Promoting Corporate Criminal Accountability
2021-2025

Over the past four years, the Justice Department has focused on identifying the most serious wrongdoers—both individual and corporate—and on holding them accountable. To support this effort, the Department consulted with a broad range of experts and stakeholders and implemented new policies and programs to strengthen corporate accountability. These initiatives are rooted in the idea that the Department can promote good corporate citizenship by deploying a mix of "carrots and sticks," with benefits for those who stay on the right side of the law and swift, significant penalties for those who do not. And the Department has worked to apply these policies in a consistent, predictable, and transparent manner, creating a clear enforcement framework that benefits the broader American public.

Shortly after taking office in 2021, Deputy Attorney General Monaco launched the Corporate Crime Advisory Group (CCAG), a team of Department prosecutors, investigators, and experts tasked with collecting data, consulting with outside experts, and developing recommendations for strengthening the Department's corporate enforcement strategy. Many of the policies discussed below emerged from CCAG's work or were developed through similar, parallel efforts launched by the Department's Criminal Division or U.S. Attorney community. The Department's approach also has emphasized that investment in compliance and practicing good corporate citizenship is good for business, good for the investing public. Taken together, these efforts reflect a comprehensive approach to support corporate crime prosecutors across the country with policies and programs that help hold corporate wrongdoers fully accountable for their misconduct.

Holding Individuals Accountable

"Accountability starts with the individuals responsible for criminal conduct. … [I]t is unambiguously this department's first priority in corporate criminal matters to prosecute the individuals who commit and profit from corporate malfeasance." – Deputy Attorney General Monaco, October 2021

Holding individuals accountable punishes the worst offenders, drives deterrence, and promotes the public's confidence in our justice system. The Department has renewed its focus on prosecuting the worst offenders committing the biggest crimes, no matter how high they rank on the corporate org chart — no matter how challenging and time-consuming the case. The Department began by restoring prior guidance making clear that to be eligible for any cooperation credit, companies must identify all individuals involved in the misconduct and provide all non-privileged information about individuals involved in the misconduct. This updated approach has generated real returns, with accountability in convictions of

- The CEOs of the world's two largest cryptocurrency platforms — FTX and Binance;
- The CEO and the COO of Theranos;
- The Founder and the CFO of Archegos;

- Two senior executives at Goldman Sachs; and
- Dozens of other high-ranking executives across a range of industries.

Preventing Corporate Crime by Promoting a Culture of Corporate Compliance

"Companies should feel empowered to do the right thing—to invest in compliance and culture, and to step up and own up when misconduct occurs. Companies that do so will welcome the announcements today. For those who don't, however, our Department prosecutors will be empowered, too—to hold accountable those who don't follow the law." – Deputy Attorney General Monaco, September 2022

The Department has strengthened incentives for companies to implement robust compliance programs that help to stop corporate misconduct before it starts. Many of these changes have been codified in the Department's publicly available guidance on compliance programs—known as *Evaluation of Corporate Compliance Programs*, or ECCP—which prosecutors use when deciding both whether to prosecute a company and what compliance reforms such companies should be required to undertake as part of any Department resolution. These policy changes take several forms:

- **Clawing back profits from wrongdoers and designing compensation structures to promote compliance**. In March 2023, the Department's Criminal Division launched a three-year pilot program designed to promote compliance and disgorge profits from offenders. The pilot program has two parts. First, for any company resolving with the Criminal Division, it can receive a dollar-for-dollar reduction in its criminal fine for any money clawed back or withheld from employees responsible for the misconduct. Second, whenever a company is resolving a criminal matter with the Criminal Division during this three-year period, the company must agree to modify their compensation and bonus system to include criteria related to compliance.

- **Discouraging "off-channel" communications that evade corporate recordkeeping**. In March 2023, the Department updated the ECCP to address how corporate compliance programs should account for risks arising from the use of personal devices and ephemeral messaging applications such as WhatsApp, Signal, and Telegram. The ECCP revisions highlighted the significant risks that companies face if they permit employees to communicate in ways that cannot be monitored, traced, or captured in corporate recordkeeping systems, thereby encouraging companies to adopt robust policies that ensure proper preservation of company records.

- **Evaluating compliance programs when assessing the need for monitorships**. In September 2022, the Department issued new guidance making clear that, when prosecutors are assessing whether to require the imposition of an independent compliance monitor as part of a corporate resolution, they should focus first and foremost on the strength of the company's internal compliance program and whether the company has

adequately rectified the compliance lapses identified during the criminal investigation. This new guidance has created clearer direction for companies seeking to avoid a compliance monitor by moving quickly to remediate their past misconduct.

