

Artificial Intelligence in Corporate Compliance Programs: A Double-Edged Sword

By Leo Tsao, Robert Luskin and Corinne Lammers

March 13, 2025

As we have explained in prior articles, artificial intelligence (AI) promises to be a game-changing tool in many areas, including corporate compliance. As more companies deploy AI tools throughout their business, the incorporation of AI in compliance programs will become presumed rather than novel, and the U.S. Department of Justice (DOJ) and regulators will increasingly expect compliance programs to incorporate AI tools. However, organizations that adopt AI solutions for their compliance programs should not expect leniency if those AI compliance systems fail and result in legal violations. The adoption of AI therefore may present a double-edged sword for organizations that are working to implement corporate compliance programs that meet DOJ and regulator expectations.

AI Promises to Be a Game-changing Tool for Corporate Compliance

Companies have already begun using AI to improve the effectiveness of corporate compliance programs, including with risk identification and mitigation. With AI's ability to process big data to find patterns and identify anomalies, AI can support the detection and prevention of violations of corporate policies or legal requirements. Potential use cases for AI-based compliance tools include:



Courtesy photos

L-R: Leo Tsao, Robert Luskin and Corinne Lammers of Paul Hastings.

- Analyzing large volumes of payment data from different ERPs to identify concerning trends and red flags;
- Using risk ranking systems to review third-party engagements and identify transactions indicating misconduct or fraud through weighted factors;
- Reviewing whistleblower complaints to identify the highest risk reports, categories of complaints, key issues, and emerging trends; and
- Synthesizing all available data sources across an organization to conduct risk surveillance and identify emerging threats and risk areas.

AI can also be used to help compliance professionals execute day-to-day tasks, such as

conducting the first level review of expense reports or requests for providing gifts or hospitality to potential customers. Also, once trained on corporate policies, the AI systems can act as an interactive knowledge base, answering questions from employees about compliance guidelines, reporting and approval processes and other procedural details.

Banks are already using AI in their anti-money laundering (AML) compliance programs, including the continuous monitoring of customer transactions, beneficial ownership, sanctions lists, and media coverage to identify red flags and conduct due diligence. AI systems also can scan and assess authenticity of customer documentation during due diligence reviews and make suspicious activity report reporting more efficient, accurate, and comprehensive.

As More Compliance and Legal Functions Begin to Use AI, the DOJ's Expectations will Correspondingly Increase

Using Data Analytics as Precedent

Not so many years ago, most companies were not yet incorporating data analytics into their compliance programs. In 2020, the DOJ began instructing prosecutors to evaluate whether companies were effectively using data analytics, specifically, whether corporate compliance teams had access to useful data, and whether that data was being used to monitor for risks and test policies and procedures. This provided prosecutors with the ability to reduce penalties and post-resolution compliance obligations for companies that had implemented effective data analytics or monitoring tools.

In response, more companies began integrating data analytics into their compliance programs,

and not surprisingly, the DOJ's expectations on the use of data analytics to effectively support compliance correspondingly increased. As then-Acting Assistant Attorney General Nicole Argentieri stated in her keynote address at the American Conference Institute's (ACI) 40th International Conference on the Foreign Corrupt Practices Act on Nov. 29, 2023, "you can be sure that, if misconduct occurs, our prosecutors are going to ask what the company has done to analyze or track its own data—both at the time of the misconduct and when we are considering a potential resolution."

The DOJ does still moderate its expectations based on the unique situation of each company. Glenn Leon, the DOJ's fraud section chief, made clear during a speech at ACI's 39th International Conference on the Foreign Corrupt Practices Act on Nov. 30, 2022, that data analytics does not "necessarily require going out and buying the shiniest tool and spending hundreds of thousands of dollars," explaining that sometimes "data analytics is measuring things you've never measured before; tracking it and looking for red flags." Despite this seemingly reassuring statement from the DOJ, as more companies continue to develop and deploy robust data analytics programs, prosecutors will expect comparable efforts from their peers.

We expect that the evolution of using AI for compliance will follow a similar path. But given the speed of the AI revolution, companies may be expected to incorporate AI into their compliance programs sooner than they think.

Evolution of Government Use of Data Analytics and AI

The DOJ has relied upon data analytics to build criminal cases in health care fraud, foreign

corruption, government contracts and securities trading. For example, the Criminal Division's fraud section has successfully used data analytics to review huge volumes of Medicare data to identify healthcare fraud. Reliance on data analytics has become so important that the fraud section has hired several individuals to focus specifically on this tool. And, just last year on Feb. 14, 2024, then-Deputy Attorney General Lisa Monaco, during her remarks at the University of Oxford on the promise and peril of AI, touted the DOJ's use of AI to investigate and prosecute crimes, including sifting through the more than a million tips that FBI receives from the public every year. It remains to be seen if the Trump Administration will take a different approach to using AI for government operations. But if past is prologue, the DOJ can soon be expected to issue a similar warning for companies to adopt AI tools as part of their compliance programs.

The DOJ and Regulators May Not Offer Leniency to Companies for Failures of AI Compliance Tools

Historically, government agencies have attempted to encourage innovative solutions to regulatory issues. For example, in December 2018, the major federal financial regulators issued a joint statement encouraging banks to use innovative technologies to combat money laundering. As a carrot to incentivize innovation, the regulators stated they would not immediately conclude that failures in new AML technologies would necessarily reflect ineffective AML controls. In the same statement, however, the regulators made clear that newly adopted innovative solutions must still comply with all AML regulations.

