Compliance Steps After ABA White Collar Crime Conference

By **Jessica Nall, Cyrus Vance and Maria Piontkovska** (March 19, 2024)

Jessica Nall

Cyrus Vance

Maria Piontkovska

The 39th National Institute on White Collar Crime, hosted by the American Bar Association's Criminal Justice Section, took place on March 6-8 in San Francisco.

Attended by members of the white collar defense bar and senior U.S. law enforcement officials from the U.S. Department of Justice, National Security Division; the U.S. Securities and Exchange Commission; U.S. Commodity Futures Trading Commission and others, the conference covered a variety of cutting-edge and emerging white collar enforcement and compliance issues.

Below are our practical takeaways from the various statements made by senior law enforcement officials at the conference.

Whistleblower Incentives

As usual, as part of the annual E. Lawrence Barcella Jr. Memorial Address on March 7, Deputy Attorney General Lisa Monaco made several notable announcements regarding changes to DOJ white collar enforcement and compliance guidance policies.

This year, building on last year's introduction of a departmentwide voluntary self-disclosure program, Monaco announced that the DOJ intends to develop and implement a whistleblower rewards program that will provide monetary rewards to whistleblowers who report misconduct previously unknown to the DOJ.

Monaco noted that the program will be further developed in a "90-day sprint" led by the DOJ Money Laundering and Asset Recovery Section that began on March 7. The plan is to formally launch the program sometime later in 2024.

Some basic guardrails of the program have already been developed. For example, under the DOJ's anticipated program, whistleblowers will be entitled to rewards — in the form of a portion of the amount forfeited from the corporate wrongdoer — if the following conditions are met:

- All crime victims have previously been properly compensated;
- The reported information was truthful and not already known to the government;
- The information was reported voluntarily and not in response to a government inquiry or as part of compliance with existing government disclosure obligations;
- The whistleblower was not involved in the criminal activity itself; and
- There is no other existing financial disclosure incentive — including qui tam or another federal whistleblower program.

Monaco emphasized that while the DOJ will accept information about any federal law violations, it is especially interested in: (1) "[c]riminal abuses of the U.S. financial system"; (2) "[f]oreign corruption cases outside the jurisdiction of the SEC, including [Foreign Corrupt Practices Act] violations by non-issuers and violations of the recently enacted Foreign Extortion Prevention Act"; and (3) "[d]omestic corruption cases, especially involving illegal corporate payments to government officials."

According to Monaco, the new whistleblower rewards program is an attempt to address gaps in the current whistleblower rewards framework, which presently limits whistleblower financial rewards to certain types of violations.

Acting Assistant Attorney General Nicole Argentieri added that the basis for the proposed whistleblower pilot program is Title 28 of the U.S. Code, which authorizes the attorney general to pay awards for "information or assistance leading to civil or criminal forfeitures."

As a result, the Money Laundering and Asset Recovery Section will play a leading role in developing the pilot, with assistance from the FBI, the DOJ and U.S. attorney's offices.

Similarly to existing SEC and CFTC whistleblower programs, this pilot may be expected to set a monetary threshold for an amount of recovery required before a whistleblower payment can be made.

In addition, to sweeten the calculus for individuals — rather than corporations — considering self-disclosure of misconduct, the U.S. Attorney's Office for the Southern District of New York in January of this year announced its Whistleblower Pilot Program, which makes nonprosecution agreements available, even for individuals who admit to having committed federal crimes, under specific circumstances.

U.S. Attorney for the Northern District of California Ismail Ramsey announced at the conference that his district will be rolling out a similar pilot program. Ramsey noted the Northern District of California program is meant to encourage reporting of any federal crimes, with a particular emphasis on crimes involving intellectual property theft and artificial intelligence-related misconduct.

According to Ramsey, under certain conditions, including extensive cooperation by the individual, the whistleblower may be entitled to a declination.

Practical Takeaways

While the new programs aim principally to incentivize reporting by individual whistleblowers, they have the flip-side effect of encouraging timely voluntary self-disclosures by corporations to a greater extent than before.

In fact, during the ABA White Collar Institute, Monaco and others repeatedly noted that the DOJ continues to promote and encourage corporate voluntary self-disclosures, and Main Justice has directed all of its components and U.S. attorneys to implement voluntary self-disclosure policies.

One of the many reasons for this is that voluntary disclosures by corporations can assist the DOJ in prosecuting responsible individuals, which is a key DOJ enforcement priority.

