May 8, 2020

Ropes & Gray and Forensic Risk Alliance Alert – COVID-19, Data Analytics & the FCA: Big Response, Big Data, Big Risk

This article was co-authored by: Jim Dowden, Ryan Rohlfsen, Kendall Dacey, and Kendall Scott Cowles of Ropes & Gray in collaboration with Matt Bedan, Jen Baskin, Neil Goradia, and William Mui of Forensic Risk Alliance. Further information about FRA is available here.

Attorneys
James P. Dowden
Ryan Rohlfsen
Kendall Dacey
Kendall Scott Cowles

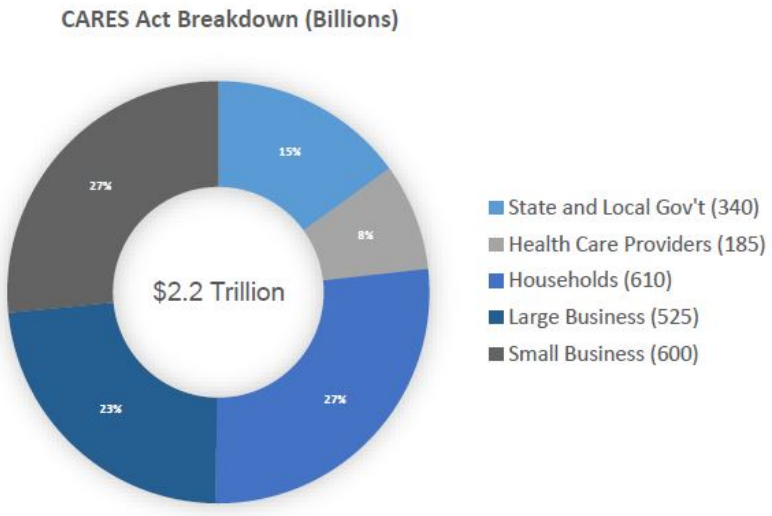
Forensic Risk Alliance
Matt Bedan
Jen Baskin
Neil Goradia
William Mui

Abstract

The U.S. federal government's record $2.2 trillion response to the Covid-19 crisis will inevitably bring with it heightened scrutiny from government and private watchdogs, and a corresponding wave of False Claims Act (FCA) enforcement. Litigation trends in the FCA space over the past decade indicate this wave of enforcement will be heavily data-driven, with whistleblowers and privately funded relators filing the large majority of lawsuits. These parties will rely heavily on advanced data mining and analytics techniques to spot potential indicators of fraud ("anomalous data") in publicly available data sets. Concurrently, the turmoil naturally caused by a public health crisis this widespread is likely to create large volumes of data that would be considered anomalous under normal circumstances. For example, as the health care system is strained with resource shortages and patient influx, organizations will be increasingly susceptible to good faith billing/coding errors, inaccurate certifications and documentation, and other anomalous data that would normally be a potential indicator of an FCA violation. It is unclear how enforcement agencies will view this data in the context of FCA enforcement, which often uses trend analysis to identify deviations from 'normal' as a means to prove guilt. Regardless, whistleblowers and privately funded relators will have immense incentives to opportunistically leverage this data to their advantage. This article seeks to predict and explain the enforcement environment that we are likely to see over the coming months and years, and provide advice for organizations seeking to mitigate the risk that their data may be creating in the context of expected heightened FCA enforcement.

An unprecedented response

In an effort to combat the devastating economic effects of the COVID-19 pandemic, the U.S. Congress recently enacted the $2.2 trillion Coronavirus Aid, Relief, and Economic Security (CARES) Act. This record expenditure includes over $100 billion for



public health services to respond to the pandemic, and over $1.8 trillion in stimulus money for individuals, businesses and state/local governments.

Although the allocation details for these funds are not fully established, what is clear is that the government intends to distribute the payments with relatively minimal bureaucratic oversight, given the urgent need. In addition to the extensive economic assistance, the federal government has collectively modified, relaxed or suspended a number of regulatory requirements, many of which were in place to prevent fraud and waste.

