**Raiders, Activists, and the Risk of Mistargeting**

*By Zohar Goshen and Reilly S. Steel*

**The Price of Your Vote: Proxy Choice and Securities Lending**

*By Joshua Mitts*

**Corporate Governance, the Depth of Altruism, and the Polyphony of Voice**

*By Jeffrey N. Gordon*

Editor-At-Large
Reynolds Holding

# THE CLS BLUE SKY BLOG

COLUMBIA LAW SCHOOL'S BLOG ON CORPORATIONS AND THE CAPITAL MARKETS

Editorial Board
John C. Coffee, Jr.
Edward F. Greene
Kathryn Judge



# Skadden Discusses Government Expectations for Companies' Data-Driven Compliance Programs

*By Gary DiBianco, Raquel Fox and Gretchen M. Wolf* October 19, 2021

**Comment**

As artificial intelligence and other data tools have proliferated, regulators and prosecutors expect companies to utilize sophisticated data analytics as part of their compliance programs. They also expect directors to take an active role, understanding and overseeing these data-driven compliance programs.

Recent lawsuits, enforcement actions and surveys suggest, however, that many companies have not kept up with the rising expectations and may not be utilizing available data to flag potential compliance problems as well as they could – perhaps not even as well as the government is already doing.

A careful reading of enforcement cases, policies and public statements shows what the government now expects. They provide directors with valuable insights about how to shape more complete, effective and defensible compliance programs.

## What the Government Is Looking For

Some aspects of business pose well-known compliance risks: business combinations, foreign operations, foreign clients, privacy protection, interactions with competitors and financial reporting. Traditional compliance programs and due diligence efforts often focus on those, quite sensibly.

Federal officials, however, are placing increasing emphasis on data-driven approaches: (a) They expect companies to monitor and analyze data that could identify potential risk factors or compliance failures. (b) When assessing culpability, they look closely at internal compliance processes and reporting lines. (c) They hold boards responsible for overseeing both.

Although some highly regulated sectors such as financial institutions, life sciences and technology have begun to implement more data-driven approaches to compliance, the importance of data may not be fully appreciated in other sectors.

### 1. Across the Federal Government, Data Is Being Mined for Enforcement

Prosecutors and regulators have become increasingly adept at crunching large volumes of data to spot potential violations and build cases.

The Securities and Exchange Commission (SEC) has been a leader in using risk-based data analytics. One system provides officials with a dashboard of approximately 200 metrics to help identify abnormalities in corporate financial reports. In August 2021, the commission announced a $6 million settlement resolving allegations that a company inflated earnings per share by failing to properly account for material loss contingencies. It was the third SEC action involving earnings management practices that grew out of the data analytics initiative. Other SEC data systems leverage Big Data to identify suspicious trades and relationships to spot potential insider trading.

The Commodities Futures Trading Commission (CFTC) employed data analytics in an investigation into alleged price manipulation ("spoofing") in the precious metals and U.S. Treasury futures markets, leading to a $920 million fine in 2020.

The Consumer Finance Protection Bureau (CFPB) utilizes natural language processing tools to analyze consumer complaints and categorize them, helping to identify patterns, and the Department of Justice (DOJ) has tapped data to identify potential False Claims Act cases.

The DOJ also established a Procurement Collusion Strike Force in 2019 that uses data analytics to identify suspicious bid patterns. It also trains auditors, analysts, attorneys and others in the use of data analysis to combat bid rigging and similar collusive actions. As a result, the role of data analytics in antitrust and other enforcement is likely to increase.

## 2. Companies Are Now Expected to Use Data Analytics for Compliance

With new, more powerful digital tools available, what constitutes a reasonably effective compliance program is rapidly changing. In one recent enforcement case, for instance, the CFPB cited a bank's lack of systemic, automated controls to detect employee misconduct involving consumer accounts.

Other applications of data-driven compliance programs might include:

(a) monitoring for Foreign Corrupt Practices Act violations by analyzing raw data about a company's foreign transactions, donations, cross-border customers or vendors;

(b) periodically evaluating the risk profiles of third-party relationships;

(c) at financial institutions, screening customer transaction data as part of anti-money laundering or "know your customer" programs.