As the agencies explained: "Compliance with the Bank Secrecy Act (BSA) and its regulations is critically important in protecting the U.S. financial system, and banks that fail to comply with BSA/AML requirements expose the financial system to abuse by illicit actors. Accordingly, banks must continue to meet their BSA/AML compliance obligations, as well as ensure the ongoing safety and soundness of the bank, when developing pilot programs and other innovative approaches." The statement even specifically addressed AI as an AML tool, stating that "when banks test or implement artificial intelligence-based transaction monitoring systems and identify suspicious activity that would not otherwise have been identified under existing processes, the Agencies will not automatically assume that the banks' existing processes are deficient." In other words, while the regulators encouraged banks to adopt innovative solutions, they made clear that they should not expect leniency beyond those agencies not "automatically" concluding that their systems violated the law. That is cold comfort for banks.

Nevertheless, the analysis undertaken by government enforcement agencies likely will include some nuanced assessment of how and why the AI tool failed. The DOJ is likely to assess two separate elements: the effectiveness of the AI system and the adequacy of human oversight. For example, on the system side, if an AI-driven payment analytics screening system at a company fails to identify a single improper payment out of millions, government enforcers likely will not view the AI system as fundamentally flawed. However, if the AI-driven payment analytics exhibits systemic issues and the company fails to take appropriate steps to monitor the effectiveness of

the system, government enforcers likely will view the system as ineffective. The consequences likely will be even more severe where the failures result in serious legal violations.

Perhaps more significant to any DOJ assessment will be the level of human oversight. If, for example, an AI system mistakenly approves a high-risk payment to a third party with multiple corruption red flags, the DOJ likely will criticize the absence of a second-level human reviewer. Similarly, if an AI-driven tool is used to identify red flags in payments or other systems, the DOJ will expect the company to dedicate sufficient resources to review the identified red flags. A company that fails to do so and, as a result, ignores or fails to take action to address red flags identified by an AI-based tool, likely will come under significant DOJ scrutiny.

For many reasons, the DOJ may be less willing to offer companies any leniency for legal violations caused by AI tools in compliance systems—depending on the type and severity of violation. As we noted in our prior articles, regarding corporate criminal liability for AI and using compliance-based criminal charges to prosecute companies for AI crimes because an AI system has no mind with which to act or form a criminal intent, DOJ prosecutors will be unable to prosecute companies for crimes based on the actions of the AI system. Instead, prosecutors will be forced to focus on compliance-based crimes looking at whether the companies complied with the law in adopting the AI systems in the first place. In short, if compliance-based crimes are the DOJ's only option for prosecuting corporations for AI-based crimes, the DOJ will be hard pressed to grant leniency to corporations where their AI compliance systems fail.

Key Takeaways

Because AI systems are imperfect, companies that delegate important decision-making to AI systems will undoubtedly experience failures resulting in legal violations. At the same time, as more companies adopt AI in their compliance programs, the DOJ and regulators likely will increasingly expect companies to use such tools. That situation presents somewhat of a Catch-22 for companies. To avoid being caught in this trap, as with any use of AI, companies should consider the following:

- Organizations seeking to implement AI solutions within their compliance programs should—at the outset—conduct an assessment to evaluate the risks associated with AI systems used in compliance-related tasks. This assessment should consider the likelihood that specific risks (e.g., AI may inadvertently allow a violation to occur or fail to identify red flags that would typically be caught by human reviewers) will materialize, along with their potential impact.
- Once an AI system is deployed within the compliance function, companies need to implement mechanisms for testing and monitoring to ensure the system functions as intended. This may include parallel assessments to verify the system's accuracy and to identify unintended outcomes. The mechanisms for testing and monitoring of the AI solutions must involve sufficient human oversight both to verify that the system is functioning as intended and, if relevant, to address red flags identified by the AI-based tool.
- The results of ongoing testing and monitoring should inform a feedback loop to refine the AI system and its role within compliance

operations. Supported by testing data, organizations should regularly reassess their use of AI for compliance to detect misconduct and emerging risks, improve mitigation strategies, and assess the effectiveness of human oversight in evaluating the appropriateness of AI-driven compliance decisions.

- Organizations should ensure that their compliance teams are equipped with the necessary tools, technologies, and data to support the responsible use of AI in compliance programs. It is also important to assess whether the resources allocated for managing AI in compliance align with the complexity and scale of its use within the organization's broader compliance operations.

—Paul Hastings of counsel Josh Christensen and associate Andrew Sterritt contributed to preparation of this article.

Leo Tsao is a partner in the investigations & white-collar defense and fintech & payments practices at Paul Hastings based in the firm's Washington, D.C., office. His practice focuses on internal corporate investigations, defense of criminal and regulatory enforcement actions, and

compliance counseling. Before joining the firm, Tsao served for more than 15 years as a white collar prosecutor with the U.S. Department of Justice (DOJ), where he led or supervised many of the DOJ's most significant corporate criminal cases involving foreign corruption, money laundering and economic sanctions.

Robert Luskin is a partner in the investigations and white-collar defense practice at the firm based in the firm's Washington, D.C., office. He concentrates his practice on complex criminal litigation at both the trial court and appellate level. Beginning his career in government service, and having later transitioned into private practice, Luskin has represented clients in virtually every high-profile matter in Washington, D.C., over the last three decades, including members of Congress, senior White House staff, and federal judges.

Corinne Lammers is the chair of the compliance & regulatory counseling practice at the firm, based in the firm's Washington, D.C., office. Her practice focuses on compliance counseling and strategy, including compliance program development and enhancement, risk assessments, and testing and monitoring.