ALM | LAW.COM

THE RECORDER

'Get Out of Jail' for NorCal Trade Secret Violators Who Blow the Whistle

By Peter Kirwan
July 18, 2024

It is no secret that Silicon Valley is ground zero for the development and advancement of intellectual property that technology companies rely upon to stay ahead of their competition. Recently, the intellectual property landscape in Silicon Valley underwent a shift that could change the way technology companies manage and protect their intellectual property. A pilot program in the Northern District of California will now seek to track down and prosecute corporate malfeasance by foregoing prosecution of whistleblowers who voluntarily come forward and disclose criminal conduct even though these individuals may themselves have unclean hands.

The Whistleblower Pilot Program (WPP), which took effect March 14, dangles non-prosecution agreements (NPAs) in front of individuals whose information and assistance can help the government identify and prosecute criminal conduct in a range of areas, including "intellectual property theft and related violations."

Theft of intellectual property is no longer just the concern of the companies that developed and own it. The government has recognized that theft of certain intellectual property can implicate national security concerns should it end up in the wrong hands; it too has a vested interest in protecting such property from theft.

Courtesy photo

Hon. Peter Kirwan (Ret.) of Signature Resolution.

The new WPP is likely to increase the reporting of corporate criminal conduct by individuals involved in intellectual property theft while raising the bar for businesses concerned about protecting their trade secrets.

Trade Secrets

Trade secrets are the secret sauce that separates businesses from their competitors. Processes, formulas, customer lists, and other unique assets derive value from the fact that they are secret. Patents may grant a government-sanctioned monopoly, but they require public disclosure and have a limited life. Trade secrets, in contrast, provide potentially unending protection but require unending efforts by businesses to monitor, police and shield them from disclosure.

Once the barn door has been thrown open, the horses are gone. No amount of punishment or penalty can restore the owner of a divulged trade secret to their prior position. Can there ever be a good outcome to disclosure?

Defend Trade Secrets Act

In fact, the law recognizes that good reasons may exist for employees and other insiders to share trade secrets with third parties. The Defend Trade Secrets Act (DTSA, 18 U.S.C. Section 1833), enacted in 2016, protects from criminal and civil liability individuals who disclose trade secrets for non-nefarious reasons. The government, in its discretion, may grant a discloser immunity if certain preconditions are met.

To qualify for immunity, the disclosure must be made "in confidence to a federal, state or local government official, either directly or indirectly, or to an attorney" and must be "solely for the purpose of reporting or investigating a suspected violation of law" or "made in a complaint or other document filed in a lawsuit or other proceeding, if such filing is made under seal." Someone who files a lawsuit for the purpose of reporting a suspected violation may disclose a trade secret to their attorney and may use trade secret information in a court proceeding as long as any documents containing the trade secret are under seal and the trade secret is disclosed under a court order.

What happens, however, when the discloser actually participated in misappropriating or otherwise violating the trade secret? Like a fifth column, such a scofflaw could end up being useful to prosecutors seeking to ferret out bad corporate actions. He or she may be able to name names and lift the curtain on possible criminal conduct at the corporate level. Granting immunity could net the government much bigger fish.

Whistleblower Pilot

This seems to be the thinking behind the WPP, created by the U.S. Attorney's Office (USAO) for the Northern District of California and applicable only to that region. Designed to "encourage early voluntary self-disclosure of criminal conduct and to promote effective enforcement of criminal laws," the WPP rewards individuals who took and divulged corporate trade secrets, as long as certain conditions are met.

That the WPP was adopted for the northern part of the state is significant. Silicon Valley is home to the largest collection of technology companies in the world. With intellectual property whose value beggars the imagination, it is a hotbed of trade secret theft and litigation. If the WPP yields good results, it may be replicated in other districts within the state.

The idea of NPAs for whistleblowers is, however, not unique to the Northern District of California. The Criminal Division of the U.S. Department of Justice announced a program, effective April 15, that will extend NPAs to corporate executives who share information about potential criminal conduct in which they were involved.

