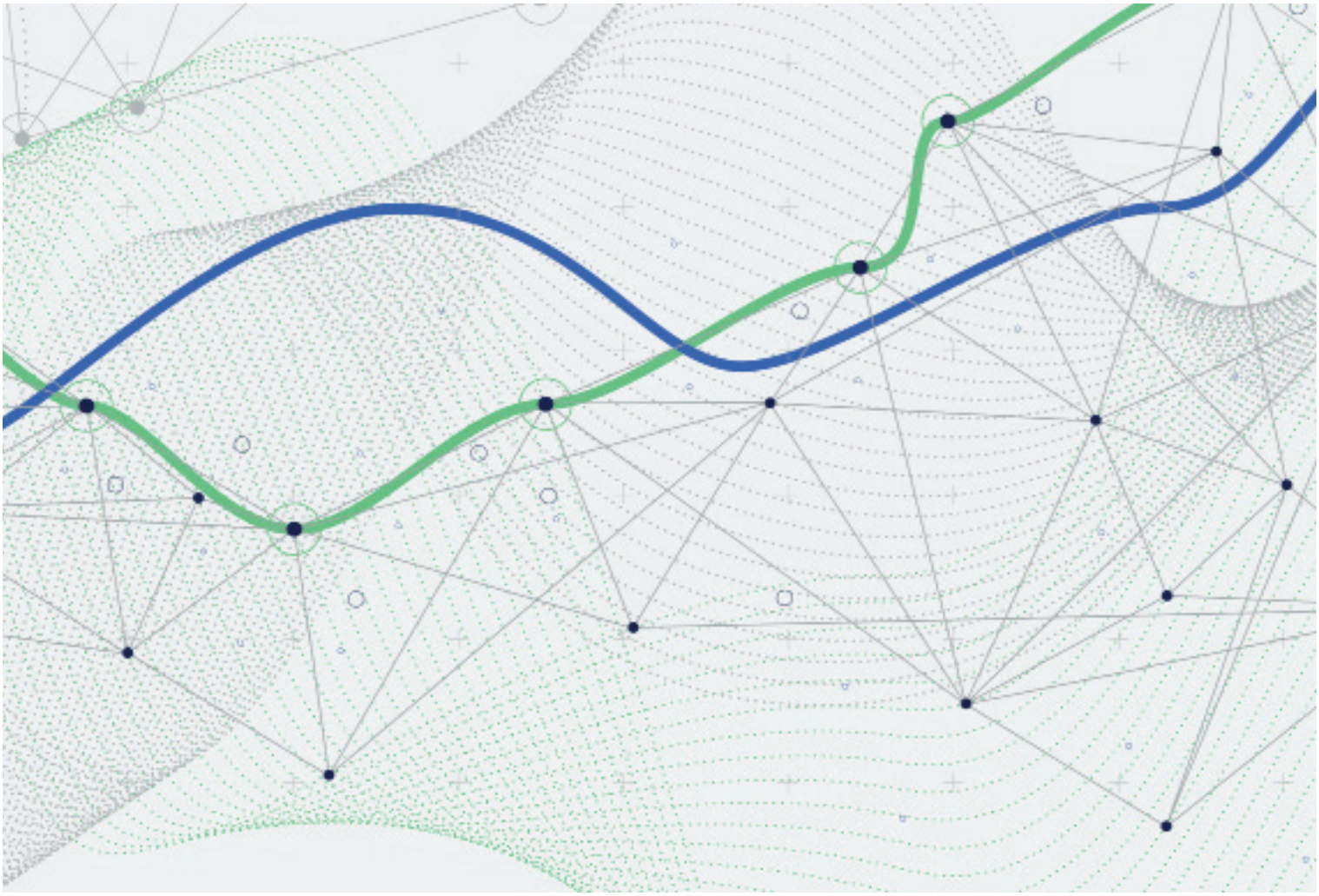
AN FTI CONSULTING REPORT – PUBLISHED 08/01/2022

Incorporating Data Analytics into a Company's Antitrust Compliance Review, Monitoring, and Audit Program



The Importance of Data Analytics in Antitrust Compliance Programs

In recent years, there has been increasing regulatory emphasis on the importance of antitrust compliance. The Antitrust Division of the United States Department of Justice (the "Division") and other enforcement entities outside of the U.S. have demonstrated the importance of antitrust compliance through issuing guidance for effective compliance programs. For example, in July 2019, the Division announced that, for the first time, it will consider compliance at the charging and sentencing stages in criminal antitrust investigations, with the intent to incentivize companies to implement robust and effective antitrust compliance programs.[1] In conjunction with this announcement, the Division published guidance describing its evaluation of corporate compliance programs which emphasized the use of data in the development, review, monitoring and auditing of a company's antitrust compliance program. [2]

