VedderPrice

Government Agencies to Continue Pursuing Core Enforcement Initiatives and Other Highlights from the ABA 40th Annual National Institute on White Collar Crime

By Ryan S. Hedges, Arianna Goodman, Junaid A. Zubairi, Jason B. Sobelman, Andrew T. Figueroa, Tamara Droubi and Samuel M. Deau

March 12, 2025

The American Bar Association held its 40th Annual National Institute on White Collar Crime conference on March 5, 6, and 7, 2025, in Miami, Florida. The conference featured robust panel discussions with the federal and state judiciary, law enforcement officials, defense attorneys, corporate in-house counsel, and members of the academic community on a variety of topics. The conference speakers and panels also provided an update on litigation, judicial, and legislative developments. Notably, this conference differed from years past because most Department of Justice officials withdrew from participation days before the conference began.

Special Session: Conversation with the Enforcers & Regulators

A highlight of the conference was a special session with enforcers and regulators, including Antonia Apps, Acting Deputy Director of the Division of Enforcement and the Regional Director of the New York Office of the United States Securities and Exchange Commission; Bryan Young, Director of Enforcement, Commodity Futures Trading Commission; and two former U.S. Department of Justice officials.

Ms. Apps emphasized support for the SEC's staff and reiterated the SEC's three-fold commitment of (i) protecting investors; (ii) maintaining fair, orderly, and efficient markets; and (iii) facilitating capital formation. Ms. Apps explained that while there may be internal changes in priorities and policies, the SEC will continue with its core enforcement agenda, including its pursuit of accounting fraud, insider trading, and other deceptive and fraudulent practices in the market. The SEC will continue to work in conjunction with federal and state prosecutors, including through the use of the whistleblower program. Ms. Apps fielded questions relating to digital assets and cryptocurrency regulations and advised that the SEC is not abandoning investigations in their entirety but rather moving forward with investigations and litigations involving fraud in these areas. She commended the creation of the Cyber and Emerging Technologies Unit and its focus on combatting cyber- and fraud-related misconduct and to protect retail investors in the emerging technologies space. Ms. Apps concluded by explaining the importance of cooperation with the SEC, self-reporting, and other remedial actions.

Mr. Young also emphasized support for the CFTC's staff and the importance of going back to the basics—specifically, cases and matters that can return money to victims of fraudulent schemes and market misconduct. Mr. Young focused his discussion on cooperation by investigation subjects. He discussed the details and framework the CFTC will use to assess self-reporting, cooperation, and remediation in investigations and enforcement actions. Self-reporting will be evaluated on a three-tier scale: no self-report; satisfactory self-report; and exemplary self-report. The CFTC will evaluate cooperation on a four-tier scale: no cooperation; satisfactory cooperation; excellent cooperation; and exemplary cooperation. These tiered scales will play a vital role when evaluating the potential mitigation credit that would be applied to reduce a civil monetary penalty imposed by the CFTC.

The other panelists focused their discussion on the Foreign Corrupt Practices Act (FCPA). While FCPA enforcement is paused, a former DOJ official said the FCPA will still be "part of our fabric," highlighting the potential pursuit of violations by other regulators and the pursuit once, and if, the enforcement pause expires. The other panelist also commented on the

FCPA pause and noted that prosecutors may shift their focus to enforcing the Foreign Extortion Prevention Act (FEPA), with emphasis on national security.

Overall, the panel unanimously agreed that while some uncertainty remains regarding this administration's enforcement priorities, consumer protection will remain at the forefront of the SEC and CFTC.

Fireside Chat with Supreme Court Justice Ketanji Brown Jackson

Another highlight of the conference was a fireside chat between former United States Attorney for the Northern District of California Ismail Ramsey and the United States Supreme Court Justice Ketanji Brown Jackson. Justice Jackson answered questions and spoke about her judicial philosophy. For example, Justice Jackson opined that she would like to see the federal sentencing guidelines "revisited as a whole" to ensure that an individual's sentence accurately reflects their culpability. Justice Jackson noted that "[f]airness requires that similarly situated defendants be treated similarly." As a former member of the United States Sentencing Commission, which is tasked with developing guidelines for district court judges to consider before imposing a sentence, Justice Jackson noted that the recommended sentences in white collar cases has increased significantly because of the amount of money involved in fraud schemes.

