ARTICLE

Leveraging Your Company's Existing Data to Reduce Antitrust Compliance Risk

I. Introduction

There is increasing emphasis for corporations to implement antitrust compliance programs that will deter and detect collusive behavior. In 2019, the Department of Justice (DOJ) announced that it will consider compliance at the charging stage in criminal antitrust investigations,[1] which means compliance programs are not only "good" to have, but they are also a primary focus for the DOJ, making them a "must-have" for any corporation that is susceptible to antitrust risk.

One important component of a compliance program is using data and analytics to mitigate antitrust risks. Antitrust compliance monitoring through use of data analytics can seem complicated, but for many executives asking questions about minimizing risks of price-fixing, market allocation, or bid-rigging exposure, most of the tools to provide answers can be found within your organization. Many times, small actions with meaningful impact can create a more robust compliance monitoring process without a huge investment in resources. Due to the sophistication of most companies' technology systems, data analytics can be seamlessly integrated into an antitrust compliance program and monitoring process to create an integrated and enhanced solution.

As companies are anticipating enhanced antitrust enforcement, and with the DOJ's Antitrust Division's (the Division) 2019 guidelines for evaluating antitrust compliance programs (Antitrust Guidelines) as a roadmap, now is the time for corporations to organize data and systems to implement or enhance monitoring tools for antitrust risk.

II. Why Compliance Programs Matter

In July 2019, the Division announced a new policy to incentivize corporate compliance. For the first time, the Division stated that it "will consider compliance at the charging stage in criminal antitrust investigations."[2] To this end, the Division also published a guidance document that focused on evaluating compliance programs at both the charging and sentencing stages of investigations.[3] The goal of any antitrust compliance program is to prevent, deter, and quickly identify collusive activity. In addition, the existence and effectiveness of a compliance program is relevant to the Division's sentencing recommendation.[4] The federal Sentencing Guidelines provide for a reduction in a corporate defendant's culpability score if the company has an "effective" compliance program under the Antitrust Guidelines.[5] Given the thoroughness of the Antitrust

[1] https://www.justice.gov/opa/pr/antitrust-division-announces-new-policy-incentivize-corporate-compliance

[2] https://www.justice.gov/opa/pr/antitrust-division-announces-new-policy-incentivize-corporate-compliance

[3] Evaluation of Corporate Compliance Programs in Criminal Antitrust Investigations (U.S. Department of Justice, Antitrust Division, July 2019)

[4] United States Sentencing Guidelines § 8D1.1.

[5] United States Sentencing Guidelines § 8C2.5.

Guidelines, one could infer that any program that was hastily set up to seemingly meet these parameters, without having the actual elements in place to detect anticompetitive conduct, would be quickly deemed inadequate. Overall, the emphasis on monitoring, auditing, and reporting mechanisms was unmistakably conveyed in the Division's guidance.

Since this update in 2019,[6] we have now seen outcomes of the Antitrust Guidelines play out. In some recent cases, the Antitrust Division announced that it had reached Deferred Prosecution Agreements (DPAs) with investigated companies to resolve charges of antitrust violations. In addition to admitting to wrongdoing and paying penalties, the DPAs required these companies to maintain an antitrust compliance program, including, in some instances, the provision of annual reports to the Division regarding the remediation and implementation of these programs.[7]

III. How To Incorporate Data Analytics into Your Company's Compliance Program

Data analytics can be a critical component of a company's antitrust compliance program. The use of technology, and specifically data-mining analytics, in antitrust compliance program monitoring provides a time- and cost-efficient means of uncovering material information quickly, which allows companies to quickly assess antitrust risk. Many times, monitoring can be done using existing data and internal systems, such as enterprise resource planning (ERP) systems and customer relationship management (CRMs), business intelligence systems, and communication platforms.

For example, a company's data could be used to proactively identify pricing and communication patterns that may indicate collusive behavior. Transactional data behavior analyses, in which price and quantity screenings are put in place, should be considered in the development of an antitrust compliance monitoring solution. This could include data that the company already uses to measure commercial success (Sales/Pricing/Operations) and technology the company uses to manage communications (e-mail, IM, mobile devices). From email and audio files to enterprise-level social collaboration and other cloud platform data, a well-rounded compliance program includes disparate sources to provide a holistic view of a company's potential antitrust risk and compliance.

When incorporating data and analytics into a compliance program monitoring process, several steps should be taken:

— **Establish Requirements:** It is important to start by identifying what is reasonable within your company's budget. Emphasize simplicity and impact over complexity and precision. You can right-size your company's monitoring solution to fit your company's needs, including leveraging existing software, or supplementing with appropriate add-ons, to facilitate seamless monitoring of communications, with minimal business interruption. You can also develop a user-friendly "dashboard" drawing from sales and operations data that displays information by utilizing charts and graphs to visually detect patterns and outliers.

