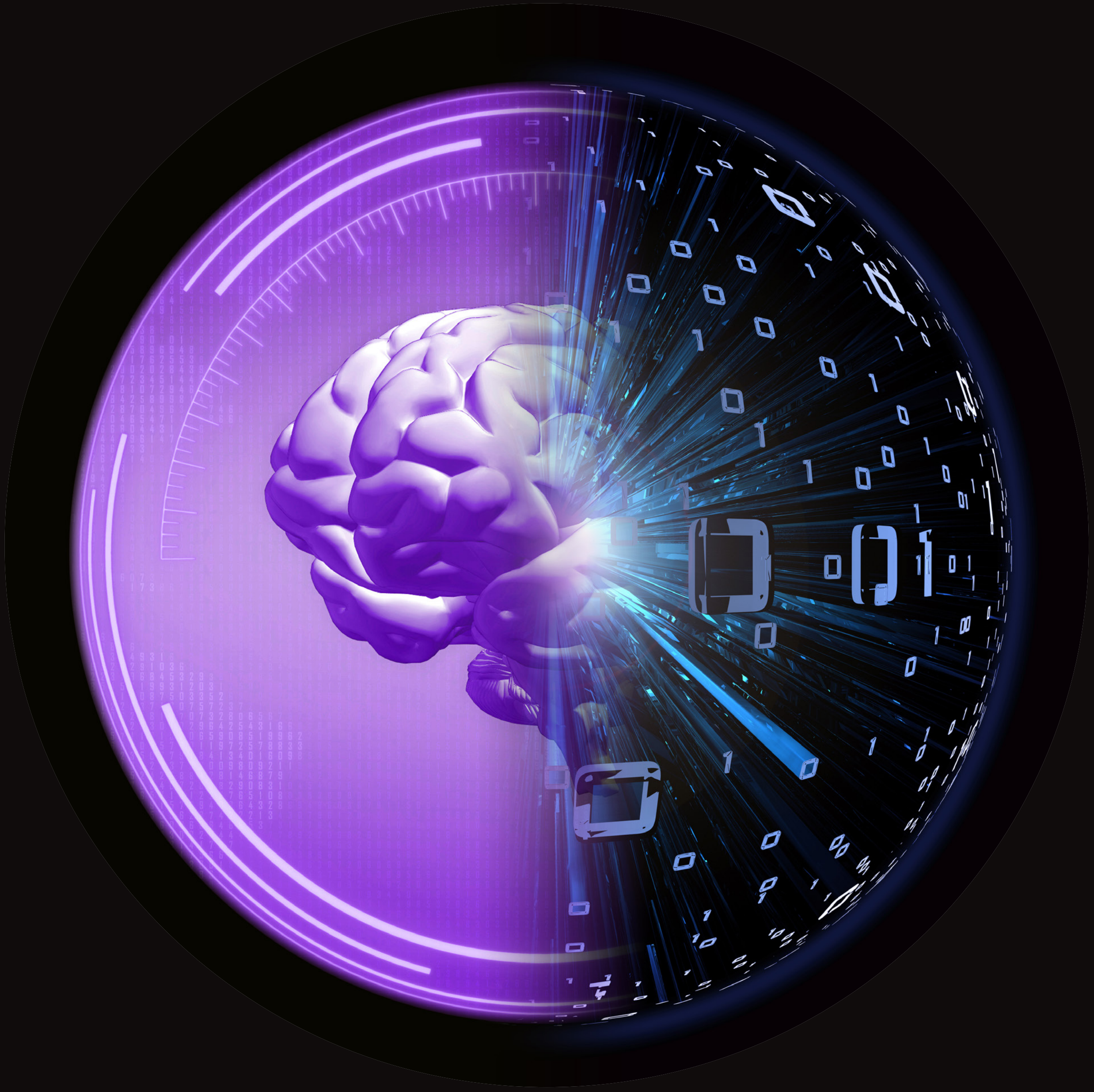
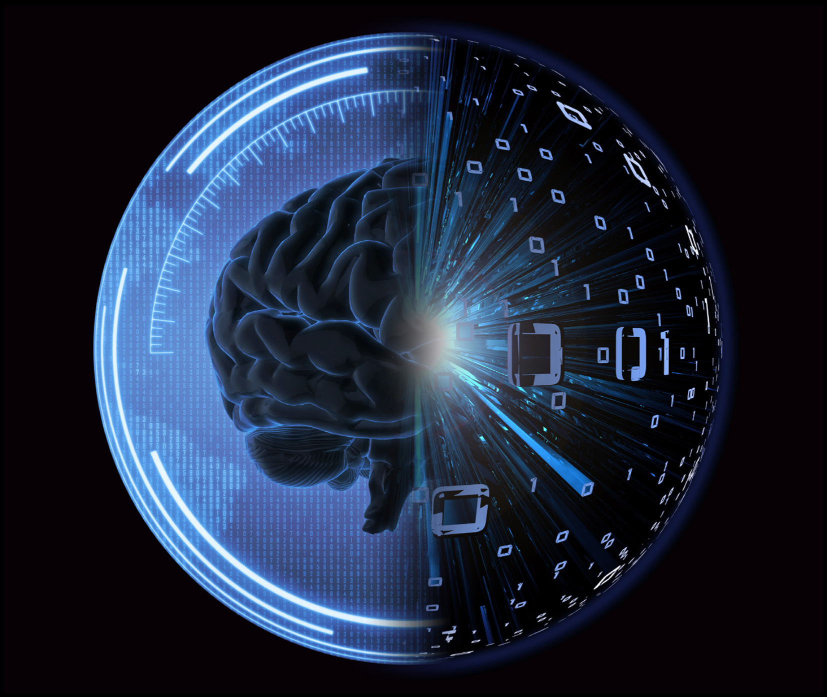
Deloitte.



