

Welcome to ComplianceWeek.com. This site uses cookies. [Read our policy.](#)

COMPLIANCE WEEK

FOR THE WELL-INFORMED CHIEF COMPLIANCE OFFICER AND AUDIT EXECUTIVE

Regulators catching up on use of analytics; compliance better take notice



By [Aaron Nicodemus](#) | Mon, Dec 14, 2020 1:23 PM

Regulators like the Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC), as well as banking agencies like the Office of the Comptroller of the Currency (OCC) and the Financial Industry Regulatory Authority (FINRA), have in recent years used sophisticated data analytics to assess the compliance programs of the industries they regulate. Including yours.

“They are applying AI, machine learning, cloud computing, and natural language processing in ways that are kind of shocking,” said Carlo di Florio, a former FINRA and SEC regulator who is now partner & global chief services officer at ACA Compliance Group, a data analytics vendor.

Regulators are using these tools to build enforcement cases and monitor patterns and behaviors in the industries in their charge, he said. It’s a big reason why expectations of regulators for the use of data analytics by the companies they regulate is so much higher than just a few years ago.

Nowhere was regulators’ emerging data analysis capabilities more on display than with the **\$920 million fine** levied earlier this year by the CFTC, SEC, and Department of Justice (DOJ) against JPMorgan Chase for the illegal manipulation of the precious metals markets by several traders, a practice known as “spoofing.” The criminal activity stretched back to 2008, but in 2013, the investigation ended because regulators did not have the data analytics in place to prove their case, the **Wall Street Journal reported**. The case was later reopened, and indictments were handed down against four traders in 2019.

“It’s not that organizations need to be leading edge with data analytics, but they do need to review their compliance architecture. It’s the laggards who could draw the attention of regulators.”

Michael Rasmussen, Compliance Consultant and Researcher

“We could not have brought the JPMorgan case without the data analytics program we have now,” James McDonald, the now-former enforcement director of the CFTC, told the *Journal*.

Another example is the SEC’s Earnings Per Share (EPS) Initiative, “which utilizes risk-based data analytics to uncover potential accounting and disclosure violations caused by, among other things, earnings management practices,” the SEC said in September, when it announced **two landmark data analytic enforcement actions**.

While the use of data analytics to assess and improve compliance functions has become the standard in industries like banking, securities, and financial services, other industries not using data analytics as part of their compliance program may be left behind, di Florio said.

“As a firm, you don’t want regulators to come in and find violations using your data and your tools,” he said. “You want to find the pattern (of fraud) before they do.”

“It’s not that organizations need to be leading edge with data analytics, but they do need to review their compliance architecture,” said Michael Rasmussen, a compliance consultant and researcher. “It’s the laggards who could draw the attention of regulators.”

Companies need to meet regulators’ expectations for data analysis

There’s a gap between where many firms are now with their data analytics capabilities as it relates to compliance and where they need to be, said Lisa Beth Lentini Walker, a former SEC regulator and chief compliance officer with CWT and Deluxe Corp.

“Most compliance programs are generally ill-equipped to gather the data,” said Lentini Walker, who now runs her own consulting firm, Lumen Worldwide Endeavors. “And even if they have the data, most people aren’t asking the right questions.”

Ask a CCO

I think the regulatory expectations **evolve with technology**. As more sophisticated ways to analyze data become available, companies are expected to **adopt them in different areas**, and compliance is not an exception.



LUIS KOLSTER

VP, Chief Compliance Officer,
Baker Hughes

Six senior compliance practitioners [share some big-picture thoughts](#) on how their companies are using data within the context of regulators' increased expectations in the area.

Increasingly, firms need to get a better handle on analyzing all the data they produce.

In June, the DOJ released [updated guidance](#) that spotlighted how the agency assesses the efficacy of a company's compliance program.

One section that raised the eyebrow of many a compliance officer was what the DOJ said about expecting a company to use data analytics to evaluate its compliance with various regulations, as well as being able to use its data to prove its compliance program is effective.

Language was included in the DOJ guidance regarding data resources and access, with the following questions: "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?”

Inherent in the DOJ guidance was the idea that data analytics could help companies continually improve their compliance programs by focusing their attention on particular areas of risk, then using data analytics to identify and monitor potentially fraudulent activity within their business.

Unless your firm is under investigation, regulators who are measuring compliance with their regulations will want to know how your firm reached compliance decisions and whether company leaders acted on the conclusions drawn from the data, Lentini Walker said.

“Most regulators aren’t going to try to re-engineer your data analytics; they’re not going to take your data and comb through it,” she said. “They’re going to look at the compliance program’s design, the processes you apply, and the output. They’re not going to do your job for you, but they want to know the program is working.”

