SPEECH

Acting Assistant Attorney General Nicole M. Argentieri Delivers Keynote Speech at the American Bar Association's 39th National Institute on White Collar Crime

Friday, March 8, 2024

Location
San Francisco, CA
United States

Remarks as Prepared for Delivery

Thank you, Maggie, for that kind introduction. And thank you to the American Bar Association for inviting me to speak today. It's an honor to be joined by so many prominent leaders of the white collar bar and the corporate compliance community.

As you all know, white collar criminal enforcement is a top priority for the department. Corrupt executives who commit crimes in the board room undermine public trust in the fairness of our financial markets. It is critical that we hold to account both the individual wrongdoers who engage in misconduct and the corporations that benefit from their crimes — to punish culpable individuals, to seek justice for victims, and to encourage companies to be good corporate citizens.

Today, I'd like to discuss the Criminal Division's unyielding efforts to combat white collar crime.

First, I'll address our focus on individual accountability and the impact our corporate enforcement efforts have had on multiple industries.

Next, I'll explain how the Criminal Division is applying our corporate enforcement policies.

Finally, I'll look ahead and discuss some of the new tools the Criminal Division is using — or will be soon — to identify and prosecute corporate crime.

Let me start with our priorities. The Criminal Division is focused on investigating and prosecuting the most complex financial crimes and having the greatest possible impact on corporate conduct. Companies act only through people, and so, above all, our number one goal is holding culpable individuals accountable — including corporate executives, no matter how prominent or influential.

Our recent case involving the CEO of the world's largest cryptocurrency company — led by our Money Laundering and Asset Recovery Section, or MLARS — is a prime example. The guilty pleas by Binance and its CEO late last year were historic. With over $4.3 billion in criminal penalties, this was the largest corporate guilty plea that also involved the plea of the company's CEO. And to be clear, that result did not happen overnight — it was the result of years of work by Criminal Division prosecutors digging through petabytes of data, listening to recordings, interviewing witnesses, and carefully building the case, piece by piece. That is the type of dedication and doggedness that is required to hold powerful executives and companies accountable for their criminal activity.

But when culpable individuals don't plead guilty, we go to trial. Big, impactful cases often mean challenging trials — presenting evidence developed through years of work in courtrooms across the country. But our prosecutors are up to the challenge. In April of last year, after a multi-year investigation and a three-month jury trial, our prosecutors convicted the CEO, the president, and the CFO — who was also the COO — of Outcome Health, a health technology start-up company, for defrauding customers, lenders, and investors.

And most recently, following an eight-week jury trial, our prosecutors convicted a now former oil and gas trader at Vitol Inc., the U.S. affiliate of the largest independent energy trading firm in the world, on FCPA and money laundering charges. This defendant paid more than $1 million in bribes to officials at Ecuador's and Mexico's state-owned oil and gas companies to obtain lucrative contracts. That case was part of a larger series of investigations into corruption at oil trading companies that began in 2017 and spanned more than half a dozen countries. I will talk about this a little later, but to brag for a moment: to date, our attorneys have held four of the world's largest commodity trading companies accountable for bribery and corruption offenses, the result of years of work, countless mutual legal assistance requests, international witness interviews, exhaustive document review, myriad calls with defense counsel, and many motions filed. We've transformed the energy trading industry with this work. And for former Vitol oil trader Javier Aguilar, all that work ended with a jury finding him guilty on all counts in a New York courtroom just two weeks ago.

Our prosecutors are trying more white collar cases against individuals than ever before. Over the last two years, the Fraud Section has tried over 100 white collar cases, a section record.

These results demonstrate our commitment to holding gatekeepers to account. In 2023, about a quarter of the more than 250 individuals charged by Criminal Division prosecutors in white collar cases were corporate executives, lawyers, or medical professionals. Companies, employees, shareholders, and patients trust these gatekeepers to set the tone and culture at an organization. And when they fail to do so, there is a cost — for the company, for shareholders, for innocent employees, for the integrity of our financial markets, and for the patients and clients that these doctors and lawyers took oaths to protect. Our job is to show that corrupt business is bad business — and comes at personal cost.

