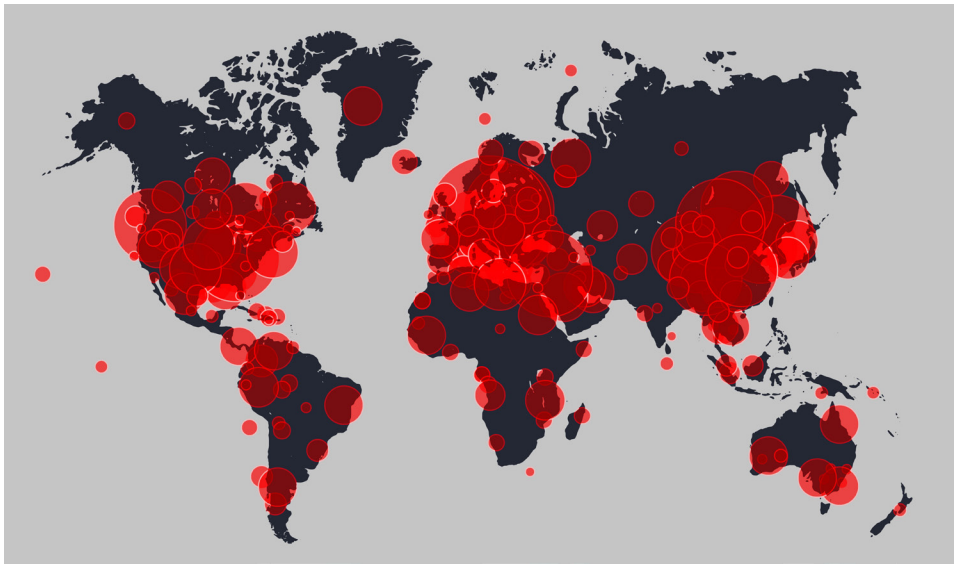
CORPORATE COMPLIANCE INSIGHTS
THE PREMIER GLOBAL NEWS SOURCE FOR COMPLIANCE, ETHICS, AUDIT & RISK

Investigating Fraud in a COVID-19 World: A Targeted Response Helps

by Sheila Mackay · May 26, 2020

Fraud levels increase in times of economic distress, and the global pandemic is creating a once-in-a-lifetime opportunity for financially rewarding mischief. H5's Sheila Mackay discusses what companies can do to quickly identify and prevent fraud.



The Brewing Storm

As companies strive to adjust to the altered state created by the COVID-19 pandemic, actors with ill intent will do the same, looking for ways to leverage the disruption and havoc the coronavirus has caused. In a recent article[1], Bruce Dorris, President and CEO of the Association of Certified Fraud Examiners (ACFE), suggests that the pandemic is a "perfect storm for fraud" and warns that organizations need to brace themselves for what will likely be an explosion of fraud in the near future.

At the same time, the U.S. government has made clear that recipients of funding from the Coronavirus Aid, Relief and Economic Security Act (CARES Act) should expect to be targeted for increased oversight and investigation by U.S. attorneys, who have been directed to "prioritize the investigation and prosecution of Coronavirus-related fraud schemes."[2]

All of this at a time when companies under economic stress may decide to cut non-revenue-generating compliance and audit functions, weakening some of the internal defense systems already in place for protection just at a time when risk oversight should probably be scaled up. With pressure to mollify investors or cut through pandemic-related barriers, companies (and employees) may be misrepresenting financial information, fast-tracking new suppliers or partners, taking due diligence shortcuts or corner-cutting or bypassing standard operating procedures in any number of ways, all of which increase vulnerability and risk. And to top it off, a newly remote workforce, including those who provide oversight, may be disoriented by modified workflows and communications channels, making it easy to overlook (or fail to report) irregularities, further increasing risk and making the enforcement of compliant behavior more difficult.

This confluence of factors that could weaken internal controls is no small matter. According to a new ACFE report[3], "a single case of occupational fraud costs the victim organization an average of more than $1.5 million" and lasts 14 months before detection. If the projected uptick in fraud pans out, many companies may face significant hardship. The faster any fraudulent activities can be detected, the better.

The report does note a few bright spots, however. Before the pandemic, there was an encouraging trend in the increase of anti-fraud controls — over 13 percent in the last decade — in the form of anti-fraud policies, hotlines, web-based forms and anti-fraud employee training. That should help, but maintenance, indeed fortification, of these tactics will no doubt be necessary.

Vigilance is Critical

What can companies do to proactively address the potential for fraud in light of these new stressors? Deterrence is key, of course, and a corporate culture bolstered by a strong code of ethics and good employee relationships should already be top of mind for any responsible company.

