Anti-Corruption Report

anti-corruption.com

Oct. 8, 2025

Whistleblowers

How a Whistleblower Can Derail a DPA

By Luke Cass, Audrey Karman and Ian O'Keefe, *Womble Bond Dickinson*

A recent suit illustrates how whistleblowers may adversely impact a company's DPA, leading to further investigation by the DOJ and additional penalties.

In 2023, Connecticut-based Freepoint Commodities LLC (Freepoint) entered into a deferred prosecution agreement (DPA) with the DOJ for violations of the FCPA, agreeing to pay a criminal penalty of $68 million and a forfeiture of approximately $30 million. The company also agreed to pay about $7.6 million in disgorgement to resolve the investigation into its conduct by the Commodity Futures Trading Commission (CFTC). The DPA stemmed from an alleged conspiracy to bribe a state-owned company in South America. As part of the settlements, Freepoint agreed to enhance its corporate governance and compliance program, and to report any subsequent FCPA violations to the DOJ.

However, in May 2025 a former employee filed a whistleblower suit in the New York State Supreme Court alleging insider trading violations and retaliation. In the past several years, the U.S. and other governments have increasingly encouraged whistleblowers to come forward with allegations of wrongdoing by corporations. The implications for companies that are bound by DPAs or other settlement agreements, like Freepoint, could be quite significant. In this article, we discuss the various programs meant to encourage whistleblowing, how whistleblowers pose risks to existing DOJ resolutions and what compliance programs can do to mitigate those risks.

See "Obligations Linger Despite Freepoint's Settlements With DOJ and CFTC" (Aug. 28, 2024).

Freepoint's DPA With the DOJ

Freepoint was charged with conspiracy to violate the FCPA's anti-bribery provisions through a scheme to make improper payments to Brazilian government officials in exchange for confidential competitor pricing and bid information to secure lucrative business opportunities. Between 2012 and 2018, Freepoint and its co-conspirators concealed the scheme by using code words and encrypted messaging applications as well as by funneling bribes through an intermediary using offshore bank accounts and shell companies. Freepoint allegedly generated over $30 million in profits from the scheme.

Individual Prosecutions

The DOJ also indicted three individuals for their roles in the misconduct, including a senior Freepoint oil trader who directed corrupt payments to the intermediary. Another individual, operating through his company, helped Freepoint obtain business opportunities in Brazil. The third individual served as an agent for Freepoint and received more than $3.9 million in consulting fees and commissions, which were used to pay bribes on the company's behalf.

These individual prosecutions reflect a broader enforcement trend, dating back at least to a memorandum issued by then-Deputy AG Sally Yates, which emphasized holding individuals accountable for corporate wrongdoing and required that companies must identify all individuals involved in misconduct in order to receive cooperation credit. In 2021, then-Deputy AG Lisa Monaco reaffirmed this approach in another memorandum, which underscored that corporate resolutions may be delayed until related individual prosecutions are resolved.

In guidance issued in June 2025, Deputy AG Todd Blanche announced that, going forward, "prosecutors shall focus on cases in which individuals have engaged in criminal misconduct and not attribute nonspecific malfeasance to corporate structures."

See "The Blanche Memo's Take on Corporate Responsibility: Individuals Versus Corporations" (Sep. 10, 2025).

Cooperation Credit

Freepoint's DPA references the nature and seriousness of the alleged misconduct, including the scope of the bribery and the profits generated. The DOJ did, however, credit Freepoint for cooperating and assisting with the DOJ's investigation as well as for accepting responsibility.

The DOJ references several remedial actions the company took, including, but not limited to:

1. conducting a root cause analysis of the underlying misconduct and remediating those root causes;
2. improving its third-party compliance program through implementation of enhanced risk-based due diligence, screening, ongoing monitoring, oversight procedures, onboarding and tracking requirements, required FCPA training for third-party agents and testing of the third-party program;
3. enhancing its corporate governance and risk management structures by utilizing data analytics and metrics to evaluate risk;
4. improving the independence and internal resources of its compliance function by hiring additional experienced compliance personnel;
5. updating the company's global anti-bribery and corruption policy to identify FCPA red flags; and
6. developing a process for reporting and investigating allegations of misconduct.

Notably, Freepoint did not receive credit for voluntary disclosure under the DOJ's Corporate Enforcement and Voluntary Self-Disclosure Policy (CEP) as the company failed to disclose the misconduct to the DOJ in a voluntary and timely manner.

