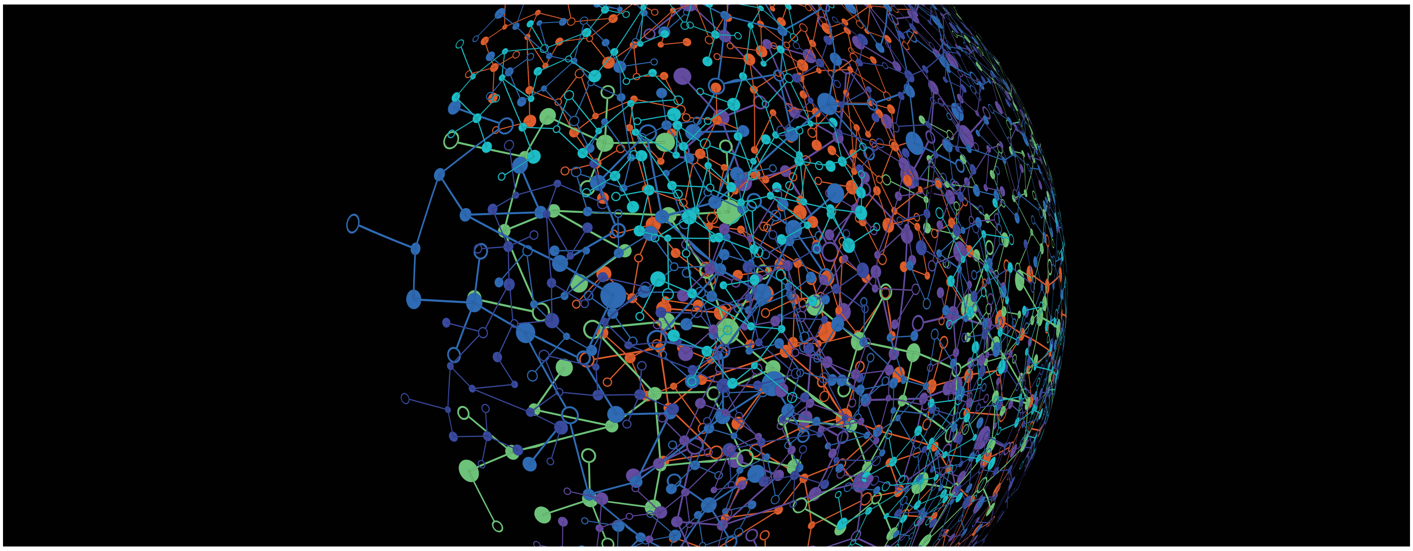


Forensic Focus on COVID-19

Unlocking the power of data: Managing fraud risk remotely

Deloitte's Forensic series around COVID-19 business impacts and steps you can proactively take to help respond to and recover from the outbreak and mitigate potential fraud and financial crime risks.

COVID-19 has resulted in significant negative economic and operational consequences for many organizations, as well as personal challenges for individuals to manage during these uncertain times. Many organizations, daily now, are analyzing the impact this crisis is taking on their supply chain, revenues streams, liquidity, and workforce, among a myriad of other impacts. The workforce is also affected by COVID-19. Two elements of the fraud triangle[1]—pressure and rationalization for organizations, employees, and third parties to perpetrate fraud during a time of crisis—typically rise, and anecdotal information to date informs us this crisis is no different.

The recent financial crisis of 2007–2008 may provide insight. After the crisis, a survey was conducted by the Association of Certified Fraud Examiners (ACFE) in which more than half of the certified fraud examiner (CFE) respondents indicated the number of occupational frauds they encountered during this financial crisis increased in comparison with prior year[2] Already during the current economic crisis, the SEC and US Department of Justice (DOJ) have identified fraud risks and issued notices that they will be actively investigating and prosecuting frauds stemming from or related to COVID-19.[3]

What is it about an economic crisis that causes organizations to become more vulnerable to fraud? Factors such as financial pressure to meet earnings expectations, employees who feel the need to protect the company or themselves, and gaps in controls resulting from decisions the business has been forced to make may contribute to increased fraud risk. Examples of fraud risks an organization might face during this crisis include insider trading, disclosure-related frauds, improper revenue recognition, inappropriate capitalization of expenses, insurance fraud, vendor fraud, and procurement fraud, among many others.

Remote-controlled investigations

Only is there a potential for a significant uptick in the volume of fraud, but organizations will also likely now be forced to investigate these frauds in a new paradigm where shelter-in-place or stay-at- home orders have been issued across the world. The traditional ways of investigating that have effectively been relied upon do not exist, or are severely restricted, as a result of the current environment. Instead, virtual methods of interviewing witnesses, reviewing documents, and obtaining access to and analyzing data will need to be used. As a result of these changes, there is an opportunity for fraud investigators to redefine how they conduct investigations, becoming more tech-enabled and relying more heavily on the insights data and analytics can provide.

Data scoping 2.0

Organizations will need to solve for this emerging paradigm: the need to monitor for increasing volumes of fraud while potentially doing so on a remote basis. One critical enabling asset to help transcend this challenge is more and better data. Data is virtual. It's the same whether accessed from an organization's offices or from someone's home and, when collected in disparate and nontraditional forms, provides the color to help unwind an alleged fraud scenario. The pandemic-induced working environment provides a different opportunity for organizations to develop a revised strategy to identify, source, and begin collecting the data that can be used to more carefully segment subpopulations and find the bad actors. Transactional data captures the behaviors, or decisions and actions, that people make when conducting a business activity. Organizations need to look at the data the same way the many bad actors do. For many bad actors, data is there to be exploited, with fraudulent acts obscured in overwhelming volumes. For organizations, data is available to identify those residual digital fingerprints that could not be wiped away. It will likely be critical to use the increasingly descriptive elements—beyond the obvious, traditional, or easy-to-work-with—captured in these large volumes of data to paint a full picture of what happened.

