Deloitte.

Overcoming technology challenges in analytics-driven investigations

Building the engine of integrated human and machine intelligence

Fraud can be as simple as intentionally making a duplicate payment. Or, it can be highly sophisticated, as fraudsters execute an ingenious play of intertwined transactions and third-party chicanery. However slick the scheme, fraud has been a persistent drain on an organization's assets and a threat to people's livelihoods. As perpetrators expand their larcenous repertoire, organizations across industries are starting to use integrated, data-driven analytics approaches to identify potentially fraudulent transactions.

Recent Deloitte points of view have discussed how the application of data-driven analytics to transactions can improve fraud-fighting capabilities, as well as how the uses and quality of data drive analytics insights. The analytics technologies used to extract and realize data's value are an equally important consideration that presents their own challenges. Legal and compliance organizations can apply and integrate technology more effectively by understanding those hurdles and taking a strategic approach to clearing them.

Technology challenges in fraud investigations

Advanced analytics are making inroads into fraud investigations, but these are still early days. Legal and compliance organizations continue to use various legacy systems to perform data-intensive reviews. Analytics use cases tend to be ad-hoc ventures, typically performed by vendors. Tools are still maturing, a state that complicates long-term planning and investments.

A legal or compliance team that aims to elevate its fraud-fighting analytics technology capabilities can expect to encounter several challenges in the effort:

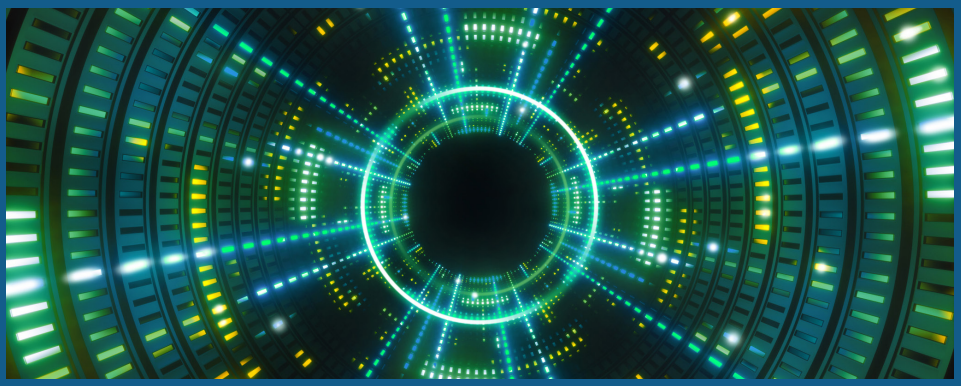
Existing technology may not be adequate, and replacing it isn't easy. While advanced analytics are trailblazing, technologies now used in legal and compliance organizations typically are not. Existing solutions often don't align with the evolving business problems that these organizations need to address, such as responding to new regulations or industry-wide risks, and investigators may lack intuitive ways such as visualization to interact with analysis results. Rules-based monitoring, a commonly used approach for compliance efforts, often produce high volumes of difficult-to-tune alerts and rules, which can consume too much of investigators' time and efforts.

Meanwhile, the technologies that might align more effectively with the business problems are evolving rapidly, and the proliferation of vendors and solutions both those specific to fraud analytics and as well as those developing more broader tools, makes it hard to choose a path. Legal and compliance teams often end up buying tools with the expectation that they'll be outdated far too quickly, leading to another round of spending to upgrade them.

Current operating structures don't (yet) align with the tools. Acquisition of new analytics tools is a starting point, not a goal. Deciding how legal and compliance personnel will use the tools requires further investments of time and resources in use cases and data mapping. Scalability both within legal and compliance, as well as tools like visualization software that plan to be shared elsewhere in the business, can also be an issue, as organizations struggle to manage different business units and disparate geographies.

Investigation professionals may not know how to use, or may resist using, new technology. It's not unusual for businesses to purchase analytics tools or other IT systems that have analytics capabilities, such as customer relationship marketing applications, cloud email systems, or even tax technology tools. Yet legal and compliance personnel are often unfamiliar with the data and features available in those tools. Even if they know how to use them, as might be common for electronic discovery tools, they are often impeded by the organization's data silos. People who have had bad technology experiences may prefer to comb through paper rather than trust technology. Ease of use and solution configuration remain common issues, especially as companies try to further integrate data analysts and business owners, as well as legal and compliance with the operational units of the business.