The evolution of forensic investigations

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.

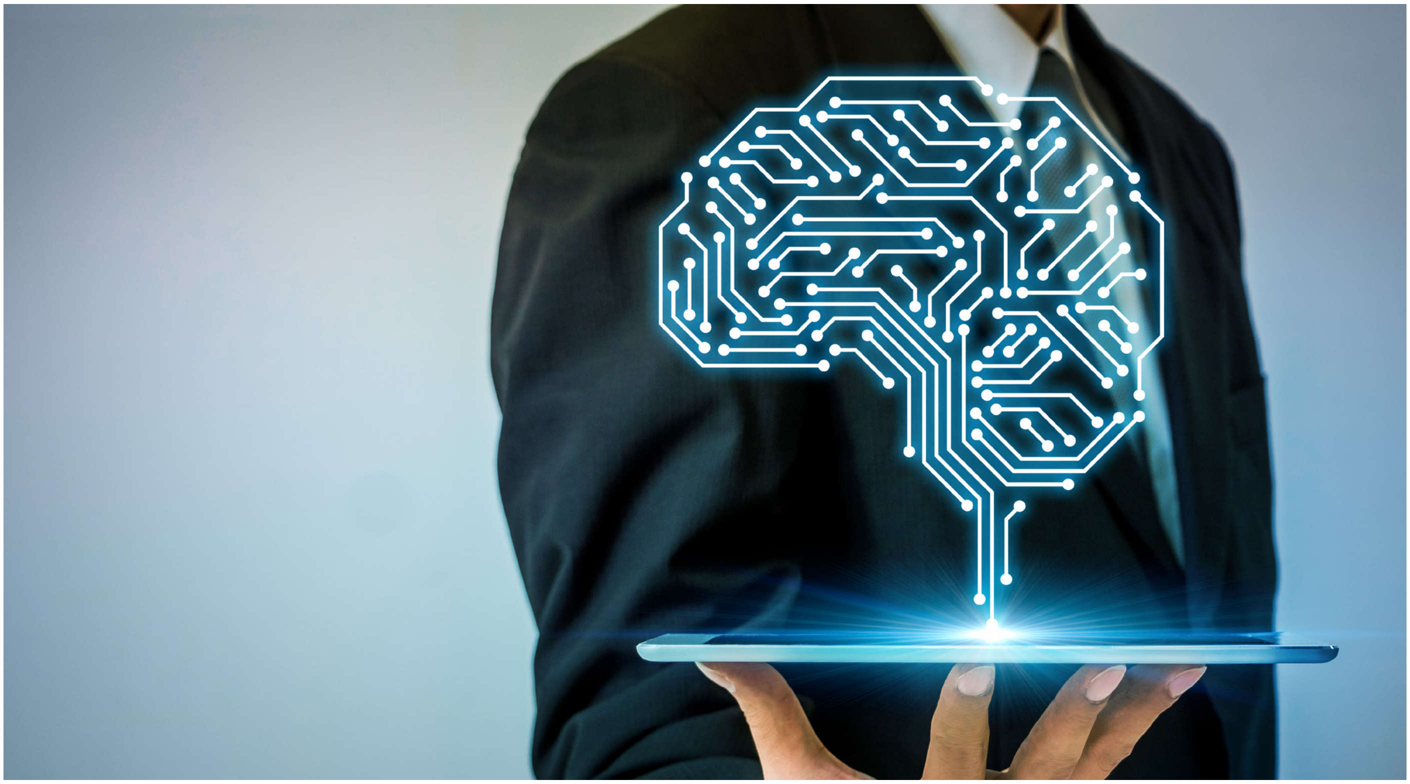
An integrated, analytics-driven fraud investigation approach has several key dimensions:

- **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

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

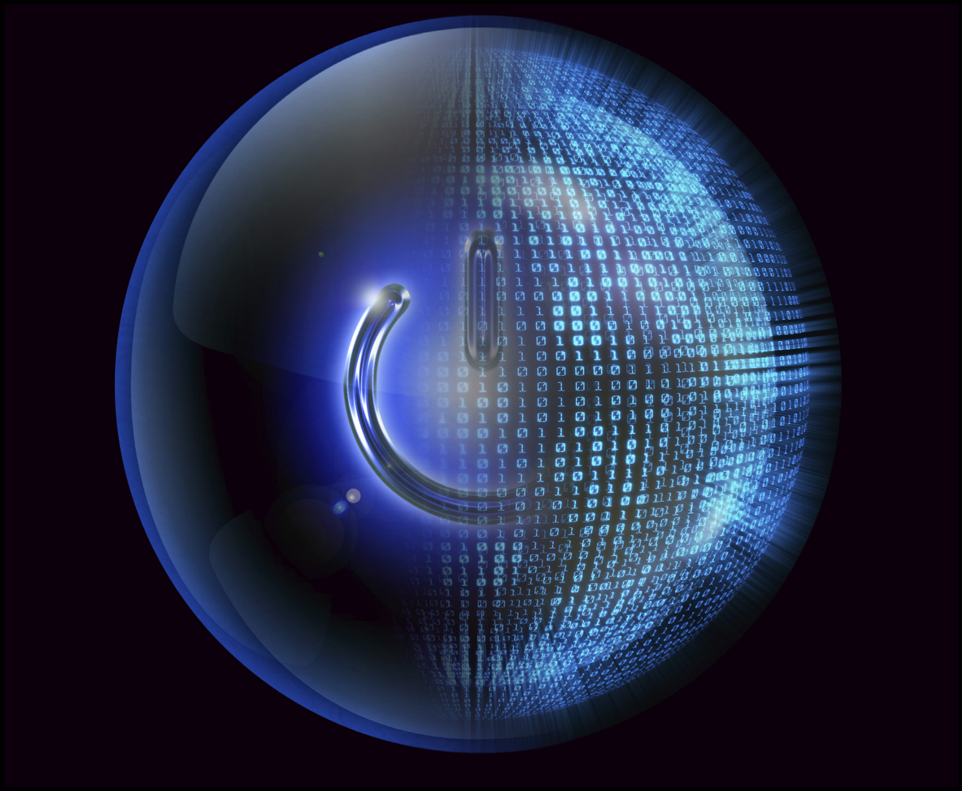
Shuba Balasubramanian
Principal | Deloitte Risk and Financial Advisory
Deloitte Financial Advisory Services LLP
+1 469 387 3497
subalasubramanian@deloitte.com

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

About Deloitte
As used in this document, "Deloitte Advisory" means Deloitte & Touche LLP, which provides audit and enterprise risk services; Deloitte Financial Advisory Services LLP, which provides forensic, dispute, and other consulting services; and its affiliate, Deloitte Transactions and Business Analytics LLP, which provides a wide range of advisory and analytics services. Deloitte Transactions and Business Analytics LLP is not a certified public accounting firm. These entities are separate subsidiaries of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Deloitte.