As user-friendly ways to deliver data analyses to compliance personnel proliferate, expectations may change about the level of information that boards should be receiving about risk trends and compliance responses.

Surveys suggest that many companies have catching up to do. According to an EY survey, 78% of companies do not "systemically track contractual obligations," for instance, and 71% do not monitor contracts for "deviations from standard terms." And while half of CEOs interviewed identified "risk management as the area in which they expect to implement the most change over the next three years" — with 61% of those same CEO's saying they "would like their organization to take a more data-driven approach" to risk management generally — 97% of general counsels report difficulty obtaining budgets for legal technology, including tools to monitor risk and compliance issues.

As enforcement agencies rely more heavily on data tools to rout out unlawful conduct, they expect companies to do the same. As Matthew S. Minor, then deputy assistant attorney general, said in 2019:

> Whereas we are able to identify indicators and anomalies from market-wide data, companies have better and more immediate access to their own data. For that reason, if misconduct does occur, our prosecutors are going to inquire about what the company has done to analyze or track its own data resources — both at the time of the misconduct, as well as at the time we are considering a potential resolution.

That could be paraphrased as: "You've got the data. Use it."

## 3. The Analysis Must Be Available to Boards

Enforcement officials have made it clear that data analysis alone will not suffice. The results must make it to decisionmakers, including boards and chief compliance officers (CCOs).

For example, under federal sentencing guidelines, if there is a plea or a conviction, defendants only receive credit for having a generally effective compliance program if directors at minimum are "knowledgeable about the content and operation of the compliance and ethics program," and "exercise reasonable oversight" of its "implementation and effectiveness." One factor in weighing charges involving businesses is "[w]hat types of information … the board of directors and senior management examined in their exercise of oversight . . . ."

Effective oversight also requires sufficient expertise at the board level, the DOJ's prosecution guidelines suggest, whether that comes through expertise among the directors themselves, advisors or compliance training. The guidelines also factor in whether directors or external auditors met privately with compliance and control officers, without management present.

A Deloitte survey suggests that these standards often are not met. At 70% of the companies surveyed, CCOs did not regularly attend board meetings. At almost 40%, they did not even regularly attend audit committee meetings.

Regulators scrutinize those organizational structures. As the SEC's Director for the Division of Examinations stated in November 2020 in the context of investment funds:

> We notice when a firm positions a CCO too low in the organization to make meaningful change and have a substantive impact, such as a mid-level officer or placed under the CFO function. We notice when CCOs are expected to create policies and procedures, but are not given the resources to hire personnel or engage vendors to provide systems to implement those policies and procedures.

This concern was reflected in a recent criminal investigation of alleged bribery. As part of a non-prosecution agreement, the company created a new position, executive vice president for compliance and audit, that reports directly to the audit committee of the company's parent.

## Taking the Hint

No board or CEO wants to discover that the government has a better read on the company's legal compliance than management does. Fortunately, through prosecutions and enforcement actions, sentencing laws and detailed DOJ policies, the government has given clear guidance about the need to employ data analytics, and how that information needs to be shared internally.

## Questions the Feds Will Ask About Your Compliance Systems

The DOJ's Criminal Justice Division published a detailed list of questions it asks about a corporate compliance program when weighing whether to prosecute a company, some of which emphasize the role of data and access to it. It is a good starting place for directors trying to oversee risk management and compliance initiatives. Key excerpts:

> **Oversight** – What compliance expertise has been available on the board of directors? Have the board of directors and/or external auditors held executive or private sessions with the compliance and control functions? What types of information have the board of directors and senior management examined in their exercise of oversight in the area in which the misconduct occurred? . . .
>
> **Data Resources and Access** – Do compliance and control personnel have sufficient direct or indirect access to relevant sources of data to allow for timely and effective monitoring and/or testing of policies, controls, and transactions? Do any impediments exist that limit access to relevant sources of data and, if so, what is the company doing to address the impediments?
>
> **Control Testing** – Has the company reviewed and audited its compliance program in the area relating to the misconduct? More generally, what 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?

*This post comes to us from Skadden, Arps, Slate, Meagher & Flom LLP. It is based on the firm's memorandum, "Don't Let the Feds Beat You at the Data-Mining Game," available here.*