Outsourcing can lock the organization into a vendor solution. Fraud analytics solutions need to be flexible, often needing to respond to threats or whistleblowers in a matter of days or weeks, as opposed to months or longer. Outsourcing tool design, development, and implementation exclusively to a vendor that has little understanding of the organization's needs can increase the cost and opacity of solution changes and general upkeep.



Keys to better fraud technology

Technology challenges are not unique to legal and compliance organizations. Indeed, each technology-enabled directorate in a given organization will likely have had to face and overcome such universal challenges. These successes are often born within a broader ecosystem of strategy, process, people, and data considerations. Strategy defines the business problem to be solved. People get the technology solution up and running. Process comprises the steps in solving the problem. And data informs activities across the ecosystem.

Strategy. Strategy aligns the investment in technology with key legal and compliance priorities. Thinking through the dynamics of fraud threats and how to respond to them can be invaluable in developing a solution roadmap and testing framework ahead of technology acquisition. A common approach involves establishing a proof of concept based on a new risk, regulatory gap, or recent industry issues, and—based on the results—newer, longer-term solutions can be scaled up over time. The business unit that will be using the technology should drive the initiative.

People. Usability questions illuminate the roles both legal and compliance, as well as other business stakeholders, will play in analytics adoption and deployment. With the affected business unit taking the lead, other organizational stakeholders should be involved in determining who will use the technology for development of analytics and review of results, how they will be trained, and how usability and accessibility issues will be addressed.

Process. One important benefit of an analytics solution is that it can uncover insights that facilitate improvements in day-to-day business processes. Understanding which processes will need to change and how is essential in formulating a solution roadmap. Too

often, the results of forensic investigation receive only cursory attention and then wither away. Particular attention should be paid to how the solution will be sustained, including creation of a feedback loop that helps guide technology enhancements and adjustments in how people do their jobs.

Data. Data needs to be analyzed and interpreted in the context of the business problem being solved. Data management helps determine and monitor the data sources being used. Data and text mining uncovers insights using tools such as predictive analytics, text analysis, model assessment and tuning, and visualization

While legal and compliance teams themselves may have limited analytical capabilities and resources, the types of tools they need are often widely used elsewhere in their organization. Marketing departments mine data to segment and target customers. Internal audit teams sample transactions with database tools. Supply chain professionals use visualization tools to manage logistics. Legal and compliance teams can benefit from exploring potential technology-sharing opportunities and synergies across the business to reduce costs and leverage existing investments while devising and ramping up a solution that fits their domain (see "Solution component snapshot"). But it will require them to overcome a learning curve to understand and make effective use of those tools.

Two other opportunities are worth exploring, as well. Case management technology can be useful as a tool to uncover consistent suspicious activity over a longer period of time, possibly exposing under-recognized issues facing the company. And, robotic process automation (RPA) can provide an efficient engine to gain access to data or achieve a more efficient solution by reducing cumbersome manual processes.

Solution component snapshot

As legal and compliance teams address the challenges described nearby, they can benefit from understanding some of the basic components of an integrated, data-driven analytics solution:

Data management. Core functionality includes the architecture, protection, and policies and procedures associated with maintaining an organization's data. As the fraud leads are often observed in the details, a data management solution is critical to ensuring that adequate and accurate data is readily available for investigation.

Data and text mining. Core functionality can include anomaly or outlier detection; predictive analytics to identify similarities based on known instances of fraud; text mining and analysis, often leveraging electronic discovery solutions; model assessment and tuning; and visualization.

Case management. Core functionality can include executive dashboards, calculated metrics, investigative lens, including focal entity and trending; flexible adjustment of requirements; system-based workflow; and a well-documented and communicated escalation process. A flexible case management solution is especially valuable when developing a workflow for a new operating process, or in response to recent regulation.

RPA. Areas of potentially effective implementation of RPA include document review, customer research, and elements of third-party due diligence.

Capturing the value of analytics

As legal and compliance organizations pursue analytics insights, several points merit consideration. First, technology alone cannot remedy every regulatory or forensic issue. An organization also needs a team that understands the tool, can ask the right questions, involves key stakeholders, and leverages the results.

It can also be useful to consider what will be required if a fraud threat becomes critical. Can the legal or compliance organization quickly and comprehensively respond? How transparent are systems and data? Can new data be pulled in and examined in new, creative ways? Can the organization show regulators and other authorities that it uses technology both to examine identified threats and to flag similar, potentially problematic transactions and people? Careful evaluation and methodical rollout of the technology tools required to fight fraud with advanced analytics can help organizations address these questions and fight fraud more effectively.

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