Deloitte.

5 insights on using a technology-enabled approach to combat fraud

For as long as there have been internal investigations, organizations have generally conducted them in a similar manner. They manually look at available historical information and sometimes, more recently, use technology such as spreadsheets or auditing software to assist in the investigation. This has been a tried and true approach that has served many organizations well, but it remains largely a slow, manual process, relatively limited in its effectiveness and providing few insights beyond the scope of the investigation.

This type of labor-intensive investigation is no longer prudent at a time when practically every detail, major and minor, is being captured in company data somewhere. It takes too long, leaves too many stones unturned, and—perhaps most importantly—risks missing important connections across an enterprise that might point to the same issue appearing repeatedly or seemingly discrete issues being part of more expansive frauds.

Today, it's that proliferation of data, the complexity of organizations' value chains, and the need to respond rapidly to regulators and other stakeholders as factors that demand a new investigative approach—one that's more consistent, defensible, and perceptive so organizations can arrive at answers faster. Here are five insights on technology (tech)-enabled ways to combat fraud and the value of a portfolio approach to investigations—an approach that combines the power of the machine with the business- and technology-savviness of the investigator.

Insight 1: Siloed is bad, integrated is good.

Different types of investigations are often necessarily conducted by different departments in an organization, such as human resources (HR), legal, compliance, security, or internal audit. Those efforts are most often carried out with limited, if any, coordination or communication between departments, probably for good reason. Unfortunately, the resulting lack of integration can cause potential fraud risks to be missed, improperly identified, and under analyzed.

For example, we were involved in assisting with a corporate corruption investigation, which—unbeknownst to us—was actually preceded by a Foreign Corrupt Practices Act (FCPA) risk assessment conducted by the company's internal audit team. The investigation identified a single instance of corruption involving an employee and a vendor, but it revealed no other indicators that would have identified broader corruption taking place across the organization.

Looking back at the risk assessment and investigation work, we later discovered the internal audit team had, in fact, identified similar types of issues elsewhere across the organization at different times, but the dots had not been connected. If the company had a process or a shared case management technology to communicate these issues and analyze them through a broader lens, internal investigators might have developed a better understanding of the true nature and scope of the corruption, as we later did.

Another reason issues may be missed is the often narrow scope of an investigation—for example, an HR department investigating a conduct issue with a single employee. If that investigation stops at just the conduct issue, it may miss signs of broader behavior issues leading to frauds that might be manifesting in other parts of the organization.

That challenge of recognizing signs of deeper or broader problems grows exponentially as companies develop digitally-connected ecosystems, such as smart factories, and extended networks of suppliers and other third-party relationships. There, the mechanisms to fight fraud and misconduct often lag significantly behind the business models and structures being deployed. They rarely take advantage of available data, the technologies that exist to sense and read signals within data populations, and available investigatory professionals from the legal department and internal audit. If bad actors can take advantage of digital connections, the people responsible for combatting fraud should too.

Insights 2: Why the time is right for a tech-enabled portfolio approach.

While the use of technology in investigations isn't new, the rapidly expanding and accelerating role of technology and data in personal and professional lives is. Virtually every action people take is being captured digitally, which means:

A. Every business transaction typically generates data, whether structured or unstructured;
B. With reduced storage costs, that data is often stored now for years; and,
C. As a result, wrongdoing—whether alleged or as yet undetected—is likely captured somewhere in those expanding data populations.

Finding that wrongdoing in ever-increasing data sets and sizes is an inherent challenge. It becomes increasingly important to apply a diverse portfolio of tech-enabled investigative techniques and approaches guided by experienced investigators and other professionals well-versed in the business. But where to begin? Typically, a good starting point is business rules (or queries) that answer specific questions the investigators have up front. That results in indicators of risk that the investigators can pursue.

However, a machine is also capable of generating leads on behalf of the investigator. For example, clustering can be used to understand the inherent patterns in data, both normal and abnormal. Given that fraud is the exception, not the norm, this can be a very powerful approach. When outliers appear, investigators—aided in some instances by data scientists and business specialists—can apply other techniques to understand how those particular deviations compare to their peers, effectively performing a form of behavioral analytics.

If, based on that analysis, an individual vendor or employee warrants additional scrutiny, the investigation team can conduct digital due diligence using public sources to:

- Identify threads to follow in the investigative process
- Confirm connections between potential bad actors
- Identify other subjects of interest

Then, depending on the jurisdiction the investigation takes place in, investigators can take this form of due diligence various directions, including corporate registries; litigation, criminal, and tax records; news media, internet, and social media searches; and regulatory findings. Because such due diligence can produce numerous and confusing results, investigators can apply link analysis technology, which visually graphs relationships between entities, to study and combine findings in a way that highlights "red flag" issues in "visualizations" or computer-generated images.