Compliance Obligations

Additionally, under the DPA, Freepoint has ongoing obligations to cooperate and timely disclose misconduct. The company is also required to continue to implement its compliance program to help mitigate corruption risks as well as continue to review and evaluate its internal controls, policies and procedures to ensure compliance with the FCPA and applicable anti-corruption laws. Further, the DPA required Freepoint to establish, and continually maintain, an effective internal reporting system that enables employees to confidentially raise concerns about potential violations of anti-corruption laws as well as company policies and procedures.

See "Do the 2025 Changes to the DOJ's CEP and Whistleblowing Programs Encourage Companies to Self-Report?" (Jul. 16, 2025).

Freepoint's CFTC Resolution

Simultaneously with the DPA, Freepoint resolved a civil enforcement action by the CFTC for charges that Freepoint engaged in unlawful misconduct to obtain nonpublic competitive fuel oil cargo bidding information as well as confidential market intelligence regarding shipping and negotiation activities.

The CFTC alleged that Freepoint committed fraud by paying bribes to officials and agents of a South American state-owned company in exchange for nonpublic information concerning fuel oil sales and purchases for the purpose of securing improper competitive advantages in the oil markets. Freepoint paid a civil monetary penalty of $61 million and disgorgement of over $30 million for violating the Commodity Exchange Act (CEA). It is worth noting that the DOJ applied up to 25% of the forfeiture amount as credit toward the disgorgement.

This coordination exemplifies the anti-piling on principles announced by then–Deputy AG Rod Rosenstein in May 2018. In 2018, the DOJ revised the U.S. Attorney's Manual to instruct that Assistant U.S. Attorneys "should also endeavor, as appropriate, to coordinate with and consider the amount of fines, penalties, and/or forfeiture paid to other federal, state, local, or foreign enforcement authorities that are seeking to resolve a case with a company for the same misconduct." While not a new concept, the principle of anti-piling on was reaffirmed in a memorandum issued by the Criminal Division on June 5, 2025.

See "Piling On? Examining the Reality of Multi-Jurisdictional FCPA Resolutions" (Jul. 11, 2018).

Whistleblower Rewards Programs

Requirements for companies to disclose misconduct – such as those in Freepoint's DPA – face growing challenges as multiple government entities increasingly encourage and incentivize whistleblowers to report externally. A range of agencies have launched dedicated whistleblower programs, some offering financial incentives and the possibility of deferred or non-prosecution of individuals who come forward, creating a powerful alternative to internal reporting mechanisms and complicating corporate compliance efforts.

CFTC

The CFTC's Whistleblower Program, established under the comprehensive financial regulatory reforms enacted through the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank), encourages individuals to report potential violations of the CEA and other CFTC regulations. Administered by the CFTC's Whistleblower Office, the program offers monetary awards for eligible whistleblowers who timely and voluntarily present original information leading to a successful CFTC enforcement action that results in monetary penalties exceeding $1 million. Whistleblowers who meet the required eligibility criteria can receive 10-30% of the monetary sanctions collected.

A whistleblower may also be eligible if the information contributes to the success of a related action brought by another government agency, provided that the CFTC's action was based on the same information. The program also provides protections against retaliation for individuals who report in good faith.

SEC

The SEC's Whistleblower Program, also created as part of Dodd-Frank, incentivizes individuals to report credible information on potential violations of federal securities laws by public companies. Specifically, whistleblowers are incentivized to report on corporate misrepresentations in public filings or financial disclosures, insider trading activities, fraudulent investments, such as Ponzi or pyramid schemes, bribes made to foreign government officials, as well as theft or misuse of investor funds or securities.

Whistleblowers who provide original information that leads to an SEC enforcement action resulting in over $1 million in monetary penalties may be eligible to receive 10-30% of the monetary penalty.

Internal Revenue Service

The Internal Revenue Service (IRS) Whistleblower Office provides monetary awards to individuals whose credible information and reporting aids the IRS in collecting unpaid taxes, penalties and other recoveries from delinquent taxpayers. Awards generally range from 15% to 30% of the amount that is collected and attributable to the whistleblower's information. To qualify for award, reporting must relate to noncompliant tax matters involving disputed amounts in excess of $2 million, and the taxpayer's gross income must exceed $200,000 for at least one of the tax years at issue.

