simple steps can energize fraud risk analytics

Organizations that recognize the seriousness of the fraud threat often struggle with where to begin in assessing the risk. Here are some helpful initial steps:

Know where you are. Carefully examining the organization's current fraud risk assessment approach in the context of COSO and other guidance and the potential for employing analytics can provide the foundation for expansion and improvement of current capabilities. Also, an assessment of an organization's current use of analytics for other purposes may reveal opportunities to leverage existing capabilities to reduce the time and costs of deploying fraud risk analytics.

Know where you want to go. Organizations may reject conducting analytics across fraud and/or compliance domains as a futile, boil-the-ocean endeavor. A more realistic approach may be to set modest, short-term goals and develop a roadmap to achieve them in increments with a vision to ultimately enhance the overall fraud risk assessment program. Proofs of concept that build on incremental successes are often an effective way to integrate analytics.

While navigating the path to where you want to go, look for signs around the organization. Both major business changes and day-to-day operations can help strengthen the case for the use or enhancement of fraud risk analytics. For example, any number of directorates—such as Internal Audit, the Office of General Counsel, Compliance, as well as core business operations—may take on the initiative of enhancing their discrete function with data. In fact, most companies already have an ecosystem of advanced analytic tools necessary to get started. Convening various stakeholders to discuss ongoing analytic efforts or recently completed proofs of concept—both broadly and with regard to specific fraud risk assessment opportunities—can help facilitate the production of data and the use of customized business analytics for risk assessment purposes.

The trip will ultimately be worth it. Data issues can offer organizations an easy excuse to hold off on fraud risk analytics. There's too much data, the data's bad, or pulling data from disparate systems is an impossible task. Organizations need not fear their data, however, because something can always be gleaned from it. And, they may have no choice. With the volume of data being generated today, not employing analytics to identify and mitigate fraud and corruption early on can invite devastating problems.

Our take: It's time to drive fraud risk management with analytics

The recent COSO guidance reinforces the important role of analytics in clearly understanding the fraud risk an organization may face and taking steps to reduce risk exposure. It is not too late for organizations to leverage analytics as part of their overall fraud risk management program and specifically related to the fraud risk assessment process. By doing so, organizations can better combat the evolving and expanding array of fraud threats.

Contact us:

Kirk Petrie
Principal | Deloitte Risk and Financial Advisory Forensic
Deloitte Transactions and Business Analytics LLP
Email: kpetrie@deloitte.com
Tel: +1 571 882 8862

Bill Pollard
Partner | Deloitte Risk and Financial Advisory Forensic
Deloitte Financial Advisory Services LLP
Email: wpollard@deloitte.com
Tel: +1 773 640 0225

Holly Tucker
Partner | Deloitte Risk and Financial Advisory Forensic
Deloitte Financial Advisory Services LLP
Email: htucker@deloitte.com
Tel: +1 214 394 5352