Some examples include:

- The Centers for Medicare and Medicaid Services (CMS) blanket waiver of certain aspects of the physician self-referral law (Stark Law), with parallel waivers regarding anti-kickback enforcement of the same statute from the Department of Health and Human Services Office of Inspector General (OIG).
- A suspension of Medicare sequestration (mandatory 2% reduction in payments to all Medicare providers) for the remainder of 2020.
- A 20% increase in maximum benefit amounts for patients hospitalized with COVID-19.
- The expansion of the range of reimbursable treatments and services under Medicare/Medicaid, including diagnostic products and treatments not yet approved by the U.S. Food and Drug Administration (FDA).
- An acceleration of Medicare payments to hospitals with cash flow shortages.
- A pledge to reimburse hospitals and physicians that treat uninsured COVID-19 patients.
- The significant expansion of telehealth services for Medicare patients, including expedited payment for telehealth services, waiver of the requirement of a pre-existing physician/patient relationship to be treated through telehealth technology, and waiver of the face-to-face requirement for dialysis, home health and hospice patients.

Out of necessity, in the context of a national emergency, many of these changes were enacted with little or no detailed guidance from the agencies responsible for oversight. For bad actors, this influx of cash and relaxation of regulatory oversight represents a unique opportunity. For the vast majority of organizations responding to this crisis in good faith, it creates complex compliance obligations and risk. The CARES Act and other aspects of the COVID-19 response are collectively creating new regulatory and contractual obligations that many organizations have no experience administering, and no infrastructure to monitor. In addition, these new obligations are appearing in uniquely difficult circumstances that, in and of themselves, are likely to challenge compliance teams. Organizations should be wary of the operational and compliance risk this entails.

Consider, for example, the government's pledge to reimburse physicians who treat uninsured COVID-19 patients, taken alongside the Centers for Disease Control and Prevention's (CDC) recommendation that doctors utilize telehealth facilities when possible. If a physician then used telehealth technology to diagnose an uninsured patient with COVID-19, but cannot confirm the diagnosis with a blood test, would the service be reimbursable? If so, what documentation should be retained regarding proof of the patient's condition and insurance status? Similar questions are raised by the executive invocation of the Defense Production Act. Reportedly intended to prohibit the export of specific types of personal protective equipment and ventilators, the Executive Order itself is not so limited. The text technically bans the export of

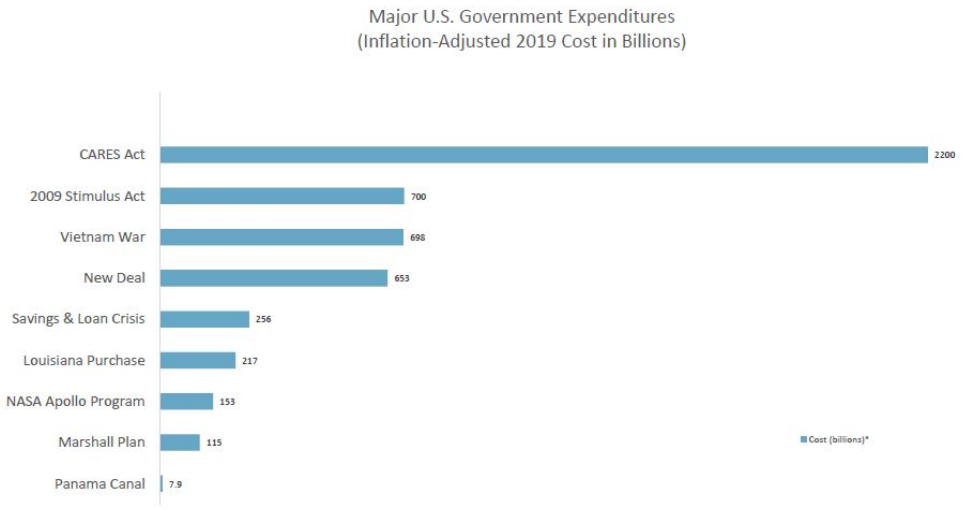
"medical resources needed to respond to the spread of COVID-19".[1] For manufacturers of other types of "medical resources" that could conceivably fall under this umbrella, the applicability is unclear.