But challenging times come with harsh and immediate realities. Heightened sensitivity to tips, rumors, suspicion or isolated reports is crucial, even as employee communications and oversight may be occurring at a distance. Companies will need to be closely monitoring their anti-fraud controls for FCPA, AML and insider-trading violations, giving incoming tips the appropriate attention. (Note that a significant downturn in tips alone should be a red flag, suggesting that normal reporting channels may be disrupted.) Even a hint that something is amiss should warrant at least a preliminary investigation to determine if there is real cause for concern, but it is possible that today's resource constraints will make this even more difficult.

Data Monitoring: On the Front Lines of Fraud Detection

There are myriad monitoring systems available to companies to detect fraud in their processes, and with proper controls to identify anomalies they are front-line weapons for identifying potential malfeasance.

But the ability to probe vast stores of unstructured data — think email, text messages and documents — that may have been created or

circulated by possible perpetrators of fraud is equally important, especially if it can link to transactional abnormalities; this, after all, is what can expose the fraudster(s) behind the fraud. In some companies, fraud detection and data monitoring systems are integrated across the enterprise, enabling the use of analytics that can link information and activities, increasing a company's agility in responding to a potential problem.

Some companies also have compliance procedures in place to monitor unstructured data using pre-defined search terms or data classifiers to examine email communications and other data sources for language suggestive of fraud. If fraud is suspected, however — whether gleaned from data monitoring, tips, interviews or some other source — and further investigation is necessary, the challenge is often in determining the nature and size of the response. What data should you look at — and how much of it — in order to decide whether to pursue the matter or put it to rest?

Need to Investigate Unstructured Data? Use a Sound Methodology to Start Small

Not every potential threat calls for a formal investigation, which is disruptive at the best of times. Most Chief Legal Officers and compliance professionals know what risk patterns tend to look like in their industries, and this information can be leveraged in a preliminary analysis. What is known so far? What seems out of the ordinary and what is at risk? What unstructured data sources might be explored to uncover pertinent facts? Which custodians are most likely to be associated with that data?

Instead of undertaking a large-scale document collection, in-house subject-matter knowledge can be paired with appropriate data sampling, search expertise and advanced analytics tools to conduct smaller, targeted "micro-investigations," which begin with searching targeted samples and grow if and as warranted, branching out in specific directions as new facts are discovered. When executed with the proper sampling and search methodologies, these investigations can be pivotal in quickly determining whether a broader investigation — or any further investigation at all — is necessary.

Leverage Advanced Linguistic Search and Analytics for Faster, More Accurate Results

The exceptional results of some micro-investigations come from the skill of linguistic search experts, who are able to develop strategic, nuanced searches that factor in the ways human beings actually express themselves. They are able to target language patterns that may indicate concern, worry, surprise or secrecy, common elements in fraud communications. Brainstormed keyword lists by legal or investigatory teams are much less effective, as are standalone TAR tools, which are better at finding large quantities of similar documents rather than handfuls of exceptional documents — or verifying the lack of them.

In addition to linguistic search, the expert use of AI and advanced analytics can play an important role here, helping surface important information more quickly. For example, analytics tools can apply algorithms to identify relationships in email threads, leverage metadata relationships related to time and place or extract data characteristics that could be informative to an investigation, such as 1:1 emails. Text analytics can leverage AI techniques to organize text in meaningful ways so as to extract and derive meaning from unstructured data. Other analytics can be applied for the identification of personally identifiable information (PII) in documents and forms, critical in the investigation of identity fraud or cyber breach investigations.

Although analytics tools to apply to micro-investigation efforts may exist in-house, the requisite expertise for implementation may not. Even the most seasoned IT professionals may not have appropriate experience in data sampling or the advanced search and retrieval techniques that make such an approach successful, and linguistic expertise may not be available. If this is the case, there are a variety of legal support service providers who have the expertise and technologies that can help.

Bottom Line

The pressure financial institutions and other companies will face to expose and deter fraudulent activities will only intensify as a result of COVID-19. The growing trend over the past years to expand anti-fraud controls will no doubt help, but companies should be prepared to leverage advanced techniques and technologies that can accelerate both the detection and investigation of fraudulent activity. For investigations that involve querying unstructured data, a methodology that leverages data sampling, linguistic search expertise and advanced analytics for small, targeted investigations, can quickly and accurately expose bad facts, providing an invaluable addition to the anti-fraud arsenal.

[1] Coronavirus Pandemic is a Perfect Storm for Fraud, ACFE press release

[2] Attorney General William P. Barr Urges American Public to Report COVID-19 Fraud, The U.S. Department of Justice press release

[3] ACFE Report to the Nations: The Average Fraud Costs Companies More Than $1.5 Million, ACFE press release

Sheila Mackay *is Senior Director of eDiscovery Services at H5. Sheila has more than 25 years of experience in the legal services industry including product development, professional services, operations, management and business development. Sheila leverages these skills working with H5's client services, infrastructure and technical services teams.*

H5