SPEECH

Deputy Attorney General Lisa O. Monaco Announces New Safe Harbor Policy for Voluntary Self-Disclosures Made in Connection with Mergers and Acquisitions

Wednesday, October 4, 2023

Location
Washington, DC
United States

Policy Designed to Encourage Disclosure of Misconduct and Hold Individual Wrongdoers Accountable

Remarks as Prepared for Delivery at the Society of Corporate Compliance and Ethics' 22nd Annual Compliance & Ethics Institute

Good afternoon. Thank you for that warm welcome. And thank you, Brett, for that kind introduction.

Thank you for inviting me to talk with you today – this is an important audience for the Department of Justice because your voice – and your work – to promote a culture of compliance across your companies is more important today than ever.

If you've been paying attention to the policies we've implemented over the past two years, you've probably noticed that I talk a lot about empowering general counsels and compliance officers – to make the case in the board room and the c-suite for investments in compliance – and to make the case that investing in strong compliance programs is good for business.

As compliance officers, you are on the front line of protecting your company and its shareholders, and in today's world, more and more frequently that means protecting national security.

Corporate enforcement is in an era of expansion and innovation.

Over the past two years, we have engaged in corporate enforcement actions to protect national security in unprecedented numbers and unexpected industries.

We have adopted new tools to fashion tailored punishments and enhance the business case for robust compliance. And we have increased consistency, predictability, and transparency for all of you and the boardrooms you advise.

And we're not done. Some of the examples I'll share today make this case: Invest in compliance now or your company may pay the price – a significant price – later. Today, I'll discuss how we have advanced the fight against corporate crime and describe where we are going next:

- First, I will discuss the dramatic expansion of our corporate enforcement efforts in the national security realm, as we confront new risks that threaten our collective security.
- Second, I will discuss new tools we are using to penalize corporate misconduct and incentivize good corporate citizenship.
- Third, I'll announce our latest effort to promote voluntary self-disclosures: our new Mergers & Acquisitions Safe Harbor policy.
- Finally, I want to briefly preview areas where we see further opportunity for innovation and expansion.

Let me start by addressing the biggest shift in corporate criminal enforcement that I've seen during my time in government: the rapid expansion of national security-related corporate crime.

Today corporate crime intersects with our national security – in everything from terrorist financing, sanctions evasion, and the circumvention of export controls, to cyber-and crypto-crime.

And we are seeing new national security dimensions in familiar areas of corporate crime – from FCPA violations to intellectual property theft that affects critical supply chains and involves disruptive technologies.

Today, companies confront a complex geopolitical environment. Many companies are responding commendably. They are implementing sophisticated compliance controls to mitigate otherwise risky business lines and, where necessary, exiting markets that

pose undue risk.

But some companies have not kept pace with today's compliance challenges, and where those companies violate the law, we are holding them accountable.

Let me highlight some notable examples.

- Last October, in the first-ever corporate guilty plea for material support to terrorism, French cement firm Lafarge admitted to paying the Islamic State and an al Qaeda affiliate to protect its profits and gain market share. The company pleaded guilty to providing material support to terrorists and paid more than $775 million in penalties.
- In April of this year, British American Tobacco (BAT) entered into a deferred prosecution agreement (DPA), its subsidiary pleaded guilty, and the company paid more than $635 million for violating U.S. sanctions. BAT admitted to selling tobacco in North Korea, which, in turn, generated revenue that advanced North Korean nuclear programs.
- And last month, the Department announced the first-ever criminal resolution for sanctions violations from illicit sales and transport of Iranian oil. The shipping company, Suez Rajan Ltd, pleaded guilty, and the United States seized nearly one million gallons of contraband Iranian oil.

More and more of our corporate resolutions implicate our national security. In fact, already this year, the number of major national-security corporate resolutions has doubled compared to last year.

To meet this moment, we are adding more than 25 new corporate crime prosecutors in the National Security Division, including the division's first-ever Chief Counsel for Corporate Enforcement. And we are increasing by 40% the number of prosecutors in the Criminal Division's Bank Integrity Unit, which holds accountable financial institutions that violate U.S. sanctions and the Bank Secrecy Act.

Our message should be clear: the tectonic plates of corporate crime have shifted. National security compliance risks are widespread; they are here to stay; and they should be at the top of every company's compliance risk chart.

Now, we're not just expanding enforcement – we're developing new tools and remedies to punish and deter. This year, we have announced corporate criminal resolutions that, for the first time, include divestiture of lines of business, specific performance as part of restitution and remediation, and tailored compensation and compliance requirements.