[6] https://www.justice.gov/opa/pr/antitrust-division-announces-new-policy-incentivize-corporate-compliance

[7] https://www.justice.gov/opa/pr/leading-cancer-treatment-center-admits-antitrust-crime-and-agrees-pay-100-million-criminal; https://www.justice.gov/opa/pr/ready-mix-concrete-company-admits-fixing-prices-and-rigging-bids-violation-antitrust-laws

— **Use Readily Available Data:** There is a wealth of data that can be used in antitrust monitoring, including time and expense entries, sales transactions, market surveys, publicly available data, internal and external communications, and much more. While external data sources can aid in robustness of analysis, companies should not shy away from implementing a data-driven monitoring solution for worry of conducting time-intensive studies, reconfiguring their internal data capture, or integrating new data sources into their systems. One way of looking at this is to utilize the underlying data many companies already use to develop *Key Performance Indicators* and to change the lens with which they are analyzed to develop into *Key Risk Indicators*. For communications monitoring, the issue is often having too much data. This issue can be addressed by identifying a subset of custodians and data sources to review based on the Company's identified antitrust risks and communication protocols. With a more manageable set of data, a company can identify communication patterns that suggest increased interaction with competitors or other antitrust red flags.

— **Define Thresholds:** Incorporating data analysis into an antitrust compliance monitoring solution requires a review of trends over long periods of time. Unlike anti-bribery or corruption compliance risk, there is no single event or transaction recorded in an ERP system that would give rise to an enforcement concern. Rather, it is a series of events or transactions, observed within the appropriate time and reference scope, that indicate potential antitrust concerns. Consequently, it is important to establish objective thresholds to know when to trigger deeper investigation.

— **Fine-tune the Model:** The best models learn and improve over time. This includes fine-tuning key words and phrases to increase accuracy of communication monitoring and incorporating contextual business information into pricing analysis, such as the length of your company's typical sales cycle, how often your company updates global prices, etc. Reviewing the data at regular intervals to assess proximity to thresholds and assess outliers is key to improving the model.

— **Determine Response Plan:** Red flags generated from pricing analysis should be investigated by drilling-down to identify the time period, product, region, person, etc., that warrants further review via individual interview or additional communication screening. In addition, a well-documented series of steps is needed to ensure that problematic information is addressed quickly and that the same process is followed in every situation.

— **Integrate With Other Audit Components:** One of the elements the DOJ will look for in any compliance program is whether the program has built-in periodic review, monitoring, and auditing components. It is crucial that your company's antitrust compliance program monitoring solution is integrated into the other audit components of your company's business to make it successful.

IV. What You Should Consider When Implementing a Compliance Program

In addition to the steps outlined above, there are key topics to consider that will be unique to each organization and industry that will aid in implementation and adoption of your company's antitrust compliance program.

— **Fact Patterns vs. Deep-Dive Analysis:** Consider using the data you already have to track basic patterns/trends rather than doing a complicated pricing study. A company's own sales and cost data is often readily available and can be used to develop screens based on econometric principles that do not require a bespoke or extensive economic analysis. The same is true for evaluating employees' communications: one out of context message does not make an antitrust violation, but a pattern of communication (particularly with competitors) can be cause for concern. An important part of taking such an approach is training the compliance team on how to interpret the monitoring results and having a plan in place for determining when it may be helpful to seek outside assistance.

— **Red Flags vs. Yellow Flags:** Unlike anti-corruption, sales and operations data alone cannot show a violation of antitrust laws related to price-fixing, market-allocation, or bid rigging. In many jurisdictions, the agreement to collude is the illegal action. As such, communication screening tools are a clear way to monitor for "red flags" such as improper communications among competitors, which can be indicative of an agreement. However, sales and operations data can identify "yellow flags" that can be combined with other data points (communications review, interviews, etc.) to determine if compliance issues exist. The yellow flags serve as a lagging indicator of potential misconduct and allow your company to better allocate resources as part of an audit review.

— **Be Objective, But Be Yourself:** As mentioned earlier, objective thresholds and tolerance ranges help minimize false positives and can provide a starting point for your company's plan of action. However, these need to align with the company's risk profile, culture, jurisdiction, and available resources.

— **Limit the Scope with Structure:** Communications analysis can be set up for specific high-risk business units or positions (*e.g.,* sales), but guardrails are needed. Information governance, specifically acceptable use policies, should direct employees to use specific communication methods that are easier to monitor (*e.g.,* e-mail vs. text).

— **Start with a Pilot:** All organizations have limited resources, and compliance and audit teams are all too often faced with limited budgets. They are also very familiar with taking a risk-based approach. Incorporating new monitoring tools has the largest probability of success if first initiated in high-risk areas and treated as a pilot program. That approach usually satisfies the ability to fit within budget and provides an opportunity to fine-tune before rolling out on a larger scale.

V. Conclusion

Ultimately, DOJ is looking to ensure that compliance programs are well designed, applied in good faith, and effective in identifying potential antitrust violations. As part of this charter, the Antitrust Division will look to see if organizations are using any type of screening, including communications monitoring tools, statistical testing, and more – all of which require data and analytics for successful completion. While there is no "one size fits all" approach to implementation of antitrust compliance screening, the solutions do not have to be burdensome. Companies do not need to overspend on advanced tools and software; instead, with the right planning, a company's current information and communications systems can be used to seamlessly incorporate data analytics into any compliance program.

ADAM BERRY
Senior Managing Director
212.651.7104
adam.berry@fticonsulting.com

NICOLE WELLS
Senior Managing Director
416.649.8060
nicole.wells@fticonsulting.com

ANDREA LEVINE
Managing Director
212.499.3617
andrea.levine@fticonsulting.com