The current regulatory setting is particularly volatile for the pharmaceutical and medical device sectors. In the past month alone, the FDA has issued at least 35 new guidance documents outlining new or modified guidelines for key risk areas such as diagnostic testing, patient monitoring and adverse event reporting, conduct of clinical trials, and supply chain integrity.[2] Although these guidance documents do not in and of themselves have the force of law, the CARES Act does create significant new statutory obligations around supply chain integrity for both pharmaceutical and device manufacturers. These manufacturers must now report to the FDA any anticipated disruptions to the supply of drugs and devices, that are "critical to the public health during a public health emergency." In addition, covered manufacturers must now create and maintain redundancy risk management plans to identify and evaluate risks to the supply chain of the drug or device.[3]

It should also be noted that potential CARES-related compliance risk is not limited to health care organizations, as the majority of the $500 billion relief fund for businesses and state/local governments comes with significant strings attached. Depending on the program, businesses that utilize federal CARES assistance will likely have to remain neutral in any unionizing efforts during the terms of the loans, keep jobs in the U.S. over the life of the loan, and use the stimulus money to retain at least 90% of their pre-pandemic workforce through at least September 2020. For organizations and industries unaccustomed to the scrutiny that comes with federal contracting, requirements such as these can create significant uncertainty and compliance risk. This is particularly true where, as here, new standards are coming into force at a rate and in a manner that makes common compliance strategies, such as analyzing industry best practices and peer-group benchmarking, all but impossible.

The coming FCA backlash will be aggressive

It seems inevitable that an expenditure of resources as extraordinary as the CARES Act will be followed by a wave of FCA enforcement. Before the Act was even passed, the Deputy Attorney General Jeffrey Rosen commented on the "unfortunate array of criminal activity related to COVID-19 pandemic" and directed all U.S. Attorneys to prioritize the prosecution of COVID-19-related fraud schemes,



[1] https://www.whitehouse.gov/presidential-actions/executive-order-prioritizing-allocating-health-medical-resources-respond-spread-covid-19/.
[2] https://www.fda.gov/emergency-preparedness-and-response/coronavirus-disease-2019-covid-19/covid-19-related-guidance-documents-industry-fda-staff-and-other-stakeholders.
[3] CARES Act, Section 3112.

emphasizing that "[c]apitalizing on th[e] crisis to reap illicit profits or otherwise preying on Americans is reprehensible and will not be tolerated."[4] In response, each U.S. Attorney's office has appointed a Coronavirus Fraud Coordinator for its jurisdiction, and most regional offices have assembled task forces in conjunction with the FBI and local law enforcement. Less than a week after passage of the legislation, the DOJ has already charged at least three cases and announced numerous other investigations related to COVID-19 fraud. This number is sure to rise as the funds are fully disbursed.

In addition, and similar to the 2008 Emergency Economic Stabilization Act (EESA) and Troubled Asset Relief Program (TARP) legislation, the CARES Act includes extensive and overlapping mechanisms of administrative oversight. The Act establishes a Congressional Oversight Commission and a Special Inspector General for Pandemic Relief (SIGPR), who will have subpoena power over private individuals and companies, as well as a $25 million budget to pursue misallocated federal funds. Moreover, the Government Accountability Office (GAO) recently confirmed reports that it is planning to task most of its 3,000 investigators and analysts to an upcoming "blizzard of audits" of CARES Act disbursements.[5] Similarly, the U.S. Treasury Department has stated that it will direct the Small Business Administration to audit every recipient of a Paycheck Protection loan in excess of $2 million.[6]

Adjacent to these layers of Congressional oversight, the CARES Act also established the Pandemic Response Accountability Committee within the Executive Branch's OIG. Shortly after the Committee was established, President Trump replaced its active chairman with Sean O'Donnell, from the Environmental Protection Agency, who spent 15 years as a fraud prosecutor with the DOJ.[7] Although the Administration has not yet publicly commented on the move, it likely signals an intent to prioritize a crackdown on fraud and abuse in the wake of CARES and COVID-19.