For example, when the Antitrust Division recently announced DPAs with two pharmaceutical companies, Teva and Glenmark, we determined that a monetary penalty alone was not sufficient. Instead, the Department required the companies to divest a widely used cholesterol medicine that was a core part of the companies' price-fixing conspiracy.

This was the first time the Department required divestiture as part of a corporate criminal resolution. As another example of innovation, we are now employing specific performance as a new remedy. As part of the recent Suez Rajan resolution – not only did the company plead guilty, but it was required to transport almost one million barrels of contraband Iranian crude oil across the globe to the United States, where it was seized pursuant to court order.

We are also keenly focused on the role compensation plays in guiding employee behavior. By rewarding compliance and deterring wrongdoing, a well-designed compensation program can align executives' financial interests with the company's interest in good corporate citizenship.

So earlier this year, I directed the Criminal Division to create a pilot program to jumpstart innovation in the design of compensation systems.

Under the pilot program, every Criminal Division resolution now requires companies to add compliance-promoting criteria to their compensation systems. These criteria are tailored to the company's existing compensation system to ensure integration with its compliance program.

The program is already bearing fruit, with incentive requirements included in several recent resolutions, such as those with Albemarle and Corficolombiana.

The pilot program also rewards companies that claw back or withhold incentive compensation from executives responsible for misconduct – or attempt to do so in good faith. For every dollar that a company claws back or withholds from an employee who engaged in misconduct – or a supervisor that knew of or turned a blind eye to it – the Department will deduct a dollar from the otherwise applicable penalty that the resolving company would pay.

Again, we are seeing positive early returns. For example, as part of last week's Albemarle resolution, the company received a clawback credit for withholding bonuses of employees who engaged in misconduct. Not only did Albemarle keep the bonuses that would have gone to wrongdoers, the company also received an offset against its penalty for the same amount. That's money saved for Albemarle and its shareholders – and a concrete demonstration of the value of clawback programs.

Companies cannot wait to enact compliance-promoting compensation policies until they are in the government's crosshairs. Companies, their boards, and their compliance officers should be addressing how their compensation policies promote compliance today and should be assessing whether their clawback programs are fit for purpose and ready for deployment.

Compliance should no longer be viewed as just a cost center for companies. Good corporate governance and effective compliance programs can shield companies from enormous financial risks and penalties.

Let me turn now to the next area where we are innovating: voluntary self-disclosure policies.

DOJ's recent corporate enforcement actions, like the ones I mentioned a few minutes ago, illustrate the enormous gulf between outcomes for companies that do the right thing – that step up and own up – and companies that do the opposite.

To enhance transparency and predictability, I announced in March that every DOJ component engaged in corporate criminal enforcement now has a voluntary self-disclosure policy. So, when companies promptly disclose misconduct, fully and in a timely manner, they can take advantage of the programs' benefits in any type of case, in any part of the Department, and in any part of the country.

Encouraging companies to self-report misconduct can result in a virtuous cycle: by giving a path to resolution and declination to companies trying to do the right thing, we are able to identify and prosecute the individuals who are not. For example, earlier this year, we declined to prosecute Corsa Coal Corporation for FCPA violations, because the company timely and voluntarily self-disclosed the misconduct, remediated, cooperated, and disgorged the profits to the extent of its capability. Crucially, the company provided information about individual wrongdoers, including two former vice presidents who were charged criminally for their involvement in the scheme.

And this brings me to the next step when it comes to Voluntary Self Disclosure: our new Mergers & Acquisitions Safe Harbor Policy. In a world where companies are on the front line in responding to geopolitical risks – we are mindful of the danger of unintended consequences. The last thing the Department wants to do is discourage companies with effective compliance programs from lawfully acquiring companies with ineffective compliance programs and a history of misconduct. Instead, we want to incentivize the acquiring company to timely disclose misconduct uncovered during the M&A process.

Now, in 2008, the FCPA Unit published an opinion requested by the energy company Halliburton, in which the Department said it did not intend to take enforcement action against Halliburton for misconduct it self-disclosed and remediated post-acquisition within a certain timeframe. That opinion applied only to that transaction, however, and did not have broader application.

Since then, some parts of the Department have addressed M&A transactions as part of their Voluntary Self Disclosure policies, though they differ from each other in approach. So today, for the first time, we are announcing a Department-wide Safe Harbor Policy for voluntary self-disclosures made in the context of the mergers and acquisition process. Going forward, acquiring companies that promptly and voluntarily disclose criminal misconduct within the Safe Harbor period, and that cooperate with the ensuing investigation, and engage in requisite, timely and appropriate remediation, restitution, and disgorgement – they will receive the presumption of a declination.