- **Encouraging companies to more fully assess risks associated with artificial intelligence and emerging technologies**. In September 2024, the Department further revised the ECCP to require prosecutors to evaluate whether a company's compliance program includes safeguards to mitigate the risks associated with the use and misuse of emerging technologies, including artificial intelligence. The revisions requires that prosecutors ask, among other things, whether the company has instituted controls to ensure such technology is used only for its intended purposes and that the company has mitigated the risk of potential negative or unintended consequences.

Creating New Incentives and Mechanisms for Reporting Corporate Misconduct

"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." – Deputy Attorney General Monaco, March 2024

The Department has developed multiple programs and policies to encourage individuals and companies to report original information about previously undetected corporate misconduct—creating new and powerful mechanisms that help Department prosecutors build cases against those responsible for the criminal activity. These programs are mutually reinforcing, since they all require that the submitting party provide original information about the misconduct, thus creating an incentive for everyone with knowledge of the misconduct to be the "first in the door." The new programs target four categories of people and entities likely to possess previously unreported evidence of misconduct, with different benefits available to those groups depending on the circumstances of the disclosure:

- **For individuals who did not meaningfully participate in the misconduct: monetary awards.** Through the Corporate Whistleblower Awards Pilot Program, the Department has closed gaps in the federal government's patchwork of whistleblower rewards programs (including those operated by SEC, CFTC, FinCEN) by creating a new program that focuses on specific categories of corporate crime, including foreign and domestic corruption and certain offenses involving financial institutions and private health care fraud. Whistleblowers who provide original information—and who did not meaningfully participate in the misconduct themselves—can receive up to 30 percent of the net proceeds forfeited, if their information results in a criminal case that involves forfeited assets.

- **For companies that discover misconduct within their ranks: additional cooperation credit, plus the possibility of no corporate guilty plea.** Each DOJ prosecuting component is now required to maintain its own publicly available policy on corporate

"voluntary self-disclosures" (VSD), providing companies with clearer guidance on what is required to qualify for a VSD and what benefits they can expect to receive if they do. For example, the Department required that, where a company meets the requirements a component's VSD policy, fully cooperates, and timely and appropriately remediates the criminal, Department prosecutors will not seek a guilty plea from the company, absent certain aggravating factors. JM 9-28.900(A)(1). And the Department has made clear that a company that qualifies for a VSD will always receive a more favorable outcome than had the same company waited until the government discovered the misconduct before the company agreed to cooperate in the investigation.

- **Promoting Disclosure and Due Diligence in Acquisitions**. Each DOJ prosecuting component is now also required to maintain a VSD policy for disclosures made in the context of the mergers and acquisition process. If a corporate acquiror that (a) discovers misconduct by the acquiree before the acquisition, (b) voluntarily self-discloses the misconduct within 180 days of the closing date of the acquisition, (c) remediates the misconduct with 1 year of the closing date, and (d) pays any disgorgement, forfeiture, and/or restitution, the Department will apply a presumption in favor of declining prosecution of the acquiror. This policy does not prevent civil or criminal enforcement against the acquiree if aggravating factors exist, nor does it impact civil merger enforcement. JM 9-28.900(A)(3).

- **For individuals who engaged in, but did not lead or originate, the corporate misconduct: *a nonprosecution agreement***. The Criminal Division and a number of U.S. Attorney's Offices have launched Whistleblower Nonprosecution Pilot Programs, which encourage participants in nonviolent, previously undetected criminal activity to voluntarily self-disclose their involvement to prosecutors. Where certain specific conditions are met, including the individual's agreement to cooperate against all responsible parties, the prosecuting office will enter into a nonprosecution agreement. (Sample policies: CRM, EDNY, EDVA, DDC, DNJ, NDCA, NDIL, SDFL, SDNY, SDTX.)

Addressing New Risks Related to National Security, Emerging Technologies, and Artificial Intelligence

"Since returning to government, I have warned that companies are on the front lines in confronting today's geopolitical realities. In today's world, corporate crime regularly intersects with national security in areas like terrorist financing, sanctions evasion, and cybercrime." – Deputy Attorney General Monaco, October 2022

Corporate criminal enforcement increasingly implicates national security interests, emerging technologies, and artificial intelligence. The crimes vary — from sanctions violations to money laundering to material support for terrorism. The corporate defendants range across industries — from construction and shipping to agriculture and telecommunications. And the national security

risks run the gamut — from money laundering for Russian interests to trafficking in Iranian crude oil to sanctions evasion to support the North Korean nuclear program. To address these new challenges, the Department has:

- **Holding corporations accountable.** The Department brought the first-ever prosecution and conviction of a company for providing material support to a terrorist organization (ISIS).