National Security Division

The DOJ's National Security Division (NSD) amended its Enforcement Policy for Business Organizations (NSD Policy) in March 2024. The NSD Policy, underscoring the DOJ's continued focus on corporate compliance and national security interests, provides guidance as to those factors – including timely and voluntary self-disclosure, cooperation and prompt remediation – that NSD considers when determining the appropriate outcome for companies that report potential export control- or sanctions-related violations. The updated NSD Policy now also includes a policy that effectively extends the NSD's voluntary self-disclosure protections to M&A (M&A Policy).

Under the M&A Policy, acquiring companies will qualify for a presumption of declination if:

1. they disclose criminal misconduct within six months of closing an M&A transaction;
2. cooperate with the ensuing investigation; and
3. engage in the requisite, timely, and appropriate remediation, restitution, and disgorgement of any ill-gotten gains.

While the M&A Policy identifies a six-month window to disclose, there does appear to be some flexibility depending on the circumstances.

In a recent case involving a private equity firm acquiring a company where sanctions and export control violations were uncovered, the private equity company did not disclose the violations until 10 months after closing. Ultimately, the DOJ found the disclosure to be timely because, in part, the issues were not identified in the pre-acquisition diligence phase, the pandemic delayed efforts and the private equity firm disclosed the violations one month after finding the information. The private equity firm entered into a non-prosecution agreement (NPA) with the DOJ, having timely disclosed, cooperated with the DOJ's investigation and taken immediate steps to remediate.

See "White Deer Sanctions Settlement Underscores the Importance of Post-Acquisition Cleanup" (Jul. 30, 2025).

DOJ Main Justice

The DOJ Criminal Division's Corporate Whistleblower Awards Pilot Program (Pilot Program), introduced in August 2024, incentivizes individuals to provide actionable information concerning certain identified categories of criminal misconduct that, for the most part, were not previously covered by other existing federal whistleblower regimes.

Specifically, the misconduct must relate to:

1. certain crimes involving financial institutions, including money laundering schemes and non-compliance with financial regulations;
2. foreign corruption and bribery;
3. domestic corruption involving the payment of bribes or kickbacks to domestic officials;

4. healthcare fraud schemes;
5. fraud against the United States involving federally funded contracts or programs;
6. trade, tariff or customs violations;
7. federal immigration law violations; or
8. violations of sanctions or providing material support of terrorism or to cartels or transnational criminal organizations.

Designed to enhance the DOJ's ability to investigate corporate misconduct, the Pilot Program allows individuals who promptly and voluntarily provide the DOJ with original and truthful information concerning criminal misconduct related to any of the identified subject areas to be eligible for an award if the information leads to a conviction and results in forfeiture exceeding $1 million. However, the Pilot Program endeavors to bolster a company's internal reporting and investigations processes by factoring whether a whistleblower first pursued internal reporting mechanisms as consideration for increasing an award.

A key feature of the Pilot Program is its 120-day reporting window for both whistleblowers and companies, which aligns with the DOJ's recent amendments to the CEP. According to the CEP, when a company notifies the DOJ within 120 days of receiving an internal whistleblower report, fully cooperates with the DOJ's investigation and timely remediates, and where there are no other aggravating circumstances, that company now has a clear path to declination.

See this two-part series on the DOJ's Corporate Whistleblower Awards Pilot Program: "A Look at Forfeiture and Culpability" (Aug. 14, 2024), and "Exclusions, NDAs and Goals" (Sep. 11, 2024).

U.S. Attorneys' Offices

Since 2024, several U.S. Attorney's Offices (USAOs) have also launched their own whistleblower programs that provide the possibility of an NPA for individuals who come forward and self-disclose criminal misconduct. USAO whistleblower programs incentivize individuals who have participated in misconduct to voluntarily and timely report, cooperate with the government's investigation and meet certain other requirements by offering the possibility of an NPA.

The USAOs offering whistleblower programs include the Southern District of New York, Northern District of California, Central District of California, Southern District of Florida, District of New Jersey, Eastern District of Virginia, Northern District of Illinois, Southern District of Texas, Eastern District of New York, District of Columbia, District of Puerto Rico, District of Arizona and Western District of Virginia.

The type of criminal activity targeted by USAO whistleblower programs varies by office, but generally includes fraud or misconduct by companies and financial entities as well as bribery of federal, state or local officials.

See "Government Enforcers Explain Their Approach to Whistleblowers and VSD" (Jul. 17, 2024).