Voluntary self-disclosures typically result in more favorable resolutions; however, a disclosure may not be considered voluntary if the information disclosed was already known

by the DOJ.

By incentivizing individual whistleblowers to come forward through offering carrots like financial incentives and potential individual amnesty — in the Northern District of California and Southern District of New York — the DOJ increases the possibility that conduct voluntarily reported by corporations will not viewed by the department as new information.

And because both the corporate voluntary self-disclosure program and the upcoming whistleblower program only reward new information, decisions about whether to disclose will now be subject to additional time pressures and increased emphasis on the risk of individual whistleblowers calling the government first.

Companies should continue to carefully consider whether to disclose any potential violations, keeping in mind that substantial delay or multiple potential whistleblowers aware of the conduct may ultimately weigh against the disclosure.

In addition, companies should evaluate their compliance controls and mechanisms related to reporting of concerns and whistleblower protection. Ineffective reporting channels, lack of training or awareness about them among company personnel, or perceived risks of retaliation increase the risk that a company employee submits their concerns directly to the DOJ, and not through the company's own reporting channels.

Although cash rewards available under certain circumstances for whistleblowing to the DOJ could cause some employees to report their concerns directly to the DOJ even if they know about the company's reporting channels and do not have concerns about their effectiveness, most employees will likely still feel more comfortable submitting their concerns to the company, at least initially.

It is also not yet clear how the cash rewards will work in practice. As per Monaco's statements, rewards will only be available to individuals with no involvement in the alleged misconduct, only after all victims have been paid and only when a case has resulted in a forfeiture — still a relatively rare outcome in the corporate criminal enforcement world — above a certain soon-to-be-determined level.

This could substantially narrow the circle of potentially eligible whistleblowers, and reduce or delay the actual receipt of cash rewards.

Finally, corporations should continue to ensure that they do not take any action that could be viewed as interference with or obstruction of potential whistleblower disclosures.

Although it is not yet clear whether the DOJ will implement sanctions specific to interference with reporting under the upcoming program, it could view such actions as obstruction of justice, and companies are already subject to potential sanctions for interference with employee reporting of misconduct to the SEC.

This could create a host of complicated issues for corporations when insiders wrongfully take corporate confidential or attorney-client privileged information outside the company for self-serving reasons that they might claim to have done under the cover of whistleblowing.

Artificial Intelligence

Multiple officials, including Attorney General Merrick Garland, SEC Division of Enforcement Director Gurbir Grewal, and CFTC Division of Enforcement Director Ian McGinley, mentioned

AI as an area of increasing regulatory and enforcement focus.

Garland said that he was concerned about AI's ability to accelerate cyberattacks and enable foreign malign actors. To address these risks, among other things, the DOJ is actively recruiting computer scientists and other experts outside of the legal field to build its capacity and expertise in AI and other cutting-edge technologies.

In addition, Monaco announced that the DOJ's Criminal Division will now "incorporate assessment of disruptive technology risks — including risks associated with AI — into its guidance on Evaluation of Corporate Compliance Programs."

She explained that the risk of misuse of AI is becoming a significant compliance risk for many businesses. Moving forward, prosecutors will be directed to consider how a company's compliance program assesses and mitigates this risk.

Grewal stated that the SEC recognizes, and intends to investigate and, where appropriate, pursue enforcement actions in connection with the following key risks associated with AI:

- So-called AI washing, i.e., investment advisers or companies making unfounded AI-related claims to the public, akin to greenwashing;
- The use of AI, including deepfakes, in fraud or market manipulation;
- The use of AI by broker-dealers, where such use leads to the prioritization of broker interests over those of clients; and
- AI hallucinations causing misstatements in investor-facing materials.

McGinley also noted that the CFTC has focused on AI-related risks, such as AI washing. While there is currently no associated rulemaking proposal, the CFTC has issued a request for comment on the use of artificial intelligence in CFTC-regulated markets.[1]

Practical Takeaways

The government enforcers' statements about AI — a theme that prevailed throughout the several days of the ABA Institute — emphasize the growing urgency for companies to review and revise their corporate compliance programs specifically to assess and mitigate potential risks posed by the development, sale and use of AI tools and technologies.

Importantly, government enforcers will assess how effectively a company's compliance program considers AI risks, and its ability to mitigate significant AI risks.

Companies with businesses that deploy AI-enabled tools should assess their compliance programs' ability to prevent employees, customers, vendors and business partners from misusing this cutting-edge technology.