- **Surged resources.** The Department has added (a) prosecutors into the Criminal Division's Bank Integrity Unit, which prosecutes violations of the Bank Secrecy Act and (b) white collar prosecutors and a Chief Counsel for Corporate Criminal Enforcement to our National Security Division to investigate sanctions evasion, export control violations, and other crimes.

- **Prioritized sanctions and export controls enforcement.** Enforced the economic countermeasures that the United States and our allies imposed on Russia as a result of its unprovoked invasion of Ukraine by launching and leading the interagency Task Force KleptoCapture (TFKC). To date, TFKC has charged more than 100 individuals and corporate entities and has seized, restrained, or obtained forfeiture orders against nearly $650 million in assets – while also working with U.S. and foreign partners to deploy other disruptive measures, including identifying new targets for sanctions designations and using creative legal solutions to route funds forfeited by TFKC to benefit the Ukrainian government.

- **Blocked hostile nation-states from illicitly acquiring sensitive U.S. technology.** Launched the Disruptive Technology Strike Force (DTSF) in partnership with the Commerce Department. To date, the DTSF has brought numerous complex, high-impact cases charging more than 30 individuals and corporate entities with export control violations and related crimes, while also leveraging other available tools with interagency and foreign partners, including issuing denial orders against dozens of businesses with roles in facilitating the illicit acquisition of sensitive U.S. technology – including defense contractors, airlines, and freight forwarders.

- **Heightened Enforcement Attention on Misuse of Artificial Intelligence.** In addition to updating the ECCP to include AI-specific questions (as discussed above), the Department has taken aggressive civil actions against companies that used AI irresponsibly. The Department has brought enforcement actions against companies using AI to evade the Fair Housing Act and price-fixing laws – highlighting that discrimination using AI is still discrimination, and price fixing using AI is still price fixing. The Department has also advocated to the Sentencing Commission and encouraged prosecutors to seek stiffer penalties for misconduct involving AI.

- **Informed the Private Sector About Enforcement Trends**. Clearly conveyed the Department's expectations as to national security-related compliance by issuing joint advisories with the Commerce and Treasury Departments – akin to the Foreign Corrupt Practices Act guidance that the Department publishes jointly with the SEC.

Holding Recidivists Accountable

"Companies cannot assume that they are entitled to an NPA or a DPA, particularly when they are frequent flyers. We will not shy away from bringing charges or requiring guilty pleas where facts and circumstances require. If any corporation still thinks criminal resolutions can be priced in as the cost of doing business, we have a message—times have changed." – Deputy Attorney General Monaco, September 2022

The Department has made clear that corporate wrongdoers are subject to same rules as individuals: if they violate the law more than once, they should expect stiffer penalties with each violation.

- **Disfavoring successive DPAs and NPAs**. The Department has updated its policies to discourage prosecutors from offering a deferred prosecution agreement or non-prosecution agreement to a company that has previously entered into such an agreement in the past, making clear that recidivist companies should expect that new criminal conduct will result in a guilty plea rather than pretrial diversion. JM 9-28.600(B).

- **Considering a company's history of misconduct**. In October 2021, the Department changed the way that prosecutors assess a corporation's history of misconduct, requiring that prosecutors consider *all* prior wrongdoing, including domestic, foreign, criminal, civil, or regulatory actions against the company or the company's parent, divisions, affiliates, and subsidiaries. By doing so, the Department has ensured that the full range of a company's prior bad acts are taken into account when determining the appropriate penalty for a company that engages in new misconduct. JM 9-28.600.

- **Ensuring companies live up to their agreements.** The Department has moved repeatedly to hold accountable companies that fail to live up to their agreements with the government. In May 2023, for example, the Department determined that Ericsson, a Swedish telecommunications company, had breached its 2019 DPA relating to foreign bribery, requiring the company to plead guilty and pay an additional criminal penalty of more than $206 million. And in May 2024, after concluding that that Boeing breached its 2017 DPA relating to defrauding the FAA, the Department required the company to plead guilty, pay the maximum allowable criminal fine, and invest hundreds of millions of dollars in its compliance and safety programs.