Since the guidance was issued in the Division has incorporated antitrust compliance programs into the resolution of investigations. In some recent cases, the Division announced that it had reached Deferred Prosecution Agreements (DPAs) with investigated companies to resolve charges of antitrust violations, many of which have been made public.[3] In addition to admitting wrongdoing and paying penalties, the DPAs require that these companies develop or enhance their antitrust compliance programs. [4]

The mere existence of a compliance program, however, does not guarantee a DPA or a reduction in fines. The July 2019 guidance explains that, at the charging stage, the Division evaluates "whether the program is adequately designed for maximum effectiveness in preventing and detecting wrongdoing by employees." [5] At the sentencing phase, the Division may also consider "any measure taken by a company to discipline personnel responsible for the offense." [6]

The Division's guidance thus makes clear that, to be effective, an antitrust compliance program must prevent and detect misconduct. Elements such as thorough training, comprehensive policies and procedures, and a strong tone at the top are necessary to educate employees about prohibited conduct and establish a culture of behaving ethically. But, without additional elements, compliance and legal departments cannot assess the extent to which employees are acting in accordance with the stated policies. Periodic monitoring and auditing of a program is necessary to ensure commitment to compliance and detect any potential violation of the program or antitrust laws. Unlike preventative measures, methods of detection are objective and do not operate under the assumption that people will act in good faith. Further, detection processes can also act as a preventative measure by alerting the company to potential new risk areas for consideration and deterring employees from engaging in misconduct that could be discovered.

The Division's guidelines state that "[a]n effective compliance program includes monitoring and auditing functions to ensure that employees follow the compliance program" [7] and specifically ask:

- "What monitoring or auditing mechanisms does the company have in place to detect antitrust violations?" [8]
- "Does the company use any type of screen, communications monitoring tool, or statistical testing designed to identify potential antitrust violations?" [9]

1 Antitrust Division's "Evaluation of Corporate Compliance Programs in Criminal Antitrust Investigations", available at https://www.justice.gov/atr/page/file/1182001/download (hereinafter "July 2019 Guidance").

2 Id.

3 For example, see:
U.S. v Heritage Pharmaceuticals, Inc. https://www.justice.gov/opa/press- release/file/1174111/download;
U.S. v. Sandoz Inc. https://www.justice.gov/atr/case-document/file/1256306/download;
U.S v. Florida Cancer Specialists & research Institute https://www.justice.gov/atr/case- document/file/1281681/download;
U.S. v. Apotex Corp https://www.justice.gov/opa/press-release/file/1274706/download;
U.S. v. Taro Pharmaceuticals U.S.A. Inc https://www.justice.gov/atr/case- document/file/1307141/download;
U.S. v. Argos USA LLC. https://www.justice.gov/opa/press-release/file/1350481/download;
U.S. v Berlitz Languages Inc. https://www.justice.gov/atr/case- document/file/1365841/download

4 Id.

5 July 2019 Guidance at 3.

6 Id. at 16.

7 Id. at 10.

8 Id. at 10.

9 Id. at 10.

The Division also encourages the use of data analytics in periodic risk assessments by collecting and using metrics to detect antitrust violations and inform revisions to the compliance program. For example, the Division asks whether "bid information [is] subject to evaluation to detect possible bid-rigging" [10] and whether a company "evaluate[s] pricing changes for possible price-fixing." [11]

The Division's guidance underscores what some compliance departments already know: data analytics create objective, efficient and cost-effective solutions to quickly identify potentially anticompetitive trends and behaviors and build a more robust compliance program. It is important to note, however, that there is no "one size fits all" approach to the use of data analytics to monitor for antitrust compliance. The right solution will depend on the company's antitrust risk profile, data points and data sources, and existing software licenses. With the right evaluation and planning, companies can quickly and cost-effectively incorporate data analysis into their antitrust compliance program.

While the guidance provides a framework against which companies can assess their compliance programs, such programs should not only be implemented to address mistakes already made. Effective compliance programs enable employees to act with confidence in all business dealings, protect the organization from risk, and save the company money.

