PAUL HASTINGS

Stay Current

April 2024

Follow @Paul_Hastings

NDCA's New Whistleblower Pilot Program: A Unique Focus on Reporting Intellectual Property Theft

By Peter Axelrod, Kenneth Herzinger, Leo Tsao, Derek Wetmore, Natasha Nicholson Gaviria & Matthew Monforte

On March 18, 2024, Ismail Ramsey ("Ramsey"), the U.S. Attorney for the Northern District of California ("NDCA"), announced the launch of NDCA Whistleblower Pilot Program (the "Pilot Program"), a significant new policy that promises immunity from prosecution by the United States Attorney's Office ("USAO") for NDCA for certain individuals who voluntarily report corporate criminal misconduct.[1] The Pilot Program is similar to the whistleblower program announced by the USAO for the Southern District of New York ("SDNY") in January (described in an earlier alert). Ramsey said, "Our District's new Whistleblower Program creates a strong incentive for wrongdoers to come forward, report crimes, and cooperate with us in several critical areas—fraud, public corruption, and theft of trade secrets." The Pilot Program follows on the heels of the March 7, 2024 announcement by Deputy Attorney General Lisa Monaco that the Department of Justice ("DOJ") would launch a pilot program offering financial incentives for individual whistleblowers who report wrongdoing to the DOJ (discussed in an earlier alert). The DOJ's, NDCA's, and SDNY's new programs are all part of a harmonized effort by the DOJ to encourage reporting of corporate criminal misconduct. However, unlike the other two programs, NDCA's Pilot Program encourages reporting intellectual property ("IP") theft.[2] Given the DOJ's identification of IP theft as a national security matter, NDCA's jurisdiction over Silicon Valley and experience handling IP-related matters, and the Bay Area as a locus of activity related to artificial intelligence ("AI") technology, we can expect to see NDCA taking a leading role in investigating and prosecuting IP-related corporate misconduct.

As discussed below, companies should immediately consider certain proactive compliance steps to address—timely and appropriately—potential criminal conduct, and thereby reduce the risk of whistleblowing.

NDCA's Whistleblower Pilot Program

Under the Pilot Program, if an individual voluntarily discloses certain criminal misconduct to NDCA, and otherwise meets the specific criteria of the Pilot Program, then NDCA will offer the individual a form of immunity called a "non-prosecution agreement," or an "NPA."

There are three important limitations to NDCA's Pilot Program. First, it applies only to NDCA and not any other DOJ office, e.g., SDNY. Second, the Pilot Program does not apply to all crimes, although the

range of crimes it covers is broad. Third, the Pilot Program does not create any enforceable right. Thus, a whistleblower cannot legally challenge a refusal to grant an NPA.

Like SDNY's pilot program, NDCA's Pilot Program has three basic requirements. First, the disclosure must be both new and voluntary. Second, the reporting individual must provide full and substantial cooperation. Third, the reporting individual must not be from a disqualified category. For a more in-depth analysis of substantially similar requirements, refer to our client alert on SDNY's Whistleblower pilot program.[3]

A Potential Increase in Reporting and Prosecution of IP–Related Crimes

The Pilot Program seeks disclosures of corporate criminal misconduct involving "intellectual property theft and related violations." Considering the importance of IP located in Silicon Valley, recent high-profile NDCA matters, and the DOJ's focus on IP theft as a national security matter, there is good reason to believe NDCA will use the Pilot Program as a springboard to increase its investigations and prosecutions of IP-related crimes.

Recent High-Profile IP-Theft Crimes in NDCA

In 2018, the DOJ accused a Chinese state-owned company, Fujian Jinhua Integrated Circuit Co. Ltd. ("Fujian Jinhua"), of economic espionage and conspiracy after a U.S. chipmaker, Micron Technology Inc., brought the DOJ a laptop from a former employee who left to work with Fujian Jinhua's affiliate that allegedly showed evidence of the former employee downloading IP to steal trade secrets.[4] On March 3, 2024, in a blow to the DOJ, a federal judge ruled in a bench trial that the United States failed to meet its burden of proof and acquitted Fujian Jinhua.

On March 6, 2024, days before announcing NDCA's Pilot Program, Attorney General ("AG") Merrick Garland ("Garland") and Ramsey announced that a federal grand jury indicted Linwei Ding ("Ding") on four counts of theft of trade secrets relating to an alleged plan to steal AI technology from Google LLC ("Google").[5] Ding is accused of downloading over 500 confidential files from Google while covertly working for overseas-based companies.

The DOJ's Statements Calling IP Theft an Issue of National Security

In announcing the indictment of Ding, AG Garland said, "[t]he Justice Department will not tolerate the theft of artificial intelligence and other advanced technologies that could put our national security at risk."[6] Deputy Attorney General Lisa Monaco added, "The Justice Department will relentlessly pursue and hold accountable those who would siphon disruptive technologies—especially AI—for unlawful export."[7] During a March 6, 2024 panel before the American Bar Association's 39th Annual National Institute on White Collar Crime, Ramsey said Silicon Valley is the most defining aspect of NDCA and that he purposely reorganized his office to focus on securing and protecting the nation's IP and most sensitive secrets.[8]

NDCA's Pilot Program Viewed in Context

IP theft has become a growing concern among members of the U.S. Government, Silicon Valley tech companies, and companies in general. As the Fujian Jinhua case shows, it is often hard for prosecutors to meet evidentiary requirements to sustain convictions. The Pilot Program's emphasis on IP theft suggests NDCA is attempting to both discourage IP-theft crimes and provide additional sources of evidence. Coupled with recent DOJ statements emphasizing IP theft as an issue of national security and Ramsey reorganizing his office to focus on protecting Silicon Valley, NDCA may soon become the

frontrunner in the DOJ's response to international IP-related crimes and IP-related crimes in general. As such, the Pilot Program may be a valuable tool for prosecutors.