With respect to her approach on the bench, Justice Jackson stated that her judicial philosophy was "still under development." Justice Jackson discussed Justice Breyer's "purposivism" philosophy, which examines the legislature's underlying purpose in enacting legislation, while acknowledging that the text of a statute is not the only component of the judicial analysis. Justice Jackson also highlighted the diversity of the judiciary and the important role diversity plays in fostering confidence in the institution.

Other Conference Highlights

Beyond the special session and address from Justice Ketanji Brown Jackson, the conference featured panel discussions on a variety of topics, including the following:

Securities Enforcement: Panel members discussed the government's latest enforcement priorities and whether there was a significant "pendulum swing" in securities enforcement with the new administration. According to certain panel members, the SEC will continue to pursue its "bread and butter" fraud and accounting cases but will significantly decline its enforcement actions in other areas, including for technical violations or claims involving sophisticated investors. Building upon the enforcers' and regulators' emphasis on cooperation, certain panel members encouraged the SEC's use of public declinations in order to increase cooperation during investigations. These panel members emphasized that the public needs to be aware of enforcement actions the SEC did not bring due to increased cooperation at the investigation stage. Panelists further discussed the recent SEC action to rescind delegating authority to enforcement attorneys—specifically, the requirement that enforcement attorneys obtain approval from the agency's commissioners for all formal orders of investigation—and the related impact that this will have on the SEC and its staff.

Health Care Fraud: A panel of members of the defense bar discussed the expected enforcement of health care fraud under the new administration. While a representative of the Department of Justice's Health Care Fraud Unit was scheduled to be on the panel, no representative appeared. All panelists agreed that both criminal and civil health care fraud enforcement will continue in full force. While many components of the Department of Justice have experienced reorganization, the Health Care Fraud Unit has not faced a reduction in force and assets from other units within the fraud section may be reassigned to the Health Care Fraud Unit.

Criminal health care fraud investigations and indictments are continuing. The panelists agreed that the government will focus on pandemic relief, telemedicine, hospice, and controlled substances frauds. Additionally, there is an expectation that fentanyl related cases and wound care fraud will be a substantial target, particularly in the Southern region of the country. Overall, the panel expects no change in the continued enforcement of criminal health care fraud.

Civil health care fraud enforcement will also continue. The panel stated that there is a significant increase in qui tam False Claims Act cases. While the panel expects the government to continue its active civil enforcement in this area, it also stated that practitioners must be arguing that the qui tam provision of the False Claims Act violates the United States Constitution's Article Two Appointments Clause, consistent with the ruling in *United States ex rel. Zafirov v. Florida Medical Associates, LLC*, 2024 WL 4349242 (M.D. Fla. Sept. 30, 2024). The case is currently on appeal in the Eleventh Circuit. However, the panel expects the Supreme Court to grant certiorari to decide the constitutionality of the *qui tam* provision of the False Claims Act. In the meantime, many practitioners will be advancing this argument to preserve the issue.

The False Claims Act: In-house and defense attorneys addressed recent developments in the False Claims Act (FCA) sphere.

Cybersecurity – Noting the government's lawsuit against Georgia Technical (litigated as part of the Civil Cyber-Fraud Initiative), and the more recent settlement with Health Net Federal Services Inc. and Centene Corporation, the panel emphasized the need for companies to strengthen the relationship between the business and compliance divisions to address FCA cybersecurity risks (e.g., not only determining what your government contract requires and what services you are providing the government, but also, if you are doing what you told the government you would do).

