SPEECH

Deputy Attorney General Lisa Monaco Delivers Keynote Remarks at the American Bar Association's 39th National Institute on White Collar Crime

Thursday, March 7, 2024

Location
San Francisco, CA
United States

Remarks as Prepared for Delivery

Thank you, Ray, for that very kind introduction — and for your continued leadership of the Institute.

I appreciate the invitation to speak again at this gathering and to give the Larry Barcella Memorial Lecture. My memories of Larry are from my time as a newly-minted AUSA in the D.C. U.S. Attorney's Office — and as an even newer member of the Edward Bennett Williams Inn of Court. More than once, I witnessed Larry pointedly critique a DOJ official about the wisdom — or lack thereof — of the latest corporate enforcement policy.

Today, I'll provide an update on our efforts and tell you what's top of mind as we confront today's corporate enforcement landscape.

And in honor of Larry, I'll no doubt give you something to critique.

The bottom line up front is that we've been executing on the priorities we set at the beginning of the administration. And our approach is straightforward. We identify the most serious wrongdoers — individual and corporate — and focus our full energy on holding them accountable. Those who break the law pay the price.

Accountability promotes fairness, drives deterrence, and fosters respect for the rule of law. At its best, it should also encourage investments in building a culture of compliance. That way, we're not simply bringing cases — we're also building an enforcement framework that promotes good corporate citizenship.

This approach benefits everyone. Consumers, investors, employees, and shareholders — of course. But also all Americans, who deserve — who demand — a criminal justice system that holds accountable those who break the law, from the street corner to the corner office.

So, we are:

- Holding individuals accountable for corporate misconduct;
- Demanding stiffer penalties for corporate recidivists;
- Using a mix of carrots and sticks to promote responsible corporate citizenship; and
- as we do, we're evolving to meet new and emerging threats — threats from disruptive technologies — including one you might have heard of: artificial intelligence.

Our first priority has been — and will continue to be — individual accountability. Companies can only act through individuals.

The rule of law demands that those most culpable for a company's misconduct are the ones being charged, prosecuted, and convicted.

From the beginning, we promised to follow every corporate case up the company's org chart — no matter where the evidence took us. We also asked prosecutors to be bold — and they've done so.

In just the last few months, Justice Department agents and prosecutors have secured convictions of the CEOs of the world's two largest cryptocurrency platforms — FTX and Binance.

That's on top of convictions, in the past few years, of the chief executive officer and chief operating officer of Theranos, two managing directors of Goldman Sachs, and dozens of executives across a range of industries, including investment firms, health care companies, and defense contractors – all charged and convicted of federal crimes.

This is challenging work. As we investigate more complex schemes, in more corners of the globe, with more evidence to gather and disclose, we're inevitably devoting more resources to each individual case.

And in part because we're bringing serious charges, with significant penalties, against senior executives, we're also taking more cases to trial.

We're driving real accountability.

We're also delivering consequences for corporate recidivists. A little over a year ago, we made clear that we would account for a company's criminal, civil, and regulatory history when considering the appropriate resolution.

Of course, not all prior conduct is created equal, and not all companies are similarly situated. But we apply the same principle to companies that we always have to individuals.

A history of misconduct matters.

After all, penalties exist, in part, to deter future misconduct. They're not the cost of doing business. So when a company breaks the law again — and it's clear the message wasn't received — we need to ratchet up the sanctions.

Take Ericsson. When it breached its 2019 DPA, we refused to resolve the case in 2023 for anything less than a corporate guilty plea.

Or Teva Pharmaceuticals. In 2016, it resolved an FCPA violation with a DPA. When the company faced investigation for price fixing in 2023 — we demanded a more substantial penalty. For the first time ever, we made specific performance a part of the remedy: we required the company to sell off an entire product line — a novel approach tailored to the company's unique circumstances.

If your company has had a recent brush with the law, now is the time to invest — and reinvest — in your compliance programs.

I can assure you the price of committing another violation will be far higher than the cost of preventing one.

But the throughline for our enforcement framework is rooted in the time-honored understanding that people — and corporations — respond to incentives.

It's human nature, and it's what makes the business world spin.

I understand the challenges and tradeoffs that your clients face when managing an organization with thousands of employees, complex operations, and a Fortune 100-level budget. I know because I'm the COO of one such organization.

Companies fulfill their fiduciary duty to shareholders when they support behavior that rejects wrongdoing for the sake of profit. When they follow the rules and anticipate problems. And when they reward pro-compliance — as well as pro-profit — behavior.

So, we've implemented policies to incentivize investing in a culture of compliance — before misconduct happens.

Take, for example, our approach to clawbacks. Nothing focuses the mind like the prospect of a pay cut. That's why the Criminal Division has been providing a dollar-for-dollar credit to companies that claw back or withhold compensation from culpable employees. It ensures that the actual wrongdoers are actually paying for their misconduct.