Once suspicious objects have been identified, connections have been made between them, and potential motivations for bad behavior have been discovered—all the result of investigator-guided data analytics—investigators can then use other techniques, such as email analysis, to assemble final pieces of the puzzle that "tell the story." In a number of instances, when we have presented these types of results to the subject(s) of the investigation, it has prompted their admission of guilt and led to subsequent issue resolution.

One of the most interesting and important aspects of a tech-enabled portfolio approach to investigations is the speed with which investigations can be conducted. According to the Association of Certified Fraud Examiners, it can take a month or more to close a fraud case using traditional methods. A tech-enabled approach wielded by an investigation team that includes forensics and business specialists, as well as data scientists, is often able to generate results in a fraction of that time, both more efficiently and with more effective insights.

Insight 3: Tech-enabled investigations can be predictive value drivers rather than cost centers

The types of behaviors underlying fraudulent activities can be reverse-engineered by investigations, data, and business specialists to develop predictive models. Think about that. If a company clearly understands what constitutes "bad behavior" among its employees, vendors, and other stakeholders, the results of tech-enabled investigations can be used to design algorithms that can predict, detect, and ultimately help prevent that "bad behavior."

For example, in the previously mentioned corporate corruption investigation, the company's internal audit team had also been looking into employee expenses. We helped them build a predictive model to classify expenses into categories. For example, an airline ticket was classified as a travel expense, a restaurant charge as a meal expense, and so on. This helped the company, going forward, to identify employees who were misclassifying expenses to distort aggregated totals—for instance, employees who were attempting to stay off compliance's radar for an unusual amount of meal reimbursements.

This example shows how the integrated capabilities of a portfolio approach can be harnessed on matters that may seem simple, but actually can be quite complex. Putting it all together effectively can lead to significant fraud reduction and risk mitigation—a major value-add from an activity that may have previously been viewed merely as a cost center and consumer of resources.

Insight 4: The same techniques can uncover performance improvement opportunities.

It's not unusual for multinational organizations to be conducting tens or even hundreds of investigations simultaneously around the world. Those investigations may involve diverse business units, departments, suppliers, or other third-party relationships that—on the surface—have no connection to each other.

But what if forensic, data, and business professionals in an organization could connect the dots between those investigations from organizational, operational, and performance management perspectives? What if data sets could be harnessed to identify patterns or trends across matters, functional silos, or even globally to identify redundancies, inefficiencies, and other improvement opportunities?

With the same tech-enabled investigations capabilities described above, organizations have the opportunity to develop a broad-based risk profile supported by a library of risk issues. These assets enable the organization to move from reactive to proactive, and eventually to predictive investigations. By focusing on breaking down silos, sharing and integrating investigation capabilities across the organization, using advanced analytics to help solve the most complex matters, and conducting root-cause analysis, the investigation team can lay the foundation for proactive, predictive fraud risk management.

The same foundation can be used to create value-added opportunities for other parts of the organization, such as supply chain or finance. For example, we previously assisted in a corruption investigation where purchasing and shipping information was used to identify the perpetrators of misconduct. This same data and investigation insights could potentially be useful to the company's supply chain or finance teams to identify inefficiencies, opportunities to improve margins, and eliminate duplication of vendors preventing the company from taking advantage of pricing discounts through consolidation.