Overcoming data challenges in forensic investigations

The foundation for integrated human and machine intelligence

Traditional corporate antifraud measures are quickly losing ground against fraud schemes that continue to grow in both frequency and ingenuity. Internal and external perpetrators draw from a menu of ploys, including procurement fraud, employee expense fraud, financial statement fraud, bribery and asset misappropriation, such as intellectual property and data theft.

These threats alone provide impetus for companies to consider new approaches to antifraud and enterprise risk management programs. However, compliance pressures are raising the stakes even more. Regulators increasingly expect companies to have controls and monitoring in place to avert fraud-related issues involving FINRA guidelines, Foreign Corrupt Practices Act (FCPA) compliance, Sarbanes-Oxley requirements, and other dictates.

As discussed in an earlier *Deloitte point of view,* the evolution of fraud risk management and forensic investigations involves the application of analytics to transactions and data, using the insights derived from the integration of human and machine intelligence to refine and improve fraud-fighting efforts. Organizations across industries, and regulators themselves, are starting to use integrated, data-driven analytics approaches to identify potentially fraudulent transactions. Those that do not could rapidly fall behind and face increasing financial, reputational, legal, and regulatory risks.

One underlying factor that will weigh heavily in the value and effectiveness of analytics and monitoring activities is the data itself—how good it is, and how well it is used. Data can make or break analytics-driven forensic investigations.

Data challenges abound

An array of factors can contribute to gaps and shortcomings in monitoring fraud and conducting an investigation, including:

Vast amounts of data. Companies now electronically collect, process, and store more information than was imaginable even 10 years ago. And while the growth in data volume is impressive, even more so is the expanding variety of data sources generating that volume, including personal and business mobile devices, Internet of Things-connected devices, social media platforms … the list goes on and continually expands. Collecting, managing, monitoring, and analyzing the data that is most relevant to antifraud activities is already a complex process, and will only become more so.

Inadequate capture and storage. Legacy systems were often designed to capture information for a specific purpose, so the data available may not be rich enough for meaningful analytics. For example, transaction time stamps and the identities of employees performing transactions might not be captured. In some cases, too, only current data is available; historical information that is crucial for forensic analytics may not be stored. These problems may be exacerbated if the systems have not been updated regularly and additional information is not made available for analysis.

Limited data accessibility. A company with decentralized operations and data sources that are siloed by geographies and departments may lack a master system to consolidate data globally, inhibiting cross-correlation. Large global investigations can involve multiple countries, each using a different financial reporting or ERP system, making it more difficult to extract and analyze data. Jurisdictional data privacy and protection mandates can also limit access.

Inadequate skillsets to process and analyze big data. When data volumes are small, basic analytical skills and spreadsheet programs might be adequate to handle preliminary analysis of structured data from enterprise systems and other software applications, as well as unstructured data such as emails, texts, and voice recordings. But when that volume grows into the millions, analysis can require technology, advanced analytics, and forensic skills that aren't readily available within many organizations. The technology and training investment required to support next-level fraud monitoring can be substantial.

Static reporting designed for business as usual. Legal, compliance, and internal audit teams may encounter barriers to gathering data from sources such as the finance, IT, procurement, and sales departments. Standard reports from those groups may provide only limited information; for example, in the context of procurement, identifying information such as a vendor contact name, address, and phone number might not exist in a standard vendor report, which could limit the ability to compare vendor contact information to employee data to determine potential overlap. Often, when reports were designed, parameters were established poorly. Or they may have been created years ago when the types of information investigators or compliance might need today weren't even considered.