Our attorneys have done incredible work over the past year in this respect, including bringing the first-ever criminal charge against the CEO of an investment firm for engaging in a "cherry-picking" scheme involving cryptocurrency futures contracts; charging the former president of a shipbuilder that constructs vessels for the U.S. Navy and others for orchestrating an accounting fraud scheme; and charging the CEO of a Georgia-

based manufacturer of law enforcement uniforms and accessories for bribing Honduran government officials to obtain $10 million worth of contracts.

We take seriously our mission to follow the evidence wherever it leads. And the numbers demonstrate the scale and complexity of our individual white collar prosecutions: for example, last year, the average alleged fraud loss in cases against individuals charged by our Fraud Section was over $28 million, an all-time high.

Corporate accountability is the other side of our white collar work, because companies are the first line of defense against misconduct. A strong compliance program is key to preventing corporate crime before it occurs and to addressing misconduct when it does take place. Our corporate enforcement policies are designed to encourage companies to invest in strong compliance functions and to step up and own up when misconduct occurs.

You've heard a lot about those policies at this conference, and I'll come back to them in a moment. But our corporate enforcement actions show the industry-wide impact of our policies in action. We have brought cases against some of the largest and most significant companies in their sectors. Cases that send a clear message to industry about the importance of — and the benefits from — strong compliance programs, and in so doing, will transform those industries.

Take Binance. Binance became the world's largest cryptocurrency exchange in part by prioritizing growth, market share, and profits over compliance with U.S. law. Binance's CEO was explicit about the company's priorities, telling employees that, when it came to compliance, it was "better to ask for forgiveness than permission." And the company's employees got the message. As one compliance employee wrote in a chat, "we need a banner 'is washing drug money too hard these days – come to binance we got cake for you.'" An independent compliance monitor will make sure that Binance doesn't repeat these criminal mistakes.

Our prosecution of Binance reaffirmed the bedrock principle that if you serve U.S. customers, you must obey U.S. law.

But this not a one-and-done for us. From the prosecution of Binance to the work of our National Cryptocurrency Enforcement Team, we are sending a clear message to the cryptocurrency industry: a business strategy that puts profits over compliance is a path to federal prosecution. And the consequences — as the Binance prosecution demonstrates — are severe.

Look, for example, at our prosecution of the founder of Bitzlato — a cryptocurrency exchange that was open for business to money launderers and other criminals. The defendant pleaded guilty to operating an illegal money transmitting business, agreed to dissolve Bitzlato, and released any claim to over $23 million in seized assets.

But we aren't just picking on the newest kids on the block.

We bring impactful cases across a range of industries. Take the energy trading business, which I touched on earlier. This enormously lucrative sector relies upon multimillion-dollar transactions with state-owned companies and relationships with government officials at those entities. Over the past several years, Criminal Division prosecutors have entered into corporate resolutions for FCPA violations with the world's largest oil and energy trading firms — including Vitol, Glencore, Freepoint, and, just last week, Gunvor — and prosecuted multiple individuals in connection with these cases.

The schemes were strikingly similar: bribe payments funneled into the pockets of foreign officials through corrupt third-party agents using sham contracts and fake invoices. And to make the schemes work, employees exploited gaps in their companies' compliance programs. For example, Javier Aguilar, the recently convicted former Vitol trader, was caught on tape saying he needed to speak with a co-conspirator from his personal phone because the company's compliance officer "scans the computers" and "has access" to "the phones." He was also caught on tape saying that a corrupt middleman "has to make up some fake contracts." To communicate with his co-conspirators, he used personal email accounts associated with fake names. And he ensured that Vitol paid co-conspirators using an off-the-books system that was not subject to the company's standard checks and controls.