It seems equally likely that the FCA will be the primary mechanism to carry out this crackdown. Not only is the FCA one of the Justice Department's most powerful tools to combat fraud, it also provides ample incentives for private whistleblowers to do the same, through private, or "qui tam," suits. Specifically, the FCA allows for mandatory treble damages for violators, of which 15-30 percent is statutorily directed to the whistleblower, or relator. According to the DOJ, of the approximately $3 billion in FCA settlements filed in 2019, over $2.1 billion arose from qui tam litigation, resulting in over $265 million in payouts to individual relators. Over the past five years, relators have collected over $2 billion in FCA awards.

The resulting enforcement will be data-driven

In 2011, CMS made the policy decision to release anonymized Medicare claims data to the public in an effort to promote health care service transparency.[8] Ever since, the clear trend in FCA enforcement has been the rise of data-driven qui tam litigation. With access to claims information, individual whistleblowers now have a wealth of data that can be put to work to spot trends and outliers, and lend credibility to allegations. Taking the trend to its extreme, a number of recent qui tam lawsuits have been pursued by corporate data analytics relators with no connection to the defendant, or first-hand

[4] https://www.justice.gov/file/1262771/download.
[5] https://www.politico.com/news/2020/04/20/watchdog-trump-coronavirus-audits-192272.
[6] https://www.cnbc.com/2020/04/28/small-business-loans-above-2-million-will-get-full-audit-to-make-sure-theyre-valid-mnuchin-says.html.
[7] https://www.wsj.com/articles/trump-removes-acting-defense-department-inspector-general-11586277895?mod=e2tw.
[8] https://www.cms.gov/newsroom/fact-sheets/final-rule-release-medicare-data-be-used-performance-measurement.

knowledge of the allegations they make. Rather, these entities use proprietary data-mining and analytics techniques to identify anomalies in Medicare and other public data sources as a means to pursue FCA judgments. Although these data-mining relators have met with mixed success, their access to data continues to grow, and they will undoubtedly seek to use it to cash in on claims irregularities.

Government enforcement efforts have followed a parallel track. A notable example is the 2015 industry-wide investigation of compound pharmacies, whereby the DOJ utilized a range of data analytics techniques to identify anomalous billing to the Department of Defense's TRICARE program. Following this, the DOJ created a dedicated Office of Data Analytics, charged with detecting fraudulent transactions and supporting the DOJ, OIG, FBI and other agencies. The Data Analytics Office has been highly effective in generating investigative leads, as evidenced, for example, by the massive crackdown on alleged opioid over-prescription seen during 2018 and 2019. In speaking to the strategy behind the DOJ's opioid fraud response, former Attorney General Jeff Sessions singled out the importance of "leveraging the power of data analytics."[9] Similarly, other enforcement agencies, such as the U.S. Securities and Exchange Commission (SEC), have advocated for robust data analytics programs.[10] SEC Chair, Jay Clayton, stated that the agency's reliance on data analytics work is "more important than ever," and that "data analytics can help [the SEC] use [its] existing resources more efficiently and effectively."[11]

As the government continues to perfect its utilization of data analytics, its access to data is likely to continue to grow in the wake of COVID-19 and CARES, and far exceed that of whistleblowers and private relators. For example, in addition to payment data, both CMS and state agencies also have access to data created through contracted audits of Medicare claims. These audits are more comprehensive than publicly available claims, and rich with data points, which enable forensic teams to focus their analytics with a high degree of specificity. In addition, this February, CMS laid out an aggressive plan to begin gathering source data directly from patient medical records to support the agency's fraud enforcement efforts. While commenting on the program, CMS's Head Administrator Seema Verma stated that the organization was "moving to a system where we're able to take quality data from the EHR [electronic health record], combine it with claims data, and see what's going on in program integrity. And we should be able to identify those high-quality providers on the front end, and then identify [fraud], I think, in a way, that's been fairly unprecedented."[12] If successful, CMS and DOJ are sure to use this unprecedented access in support of their mandate to aggressively enforce FCA violations in the wake of CARES.