Benefits of Cooperation – Generally, while the greatest benefit of cooperating with the government in an FCA case is a reduction in the 3x "multiplier" that is applied to FCA damages, there remains a lack of clarity about what the government views as cooperation. According to one panel member, the government's settlement with Consolidated Nuclear Security, LLC is instructive as to what the company did that led the government to agree to 1.1x multiplier—a highly extraordinary result given that settlements routinely average a 2x multiplier. Ultimately, the "linchpin" of cooperation credit is early detection, with a focus on culture and training, and how a company uses data to identify and mitigate risk.

Constitutionality of qui tam (whistleblower) lawsuits – Practically speaking, while the *Zafirov* rationale provides another possible defense, the focus remains on training and internal reporting mechanisms and follow up. It is also important to mine employee surveys for whistleblower risks.

Loper Bright decision – Following the U.S. Supreme Court's decision in *Loper Bright Enterprises v. Raimondo*, 603 U.S. 369 (2024), courts will independently decide the meaning of ambiguous statutes and no longer defer to an administrative agency's interpretation. This may lead to inconsistent judicial interpretations, thereby complicating compliance efforts if the meaning of a regulation is not uniform nationwide, as evidenced by the Supreme Court's decision in *U.S. ex rel. Schutte v SuperValu Inc.*, 598 U.S. 739 (2023), deciding that the defendant's subjective knowledge is always relevant to the question of whether the defendant knows the claim is false, even where a relevant provision is ambiguous.

Settlement negotiations – In the case of multiple defendants, the D.C. Circuit opinion in *U.S. v. Honeywell International, Inc.* is instructive about offsetting settlement damages. Applying the *pro tanto* rule, the court concluded that a defendant's damages should be reduced by the settlements already obtained by the government. While for Honeywell this provided a complete offset based on the government's settlements with other companies, a non-settling party can be liable for more than its proportional share of the harm. Thus, companies need to consider the applicability of the *pro tanto* rule from the get-go.

Sanctions and Export Control Enforcement: Looking at 2024 enforcement actions, panel members discussed the anticipated enforcement agendas of the Bureau of Industry and Security (BIS), Office of Foreign Assets Control (OFAC), U.S. Department of Justice (DOJ), and U.S. Department of Homeland Security (DHS), while also providing thoughts about best practices for the industry.

BIS – With a focus on keeping the most sensitive items out of the most dangerous hands, BIS's mission is linked to national security and will remain a priority of the current administration. The Disruptive Technology Strike Force saw a lot of activity in 2024 focusing on Russia, Iran, China, North Korea and Venezuela, with BIS using denial orders, forfeiture actions and the Entity List (a list of companies subject to restrictive conditions). Not only is this trend expected to continue, but also, BIS will likely bring more standalone administrative cases similar to the Seagate Technology LLC and Seagate Singapore International Headquarters Pte. Ltd. matter—BIS imposed a $300 million civil penalty to resolve the sale of hard disk drives to Huawei Technologies Co. Ltd. in violation of the foreign direct product (FDP) rule. Similarly, the January 20, 2025 America First Trade Policy Executive Order shows an increased focus on industry and other countries, particularly China and artificial intelligence (AI).

OFAC – Although it is unclear how the Russia sanctions policy may change, the current administration seems very willing to tighten or impose new sanctions against Iran (and possibly Cuba and Venezuela). Also notable is the extension of OFAC's recordkeeping requirement to 10 years, thereby extending the scope of OFAC-issued subpoenas, as well as the inclusion of sanctions under the FinCEN whistleblower program (which is reported to be very active). With the America First perspective, there may be more enforcement actions against non-U.S. companies violating sanctions through the use of the U.S. financial system—where U.S. dollars are a bridge currency—and possibly, against individuals.