Lack of diverse data to correlate findings. Companies may not adequately explore external data sources, such as third-party reporting databases and social media, to capture a comprehensive view of the fraud risk presented by a company's supply chain, sales channel, and employees.

Any one of these challenges by itself can slow a legal or compliance team's efforts to apply machine learning and cognitive analytics. Together they represent a significant barrier if they aren't addressed in the ramp-up to using advanced artificial intelligence capabilities to better identify and deter fraud.

Data considerations for analytics-driven fraud risk management

Organizations can take several steps to prepare an effective foundation for analytics-driven investigations and fraud monitoring:

Involve stakeholders in building the transformation roadmap. Specific areas of a company may be primed and ready to undertake analytics-driven fraud risk management, but others need in on the plans, too. Internal audit, legal, compliance, IT, and the businesses can all have roles and interest in the analytics efforts. Discussions with relevant stakeholders can identify synergies and ways to leverage technologies in use elsewhere in the organization. And, stakeholders can help identify high-risk areas that warrant focus, such as time and expense reporting, vendor management, and third-party payments (see "Choosing a starting point"). Also, by keeping in contact throughout the analytics initiative, data scientists can stay aware of evolving business needs and business users can understand how data is being stored, accessed, and secured.

Centralize as much data as possible to support fraud monitoring. While centralizing all enterprise data would be the Holy Grail for the fight against fraud, it may not be realistic in many organizations today due to disparate data sources, geographic locations, and gaps in systems integration. Still, emphasis should be placed on bringing as much data together as possible to maintain data integrity, consistency, and control and for enhanced fraud monitoring, analysis, and insights. A good starting point is consideration of requirements for and possible impediments to drawing data from different departments and geographic regions.

Establish secure, structured access to data. A compliance department planning to conduct analytics can benefit by defining early on how data will be handled, where it will be stored, and who will be allowed access to it. Considerations include needed safeguards against breaches and policies and procedures for treatment of personally identifiable information (PII) and other sensitive data.

Incorporate relevant external data. External data can be brought into the centralized repository to cross-correlate with internal data.

Begin to lay a solid technology foundation. It is important to plan for investment in technology and software applications, as part of an overall enterprise solution, that can support effective data collection and analysis for fraud monitoring and to leverage the same data for multiple purposes. The technology should be scalable so both structured and unstructured enterprise data can be included in the analysis.

Better data, richer forensic investigation, and fraud risk management

The success of an analytics-driven fraud risk management program relies on the availability and accessibility of accurate, relevant, and rich data from different geographical locations, service lines, products, and external data sources. As mentioned previously, a centralized, enterprise-wide data solution would be optimal, but in its absence companies can still significantly improve their fraud monitoring and forensic investigation by considering these questions:

- What is the strategy to manage the ongoing proliferation of data?
- What type of analytic capabilities would fit the organization's specific needs?
- Can tools or insights serve multiple purposes across the organization?
- What are key technology trends within the industry and how will the organization's transformation roadmap keep the organization ahead of the industry?

The transformation to an analytics-driven program, including answers to these questions, is likely to require significant time and effort. As typical in the rollout of a new technology, a pilot program using a Test/Prove/Implement/Scale/Repeat methodology can be a helpful starting point. Focusing on early results while staying attuned to the big picture can help equip organizations to address future fraud risks.

Choosing a starting point

Ask a risk and compliance professional to identify fraud risks that would be top candidates for advanced analytics techniques, such as machine learning and cognitive computing, and you may well hear about dozens. One risk team, knowing it would have to show return on its analytics investment to secure funding for broad deployment, distilled down its list of over 100 areas and chose three in which to begin the analysis. The demonstrated value of these initiatives supported expanding the analytics effort to additional risks. The lessons learned: Start small, pick smart, drive value.