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

At the outset, an effective antitrust compliance program requires periodic assessments to identify the business practices at greatest risk for misconduct and ensure the program is tailored to address these activities. A company's risk profile serves as the basis for ensuring that its antitrust policy, procedures, training, and monitoring efforts address the business practices at greatest risk for misconduct. At a high level, an antitrust risk assessment should consider inherent industry risks, prior misconduct that occurred within the company or a competitor company, and recent developments in enforcement by the Division and other agencies. Review of company documents and interviews with key stakeholders should also be conducted to identify risks unique to the specific company and its business units, including the extent of competitor interactions, pricing and customer negotiation strategies, use of public and subscription- based market intelligence, and relationships with third parties including suppliers, brokers, and distributors.

A comprehensive risk assessment can help the company establish the scope and priorities for its compliance program, including further data monitoring efforts to test the effectiveness of the program. All organizations have limited resources, and compliance and audit teams are all too often faced with limited budgets, so monitoring efforts must reflect a company's risk profile and available resources.

Fortunately, significant resources are not necessary to develop screening procedures, which can be further improved over time. Once a company understands its most significant antitrust risks, it can identify the business units (or products), data points, and individuals most relevant for assessing compliance and developing appropriately tailored monitoring processes. In most instances, companies can utilize existing systems to assess compliance, such as enterprise resource planning (ERP) systems, customer relationship management (CRMs), business intelligence systems and communication platforms. Oftentimes, enabling additional functionalities or features to these existing systems or tools allows for collecting, screening, and assessing financial and communication data related to a company's key antitrust risk areas without significant added costs or technical challenges. The extent to which these capabilities can be leveraged will be dependent on the company's existing maturity level in data management.

In conjunction with the company's risk assessment, the company should conduct a detailed review of readily available data sources, including but not limited to internal and external communications, sales transactions, quote-to-cash or bidding data, procurement and supply data, and time and expense entries. A company can utilize existing data visualization software to serve as user-friendly tools to assist the company in visually detecting outliers and anomalies that may merit additional review, internal controls, and training to affected employees. Easy-to-build dashboards and trend analysis can identify areas for further evaluation such as margin variations unexplained by market conditions, deviations from standard business practices, or increased volume of interactions with competitors.

10 Id. at 7-8.
11 Id. at 7-8.

Further, ordinary course profitability and operational data can help a company identify which of these risk areas or business practices have the greatest likelihood of occurrence and impact on its business. A company should also evaluate whether certain data systems can also be integrated to streamline monitoring processes to create efficiencies elsewhere in a company's operations. Disparate data sources can be normalized and standardized, where applicable, and combined into a single data warehouse to combine attributes and dimensions for a wide and flexible range of analyses.

Finally, to increase likelihood of success in launching data monitoring, a company should consider a pilot program focused on only one risk-type or business unit. This will allow time for compliance to fine-tune the software, review process, and related workflows as needed before undertaking a larger monitoring effort. In the following sections, we will highlight specific considerations for the development and implementation of financial, operational and communications monitoring tools that can be incorporated into a company's antitrust compliance program.

Financial and Operational Data Monitoring Solutions

Companies utilize their financial and operational data to analyze historic performance and plan for future objectives. This data is also often used by companies to test compliance with other regulatory areas including bribery and corruption. For many companies, the same historical data available within the walls of its own organization can be utilized to develop monitoring or screening tools to evaluate whether indications exist that a potential antitrust violation has occurred. Companies should consider the following steps when incorporating data and analytics into a financial and operational monitoring process:

Identify key financial and operational data: As a starting point, a company should evaluate which financial metrics serve as the best indicators for evaluation based on its market and industry. For example, it is often appropriate to utilize the underlying data many companies already use to develop Key Performance Indicators and view it through a lens in which they are analyzed to develop into Key Risk Indicators. Operational data, including, for example, capacity, production, and output, may be relevant to the evaluation as well. A company should also consider incorporating other data points that may be readily available in their ERP or CRM systems, including, for example, sales region and sales team responsible for the contract or transaction. Additionally, external data sources can add robustness to a company's screening processes. Incorporating macro-economic indicators, new regulations and guidance, third-party industry data and surveys, and publicly available competitor data can be critical for improving the accuracy of the monitoring processes as well as the efficiency of the company's process of investigating outliers, trends, and patterns.

Define thresholds: While bribery or corruption compliance misconduct occurs in a single event or transaction, a review of several events or transactions occurring over months or years is necessary to identify potential antitrust misconduct. Understanding the appropriate time periods of comparability for each respective measure is necessary for establishing the appropriate benchmark. Further, benchmarks must be defined within transaction types to ensure the accuracy of the screening process. For example, identifying which transactions and time periods should be comparable in terms of pricing or profit margin will result in more accurate identification of outliers and anomalies and save a company time in its review of outlier data. Notably, a company considering the development and implementation of a financial monitoring tool should know that it is not necessary to do a complicated pricing study or extensive analysis to develop screening processes. By applying basic econometric principles to existing company data, a company can develop effective screens; however, engaging experts to advise on the development of such models can save a company time and resources.