We've also implemented new Department policies on voluntary self-disclosure. Those policies are consistent, transparent, and predictable.

We want to make the math easy. When a business discovers that its employees broke the law, the company is far better off reporting the violation than waiting for DOJ to discover it.

Now, when DOJ does discover the violation, the company can still reduce its exposure by proactively cooperating in our investigation.

But I want to be clear: no matter how good a company's cooperation, a resolution will always be more favorable with voluntary self-disclosure.

We've structured our Voluntary Self Disclosure (VSD) programs to encourage companies to take responsibility for misconduct within their organizations. And we've conditioned benefits on the company's willingness to step up and own up — requiring it to disgorge profits, upgrade compliance systems, and cooperate in investigations of culpable employees.

That's good for everyone, especially general counsels and compliance officers.

We want to empower them to make the business case for investing in compliance. And when they do, they can point to our policies.

Early reports on this work are promising. We directed all components and U.S. Attorneys to implement self-disclosure programs, and we're seeing innovation — as you'd expect from our talented women and men.

Offices are starting to explore variations. At least two U.S. Attorney's Offices — led by the Southern District of New York and recently the Northern District of California — are piloting initiatives that are, in essence, voluntary self-disclosure programs for individuals.

Both are offering non-prosecution agreements to certain categories of at-fault individuals who self-disclose wrongdoing and cooperate against other, more culpable targets. We look forward to evaluating the results of these pilots and determining what's to come later this year.

As we work to encourage more reporting, we also want to engage traditional corporate whistleblowers — the people not involved in the wrongdoing but who discover misconduct by others and blow the whistle.

Now, whistleblowing can take many forms.

Take corporate acquisitions. Last October, we announced a disclosure program to incentivize companies engaged in acquisitions to surface misconduct in their due diligence and report it. That way, we identify wrongdoing and the wrongdoers.

In these situations, the acquiror hasn't done anything wrong — and we want it to report the acquiree's misconduct, so we can prosecute the responsible individuals, make victims whole, and rectify problems.

To be clear, this policy does not limit the Department's robust antitrust enforcement efforts. In fact, it complements them by ensuring that misconduct doesn't get swept under the rug.

So, I'm pleased to say that, today, we've codified this policy in the Department's Justice Manual, including the key provision that it only applies to bona fide, arms-length transactions.

But we recognized there's another way we can encourage individuals to report misconduct: by rewarding whistleblowers. And how do we do that? Money.

Going back to the days of "Wanted" posters across the Old West, law enforcement has long offered rewards to coax tipsters out of the woodwork. And today, we're announcing a program to update how DOJ uses monetary rewards to strengthen our corporate enforcement efforts.

Ever since Dodd-Frank created whistleblower programs at the SEC and the CFTC, those agencies have received thousands of tips, paid out many hundreds of millions of dollars, and disgorged billions in ill-gotten gains from corporate bad actors.

Yet both programs, and similar ones at IRS and FinCEN — by their very nature — are limited in scope. They only cover misconduct within their agencies' jurisdictions. And *qui tam* actions, which offer their own whistleblowing incentives, are only available for fraud against the government.

These programs have proven indispensable — but they resemble a patchwork quilt that doesn't cover the whole bed. They simply don't address the full range of corporate and financial misconduct that the

Department prosecutes.

So, we are filling these gaps.

Under current law, 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.

Now's the time to expand our use of this tool in corporate misconduct cases and apply it to reward whistleblowing.

So we're planning something new: a DOJ-run whistleblower rewards program. Today, we're launching a 90-day sprint to develop and implement a pilot program, with a formal start date later this year.

The premise is simple: if an individual helps DOJ discover significant corporate or financial misconduct — otherwise unknown to us — then the individual could qualify to receive a portion of the resulting forfeiture.

Over the next several months, we'll fill out the particulars, and Acting Assistant Attorney General Nicole Argentieri will discuss that process in greater detail tomorrow. But we've already established some basic guardrails. For example, we'd offer payments:

- Only after all victims have been properly compensated;
- Only to those who submit truthful information not already known to the government;
- Only to those not involved in the criminal activity itself;
- And only in cases where there isn't an existing financial disclosure incentive — including *qui tam* or another federal whistleblower program.

Used proactively, this program will fill gaps. It will create new incentives for individuals to report misconduct to the Department. And it will drive companies to invest further in their own internal compliance and reporting systems.

Now, for all the potential whistleblowers listening today, you might be wondering what to look out for. While we'll always accept information about violations of any federal law, we're especially interested in information about:

- Criminal abuses of the U.S. financial system;
- Foreign corruption cases outside the jurisdiction of the SEC, including FCPA violations by non-issuers and violations of the recently enacted Foreign Extortion Prevention Act; and
- Domestic corruption cases, especially involving illegal corporate payments to government officials.