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

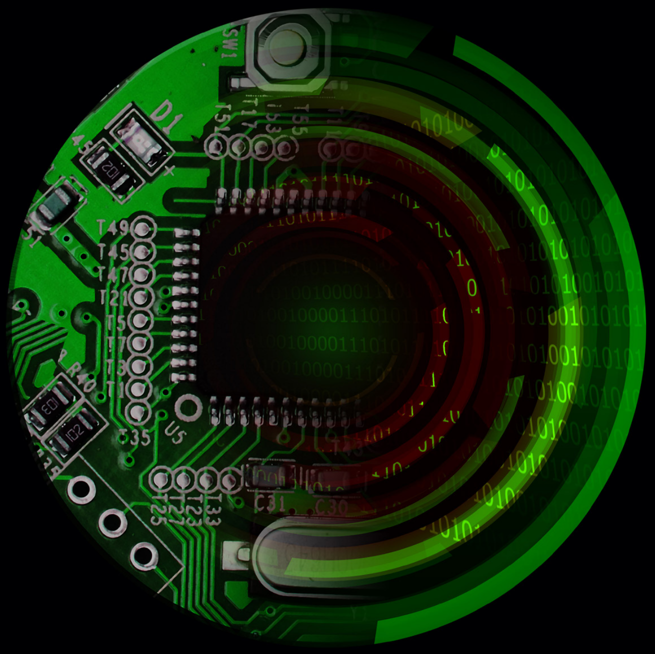
Shuba Balasubramanian
Principal | Deloitte Risk and Financial Advisory
Deloitte Financial Advisory Services LLP
+1 469 387 3497
subalasubramanian@deloitte.com

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

About Deloitte
As used in this document, "Deloitte Advisory" means Deloitte & Touche LLP, which provides audit and enterprise risk services; Deloitte Financial Advisory Services LLP, which provides forensic, dispute, and other consulting services; and its affiliate, Deloitte Transactions and Business Analytics LLP, which provides a wide range of advisory and analytics services. Deloitte Transactions and Business Analytics LLP is not a certified public accounting firm. These entities are separate subsidiaries of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

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:

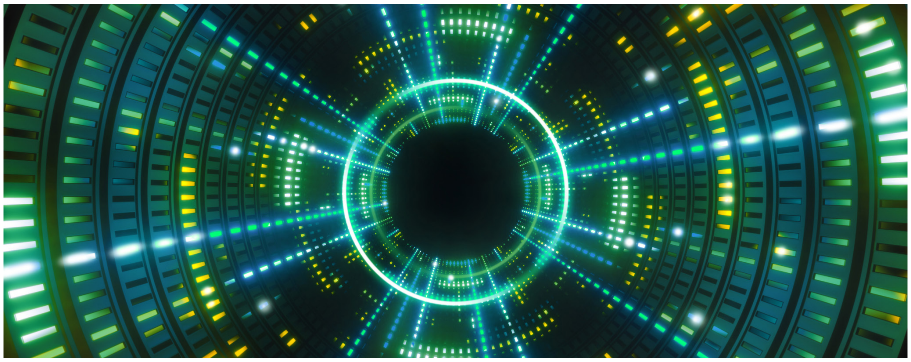
Existing technology may not be adequate, and replacing it isn't easy. While advanced analytics are trailblazing, technologies now used in legal and compliance organizations typically are not. Existing solutions often don't align with the evolving business problems that these organizations need to address, 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

