Deloitte.

Forensic analytics in fraud investigations

Identifying rare events that can bring the business down

A "rare event," in the abstract, is just a low-frequency occurrence, something that doesn't happen often. In the real world, that dry coinage can translate into significant disruption and far-reaching consequences. A rare event could take the form of a large-scale calamity –a deadly storm, an epidemic, a financial crisis. For a business, the rare event might be a cyberattack or employee fraud. Alternatively, it could be a product flaw that surfaces in the marketplace threatening operations, profits, and brand. Or even a subcontractor's misdeeds could create new compliance risks for you and others in the supply chain.

Mankind hasn't yet figured out how to prevent storms, pandemics, and crashes. But businesses are making breakthroughs against the rare events perpetrated by bad actors, slipshod operations, and regulatory peril, using *forensic analytics*. Forensic analytics combines advanced analytics with forensic accounting and investigative techniques to identify potential rare events of consequence—needles in the massive haystacks of data and information that can signal trouble in the making.

Urgently needed to meet growing regulatory and customer demands for fraud mitigation, forensic analytics can reveal signals of emerging risks months or even years earlier than possible otherwise.

Enabled by advances in computing power and data management, forensic analytics is a critical capability in the **future of investigations**, the overarching theme of a five-part point of view series that concludes with this installment. Previous installments have explored other aspects of an analytics-driven fraud-fighting approach: the need for available and accurate data; the **technologies** required to extract data and realize its value; and, **continuous monitoring** of transactions and activities, a process that produces invaluable input for forensic analysis.

Forensic analytics resources

Detection of fraud schemes has long involved searching for patterns in behavior, actions, relationships, and the movement of money. Forensic analytics helps organizations identify, thwart, and prevent attacks by integrating artificial intelligence (AI)-based data analysis with skilled forensic investigation of fraudsters' motives and methods.

In addition to its fraud-fighting applications, forensic analytics can be used to address operational issues, such as how an organization's processes and controls can create vulnerabilities as well as how they respond to evidence of possible issues. For example, one automaker discovered that, on average, defects could have been identified a year and a half earlier with a forensic analytics approach.

Application of forensic analytics in risk management differs somewhat from its use in areas such as financial forecasting and customer targeting. In those cases, the objective is to identify predictable behavior patterns such as customer preferences and purchasing activity at particular price points. In risk management, the analytics goal is the opposite, to find activity outside the norm, a much more difficult task. Prediction of events that take place a miniscule percentage of the time can be plagued by false positives and wasted effort. Using well-designed forensic analytics, organizations have been able to reduce false positives to single-digit percentages.

Methods employed to address these challenges include:

An analytics repository integrates disparate data sources so analytical models can identify and consolidate signals from across an enterprise. Organizational silos and multiple, dispersed data marts often provide a fragmented view of potential risks. Data may also be collected and used for a single purpose, effectively segregating it from other data sources. An analytics repository integrates both internal and external datasets to provide a clearer and more complete picture of risks and related signatures.

Network mapping and analysis explores a fraudster's relationships, or networks, to reveal other people conducting similar deeds, as well as key figures driving the schemes of a collusive network.

Unsupervised modeling employs algorithms that can sift through data without information about previous instances of the rare event in question. The models help uncover new fraud schemes by identifying suspicious deviations from normal behavior patterns and detecting outliers and anomalies at a granular level, down to a transaction ID, employee, product code, or SKU. For example, purchases in quantities inconsistent with past practice or actual procurement needs could be found to have ensued following a change in suppliers.

Supervised modeling involves development of algorithms that articulate similarities between groups of historical fraud patterns and identifies what separates them from the rest of the data population. For example, regression equations, decision trees, and neural networks can be designed to classify historical instances of fraudulent actions as being either high or low risk. The resulting algorithm can then be used to score new instances to determine their level of risk, monitor data sources for such instances on an ongoing basis, and even identify and score past patterns that may relate to a current investigation.

Text and computer vision analytics are increasingly valuable investigative tools amid the explosive growth in unstructured data, including emails, messaging, audio, and video. Natural language processing (NLP) techniques can identify what is being conveyed in troves of such data, information that could give the lie to assumedly reliable structured data. For example, NLP helped one company discover a spreadsheet that showed that a particular item was being procured using a standard product code. Analysis of the buyer notes accompanying the order, however, revealed that extraneous items such as TVs and laptops had been larded into the transaction.