The devil will be in the details

Although the headline-making FCA cases still involve classic fraud and bad actors, most modern FCA enforcement actions are pursued under a Legal False Certification theory. What this means is that many companies are incurring FCA fines not because their claims are false per se but because they submitted accurate claims that were not in compliance with an applicable statute, regulation or government contract provision. These violations are often highly technical, and under normal commercial circumstances would most likely be considered a breach of contract, not fraud. For example, in

[9] https://www.justice.gov/opa/pr/national-health-care-fraud-takedown-results-charges-against-601-individuals-responsible-over.
[10] https://www.law360.com/articles/1164564/what-securities-pros-need-to-know-about-sec-data-analytics.
[11] Jay Clayton, SEC Chairman, Keynote Remarks at the Mid-Atlantic Regional Conference (June 4, 2019), https://www.sec.gov/news/speech/clayton-keynote-mid-atlantic-regional-conference-2019.
[12] https://www.fiercehealthcare.com/tech/cms-launching-pilot-program-to-give-providers-direct-access-to-claims-data.

2019 Cisco Systems paid $8.9 million to settle an FCA whistleblower claim based on the allegation that the video surveillance equipment the company provided to the federal government did not meet all of the cybersecurity standards outlined in the procurement contract.

It should also be noted that the FCA does not necessarily require that the defendant be aware of the contract/compliance violation; only that the violation should have been discovered through reasonable due diligence. For practical purposes, this means that corporations must implement "proactive compliance activities conducted in good faith by qualified individuals" to monitor compliance with their regulatory and contractual obligations to the government.[13]

Any organization familiar with the byzantine landscape of federal contracting can attest to what a challenge this is in practice. When the federal government is the customer, even the most mundane of transactions can be maddeningly complex and time-consuming. Take, for example, the (borderline comedic) standard federal contract for suppliers of office desks and chairs—otherwise known as GSA Multiple Award Schedule No. 47QSMD20R0001. This document is 47 pages long, with nine subsections and countless pricing, contracting, delivery, invoicing and service processes, including detailed requirements for wood joinery methods, plywood thickness, and design of coil springs in seats. Extrapolate this complexity out over tens of thousands of federal contracts covering everything from staplers to stealth bombers, and a picture begins to form of the massive scope of contract compliance risk for government suppliers.

Companies in certain industries, such as aerospace, defense and pharmaceuticals, are familiar with the complexity and have the structure and expertise in place to ensure compliance. However, the sweeping breadth of the CARES Act will create compliance obligations for many other industries, which likely do not have the same experience and resources. Hotels and restaurants, construction firms, airlines and banks, to name a few, are all going to be taking on compliance risk that their industries are unaccustomed to under normal circumstances.

Health care organizations in particular must be aware of the scrutiny that lies ahead. Though they are generally well-equipped to process typical fee-for-service claims, those organizations that accept cash infusions through the CARES Act, or partake in the blanket Stark Law waiver, must ensure effective compliance oversight of any associated regulatory and contractual obligations. For most organizations, this means understanding and controlling their operational data.

Avoiding the cross-hairs

For organizations contracting with the government via the CARES Act, or the COVID-19 response in general, it is essential to consider the full context of the risk landscape they have just entered. Part of this process should be to acknowledge the highly politicized environment in which CARES was enacted. As scrutiny follows over the effectiveness of the program, it will fuel the political impetus to prosecute fraud, both for reasons of optics as well as legitimate oversight. We are already seeing the early stages of this process play out.