To be eligible for an NPA under the WPP, the whistleblower must share information not already public or known by authorities, and the disclosure must be voluntary. The whistleblower must cooperate fully with the USAO, testifying under oath if necessary, and the target of the investigation must be equally or more culpable than the whistleblower.

The whistleblower seeking an NPA cannot be an elected official, the head of a public agency, a member of law enforcement, or a top-level corporate executive, and all whistleblowers must disclose prior criminal conduct in which they were involved. They must also agree to forfeit any proceeds involved in their criminal misconduct.

Impact on Trade Secret Owners

Intellectual property theft happens all the time; the WPP is unlikely to change the rate of its occurrence. But because the program provides wrongdoers with a means of evading liability for their own criminal activity, it creates an incentive for those who misappropriate trade secrets to become whistleblowers about corporate misdeeds.

Like a "get out of jail" card, the prospect of an NPA could motivate individuals who have absconded with trade secrets to implicate the owners of those trade secrets in their own misconduct. When trade secrets are easy to obtain and disclose, the risk of such exposure is high.

Trade secret owners should therefore be reviewing and revamping their protection and compliance programs. They should increase audits of intellectual property; regularly train and supervise employees and contractors; properly label, store and safeguard trade secrets; and maintain and enforce nondisclosure agreements.

With heightened risk posed by the WPP, the standard for what constitutes "reasonable" efforts to maintain and protect trade secrets could become much higher than in the past. Potential immunity for whistleblowers should motivate companies to create a culture that encourages and rewards reporting while responding timely and effectively to reports of wrongdoing.

Civil Liability

The DTSA imparts both criminal and civil immunity upon defendants who disclose trade secrets to the government for specified purposes. It is an affirmative defense to be established by defendants at trial. (See *Knox Trailers v. Maples*, 581 F. Supp. 3d 1000, 1016 (E.D. Tenn. 2022).)

The DTSA does not, however, protect individuals who have wrongfully acquired trade secrets or who use them against their owner. It states as follows: "Except as expressly provided for under this subsection, nothing in this subsection shall be construed to authorize, or limit liability for, an act that is otherwise prohibited by law, such as the unlawful access

of material by unauthorized means." (See *FirstEnergy v. Pircio*, 524 F. Supp. 3d 732, 741 (N.D. Ohio 2021).)

The WPP likewise extends protection from criminal prosecution to individuals who disclose trade secrets, even when done for personal gain, as long as they help the government go after trade secret owners. It does not deal with civil liability.

Could blowing the whistle lower the risk of civil liability for those who misappropriated trade secrets? Why would an individual choose to cooperate with the government if he or she continued to face civil exposure? In fact, by coming forward and cooperating with investigators that individual will likely have placed themselves directly in the crosshairs of a lawsuit by the trade secret owner.

Only time will tell whether wrongdoers are willing to assume this level of risk. If their misdeeds would have been discovered anyway, it may make perfect sense for them to limit the damage by at least knocking away potential criminal liability.

Ultimately, the question of immunity from civil charges may redound to the DTSA and require a fact-based analysis. At the discretion of the USAO, the WPP may provide a clean criminal slate to trade secret offenders, but it will not, by itself, bar trade secret owners from seeking monetary redress for their loss.

When trade secrets have been misappropriated, the harm suffered by a business could be incalculable. Even for a company engaged in improper, unethical or criminal activity, the nexus between that activity and misappropriated trade secrets may be nebulous or nonexistent.

Conclusion

The Northern District pilot program is in its infancy stage, and many eyes will be watching. Ultimately, only time will tell as to how the WPP impacts the way companies internally manage and protect their intellectual property, as well as whether the program motivates whistleblowers with unclean hands to come forward, even in the absence of civil immunity.

Peter Kirwan *is a neutral with Signature Resolution, recently retired from the Santa Clara County Superior Court. He served in the court's civil division for 14 years, presiding over numerous class action lawsuits, trade secret litigation, business disputes, PAGA and employment litigation, groundwater rights lawsuits, and a variety of other complex matters.*