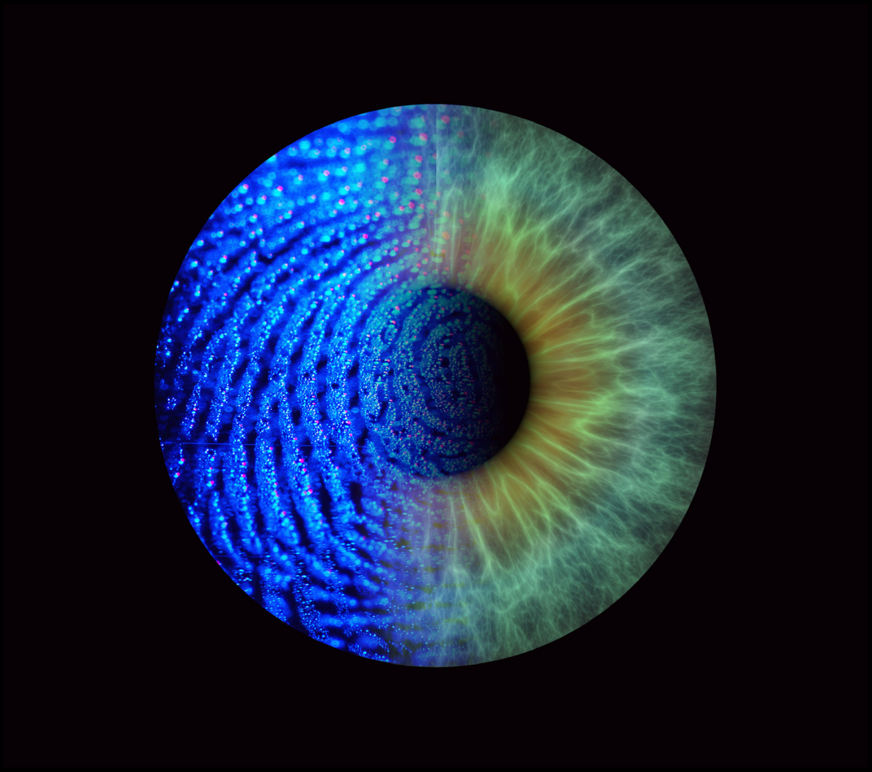
Shuba Balasubramanian
Principal | Deloitte Risk and Financial Advisory
Deloitte Financial Advisory Services LLP
+1 469 387 3497
subalasubramanian@ deloitte.com

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

About Deloitte
As used in this document, "Deloitte Advisory" means Deloitte & Touche LLP, which provides audit and enterprise risk services; Deloitte Financial Advisory Services LLP, which provides forensic, dispute, and other consulting services; and its affiliate, Deloitte Transactions and Business Analytics LLP, which provides a wide range of advisory and analytics services. Deloitte Transactions and Business Analytics LLP is not a certified public accounting firm. These entities are separate subsidiaries of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Deloitte.



Continuous fraud monitoring and forensic investigations

Acknowledging and addressing the risk of being blindsided

A whistleblower's hotline call prompts a bid-rigging investigation. Payroll analysis finds ghost employees lurking in the ranks. A vendor audit points to a possible kickback ring. Whether internal or external, successful or thwarted, a fraudulent act compels an organization to address critical questions. Who all is involved? What has the scheme cost us? How long has it been going on?

Recent Deloitte POVs have discussed key dimensions of an organization's analytics-driven fraud-fighting approach: the role of analytics, the need for available and accurate data, and the technologies required to extract and realize data's value. Another critical component of fraud defense, one that can help address the questions above, is continuous monitoring of transactions and activities. Organizations that use technology to monitor for potential risks, as well as analytics to identify new emerging threats, may be better positioned to mitigate the blind spots in their fraud defenses and address the risks of being blindsided financially, operationally, and legally.

The challenges in combating fraud
The longer fraud perpetrators go undetected, the greater financial harm they cause. And, recovery becomes more difficult with time. The duration of typical schemes amplifies the need for continuous monitoring to uncover threats. Research has found more than half of frauds continue at least 18 months before detection and nearly one-third go undiscovered for two years or more.

Various factors impede fraud detection and avoidance, including overwhelming data volumes, scarce forensic analytical skills, and the expense of needed technology and training. An organization that hires data scientists to conduct fraud analysis may discover they can crunch numbers but lack critical domain knowledge.

Often, fraud fighting is primarily reactive, with resources focused on chasing perpetrators after an incident, at the expense of detection and prevention. Internal audit, supply chain, and other functions may search for fraud in silos, missing opportunities for collaboration and information sharing. Risks may be monitored based on established criteria and past incidents, rather than using a more robust, data-driven approach that considers potential unknown threats.

Constantly advancing technologies create other concerns. The proliferation of digital devices increases efficiency and automation, but also elevates the organization's risk exposure as internal audit may fall behind the business units in technology deployment and expertise.

The nature and potential of continuous fraud monitoring

One might reasonably think of continuous monitoring as an automated process that flags suspicious transactions the moment they occur. The process may be rule-driven, for example producing an alert anytime a transaction exceeds a threshold amount or is processed outside of normal business hours.