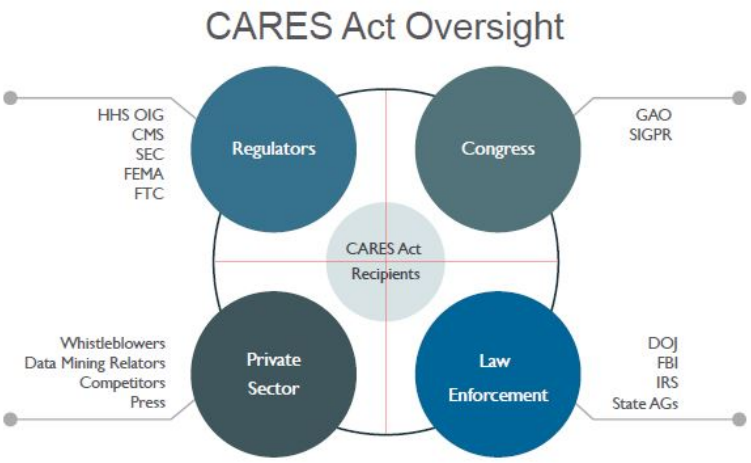
Another key element is the risk of anomalous data stemming from the uncertainty that is common around new federal programs. Even well-established programs with years' worth of administrative guidance can be challenging from a contractual and regulatory compliance perspective. For example, the Medicare program is over fifty years old, and is supported by a vast library of guidance documents, training resources and certification classes to assist providers with

[13] https://www.aafp.org/fpm/2016/0500/p12.html.

billing compliance. Despite these resources, the billing error rate for Medicare claims consistently hovers between 8–12%, resulting in billions of dollars in overpayments annually.[14] These sorts of compliance challenges will be compounded for organizations in the wake of CARES, which out of necessity was rolled out with unprecedented speed and minimal controls.

A third element is the disruption caused by the virus itself, which has impacted virtually every facet of corporate life in America. Many organizations are simply struggling to survive, working with staff shortages and hastily formed remote infrastructures. Many compliance organizations are not set up to provide oversight and advice in this environment, and are finding themselves on the sidelines. Adding to the complexity, almost all organizations are being forced to do more through remote technology than they have ever done, including increased email and teleconferencing, and utilization of web-based technologies for their procurement, logistics and contracting. All of these activities create data – in many cases it will be data that reflects on regulatory or contractual compliance, or otherwise creates risk that the organization may not have the policies, procedures or infrastructure to address.

The healthcare industry is likely to be particularly vulnerable. As the COVID-19 epidemic strains the system with resource shortages and patient influx, healthcare organizations will be increasingly susceptible to good faith billing/coding errors, inaccurate certifications and documentation, and other anomalous data that would normally be a potential indicator of an FCA violation. The final ingredient in the witches' brew, so to speak, is the backdrop of well-funded professional data-mining relators, incentivized whistleblowers and sophisticated government analytics watchdogs, who are ready, willing and able to capitalize on anomalous data.



To avoid the crosshairs, we recommend five critical activities:

1. Understand and document your obligations.

Organizations must carefully review eligibility requirements, reimbursement and invoicing procedures, certifications and other restrictions associated with every government transaction. Each program or contract should have a carefully thought out and documented end-to-end process. Checklists for regulatory/contractual obligations and maker/checker controls are also key. For government vendors, particular care should be paid to material pricing elements, such as Most Favored Nation clauses, fixed/long term pricing requirements, and price change triggers. As the obligations are

[14] http://medicareintegrity.org/error-rate-drops-but-medicare-still-lost-31-6-billion-to-preventable-billing-errors-in-fy2018/.

determined, each should be translated into corresponding rules and metadata to facilitate monitoring and alerts of potential violations.