How to get started with data analytics

To launch a data analytics program, start by making sure compliance and control personnel have access to the data sources they need and eliminate any impediments that exist. Compartmentalization of data is a particular issue with small- and mid-sized companies, Lentini Walker said. This may take buy-in from C-suite executives to gain access to the necessary data.

“Most regulators aren’t going to try to re-engineer your data analytics; they’re not going to take your data and comb through it. They’re going to look at the compliance program’s design, the processes you apply, and the output. They’re not going to do your job for you, but they want to know the program is working.”

Lisa Beth Lentini Walker, Founder and CEO, Lumen Worldwide Endeavors

“Odds are your company is already doing data analytics—it’s just that compliance isn’t invited to the party,” said Vincent Walden, managing director with the New York firm Alvarez & Marsal, on a [Nov. 12 Webinar on data analytics in compliance](#). “The business questions that compliance is going to ask will be different than what finance and internal audit are asking.”

In the Webinar, attendees heard about BrewRIGHT, a machine learning compliance platform developed by Anheuser-Busch InBev (AB InBev). The platform can scan company data from multiple sources to proactively flag high-risk vendor transactions in over 60 countries with statistical accuracy. It also monitors employee behavior, particularly in the areas of expense reports and travel and corporate credit card use, for irregularities that may require further examination.

The platform draws from multiple, disparate data sources including payments data, investigations data, third-party due diligence data, hotline calls, and third-party data sources.

According to Dheeraj Thimmaiah, AB InBev's global compliance director and leader of the company's data analytics team, BrewRIGHT applies key compliance risk indicators to company data.

For example, let's say AB InBev wants to use BrewRIGHT to identify when employees are using their corporate credit card for personal expenses, Thimmaiah said. The program can identify the patterns where such spending is likely to be occurring. The company can pull the employee aside for education and training about which business expenses are valid, and which are not, before the problem escalates.

To begin the process of analyzing your company's data for compliance risks, do not underestimate the power of a good question. Asking specifically what question you'd like your data analysis to find is a good place to begin. There's no one-size-fits-all question: It should be tailored to account for your industry, risk profile, and geographic footprint.

That said, here are some **potential starting-point questions** to answer:

- How has the pandemic changed organizational behavior?
- How is data being used to influence risk assessments?
- How is data influencing policies and procedures?
- What do we know about fraud historically and how it can be detected earlier?
- Is the company mission, vision, and purpose in alignment with articulated values and incentives?
- How do compensation practices align with measurable desired behaviors?

- Is performance on training predictive of risk area and hotline complaint trends?
- How many payment transactions were modified, stopped, or more closely examined for compliance concerns?
- How many questions required follow up in due diligence for M&A activity, and how quickly did remediation take place?
- How many third parties were identified in each tier of risk, and how many were suspended, terminated, or audited for compliance issues?

Let's say your firm has identified a particular compliance risk with third parties, like bribery and money laundering issues among overseas vendors. Or closer to home, you suspect corruption within company sales agreements or vendor payments. Collect all the data that is necessary to answer your question.

Start small, Lentini Walker suggests, with a clean dataset. What patterns already generate red flags? What generates too many false positives? Once you know what you're looking for, you can begin to use data analytics to home in on those risk factors, she said. Show what's possible and build up the analytics over time, adding datasets and new questions as you go.

Analyzing the data sounds like the easy part—just hand the data and the question over to your IT department and await results, right? Alas, there are pitfalls.

A common one is that the data turns out to be flawed or biased, so the results aren't worth much. Amazon, for example, had a **secret AI recruitment tool** that attempted to measure the perfect new hire but turned out to be biased against women.

One way to avoid Amazon's mistake is to draw from multiple datasets, or to have someone from outside compliance weigh in on the conclusion of the analytics before moving it up the chain.

The last step is to communicate the results of the analysis to company executives and convince them to act on its conclusions.

Selling compliance analytics to the board

How do you convince your bosses that a data analytics program for compliance is money worth spending?

Compliance is often viewed as revenue negative. One way to make your case is to explain the return on investment on data analytics for compliance and the potential future successes that can be wrung from the idea.

“Show, ‘What does this mean to the company’s bottom line?’” suggested Thimmaiah. “Then, to the long-term growth and strategy of the business.”

Another tact is to frame the issue as preventative. Good compliance helps a firm avoid fines, penalties, and reputational damage caused by an investigation and/or enforcement action. Regulators are generally **more willing to reduce penalties** of an enforcement action if a company can show it has a robust compliance program.

Funding compliance data analytics will keep a company fully aware of its risks and better able to explain to regulators how it monitored them. It’s akin to a person who goes to the doctor and dentist regularly, Lentini Walker said.

“You shouldn’t only go to the doctor when you’re sick,” she said, and companies shouldn’t place compliance on the sideline until there’s a crisis.