Assign appropriate designated owners for implementation and review: Ensuring the respective designated owners of the screening tools are appropriately trained to interpret the results of the screening is key. Unlike anti-bribery or corruption, transaction data, on a standalone basis, cannot demonstrate that antitrust violations such as price-fixing, market-allocation, or bid-rigging have occurred. Financial screening may often identify "yellow flags" as compared to "red flags," which, in conjunction with communications monitoring (referenced below), can help a company determine whether a potential anticompetitive issue exists that requires further investigation and a deep-dive analysis. It is equally important to ensure that the proper resources are assigned to evaluate the risk of results indicating false positives or negatives that could lead to over-reaction or complacency.

Fine-tune the model: Validating and calibrating the model should be done at regular intervals to ensure the tool continues to improve its effectiveness. The owners who are responsible for investigating outliers and anomalies can provide feedback for improving the tool, for instance, if there is a simple adjustment to the process that would eliminate a group of false positives. The process of reviewing screening results does not have to require extensive resources and it can often be included as part of an existing audit conducted on an annual basis. Further, a company can incorporate contextual business, market, and regulation information, and other public or third-party data as described above to build a more robust screening process that minimizes false positives. For example, information such as price change announcements, seasonality, or typical sales cycle length could help improve the tool's accuracy and expedite the investigation process. Additionally, as a company's business and risks evolve, the data points and thresholds applied to the monitoring tool should be a re-assessed.

Communications Monitoring Solutions

Just as one sale does not constitute an antitrust violation, one message does not establish antitrust misconduct, but a pattern of communication (particularly with competitors) can be cause for concern. Awareness of communications consistent with antitrust misconduct can not only help companies prevent or remediate actual violations of the antitrust laws, but also provide insight on how the company can strengthen its antitrust compliance program by identifying business practices or departments that would benefit from additional guidance, procedures, or internal controls. Communications can also help provide necessary context for financial data trends indicative of misconduct, as described above. The challenge becomes how to detect the relevant communications among the terabytes of data employees create and receive.

With any monitoring solution, the objective is to look for documents, not at documents—the volume of communications actually reviewed should be defensibly limited to only those reasonably likely to indicate potential wrongdoing. At the outset of implementing any communication monitoring, a company should identify the business practices at greatest risk for misconduct based on the company's antitrust risk assessment; the business units and individuals with these higher risk responsibilities will be most appropriate for monitoring. In addition to narrowing the number of custodians for review, monitoring can be made more effective using advanced analytics, combined with human review, to hone in on relevant communications, minimize the risk of missing key information by relying solely on contrived terms and phrases, and refine underlying analytics models through continuous review and decision making to produce more robust results over time. Analytics can also help recognize patterns in communications beyond specific text, including messaging outside standard business hours, increased volume of certain intents or concepts, or other outlier behavior. Taken together, these efforts can increase the accuracy of any monitoring workflow and reduce the number of false positives generated.

As the Division notes, effective antitrust compliance programs should also "evaluate and manage the antitrust risk associated with …new forms of communication." [12] Thus, companies should consider revising or developing information governance policies (*e.g.*, acceptable use policies) to direct employees to use specific communication methods are that more readily available for monitoring (*e.g.*, e-mail vs. text messaging). This can help minimize the burden on compliance departments to collect and monitor mobile data sources or emerging data sources. Such policies can also be used to alert employees to the company's right to collect, monitor, or otherwise access company data and advise on the appropriate use of company property (*e.g.,* restricting use of company property to send personal messages to competitors).

When developing a proactive communications monitoring solution, it is important to tailor the effort to the company's unique situation, including its data sources (*e.g.*, e- mail, collaboration apps, mobile device messaging), available technologies, and human resources. Monitoring can be accomplished through hosting and managing review off site by third-party vendors or by scanning communications on a company's own systems in real time. The right option depends on the company's software licenses, compliance staff, and complexity of data.

Continuous Improvement, Periodic Review, Monitoring, Auditing

As noted above, the Division's guidance states that an effective compliance program "includes monitoring and auditing functions to ensure that employees follow the compliance program." [13] Further, it states that testing "helps

12 Id. at 7.

ensure that there is continued, clear and unambiguous commitment to antitrust compliance from the top down, that the antitrust risks identified or the assessment of these risks have not changed (or if they have changed, to reassess controls) and that the risk mitigation activities/ controls remain appropriate and effective." [14] Prosecutors may reward efforts made by a company that promotes continuous improvement and sustainability. Effective internal controls can be both preventative and detective as it relates to anticompetitive activity.

