Motorola Wins Massive $407M Award in International Trade Secrets Dispute: 10 Tips for Employers to Protect Your Data

Insights
7.23.24

A federal appeals court recently applied a U.S. trade secrets law to sales outside the country, finding that Motorola was entitled to $407 million in damages from a foreign competitor for trade secrets misappropriation. A China-based company admitted to poaching key engineers who stole trade secrets and used them to develop a line of two-way radios identical to Motorola's products. The 7th U.S. Circuit Court of Appeals concluded that Motorola was entitled to recover the competitor's foreign profits from the misappropriation under the Defend Trade Secrets Act (DTSA). While the ruling is good news for global businesses seeking damages in such situations, it also comes with a few cautions. Here are the key takeaways and 10 tips for employers to protect your trade secrets and other confidential information.

What Happened?

These are the key facts, as described by the 7th Circuit:

- Motorola and China-based Hytera Communications are the two main competitors in the global market to design, manufacture, and sell two-way radios and related products.
- Hytera poached three Motorola engineers in Malaysia, and at least one of them initially remained on Motorola's payroll while secretly working for Hytera.
- The secret employee downloaded Motorola documents in response to specific requests from Hytera about unresolved issues with its own radios.
- Segments of stolen code were directly inserted into Hytera's products, which was proven through minor coding errors in Motorola's code that appeared in exactly the same spots in Hytera's code.
- The employees knew their conduct was unlawful.
- Hytera admitted that it engaged in "the blatant theft of trade secrets and copying of proprietary computer code," according to the 7th Circuit. "Hytera raises several challenges only to the damages awards under the Copyright Act and the DTSA." We'll just be focusing on the DTSA damages award in this Insight.

Does the Trade Secrets Law Apply Extraterritorially?

- The DTSA is subject to a general presumption that U.S. law does not apply to conduct occurring outside the U.S.
- To defeat this presumption, courts will look at whether the specific statute "gives a clear, affirmative indication that it applies extraterritorially."
- Two decades before the DTSA was enacted, the Economic Espionage Act of 1996 added a chapter to the United States Code making the theft of trade secrets a federal crime in many situations. It included the following language: "This chapter also applies to conduct occurring outside the United States if … an act in furtherance of the offense was committed in the United States."
- Then, the DTSA, which took effect in May 2016, amended that chapter, creating a private right of action and adding a definition of "misappropriation."
- The district court found that the EEA's language on extraterritorial application included the DTSA amendments. Because "Congress was not acting to change an existing interpretation of the EEA, but rather was creating a private right of action in the statutory chapter," the district court concluded that "the chapter amended through the DTSA should be read as a cohesive whole."
- The 7th Circuit agreed with the district court and also found that Hytera's misappropriation fell within the limits on extraterritoriality.
- The appeals court also agreed that an "offense" could mean either criminal or civil violations, so the extraterritorial provisions apply to civil claims like this one.

What Does the Ruling Mean for Businesses?

- For businesses with an international workforce, this is likely a welcome development. The DTSA provides robust protections for employers, and now there is strong precedent for the application of the DTSA to punish foreign acts.
- However, the ruling can be used as both a sword and a shield. U.S.-based businesses should expect that their own international employees will be required to comply with the DTSA. A foreign company may file suit in the U.S. for violation of the DTSA, even if the alleged misconduct occurred in another country.
- It is worth noting, however, even when your business wins a judgment against a foreign entity, enforcement is extremely tricky (if not impossible) against foreign parties without assets in the U.S. This is especially true for parties located in countries like China and Russia where relations with the U.S. are strained. The Hague Convention provides a global legal framework for cross-border enforcement, but in practice, any successful enforcement depends heavily on the willingness and cooperation of the local courts. Therefore, it's always better to prevent wrongdoing than to remedy it.

10 Tips for Employers to Protect Your Confidential Information

The 7th Circuit called the conduct in this case "a large and blatant theft of trade secrets," which

serves as a reminder to employers to be proactive in protecting your confidential information. Consider taking these 10 steps to strengthen your practices:

1. **Review your current policies and contracts** that prohibit the unauthorized acquisition, use, or disclosure of confidential information to ensure they are sufficiently robust but also legally enforceable. All employees with access to confidential information should be required to sign a non-disclosure agreement.
2. **Implement or update policies governing the use of personal devices or accounts**, such as smartphones, external drives, or cloud-storage accounts, that could be used to store, download, or transfer confidential company information.
3. **Assess your physical security measures** that restrict access to facilities and areas where confidential information is used and stored.
4. **Provide training** to all employees that reinforces relevant policies and procedures and explains the disciplinary consequences for their violation.
5. Ensure all employees with computer access are provided with **unique passwords** (that are regularly changed).
6. Ensure access to confidential and proprietary information is limited to **a need-to-know basis**.
7. **Utilize data loss prevention software** to detect and promptly investigate suspicious employee computer activity.
8. **Retain and image company-issued devices** of departing employees when there is a reasonable suspicion that trade secret misappropriation has occurred.
9. **Remind departing employees of their obligations.** You should also consider adopting contractual provisions and policies that require departing employees to immediately return company property, allow an inspection of personal devices used for work, and participate in an exit interview.
10. **Work with your counsel to develop a strategy and action plan** so you are ready to respond if you discover trade secret misappropriation or a breach of your restrictive covenants. Depending on the urgency and severity of the situation, your plan for how to respond could include seeking an *ex parte* temporary restraining order or civil seizure order under the DTSA.

Conclusion

We will continue to monitor the latest developments and provide updates as warranted, so you should ensure you are subscribed to Fisher Phillips' Insight System to gather the most up-to-date information directly to your inbox. If you have questions, please contact the authors of this Insight, your Fisher Phillips attorney, or any attorney in our International or Employee Defection and Trade Secrets Practice Group or our Crisis Communications and Strategy Team.

Related People

Nazanin Afshar
Partner
818.230.4259
Email

Jonathan Crook
Partner
704.334.9313
Email

Nan Sato, CIPP/E, CIPP/C
Partner
610.230.2148
Email

Service Focus

Employee Defection and Trade Secrets

International

Crisis Communications and Strategy