Continuous, however, is a relative term in this context. Real-time, 24/7 monitoring may not be necessary or useful, especially in detecting complex fraud schemes. As noted, research has shown that frauds typically evolve over time. A single transaction may mean little, but monitoring the transaction trend on a monthly, weekly, or other basis could speak volumes.

Proactive monitoring that leverages advanced analytics can help organizations identify trends, as well as fresh schemes that aren't based on known instances of fraud. Rather than relying on rules, analytics produce new insights driven by what the data is showing.

Attention to several considerations can help an organization generate greater value from its monitoring activities:

Embrace the deterrent effect. People have a way of falling in line when they're being watched, whether by humans or machines. The mere existence of monitoring, properly communicated, can help nurture compliance with protocols, policies, and guidelines.

Keep it in house. Conducting monitoring within the organization instead of turning to an outside party offers several advantages, including data security and privacy. Data can be analyzed more easily on a continuous basis, and the in-house personnel can learn both how the solution works and how to maintain it. Plus, if the solution needs to be expanded in the future, the work can be done within the organizational infrastructure and not require additional data exporting.

Customize monitoring to specific risks. Disparate organizations, industries, and locations can present different exposures and threats. Data formats, complexity, and availability can vary widely. Understanding trends and tailoring fraud solutions to specific organizational characteristics and situations, with business unit involvement, can help capture greater value from monitoring activities.

Capitalize on available resources. Some of the tools needed to conduct monitoring may already exist within the organization in areas such as finance and supply chain. Opportunities may exist to leverage these investments for risk management. Such collaboration can also enhance communication among different parts of the business, further strengthening fraud awareness.

Use a range of approaches. Different risks can require different analytical tools. Unsupervised modeling creates statistical profiles of normal transactions or entities and identifies outliers from these profiles. Supervised modeling uses documented fraud cases and output from unsupervised modeling to learn fraud characteristics, classify new observations as fraudulent, and detect what human observation cannot. If an apparent scheme involves collusion, network analysis may be required. And, if important clues appear to lie in unstructured text, natural language processing may be a valuable approach.

Involve stakeholders. Risk management is no longer just the responsibility of internal audit and compliance. Business units and other functions have roles to play in identifying, understanding, and addressing fraud risks.

Focus the effort. Monitoring solutions are complex, touching disparate parts of the business. The investment and time required to implement them can seem overwhelming. Rather than casting a wide net, consider conducting a focused, specific proof of concept to understand how a solution works and the value it could potentially provide.

Stop chasing, start preventing

Establishing effective fraud monitoring can seem a monumental task, one requiring significant investment, a major implementation initiative, and huge effort to wrangle the needed data. It needn't be overwhelming, however.

Start by abandoning the idea that an ideal situation and perfect data are required. Deploying analytics is just element of a longer and broader enterprise risk management and compliance journey — a vital part, but just one nonetheless.

Next, conduct a current state assessment to determine where relevant data resides, as well as the infrastructure and tools available to house and carry out continuous monitoring. Then, define objectives, establish focus areas, and prioritize needs and actions.

With such an approach, monitoring capabilities can improve iteratively over time, yielding deeper insights, fewer false positives, and a resilient organization less vulnerable to being blindsided by fraud threats.

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

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

About Deloitte
As used in this document, "Deloitte Advisory" means Deloitte & Touche LLP, which provides audit and enterprise risk services; Deloitte Financial Advisory Services LLP, which provides forensic, dispute, and other consulting services; and its affiliate, Deloitte Transactions and Business Analytics LLP, which provides a wide range of advisory and analytics services. Deloitte Transactions and Business Analytics LLP is not a certified public accounting firm. These entities are separate subsidiaries of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

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

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

About Deloitte
As used in this document, "Deloitte Advisory" means Deloitte & Touche LLP, which provides audit and enterprise risk services; Deloitte Financial Advisory Services LLP, which provides forensic, dispute, and other consulting services; and its affiliate, Deloitte Transactions and Business Analytics LLP, which provides a wide range of advisory and analytics services. Deloitte Transactions and Business Analytics LLP is not a certified public accounting firm. These entities are separate subsidiaries of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Deloitte.