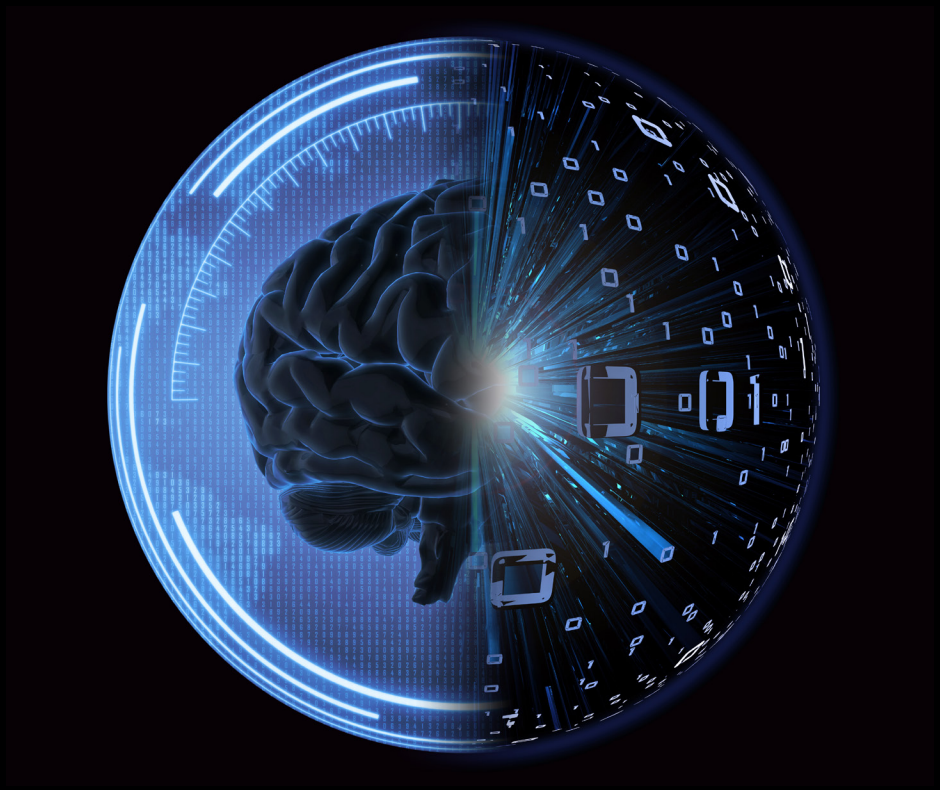
Deloitte.



The evolution of forensic investigations

Integrating human and machine intelligence

Fraud schemes continue to emerge, spread, and morph at blazing speed, fueled by technological advances and the ambition and creativity of unscrupulous actors. An axiomatic challenge that organizations face in detecting, investigating, and fighting fraud is that companies very well may be outnumbered by fraud perpetrators. Internal fraud alone costs the typical organization five percent of annual revenue.[1] As for the outside world, it's teeming with crooks talented and motivated enough to pose danger, some with just connectivity and computing power.

One step organizations can take to better identify and investigate attacks, as well as thwart future ones, is to combine artificial intelligence (AI), machine learning, and statistical concepts of cognitive analytics with skilled forensic investigation of fraudster motives and methods. Such an approach can help investigators get to the bottom of the problem quicker and identify the root cause of incidents to improve their sensing capabilities and help prevent re-occurrence. The future of investigations and fraud risk management for many organizations will likely be an integrated, analytics-driven approach.

Current challenges of fraud investigation

Protecting data, intellectual property (IP), and finances has become an increasing priority at the board room level as fraudsters proliferate and constantly adapt to more sophisticated controls and monitoring. While most organizations are susceptible to seemingly boundless criminal ingenuity, those lacking antifraud controls are predictably worse off, suffering twice the median fraud losses of those with controls in place.[2]

[1] "The Staggering Cost of Fraud" 2016 Global Fraud Study, Association of Certified Fraud Examiners (ACFE)

[2] Ibid.

However, even organizations with antifraud controls can have their investigative efforts impeded by several factors.

Reliance on rules-based testing is a primary culprit. Rules-based tests typically assess and monitor fraud risks across a single data set, giving only a yes or no answer. Investigators scan data for potential fraud triggers such as threshold-exceeding payments or round-dollar transactions. Aside from generating numerous false positives, this approach falls short in other ways. For example, straightforward analysis of accounts payable can identify a questionable direct payment. However, it can miss sophisticated schemes underway in lower tiers of the financial structure, which require advanced analysis of factors such as profit margins or location data.