As part of their resolutions with the Criminal Division, each of these trading companies was required to make critical enhancements to their compliance programs to prevent future violations of the FCPA. Companies that take forward-leaning steps on compliance will be better-positioned to certify that they have met their compliance obligations at the end of the term of their agreements, as is now required in corporate resolutions with the Criminal Division. These prosecutions also help set the tone for the energy trading industry as a whole — they show that a robust compliance function is critical.

Because we are focused on having a real impact on corporate culture and compliance, our work is not done when we announce a resolution with a company. The Criminal Division now has a long track record overseeing companies as they make compliance enhancements. Today, there are nearly 40 companies under supervision by the Fraud Section or MLARS. Twenty-four of those companies have a market capitalization of more than $1 billion and 22 of them are public companies. Over the past decade, hundreds of other companies, across a wide range of industries, have similarly been subject to compliance obligations in cases brought by the Criminal Division.

Criminal enforcement is just one of the tools in our white collar crime toolkit.

That is why we look beyond just statistics to measure our impact. We engage with the defense bar and business community to understand how our actions are received. We craft and publicize our enforcement policies — and explain our enforcement actions — to incentivize companies to act as good corporate citizens.

As you all know, the Criminal Division has been the department's thought leader in creating and implementing these policies. And 2023 was a year of many new policies — including our revised Corporate Enforcement and Voluntary Self-Disclosure Policy, or CEP, and the launch of our Compensation Incentives and Clawbacks Pilot Program.

These policies articulate transparent criteria for our prosecutors to apply and, in turn, guideposts for companies and their counsel to consider when deciding what to do when faced with the prospect of a government investigation. One of our goals is to demonstrate the benefits that await those that voluntarily disclose misconduct.

It's one thing to issue and update policies. It's another to actually change corporate behavior. That is why we track the number of disclosures from companies. I'm proud to announce that early indications are that our policies are bearing fruit.

Specifically, since 2021, there have been substantial year-over-year increases in disclosures from companies to the Fraud Section. In 2023, we received nearly twice as many disclosures as in 2021. We expect this trend to continue as more companies take advantage of the benefits of voluntary self-disclosure and the CEP more generally.

But we know that companies and their counsel need to understand how our policies work in practice, which is why we include relevant considerations in every resolution. In that same spirit, let me discuss one of our recent cases — the January resolution with SAP — that illustrates how we are implementing three recent features of our revised policies: the CEP, the department's consideration of corporate recidivism, and the Criminal Division's Compensation Incentives and Clawbacks Pilot Program.

SAP — a global software company based in Germany that is a U.S. securities issuer — entered into a three-year DPA for bribing South African and Indonesian officials in violation of the FCPA. The company agreed to pay over $220 million in penalties as part of a global resolution with the department, SEC, and authorities in South Africa. So, how did we apply our policies in this case?

Let's start with the CEP. Even though the company didn't voluntarily self-disclose the misconduct, SAP's cooperation and remediation earned a 40% reduction in the criminal penalty — near the maximum reduction available for companies that do not voluntarily self-disclose. SAP immediately began to cooperate after news reports in South Africa publicized some of the allegations. At the beginning of its internal investigation, the company imaged the phones of relevant employees, preserving highly probative communications that were sent on mobile messaging applications.

This sort of proactive, impactful cooperation makes a real difference in our ability to advance our independent investigation.

The same theme underpins many aspects of the company's remediation. Not only did the company promptly discipline the employees involved in the misconduct, it also took affirmative steps to improve its compliance program and reduce its risk profile, including by making changes to its business model. These actions included eliminating its third-party sales commission model globally, prohibiting all sales commissions for public sector contracts in high-risk markets, and significantly increasing the budget, resources, and expertise devoted to compliance. And importantly, SAP expanded the data analytics capabilities of its compliance program to over 150 countries, including all high-risk countries globally. That is the type of decision we saw only rarely 10 years ago.

These proactive, impactful measures are designed to model good corporate citizenship — including a robust compliance program. They also earned the company a substantial reduction in its financial penalty. Because remember, the reduction under our Corporate Enforcement Policy is for both cooperation and recidivism.