Unresolved Conflicts Between NDCA and Other United States Attorney's Offices

With SDNY launching a similar pilot program this January, questions may arise about potential competition between offices. Both NDCA's and SDNY's policies say the NDAs will be between the reporting individual and the specific office. Thus, it seems, NDCA could enter into an NDA with a reporting individual, but SDNY could still bring charges against that person or vice versa. Time will tell if that will be the case, but potential whistleblowers might refrain from reporting criminal misconduct for fear of not being granted an NDA that applies to all DOJ entities.

What Should Companies Do—Key Takeaways

It is too early to know how many whistleblower reports will be generated by the Pilot Program. But if the Pilot Program comes anywhere close to matching the success of previous DOJ policies—such as a similar immunity program from 1994—the Pilot Program might lead to significantly more prosecutions and investigations. Time will also tell if the Pilot Program's emphasis on IP theft deters IP-related crimes.

Companies should immediately consider the risks associated with increased detection opportunities for NDCA. Given the emphasis on IP theft, Silicon Valley-based companies and technology companies in general should ensure they have appropriate measures in place to protect their IP and a vigorous reporting process for employees to report any concerns. Companies should consider the following actions:

- Companies should ensure that their ethics and compliance policies and programs contain provisions for reporting IP misconduct.
- Companies should review their policies, procedures, and protocols to ensure employees and other agents have clear and accessible communication channels to report misconduct.
- Companies should ensure they take swift and appropriate action to investigate reports, with escalation where appropriate. Such measures may dissuade whistleblowers from escalation outside of the company.
- Companies should ensure that employment agreements forbid transferring company data to personal devices, or if data must be transferred to personal devices, ensure there are means of controlling and tracking such transfers.
- Where companies do detect serious misconduct that may be criminal, companies should work with counsel to consider whether a voluntary self-disclosure is appropriate.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

New York

Peter B. Axelrod
1.212.318.6067
peteraxelrod@paulhastings.com

Natasha Nicholson Gaviria
1.212.318.6675
natashanicholsongaviria@paulhastings.com

San Francisco

Kenneth P. Herzinger
1.415.856.7040
kennethherzinger@paulhastings.com

Derek Evan Wetmore
1.415.856.7034
derekwetmore@paulhastings.com

San Francisco

Matt Monforte
1.415.856.7094
mattmonforte@paulhastings.com

Washington D.C.

Leo Tsao
1.202.551.1910
leotsao@paulhastings.com

[1] Press Release, U.S. Atty's Off., N. Dist. of Cal., U.S. Attorney Ismail Ramsey Announces Policies Underlying Whistleblower Pilot Program (Mar. 18, 2024), https://www.justice.gov/usao-ndca/pr/us-attorney-ismail-ramsey-announces-policies-underlying-whistleblower-pilot-program.

[2] *See SDNY Whistleblower Pilot Program*, U.S. Atty's Off., S. Dist. of N.Y. (Jan. 10, 2024), https://www.justice.gov/d9/2024-01/sdny_wbp_1.9.24.pdf; *see also* our Client Alert, "SDNY's New Policy on Self-Disclosures for Individuals May Be a Game Changer," dated Jan. 18, 2024, *available* at https://www.paulhastings.com/insights/client-alerts/sdnys-new-policy-on-self-disclosures-for-individuals-may-be-a-game-changer.

[3] *See* our Client Alert, "SDNY's New Policy on Self-Disclosures for Individuals May Be a Game Changer," dated Jan. 18, 2024, *available at* https://www.paulhastings.com/insights/client-alerts/sdnys-new-policy-on-self-disclosures-for-individuals-may-be-a-game-changer.

[4] Aruna Viswanatha & Heather Somerville, *U.S. Defeat in Micron Trade-Secrets Case Reveals Struggle Countering Beijing*, Wall Street J. (Mar. 3, 2024), https://www.wsj.com/tech/micron-chipmaker-ip-theft-trial-verdict-6f839f15.

[5] Press Release, U.S. Atty's Off. Pub. Affairs, Chinese National Residing in California Arrested for Theft of Artificial Intelligence-Related Trade Secrets from Google (Mar. 6, 2024), https://www.justice.gov/opa/pr/chinese-national-residing-california-arrested-theft-artificial-intelligence-related-trade.

[6] *Id*.

[7] *Id*.

[8] Video, U.S. Atty's Off. Pub. Affairs, Enforcers and Regulators Panel at the ABA's 39th Annual National Institute on White Collar Crime (Mar. 6, 2024) (Ramsey speaking at 22:40), https://www.justice.gov/opa/video/enforcers-and-regulators-panel-abas-39th-annual-national-institute-white-collar-crime.