To ensure consistency, I am instructing that this Safe Harbor policy be applied Department-wide. Each part of the Department will tailor its application of this policy to fit their specific enforcement regime, and will consider how this policy will be implemented in practice.

To ensure predictability, we are setting clear timelines. As a baseline matter, to qualify for the Safe Harbor, companies must disclose misconduct discovered at the acquired entity within six months from the date of closing. That applies whether the misconduct was discovered pre- or post-acquisition.

Companies will then have a baseline of one year from the date of closing to fully remediate the misconduct. Both of these baselines are subject to a reasonableness analysis because we recognize deals differ and not every transaction is the same. So, depending on the specific facts, circumstances, and complexity of a particular transaction, those deadlines could be extended by Department prosecutors. And of course, companies that detect misconduct threatening national security or involving ongoing or imminent harm can't wait for a deadline to self-disclose.

For transparency, we are making clear that aggravating factors will be treated differently in the M&A context. The presence of aggravating factors at the acquired company will not impact in any way the acquiring company's ability to receive a declination. Now, one question we have heard is how the Department will treat the acquired entity when an acquirer voluntarily self-discloses under the Safe Harbor Policy. Unless aggravating factors exist at the acquired company, that entity can also qualify for applicable VSD benefits, including potentially a declination.

Finally, misconduct disclosed under the Safe Harbor Policy will not affect any recidivist analysis at the time of disclosure or in the future. Put another way, any misconduct disclosed under the Safe Harbor Policy will not be factored into future recidivist analysis for the acquiring company.

Of course, this policy will only apply to criminal conduct discovered in bona fide, arms-length M&A transactions. The Safe Harbor does not apply to misconduct that was otherwise required to be disclosed or already public or known to the Department. Nor will anything in this policy impact civil merger enforcement.

So, for those advising boards and deal teams – here are the takeaways. We are placing an enhanced premium on timely compliance-related due diligence and integration. Compliance must have a prominent seat at the deal table if an acquiring company wishes to effectively de-risk a transaction.

By contrast, if your company does not perform effective due diligence or self-disclose misconduct at an acquired entity, it will be subject to full successor liability for that misconduct under the law. Our goal is simple: good companies – those that invest in strong compliance programs – will not be penalized for lawfully acquiring companies when they do their due diligence and discover and self-disclose misconduct.

And we are doubling down on clarity and predictability. Through careful due diligence and timely post-acquisition integration – alongside self-disclosure, remediation, disgorgement, and cooperation where warranted – acquiring companies can protect shareholders, promote compliance, and advance the goal of fighting corporate crime.

So, what is next?

We are looking to apply our corporate enforcement principles across the entire Department, especially in areas implicating cybersecurity, tech, and national security.

The entire Department shares the same principles in both civil and criminal enforcement: (1) holding corporate and individual wrongdoers accountable, (2) incentivizing compliance, self-disclosure, remediation, and cooperation, and (3) deterring and penalizing repeat bad actors. You should expect more to come on this topic as we continue to extend consistent, transparent application of our corporate enforcement policies across the Department, beyond the criminal context to other enforcement resolutions – from breaches of affirmative civil case settlements to violations of CFIUS mitigation agreements or orders.

Gone are the days when executives could view corporate enforcement matters as the cost of doing business. In this new era, corporate executives need to redouble time and attention to compliance programs, compensation programs, and diligence on acquisitions. Failing to do so can have dire consequences for companies, shareholders, and our nation.

The world is full of risks. Corporations, and by extension, all of you in corporate compliance, are on the front lines. Of course, your job is to protect your company, but in doing so, by focusing on robust compliance and by investing in good corporate governance, you are also protecting our national security.

Thanks for having me – I look forward to taking some questions.

Speaker

Lisa Monaco, Deputy Attorney General

Component

Office of the Deputy Attorney General

Updated February 5, 2025

Related Content

PRESS RELEASE

United States Announces Plans to Extradite Three Tren de Aragua Members, Who Have Been Declared Alien Enemies, Wanted by Chile for Homicide and Kidnapping Offenses

Earlier today, the United States declared three members of Tren de Aragua (TdA) Alien Enemies and announced plans to extradite them to Chile, where they are wanted for violent crimes…

March 24, 2025

PRESS RELEASE

Statement of Deputy Attorney General Todd Blanche on Investigation into Intelligence Leak

Deputy Attorney General Todd Blanche made the following statement today regarding an investigation into the leak of intelligence information.

March 21, 2025

VIDEO

Attorney General Pamela Bondi Welcomes President Donald J. Trump to the Justice Department

March 14, 2025

Office of Public Affairs

U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington DC 20530

Office of Public Affairs Direct Line
202-514-2007

Department of Justice Main Switchboard
202-514-2000