Information silos further impede analytics-aided investigative efforts. Organizations often struggle to balance the need for locally-tailored processes with the potential benefits of integrated data sharing, unintentionally creating barriers to investigative exploration as a result. A company looking into potential employee fraud might analyze time and expense reports, but overlook clues contained in travel agent data or in public social media. Analysis of travel agent data can help determine if the employee took trips for which no expenses were submitted and potentially paid for via an off-the-books fund. Social media analysis can uncover the true activities on the trip or relationships with external parties that may explain certain transactions.

Supplemental data sets allow for more meaningful insights through correlations that can be drawn.

Another issue is the vast and growing volumes of **unstructured data** amassing in organizations, such as videos, images, emails, and text files. While potentially invaluable, such data is difficult to access with traditional investigative approaches and tools, much less integrate and analyze with structured datasets.

Finally, internal audit and compliance organizations are **often overmatched** in the fraud wars. They rely on manual processes and ad-hoc data analysis, at significant dollar and time expense. They also typically lack full-time, dedicated analytics staff with skills appropriate for the investigative environment.

A path to integrated, analytics-driven fraud investigations

To recap, traditional, rules-based fraud analytics is a form of intuition-driven investigation. Analysts construct such inquiries using tests or rules they create based on their industry knowledge and experience. The shortcomings of this approach can be seen in the simple example of how to analyze client gift-giving activity in a particular region. Establishing fraud tests for potential gift types could require development of dozens of specific queries, and even then some could be missed.

In contrast, a cognitive *data-driven* approach starts with examining transaction data to identify abnormal gift purchases. This approach allows the data to tell investigators where to look for problems, unlike an intuition-driven approach that is purely based on their experience and knowledge. Instead of writing those dozens of queries, investigators can focus on using their forensic investigative skills and experience to examine the narrowed down population of items being purchased and identify the few that warrant attention. This approach can save considerable time and more accurately hone in on potentially troublesome activities. It also can result in fewer mistakes while supporting more thorough analysis — a machine does not miss a trend that can often get overlooked by tired pair of eyes. Also, letting the data identify abnormalities can support the writing of smarter rules to identify outliers and learn why they deviate from the norm, helping address problems faster.

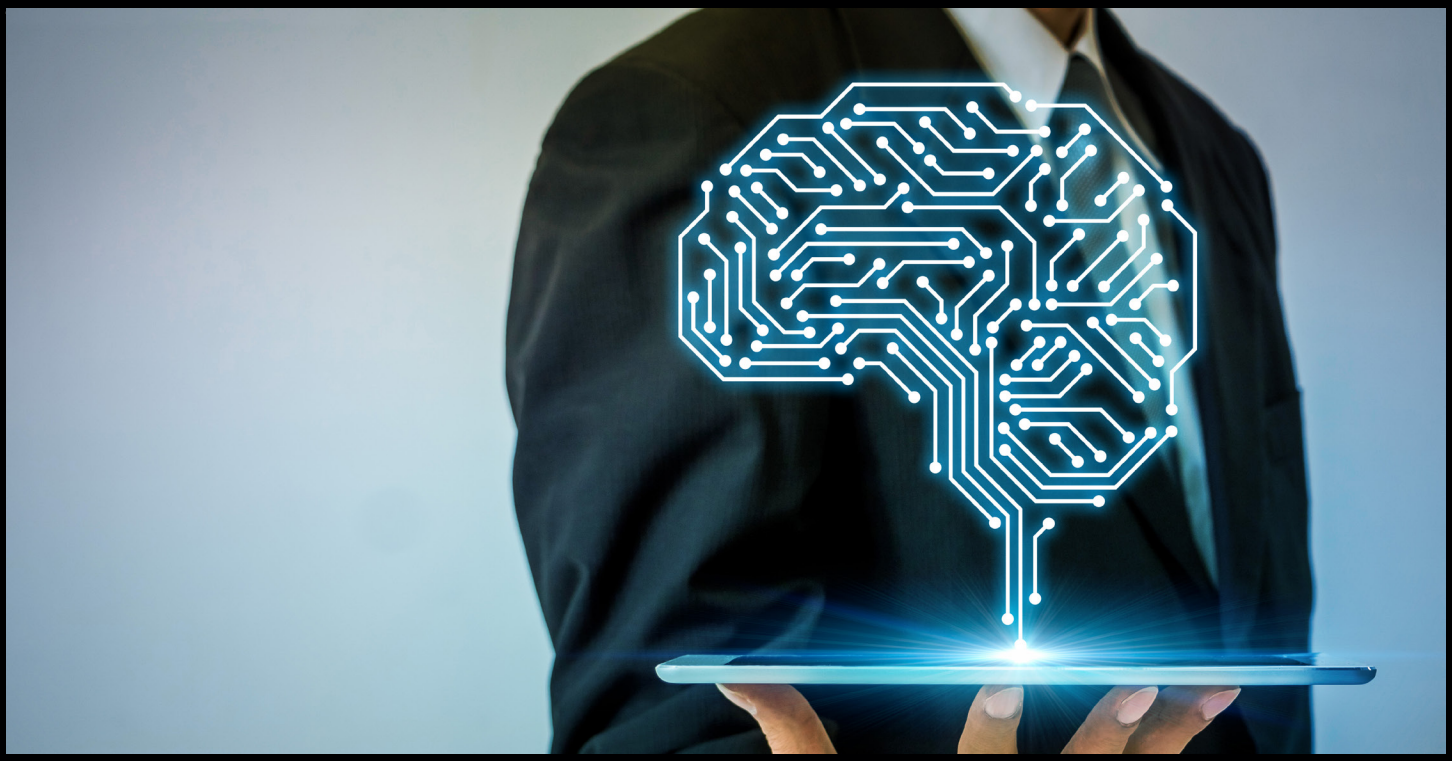
An integrated, analytics-driven fraud investigation approach has several key dimensions:

- **Analytics maturity.** The ability to conduct an analytics-driven investigation begins with determining where an organization resides on a maturity model that captures the people, process, and tool dimensions of fraud analytics and forensics. Factors contributing to an organization's analytics maturity include the frequency with which the organization conducts analysis, the types of analytics tools being used, and whether analysis is conducted in silos or in an integrated, enterprise-wide manner. In assessing analytics capabilities, an important consideration is the significance given to analytics across the enterprise by different business units. Functions such as marketing, customer experience management, and supply chain, which typically have strong analytics operations, could be sources of assistance and resources in spinning up analytics capabilities as part of an investigation.
- **Integrated data marts.** The ability to integrate structured and unstructured data from internal and external sources into risk models is fundamental to an advanced analytics response. As mentioned earlier, structured data alone provides a severely limited view of patterns that might point toward fraudulent activity. Likewise, when data is only available in organizational silos, the links between potential patterns may be hidden. An integrated approach brings together structured and unstructured data from across the enterprise, along with data from external sources such as watch lists and social media, to present a broader picture of activities and transactions, which experienced forensic investigators, aided by advanced analytics, can piece together with fewer false positives.
- **Risk-scoring of the entity rather than the transaction.** Transactions don't commit fraud. Employees, vendors, customers, and others do. Data-driven advanced analytics models incorporating text analytics and network analysis enable organizations to rank risks at the individual or entity level, rather than the transaction level. This approach, which incorporates statistical concepts rather than arbitrary risk ranking, can provide a broader picture of what is happening with an entity than analysis conducted on a test-by-test basis. Letting the data talk instead of subjectively assigning risk scores can improve ranking accuracy and efficiency.
- **Application of predictive tools.** Advanced analytics techniques, such as machine learning and cognitive computing, enable the study of transactions associated with bad actors. Insights into fraudster attributes gained through this analysis and reinforced by the knowledge and experience of forensic investigators can be used to "teach" models that can identify individuals or entities exhibiting the same or similar traits in a broader population. Machine intelligence and computer decisions through AI are starting to take precedence in detecting the digital footprint left behind by fraudsters. Development of this capability is a significant step in the maturation from reactive to proactive fraud analytics, helping to elevate compliance from a "man vs. machine" team to more of a "man and machine" team.

Uncovering the unknown with integrated analytics and forensics

How does an organization determine whether it **has been or continues to be** defrauded? Did fraudulent transactions and other inappropriate activity occur under the watchful eyes of internal audit, compliance, and legal departments? Have isolated fraud instances been uncovered without further investigation to determine if the problem has been conquered?

The continually growing appetites and capabilities of fraud perpetrators suggest that answering these questions will likely only get tougher. By employing advanced analytics approaches in combination with field-demonstrated forensic techniques, organizations can better detect, isolate, and deter fraud attacks, with potentially significant positive impact on an organization's performance and productivity.



Contact us

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

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

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

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