In another NLP application, AI was used to review audio files from a customer contact center to determine if agents were pressuring customers to buy products they shouldn't. The analysis included agents' tone of voice and customers' stress levels. NLP can also help identify connections between people who otherwise have no noticeable links by analyzing similarities in their comments.

Use of the approaches above is enhanced dramatically through human involvement in the process, a key component of forensic analytics. Experienced, knowledgeable people can both pursue investigations based on the analytics and provide feedback on its utility and effectiveness, expanding investigative capabilities and reach.

Analytic deployment considerations

Several methods warrant consideration in developing and applying forensic analytics:

Training and self-learning. Analytics can learn from a variety of data sources, such as risk issues the organization has confronted in the past. The corresponding models can adapt over time to future risks, thereby expanding their reach and making better use of forensic resources.

Backtesting. Organizations can scientifically test forensic analytics performance in determining whether to use it. Backtesting can help establish confidence that pattern recognition models and algorithms work well and are effective in finding suspicious patterns of interest.

Iterative approach. As a forensic analytics solution is being implemented, models can be iteratively developed, adapted, and scaled so they respond to new and evolving fraud patterns and, at the same time, continually gain a broader view of the risks an enterprise may face. This approach allows an organization to build the forensic analytics platform in stages—a step at a time with input and validation from the business stakeholders —while still staying a step ahead of bad actors.

Feedback and continuous improvement. Once the forensic analytics solution is in place, its effectiveness can be continually improved by incorporating feedback from results of each investigation, from the continually growing body of forensic accounting and investigation knowledge and insight, and from the input of stakeholders across the enterprise.

Advanced analytics considerations

As noted earlier, using forensic analytics to identify rare events and other risks is much harder than applying analytics to customer segmentation or demand forecasting. Resource inefficiencies, safety issues, compliance violations, patent infringements, sketchy sales practices, and fraud, waste, and abuse are among the litany of threats requiring thoughtful application of analytics resources. Here are some approaches and tools to consider in formulating a forensic analytics capability:

Contextual analysis. Effective use of analytics involves detailed exploration of different contexts and use of different types of tools.

Probabilistic scores. Forensic analytics involves mining different types of data and applying various types of algorithms and models to find types and patterns of suspicious activity. These efforts are ultimately combined to assign probabilistic scores to entities that are flagged as potential threats.

Multiple layers. Information streams can be prioritized, and analytics can be designed to scan various data sources, to find different problems. Layering of the disparate analytics efforts can help provide a tight safety net, making it easier to find suspicious deviations from operational norms.

Ensembling. The array of algorithms an organization uses to explore fraud risks can ultimately be combined into a framework that scores and ranks different transactions and entities based on their relative suspiciousness and importance, helping prioritize fraud research and investigation.

An indispensable capability

The complexity and demands of today's world compel organizations to understand the risks they face and take action to protect their operations from fraud, waste, abuse, and regulatory exposure. New fraud schemes continue to emerge. Regulators are increasingly attuned to the risk management role that forensic analytics can play. They are using such tools themselves to identify compliance shortcomings and increasingly expect no less from those under their authority. Forensic analytics can help organizations find the potentially deadly needles in the haystacks, helping safeguard assets, improving competitiveness, saving money, and strengthening compliance.

Contact us

Don Fancher
Global Leader|Deloitte Risk and Financial Advisory
Deloitte Financial Advisory Services LLP
+1 770 265 9290
dfancher@deloitte.com

Satish Lalchand
Principal | Deloitte Risk and Financial Advisory
Deloitte Transactions and Business Analytics LLP
+1 202 220 2738
slalchand@deloitte.com

Ed Rial
Principal | Deloitte Risk and Financial Advisory
Deloitte Financial Advisory Services LLP
+1 212 436 5809
erial@deloitte.com

Shuba Balasubramanian
Principal | Deloitte Risk and Financial Advisory
Deloitte Financial Advisory Services LLP
+1 469 387 3497
subalasubramanian@deloitte.com