Maybe you work — or your client does — at a fast-growing private startup here in the Bay Area, and you discover the company's been paying bribes to get regulatory approvals and doctoring the books to hide the payments. If you come forward, you could get paid as part of the recovery from that criminal case.

Or maybe you've got a client at a private equity firm, and she discovers the CFO is forging underlying loan documents. Once again, if your client reports it, a portion of the recovery could be hers.

As we take this on, it's important to underscore a central aspect of all whistleblower programs. To be eligible for a reward, you have to tell us something we didn't already know. You have to be the first in the door.

Now this is key. Why? Because the same rule applies to the Department's VSD programs.

When everyone needs to be first in the door, no one wants to be second — regardless of whether they're an innocent whistleblower, a potential defendant looking to minimize criminal exposure, or the audit committee of a company where the misconduct took place.

These incentives reinforce each other and create a multiplier effect, encouraging both companies and individuals to tell us what they know as soon as they know it.

This helps us build the strongest criminal cases against the most culpable wrongdoers. It helps us impose the most significant penalties on those who most deserve it. And it helps us use our carrots to wield larger sticks.

With these announcements, our message to whistleblowers is clear: the Department of Justice wants to hear from you. And to those considering a voluntary self-disclosure, our message is equally clear: knock on our door before we knock on yours.

Today, there are more doors for us to knock on than ever. The global threat landscape is changing rapidly — and, as always, we're evolving to meet new and emerging threats, including those from the malicious use of disruptive technologies.

And now, the ultimate disruptive technology — artificial intelligence — looms larger than ever.

Last month, in a speech at Oxford University, I laid out the Department's focus on AI and its potential impact on our justice system.

All new technologies are a double-edged sword — but AI may be the sharpest blade yet. It holds great promise to improve our lives — but great peril when criminals use it to supercharge their illegal activities, including corporate crime.

While we work to responsibly harness the benefits of AI, we are alert to its risks, and we will be using our tools in new ways to address them.

To be clear:

Fraud using AI is still fraud.

Price fixing using AI is still price fixing.

And manipulating markets using AI is still market manipulation.

You get the picture.

We have long used sentencing enhancements to seek increased penalties for criminals whose conduct presents especially serious risks to their victims and to the public at large — like increased penalties for criminals that use firearms or other dangerous weapons.

The same principle applies to AI. Where AI is deliberately misused to make a white-collar crime significantly more serious, our prosecutors will be seeking stiffer sentences — for individual and corporate defendants alike.

And compliance officers should take note. When our prosecutors assess a company's compliance program — as they do in all corporate resolutions — they consider how well the program mitigates the company's most

significant risks. And for a growing number of businesses, that now includes the risk of misusing AI.

That's why, going forward and wherever applicable, our prosecutors will assess a company's ability to manage AI-related risks as part of its overall compliance efforts.

To that end, I have directed the Criminal Division to incorporate assessment of disruptive technology risks — including risks associated with AI — into its guidance on Evaluation of Corporate Compliance Programs.

I recently also announced a new initiative called "Justice AI" — a series of convenings with stakeholders across industry, academia, law enforcement, and civil society — to address the impacts of AI.

I will convene the first of those Justice AI discussions today here in the Bay Area. And we will use these conversations to inform the Department's AI policy on a range of fronts, including the corporate compliance issues I've asked the Criminal Division to consider.

Now, in the coming days, your clients may want the scoop on what we've discussed today.

So before I wrap up, here's the Cliffs Notes version.

First, we're continuing to execute on our core strategy: invest the most significant resources in the most serious cases; hold individuals accountable; and pursue tough penalties for repeat offenders.

Second, we're using carrots and sticks to encourage companies to step up and own up and report misconduct to the government. With a first-in-the-door strategy, we're making clear that neither companies nor individuals can afford to sit on evidence of wrongdoing.

Third, we're designing our own whistleblower rewards program, as part of our broader effort to fill gaps and innovate in this space. Stay tuned.

And finally, we're applying DOJ tools to new, disruptive technologies — like addressing the rise of AI through our existing sentencing guidelines and corporate enforcement programs.

I hope I've given you a clear picture of our enforcement priorities and what to expect in the coming months. And I trust I've also given you plenty of fodder for discussion in the days to come.

Every day, we're working to ensure the Department of Justice lives up to its promise for the American people.

Whether we are deploying old school methods like flipping cooperators or responding to the newest game-changing technology, the women and men of the Justice Department will continue to be unrelenting in our work to enforce the laws that protect jobs, guard savings, and maintain faith in our economic system.

Thank you for having me today and thank you for being here.

Speaker

Lisa O. Monaco, Deputy Attorney General

Component

Office of the Deputy Attorney General