Data sources can be used to ensure that a company's employees are complying with its preventative controls. For example, a company may have a policy that requires employees to report attendance at trade associations and industry events. A company can use its CRM system as the tool for documenting attendance at these events. Further, it can compare these CRM reports against other existing data sources such as Travel & Expense system reports as a process for reviewing compliance with this policy.

As it relates to the creating and testing of data and communications monitoring processes, a company should consider what key risks need controls that deter and detect anticompetitive behavior. Further, due to the changes within the business and environment it operates in, it is important to consider the frequency in which controls and processes need to be evaluated for effectiveness, whether certain controls or processes are antiquated, and whether additional controls and processes are needed.

To ensure information identified as potentially anticompetitive is addressed quickly and consistently, a company should prepare a well-documented response plan with designated owners assigned to each step of the process and ensure the process and results are documented and retained in a designated repository.

The process of improving a company's monitoring tools will depend on available resources and expertise, but it is vital that a company assign designated owners for improving the tools. There should be owners who are responsible for the investigation of identified flags, a documented feedback process on the accuracy of the results (*i.e.*, a trend of false positives), and individuals who are responsible for adjusting monitoring tools and processes based on the results of the feedback and recommendations.

It is crucial that a company's antitrust compliance monitoring solution is integrated into the other audit components of a company's business to make it successful. Antitrust monitoring processes can be tested as part of cycle audits (*e.g.*, Sales or Procurement audits) or stand-alone antitrust audits. Below is an example of an activity and review process related to antitrust risk that a company may incorporate as part of its current sales and/or pricing audit process:

Activity and Risk

On a quarterly basis, a company's competitors publicly announce price changes which could be identified as signaling for price change action to also be taken by the company.

Monitoring Process

As part of a company's periodic audits on its sales and pricing processes, develop a dashboard utilizing existing transaction data that shows a company's prices over time and incorporates competitors' quarterly price change announcements.

Determine appropriate thresholds and alerts for pricing activity within a certain period following a competitor's price change announcement.

To the extent not already included, ensure any proactive communication screening is actively looking for concepts that indicate anticipation of or commitment to follow a competitor's price announcement, paying particular attention to communications with competitors and those of employees with sales and pricing responsibilities or with regular competitor contact. This could include addition of relevant key terms to screening software, audit of mobile messages or other data, and analyzing trends in communication patterns relative to earlier periods in time.

Periodic Review & Improvement

Investigate outlier data for potential anticompetitive activity. Based on results of the review, further refine the tool to reduce false positives. Handle potentially problematic behavior according to the company's response plan.

13 Id. at 10.
14 Id. at 10.

CLOSING REMARKS

The Division has emphasized importance of utilizing financial data screening, communications monitoring tools, statistical testing, and other proactive screening tools and processes that identify potentially anticompetitive behavior in order to meet the Division's effectiveness requirements. The increasing amount of data collected and stored indicates that screening processes will only become more important in years to come.

While there is no "one size fits all" approach to implementing monitoring procedures, there are steps any company can take to develop pilot monitoring processes. Start by prioritizing a company's key risks and identifying appropriate data systems, benchmarks and resources. Then set objective thresholds and tolerance ranges or seed exemplary language indicating misconduct into the appropriate tool, to help minimize false positives as the company launches the monitoring workflows. Finally, create a plan for refining the tools through review, revision to benchmarks or underlying models, and periodic audits to assess efficacy of detection.

Financial data analytics and communications monitoring solutions are complementary solutions; oftentimes, they can be utilized together to develop effective screening processes. Companies do not need to invest significant resources or purchase additional tools, software or data. With the right planning and expertise, a company's existing data and systems can be used to incorporate data analytics and communications monitoring into any compliance program.

The views expressed herein are those of the author(s) and not necessarily the views of FTI Consulting, Inc., its management, its subsidiaries, its affiliates, or its other professionals.

NICOLE WELLS
Senior Managing Director
+1 (416) 649-8060
nicole.wells@fticonsulting.com

ANDREA LEVINE
Managing Director
+1 (212) 499-3617
andrea.levine@fticonsulting.com

AUDREY O'CONNOR
Director
+1 (312) 553-6756
audrey.oconnor@fticonsulting.com

FTI CONSULTING