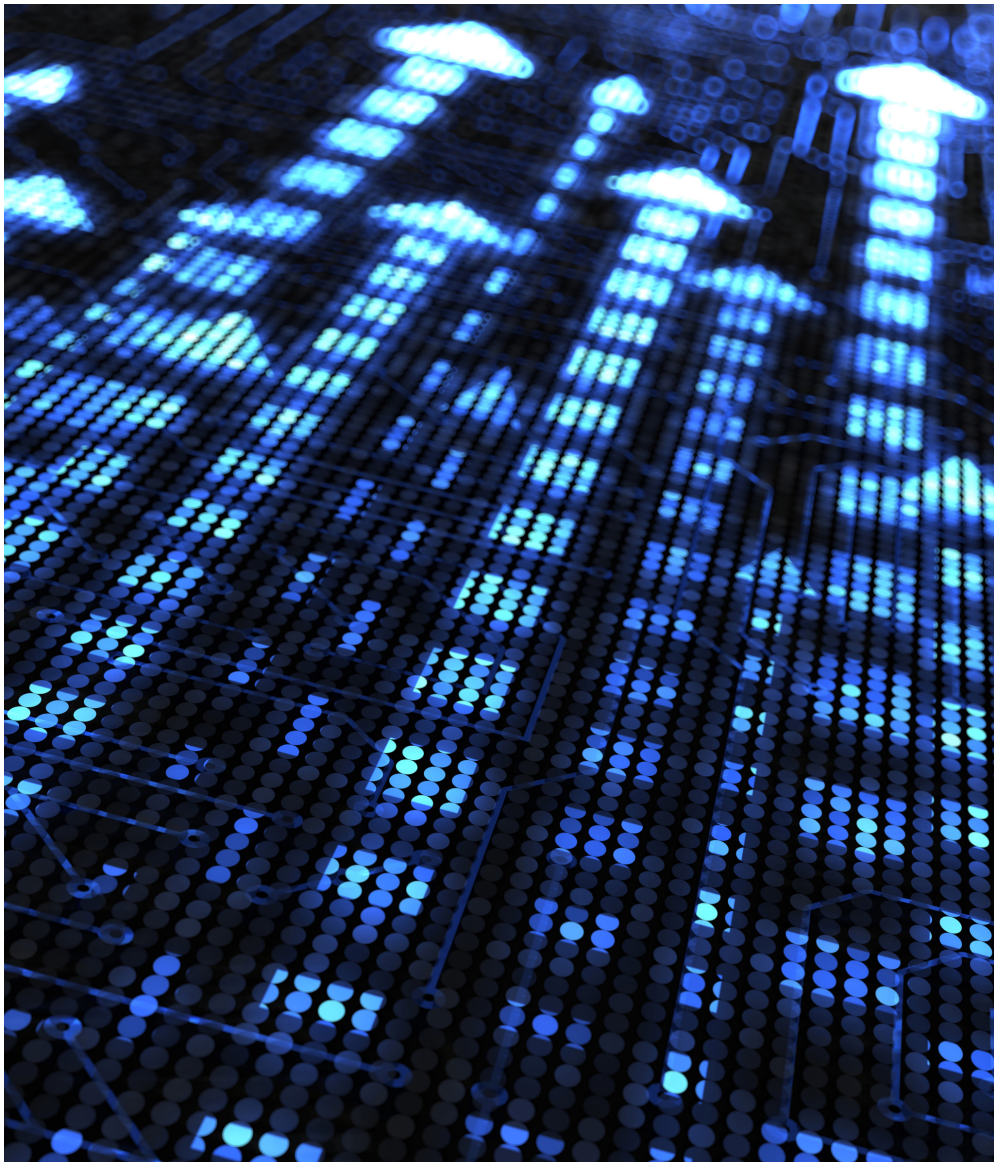
Insight 5: Even more opportunities exist for tech-enabled investigations.

The broader body of investigative work we refer to as enterprise fraud management includes wide-ranging fraud, bribery, corruption, and other financial crimes. With the types of tech-enabled investigations capabilities described in this POV, an organization can build a program comprising the people, processes, and technologies that come together to seek out and programmatically respond to the rare events that can cripple the organization. We consider this the future of investigations because we've seen few organizations with these capabilities today.

Consider the opportunity this represents. Organizations with predictive capabilities could find problems before they become systemic. If a rare event does slip through undetected, the organization could accurately report to regulators and the public that its capabilities are evolving and that the learnings from the event can be applied to prevent such an event from happening in the future.

Moreover, artificial intelligence (AI)-powered "intelligent models" can help develop better risk detectors and investigators by extracting important themes and concepts from documents that investigators review. AI can use voice recognition to transform audio from interviews into structured formats that can be analyzed for new insights, and it can learn from evolving fraud patterns to predict future frauds. The path to this type of AI enablement begins with the portfolio approach to analytics described above.

An important reminder is that data is the fuel for all of this. The more data, the smarter the machine, and the more opportunities for investigation team. So rather than being an inherent challenge that limits effectiveness, the proliferation of data can serve an opposite end. The future of internal investigations, in our view, will be include teams of forensic, data, and business specialists using AI to develop insights from a much broader ecosystem of data. In this way, AI is likely to become a valued team member for investigators.



Our take

The technology and advanced analytics capabilities we've described are available now. Deloitte is actively using them in client engagements and we're seeing other organizations taking the first steps to use them, too.

However, as hinted at throughout the insights offered above, it's important to remember the vital role of humans in investigations. The human element is necessary to bring tech-enabled investigations to life; data science on its own cannot solve fraud and misconduct issues. Effective investigations require humans with a strong understanding of data science and business, and an even deeper understanding of criminal behavior. That combination of data, technology, business, and fraud fluency is what drives effective investigations, enterprise fraud management, and value.

Let's talk about how your organization can harness investigation capabilities for accelerated performance through our Tech-Enabled Investigations Spark Experience, powered by the Deloitte Greenhouse™.

Learn more:

Samantha Parish
Principal
Deloitte Financial Advisory Services LLP
Tel: +1 415 783 4930
Email: saparish@deloitte.com

Brian Merrill
Managing Director
Deloitte Transactions and Business Analytics LLP
Tel: +1 617 905 0569
Email: bmerrill@deloitte.com

Vinnie D'Eramo
Senior Manager
Deloitte Services LP
Tel: +1 516 382 0368
Email: vderamo@deloitte.com

Deloitte.