DOJ's Antitrust Division

In July 2025, the DOJ's Antitrust Division, together with the U.S. Postal Service (USPS) and USPS Office of Inspector General, announced the Antitrust Whistleblower Rewards Program (AWP), which encourages whistleblowers to report criminal antitrust violations that impact the USPS, including price-fixing, bid-rigging and market allocation schemes, by offering monetary rewards in qualifying cases. The USPS frequently assists with procurement fraud investigations that extend beyond its own procurement activity.

To be eligible for reward under the AWP, whistleblowers are required to voluntarily provide original information related to violations of Sections 1-3 of the Sherman Act, criminal acts to conceal violations of the Sherman Act, criminal conduct pertaining to procurement, and criminal conduct directed at or impacting federal competition investigations or proceedings. Whistleblowers who provide information that leads to criminal fines or recoveries exceeding $1 million are eligible to receive up to 30% of the resulting fine or penalty.

The Freepoint Whistleblower Suit

Former Freepoint senior analyst Andrew Martin filed a complaint in the New York State Supreme Court (Complaint), alleging that Freepoint employees engaged in market manipulation and retaliated against him for reporting the issues.

The Allegations

In the Complaint, Martin alleged that two Freepoint superiors urged and pressured him to conduct illegal insider trading by using proprietary information. Two senior executives attempted to maximize company profits by engaging in market manipulation schemes to acquire nonpublic information from producers and refiners of oil and gas, "pressur[ing] other Freepoint employees to steal and illegally disseminate proprietary copyrighted information," the Complaint alleges. It further indicates that these allegations occurred both before and after Freepoint entered into its DPA with the DOJ in December 2023.

Martin and others reported concerns about unethical conduct by these two executives through multiple internal channels, according to the Complaint. Martin advised colleagues to report misconduct to HR and compliance functions, and submitted what he believed was an anonymous note to the compliance team ahead of a DPA-related site visit. The Complaint describes a disturbing incident in which Martin witnessed one of the executives receiving a call related to a prior HR allegation and responding by shouting profanities and threatening to "kill" someone if they "ever came around again." Martin also escalated concerns to Freepoint's CEO via email and in one-on-one meetings, where Martin detailed a pattern of illegal conduct and retaliation. Despite receiving recent positive feedback and a significant raise and bonus, Martin's employment was terminated in November 2024, shortly before a scheduled visit to assess Freepoint's compliance with its DPA obligations.

Possible DPA Violations

Freepoint's DPA imposes strict obligations that go beyond general cooperation. Three requirements are particularly noteworthy.

First, under paragraph 20, Freepoint risks breaching the DPA if it "commits any felony under U.S. federal law." This provision underscores that any new criminal conduct – whether or not it is related to bribery – could trigger prosecution of the deferred charge.

Second, paragraph 6 requires Freepoint to promptly report to the DOJ any evidence or allegation of conduct that would violate the FCPA's anti-bribery provisions if it occurred within U.S. jurisdiction. This is a proactive disclosure duty, meaning the company cannot wait for confirmation of wrongdoing; even an allegation must be escalated to the DOJ's Fraud Section and USAOs.

Third – and most critical for the company's compliance infrastructure – Freepoint must maintain an effective internal reporting system that allows employees, officers and third parties to confidentially report suspected violations of anti-corruption laws or company policies. This system must not only exist on paper but function in practice. If an employee's attempt to report misconduct goes unanswered, the DOJ could view that as evidence the system is ineffective, putting Freepoint in breach of its DPA obligations.

How the DOJ Might Respond

Even if the misconduct falls outside the FCPA's anti-bribery provisions, the DOJ expects companies under DPAs to interpret reporting obligations broadly. Thus, the DOJ may be inclined to view the whistleblower suit with scrutiny given that the CFTC's resolution highlighted similar misconduct to the whistleblower allegations concerning the exchange of nonpublic information and insider trading activities.

Under such circumstances, companies should consider documenting a clear, defensible rationale for any decision not to disclose, noting that delay or failure to report could later be characterized as concealment.

Further, the whistleblower's assertion that internal reports were ignored – and that retaliation followed despite escalation to HR, compliance and the CEO – goes to the heart of whether Freepoint's reporting system is "effective," as required by the DPA. If the DOJ concludes the system failed in practice, it could determine that Freepoint has not met its compliance obligations, jeopardizing its ability to exit the DPA without prosecution.