2. Harness and organize your data.

The DOJ's 2019 "Evaluation of Corporate Compliance Programs" guidance makes it clear that organizations are encouraged to leverage data, metrics, and other objective evidence to test that their compliance program is working effectively. This guidance is premised on the DOJ's stance that a "hallmark of an effective compliance program is its capacity to improve and evolve" and that prosecutors should, accordingly, "consider whether [a] company has engaged in meaningful efforts to review its compliance program."[15] Particularly for larger, multinational companies, this process should go beyond simply tracking traditional compliance data (such as training and audit metrics) and encompass all of the various sources of operational data that could potentially be put to use. For example, in evaluating a company's compliance program, the Justice Department's guidance prompts prosecutors to ask: "[W]hat testing of controls, collection and analysis of compliance data, and interviews of employees and third-parties does the company undertake? How are the results reported and action items tracked?"[16] Further, the guidance focuses on what a company is doing to analyze reports and data for "patterns of misconduct or other red flags for compliance weaknesses."[17] The appropriate answers to these questions may vary depending on the size, structure, and risk profile of a company—there is no one-size-fits-all requirement. Rather, a company should be thinking about the most meaningful way to harness data, given its particular circumstances.

For some companies, this may mean setting up additional general ledger accounts or cost centers to track and account for every cent tied to their government contracting requirements. Financial tracking in this manner should be very much intertwined with the tracking rules discussed above, so that there is a clear correlation between the regulatory/contractual obligations mapped out in step one, and the sources of data that could potentially indicate compliance, or non-compliance, for each. Further to this step, vendors should see clear alignment between the accounting data that gets invoiced, and the operational data underlying it. If there is disagreement between the two sources, it should be cause for further investigation.

Finally—and consistent with the theme of focusing on meaningful efforts to optimize effective compliance—do not blindly trust outside data sources. Approach them critically and do the due diligence necessary to understand where the data comes from and how it was created. Validate it using related data sets you have access to, and exercise audit rights for higher-risk vendors. The better you know the data you are using, the better you can leverage it in your internal monitoring, investigations and compliance analysis.

3. Prioritize compliance and monitor systematically.

In the absence of clear guidance, companies should adopt stringent compliance and risk management oversight, focusing particularly on data monitoring and documentation. Organizations should be aware that a robust and current data environment (complementing a risk-based compliance program) is seen positively by regulators. To that end, maintain a

[15] https://www.justice.gov/criminal-fraud/page/file/937501/download.
[16] *Id.*
[17] *Id.*

clear and comprehensive audit trail in ERP [enterprise resource planning] and data systems, and ensure that you document all system reviews, upgrades, or enhancements undertaken in response to new regulation.

Once the necessary tracking and rules are implemented, the output and reporting should be systematic, transparent, and insightful. In short, if your monitoring mechanisms do not give clear insight into possible issues and escalate red flags to the appropriate stakeholders, then they are not serving their purpose. Additionally, human reviewers should be trained thoroughly on the underlying obligations and corresponding monitoring rules to test compliance. For example—What constitutes an issue? What is a false positive? And how can this information be cycled back into the process to make it more efficient, but more importantly, more effective?

4. Utilize data analytics.

By utilizing advances in data analytics, organizations can enhance conduct detection and replace extensive manual controls and verification activities. To do this effectively, you must leverage the data of all relevant sources, including sales and product data, performance-management data, and customer/patient records. An inclusive data analytics model can give a view of risk across activities, business units and geographies. Advanced analytics like machine learning and artificial intelligence can be very useful in these constructs. That being said, effective monitoring can be developed and deployed quickly using well-thought-out rules and checks if you understand your data's strengths and weaknesses. This approach gives you time to develop more advanced analytics to ultimately help validate and enhance your core approach.

You should also consider creating specific sets of compliance reports built directly around government claims or government compliance, and embedding them directly into your Executive Reporting Portfolio. Finally, diligent audit and issue remediation should be applied as soon as possible, including continuous review of analytics to remediate findings.

5. Bolster internal whistleblower programs.

An effective internal reporting mechanism is not only a key part of the DOJ's Guidance, but also an essential element of a strong compliance culture. Studies have shown that strong internal whistleblower programs help foster an atmosphere of trust and open communication, which increases the odds that an employee with a compliance concern will report internally, instead of through the government. Ultimately, companies with higher usage of whistleblower programs have statistically fewer lawsuits and enforcement actions.[18] As such, it is critical that organizations take internal whistleblower reports very seriously, and remediate accordingly.

[18] https://hbr.org/2018/11/research-whistleblowers-are-a-sign-of-healthy-companies.