Now on to corporate recidivism. Prior misconduct can be a window into a company's corporate culture. Companies that learn from their history and take significant remedial steps to prevent the recurrence of misconduct can expect better outcomes. Of course, the facts of each case drive our analysis. How serious was the prior misconduct? Was it criminal? How similar was it to the current misconduct? Are the same bad actors involved? Those questions are at the forefront of our thinking.

SAP had some significant prior misconduct. In 2021, following its voluntary self-disclosure of potential export control violations, the company entered into a non-prosecution agreement with the department's National Security Division as well as administrative agreements with the Departments of Commerce and the Treasury. Five years before that, SAP had entered into a resolution with the SEC concerning alleged FCPA violations in Panama. In considering this history, we evaluated a number of factors, including that SAP does business all over the world, including with many governments and state-owned entities, and, as a result, may have touchpoints with various regulators internationally.

Given the facts, including that the company's prior NPA resulted from a voluntary self-disclosure, the date of each prior resolution, and the lack of overlapping personnel, we calculated the monetary penalty by starting at the 10th percentile of the Guidelines range before applying the 40% reduction for cooperation and remediation.

Contrast SAP with Gunvor, which just last week pleaded guilty for paying bribes to Ecuadorian government officials to obtain business from Ecuador's state-owned oil company, Petroecuador. As was publicly announced, the company agreed to pay over $660 million in penalties, including forfeiture of over $287 million in ill-gotten gains.

Gunvor received a 25% reduction from the applicable fine for cooperation and remediation, but we applied that reduction starting from the 30th percentile above the bottom of the Guidelines range. As explained in the public resolution papers, that starting point was due in large measure to the fact that Gunvor committed the scheme to bribe Ecuadorian officials, in part, while it was under investigation by Swiss authorities for a separate scheme to bribe officials in Africa, which ultimately was resolved in 2019.

We will continue to assess all of a company's prior misconduct in determining both the appropriate form of a resolution and the financial penalty. But not all prior misconduct is alike. And we will not hesitate to require substantial penalties — including, where appropriate, guilty pleas — for companies that show themselves to be repeat offenders.

Let me now turn to how we applied our clawback policy in SAP.

Even before its criminal resolution, SAP had adjusted its compensation incentives to align with compliance objectives and reduce corruption risk.

As part of its criminal resolution, under the Pilot Program, SAP committed to further incorporating compliance into the company's compensation and bonus system, subject to local labor laws — as is now required in all Criminal Division corporate resolutions. SAP is now the 8th company to do so.

SAP also took advantage of the second part of the Pilot Program, which allows companies to reduce their fines when they withhold compensation from culpable employees. We reduced SAP's criminal penalty by over $100,000 for compensation that the company withheld from certain employees.

But the company didn't stop there. It went to great lengths to defend this corporate decision, including through litigation. These actions sent a clear message to other SAP employees — and employees of companies everywhere — that misconduct will have individual financial consequences. This is another example of the company's remediation that supported our decision to award a 40% fine reduction.

SAP followed the lead of Albemarle, which was the first company to receive a fine reduction under the Pilot Program in an FCPA resolution last year. Gunvor also recognized the critical relationship between compensation and compliance. Prior to pleading guilty, Gunvor had already updated and evaluated its compensation policy to better incentivize compliance with the law and corporate policies.

These examples show the benefits to companies that implement compliance-related criteria in their compensation systems and, where appropriate, withhold or claw back compensation from wrongdoers.

All of these policies should send a simple, but strong, message: being a good corporate citizen is not just the right thing to do. It is good business. Those who step up will be able to unlock the benefits afforded by our

policies. And those who do not will face stiff punishments. And for companies that are making the tough decision of whether to disclose, take note — we now have more ways than ever to discover misconduct.

And we are constantly evaluating ways to enhance the effectiveness of our policies.

As the Deputy Attorney General (DAG) announced yesterday, the department plans to spend the next several months designing and then launching a pilot program to pay monetary rewards to whistleblowers. And I'm pleased to say that the Criminal Division — and especially MLARS — will be at the forefront of this effort.