Companies using AI technology, particularly in sales and procurement or with other external-facing functions that affect pricing or bids, should take additional cautions to safeguard sensitive company information.

Companies should also consider potential improvements to their compliance programs to

strengthen internal protocols to assess and manage AI risks, including in product development and deployment, as well as in training employees on the responsible use of AI applications.

U.S. Data and Intellectual Property Protection

DOJ National Security Division Assistant Attorney General Matthew Olsen stated that in furtherance of Executive Order No. 14117 on protecting Americans' sensitive personal data,[2] issued on Feb. 28, the DOJ published an unofficial draft of the advanced notice of proposed rulemaking with the aim of restricting foreign adversaries' access to U.S. sensitive data.[3]

Pending input from stakeholders, the proposed regulations are expected to come into force next year, with no retroactive effect.

Further, Olsen announced that the National Security Division will develop "a strategy for enforcement and compliance" with these new rules, violations of which will carry civil and criminal penalties. He added that advisory opinions and other guidance on compliance with the new rules will be issued in due time.

According to Olsen, to comply with the upcoming regulations, companies will need to develop risk-based compliance programs focused on these four key elements:

1. The nature of the data collected by the company — understand fully what categories of data exist within the company so that sensitive information can be adequately protected;

2. How and with whom the data is being shared — companies should check the agreements they have in place with vendors and advertisers and consider proactive updates to restrict any data sharing that might raise a national security concern;

3. Who has access to company data — understand whether there are any data transfers to consultants, advertisers or other vendors in the countries of concern; and

4. Where the data is going to end up — if a company is selling data in any transactions, whether there are reasons to have confidence in the third-party data brokers you are dealing with.

At the same time, multiple officials emphasized that the U.S. government continues to view protection of U.S. IP and trade secrets as vital to the United States' national security interests.

IP and trade secret protection in the face of perceived foreign national threats has been a priority for the DOJ for several years, and prosecutors across the country — but especially those in New York and California — have now built up significant expertise on the subject.

During the conference, Ramsey reiterated that white collar crimes, and IP protection more specifically, is a strong area of focus for the district, which includes Silicon Valley and the greater San Francisco Bay Area, and noted that a special unit focused on national and cybersecurity was created in 2023 to pursue these cases.

Key Takeaways

Per Olsen's explicit recommendation, companies should proactively update their compliance

programs to meet the above requirements.

While many of these best practices may overlap with compliance programs focused on privacy protections, the forthcoming rulemaking will be focused primarily on national security concerns.

Therefore, companies should be particularly mindful of any data flows to the so-called countries of concern, which will include China, including Hong Kong and Macau; Russia; Cuba; Iran; Venezuela and North Korea.

Companies should also review and seek to understand the types of data they collect and share to assess if any of it could be considered sensitive under the regulations.

The proposed regulations identify the following six categories of personal data that will be considered sensitive: (1) U.S. persons' covered personal identifiers, (2) personal financial data, (3) personal health data, (4) precise geolocation data, (5) biometric identifiers, and (6) human genomic data.

However, these categories are rather broad and do not capture the many types of personal data considered sensitive under other U.S. state and federal laws.

Conclusion

The annual updates on enforcement trends and priorities this year build upon last year's guidance by substantially sweetening the calculus for whistleblowers and voluntary self-disclosures, and reflecting the nation's rapid adoption of disruptive technology tools especially including AI.

Previous trends, such as the government's ongoing enforcement effort aimed at protecting U.S. intellectual property from perceived threats by foreign adversaries, are not letting up, but instead are increasing in specificity as to related corporate compliance expectations.

As companies increasingly engage in the race to use and sell AI tools and the datasets that fuel them, now is a great time to also put in place corporate compliance strategies to avoid becoming the next poster child for the government's deterrence efforts.

Jessica Nall is a partner at Baker McKenzie and leads the firm's West Coast investigations and compliance practice.

Cyrus Vance Jr. is a partner at the firm, co-chair of the North America litigation and government enforcement practice, and global chair of the cybersecurity practice. He previously served as Manhattan District Attorney.

Maria Piontkovska is an associate at Baker McKenzie.

[1] [CFTC website] /PressRoom/PressReleases/8853-24.

[2] [Whitehouse Website] /briefing-room/presidential-actions/2024/02/28/executive-order-on-preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related-data-by-countries-of-concern/.

[3] [federal register website] /documents/2024/03/05/2024-04594/national-security-division-provisions-regarding-access-to-americans-bulk-sensitive-personal-data-and.