DOJ – In 2024, DOJ's National Security Division (NSD) issued its first-ever corporate declination under NSD's voluntary self-disclosure program. Also, the Committee on Foreign Investment in the United States (CFIUS), in connection with a partnership between DOJ and the U.S. Department of Treasury, imposed a $60 million penalty on T-Mobile US, Inc. for violating a material provision of a 2018 National Security Agreement. Looking forward, NSD's final rule implementing Executive Order 14117 (Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government Data by Countries of Concern) will come into force this year, requiring a significant compliance effort by companies to identify where their data is going. Already, there is tremendous focus on investment policies concerning the risk of sensitive technology going to China; on North Korea, and its use of cyberattacks against cryptocurrency companies; and on Latin American, as seen through the designation of cartels as foreign terrorist organizations—a very powerful tool the DOJ can use against companies, much as it did prosecuting Lafarge S.A. and Lafarge Cement Syria (LCS) S.A. for supporting ISIS, which lead to guilty pleas and financial penalties, including criminal fines and forfeiture, totaling $777.78 million.

DHS – Through the work of Homeland Security Investigations (HSI), a law enforcement agency within DHS, 2025 should continue the use of HSI's Project Shield America to educate and train industry on awareness of and compliance with export control laws (e.g., if you are manufacturing military grade components or dual-use items)—essentially, what items U.S. enemies are looking for, and how to recognize if you are being approached by an illicit procurement agent. Another likely priority is the continuing focus on ghost ships, most of which take sanctioned oil from Iran to China. This is particularly important for financial institutions and insurance companies, and their compliance with the Know Your Customer (KYC) principle. A third priority focuses on drones, and the use of drones on battlefields, e.g., in Ukraine. The majority of such drones (e.g., the HESA Shahed 136 series) are manufactured in Iran and shipped to Russa. When deconstructing a Shahed 136 drone, it was found that approximately 77% of the parts were manufactured in Western counties, including parts from 113 American companies. As such, these cases are of absolute priority to the government, as demonstrated by the indictment of two men related to an illegal scheme to export sophisticated electronic components from the United States to Iran. Indeed, from a corporate perspective, a drone-related case can escalate from a licensing issue to more serious criminal issues if the part(s) at issue is connected to loss of life on a battlefield.

Industry – The dynamic nature of the trade policy landscape (e.g., the different enforcement priorities, agencies and regulations) reinforces the importance of (1) having strong, effective, risk-based compliance programs, including training modules conducted in an employee's native language and continuous evaluation programs to monitor customers and vendors; (2) conducting more frequent risk assessments about a company's business profile (e.g., how your supply chain has changed, where your supply routes are, where you are operating, who your new business partners are, what kind of KYC intelligence you need, and whether you have physical security issues with the delivery of items); (3) voluntary self-disclosure considerations; and (4) compliance officers. As relating to China, the focus is on China, Macau and Hong Kong, inbound and outbound, relating to specific technologies like AI, semiconductors and quantum computing (and, as noted, sensitive personal data based on the forthcoming final rule implementing Executive Order 14117). In the outbound sphere, there must be consideration of contacts with friendly countries where the target has significant connections to China, Macau or Hong Kong, as well as transactions—supply chain transactions as well as investment and other M&A deals—that are considered sensitive (vs. prohibited) and subject to notice requirements. Of further note, trade issues implicate multiple jurisdictions from a multilateral standpoint (e.g., EU harmonization on criminalizing sanctions, and the cooperation between the United States and the United Kingdom on sanctions). Additionally, Congress extended the statute of limitations for sanctions violations under the International Emergency Economic Powers Act (IEEPA) and the Trading with Enemy Act (TWIA) from five years to ten years for any violations committed after April 24, 2019. Such a long statute of limitations period will cover multiple policy changes and iterations, as well as changes to the enforcers and their agendas.

If you have any questions about this article, please contact **Ryan S. Hedges** at rhedges@vedderprice.com, **Arianna Goodman** at agoodman@vedderprice.com, **Junaid A. Zubairi** at jzubairi@vedderprice.com, **Jason B. Sobelman** at jsobelman@vedderprice.com, **Andrew T. Figueroa** at dfigueroa@vedderprice.com, **Tamara Droubi** at tdroubi@vedderprice.com, **Samuel M. Deau** at sdeau@vedderprice.com or any other Vedder Price attorney with whom you have worked.