The Criminal Division has successfully used whistleblower tips for years to open or advance white collar investigations. Our colleagues at the SEC, CFTC, and now at FinCEN have established programs, and we coordinate closely with them when whistleblowers provide tips that identify potentially criminal misconduct. This experience has positioned us well to help design DOJ's new pilot program.

Of course, when it comes to the pilot, there are only so many details I can share at this point — the whole point of the DAG's 90-day "policy sprint" is to gather information, consult with stakeholders, and design a thoughtful, well-informed program. But I can share some preliminary thinking.

Under Title 28 of the U.S. Code, the Attorney General is authorized to pay awards for "information or assistance leading to civil or criminal forfeitures." In the past, we've used this authority here and there — but never as part of a targeted program.

Because the statutory authority is tied to the department's forfeiture program, MLARS will play a leading role in designing the nuts and bolts of the pilot. MLARS will be working closely with U.S. Attorneys, the FBI, and other DOJ offices to develop the program guidelines that will address eligibility requirements for potential whistleblowers.

As the DAG said, we intend for this pilot program to fill gaps in the existing framework of federal whistleblower programs. In other words, we believe that we can make the greatest impact by offering financial incentives to disclose misconduct in areas where no such incentives currently exist. For example, we anticipate that the program could prove especially useful in developing foreign corruption cases that are outside the jurisdiction of the SEC, including FCPA violations by non-issuers.

As part of the policy sprint, we will consider requirements for program eligibility. Like the SEC and CFTC, we will only provide rewards to whistleblowers who submit original, non-public, truthful information not already known to the department, and only when that information is provided voluntarily and not in response to any government inquiry, preexisting reporting obligation, or imminent threat of disclosure.

In addition, both the SEC and CFTC whistleblower programs limit rewards to cases in which the agency orders sanctions of $1 million or more. We expect to also establish some sort of monetary threshold, as a way of focusing our resources on the most significant cases. We look forward to receiving input about what the proper threshold should be.

I look forward to sharing more about this initiative in the coming weeks and months. And I am confident this will be an important tool in generating impactful white collar investigations and prosecutions, as we provide stronger incentives to both companies and individuals to come forward and report misconduct. Stay tuned.

These are not the only innovations we're bringing to expand our white collar practice. We will use the recently enacted Foreign Extortion Prevention Act (FEPA) to hold corrupt foreign officials accountable.

We appreciate the sensitivities of prosecuting a foreign government's officials. Prosecutors in our FCPA Unit and our Kleptocracy Initiative in MLARS are very experienced at handling these sensitive matters, having investigated and prosecuted foreign bribery cases spanning the globe, criminal misconduct by foreign officials, and asset forfeiture matters involving money stolen from foreign governments by corrupt officials.

It makes sense that the same attorneys who investigate and prosecute FCPA violations would also handle cases brought under FEPA.

I'm pleased to announce that we've now codified this policy by revising the Justice Manual (JM), which we rolled out yesterday. The updated JM provision makes clear that the department will handle FEPA cases the same way we've treated FCPA cases — with centralized supervision by the Fraud Section, working in partnership with U.S. Attorneys' Offices across the country.

This is just the latest example of how the Criminal Division leads on white collar criminal enforcement.

It has been a privilege to speak with you about the work of the Criminal Division — what we've accomplished and what we expect to see looking ahead. We will continue to investigate and prosecute the most complex and high-impact white collar cases, using every tool at our disposal — both old and new — and through the incredible efforts of our hardworking prosecutors.

Thank you very much.

Speaker

Principal Deputy Assistant Attorney General Nicole M. Argentieri

Topics

FINANCIAL FRAUD | FOREIGN CORRUPTION | PUBLIC CORRUPTION

Components

Criminal Division | Criminal - Criminal Fraud Section | Criminal - Money Laundering and Asset Recovery Section

Updated March 8, 2024

Related Content