Key Takeaways

A company's breach of its DPA could lead to significant consequences, including the risk of exposing it to further government scrutiny and investigation, extending the length of the DPA, and levying additional fines and penalties on the company. Further, while we may be seeing a shift away from

the imposition of compliance monitors, a DPA violation could be renewed grounds for requiring a compliance monitor, carrying hefty costs for the company, when reassessing risk of recurrence.

The Freepiont whistleblower suit offers some key takeaways for companies, particularly those that have inked DPAs with the DOJ and similar agreements with other enforcers.

Importance of Compliance Programs

While valuable for all companies, for those companies currently under a DPA, it is especially imperative to maintain heightened vigilance for any potential violations or misconduct, ensuring that the necessary steps are taken to remediate and disclose, as appropriate. This may involve, for instance, proactively maintaining open dialogue with prosecutors as well as considering regular compliance audits, frequent evaluation of compliance program effectiveness, and continued strengthening and review of internal reporting mechanisms, investigation protocols and whistleblower protections.

Overall, enforcement trends demonstrate that companies with strong compliance programs and effective whistleblower protections are better positioned to detect and prevent misconduct, thereby potentially avoiding high costs associated with government investigations, regulatory penalties and reputational damage. Further, the DOJ credits strong compliance programs when assessing penalties, often resulting in a more favorable resolution and meaningfully reduced fines.

Strengthen Internal Reporting and Investigating Systems

Companies should strive to create internal systems that detect and deter misconduct as well as encourage internal reporting and remediation of concerns. Companies would be well-advised to consider the following when establishing reporting processes and whistleblower protections. These steps help companies to swiftly and efficiently conduct internal investigations, make critical and timely determinations regarding voluntary disclosure, and effectively remediate.

1. Implement a robust, easily accessible reporting mechanism for employees and third parties, ensuring confidentiality and multiple avenues for escalation.
2. Develop and maintain written policies and procedures for investigating concerns, including timelines, documentation standards and escalation paths.
3. Conduct periodic audits and “mystery reporter” exercises to confirm that reporting systems function as intended and that reports are tracked and resolved.
4. Review recent investigations for timeliness, thoroughness and consistency; identify gaps; and implement corrective measures.
5. Update and communicate anti-retaliation policies, ensure disciplinary consequences for violations and provide clear protections for whistleblowers.

Ultimately, robust whistleblower programs are essential as retaliation allegations could compound underlying violations. Recent edits to the CEP have shifted the “presumption” of a declination to a “clear path to declination,” and companies may now be more inclined to report and voluntarily

self-disclose. Further, with the incentivizing of whistleblowers to come forward across various government agencies and whistleblower programs, companies must prepare for increased external reporting of both prospective and historical issues, as evidenced by the Freepoint whistleblower lawsuit. To that end, the arguably larger carrot of a "clear path to declination" should prompt companies to ensure their reporting, investigations and whistleblower protections programs are not only well-designed but also tested and effective in practice.

See this two-part series "The FCPA Lives": Targeting the TCO Ecosystem (Jul. 30, 2025), and Protecting American Interests (Aug. 13, 2025).

Luke Cass is a partner in Womble Bond Dickinson's Washington, D.C., office. A former federal prosecutor, he defends corporations and individuals from a variety of federal criminal allegations, including healthcare fraud, price-fixing, conspiracy, mail and wire fraud, embezzlement, bank fraud and money laundering. He also conducts proactive, corporate investigations related to bribery, misbranding, bid-rigging, drug diversion, the FCPA and the False Claims Act.

Audrey Karman is a senior counsel at Womble with extensive anti-corruption compliance experience, including designing, implementing, enhancing and testing global compliance programs; assisting clients with performing global risk assessments; and conducting anti-corruption diligence on high-risk third-party commercial partners and large M&A transactions. Her practice extends to guiding clients through remediation requirements and post-resolution compliance obligations, including corporate monitorships.

Ian O'Keefe is an associate at Womble, based in Raleigh, North Carolina. His practice focuses on complex litigation, government investigations and internal investigations, with particular experience in anti-corruption matters. Ian has significant experience evaluating and strengthening anti-corruption compliance programs, having served on the team of an independent compliance monitor appointed by the U.S. Department of Justice following a Foreign Corrupt Practices Act (FCPA) resolution, and later as part of the in-house compliance team of a company undergoing post-FCPA remediation.

The authors extend a special thanks to Ting-Yu Huang, a Womble staff attorney, for her research efforts in preparing this article.