While transactions capture the act, communications can capture the intent or rationale. In other words, the "why" to the transactional "what." Organizations and consumers are increasingly becoming reliant on digital communication methods like email, video teleconferencing, SMS messages, and other nonconventional communication methods adding to the variety of data collected (such as odd timestamps of instant messages or logfiles that may demonstrate security control evasion). This creates opportunities for organizations to leverage their captured data to either detect fraud before any financial loss, compress the timeline in which fraudsters can effectively commit fraudulent acts, or enhance retroactive lookbacks on fraud.
It will often be critical to collect and synthesize multiple data sets, each capturing a part of the story, to enable the downstream analytics that better define the digital fingerprint of fraudsters and detect the fraudulent acts they commit.

Bytes to insights

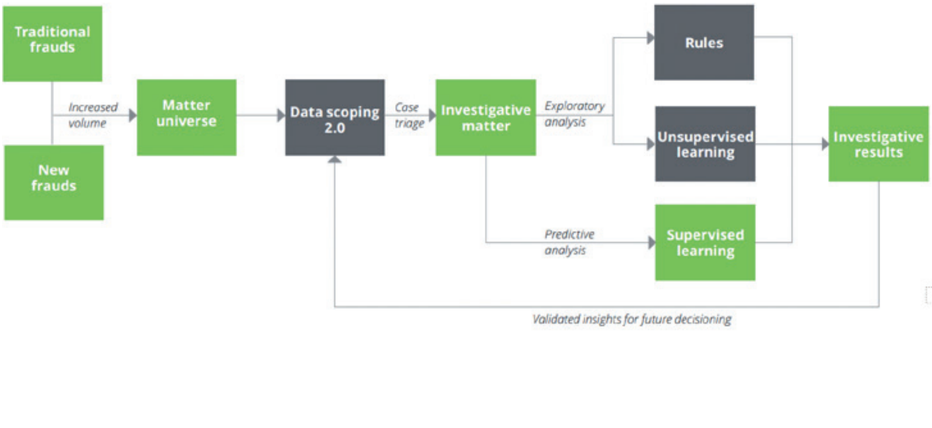
More and better data provides an opportunity for diverse and more effective analytics. This means a portfolio approach to case analysis, selecting an effective analytic technique for the given problem set. This starts with rules, which investigators can use to help understand fact patterns, perform conditions testing, identify threshold exceptions, and so on. Moving beyond rules, machine-driven analysis can also be used to efficiently identify outlier activity in the form of unsupervised or exploratory analytics (for example, density- based unsupervised machine learning to cluster segments of the population and automatically highlight outliers given specific mathematical thresholds).
And last, supervised machine learning leverages historical fraud cases to learn patterns and estimate the likelihood that a new investigation case is fraudulent.

Each technique in the portfolio serves a purpose in understanding the bigger picture. Rules-based machine learning and unsupervised methods can provide organizations with helpful insights to fight fraud—they can supplement and enhance traditional investigation practices by allowing analysts to mine data in a semi- automated fashion to find fraud and identify emerging vulnerabilities—while supervised machine learning can help organizations to monitor and control fraud sustainably..

This portfolio of techniques ultimately coalesces into a predictive fraud investigation methodology. The end result is probabilistic, or predictive, risk scores assigned to investigation cases based on the attributes of that case, thereby facilitating triage, as well as the discrete activities making up that case. These attributes can include statistical signals derived from metadata elements related to the case (for example, employees or functional units with a history of noncompliance with organizational controls) or data elements about the case itself (such as the volume, frequency, and price of a buying event in the supply chain). Data from transaction ledgers, emails, or conferencing software can provide meaningful insights on the behavioral tendencies of fraudsters, their prefraud actions, and the control vulnerabilities they take advantage of to commit crimes.

Resilience for the next time

Wherever an organization's antifraud capabilities sit on the maturity spectrum, data is the asset that can help transcend the limitations of time and physical presence. With more data and an understanding of how to effectively use it, organizations have the opportunity to embed more analytics into their processes to define, detect, and prevent fraud. Whether this involves selectively narrowing down segments of the population that need to be further investigated; reducing cycle times to enable organizations to more carefully monitor, triage, and investigate fraud; or automating more investigative processes, the efficiency and effectiveness of the investigator in this new world may be limited only by their willingness to become more tech-enabled. COVID-19 has changed the way many organizations do business and how some bad actors may evade the controls in place today. These changes will likely



persist in the post-COVID environment as organizations look to normalize operations. Companies should look to new processes and fraud methodologies to modernize compliance and fraud investigation functions to stay vigilant and guard against risk exposure resulting from the current pandemic and any future vulnerabilities.

Endnotes

[1] https://www.agacgfm.org/Intergov/Fraud-Prevention/Fraud-Awareness-Mitigation/Fraud-Triangle.aspx.

[2] https://www.acfe.com/uploadedFiles/ACFE_Website/Content/documents/occupational-fraud.pdf.

[3] https://www.sec.gov/news/speech/2009/spch120809rsk.htm

Vos contacts

Dawn Neisen
Director
Deloitte Forensic
dneisen@deloitte.fr
01 55 61 43 64

Gilles Granger
Director
Deloitte Forensic
ggranger@deloitte.fr
01 55 61 61 81

Géraldine Llorente
Partner
Deloitte Forensic
gllorente@deloitte.fr
01 40 88 78 30