Trade Secret Quarterly

January 2024

Your Information May Be Valuable … But That May Not Be Enough

A recent decision by the Fourth Circuit highlights the fact that a plaintiff in a trade secret action must prove that its information is not just commercially valuable, but that the commercial value is based upon the fact that it is secret.

The case involved two competitors in the business of identifying vulnerabilities in source code for open-source software so that those vulnerabilities can be corrected. The plaintiff spent years identifying and disclosing open-source-code vulnerabilities. In 2011, it acquired a database of vulnerabilities and invested heavily in expanding its content then licensed the updated database to its competitors and others.

The defendant, through a subsidiary, was one of the plaintiff's licensees. While the license agreement was in place, the subsidiary created a database that also managed and stored information about open-source-code vulnerabilities. The defendant found out, revoked the license agreement and sued.

The district court granted the defendant's motion for summary judgment. The key issue in the case was whether the plaintiff demonstrated that its alleged trade secrets derived any value from being kept secret. The plaintiff asserted two theories on the value of the information. First, it pointed to the price that an acquirer had recently paid for the company. Second, it relied upon the fact that most of its revenue (at least 90%) came from licensing its database of vulnerabilities.

In granting the defendant's motion, the district court held that the plaintiff did not show that its trade secrets derived value from being kept secret. The Fourth Circuit agreed, finding that while the plaintiff's evidence may have showed commercial value, it could not prevail because it did not show that any of that value was tied to the secrecy of the information.

This case serves as a reminder to plaintiffs in trade secret cases that the value of a trade secret must be derived from the information's secrecy and not merely because the trade secret has some commercial value. As the Fourth Circuit noted, "Not everything with commercial value constitutes a trade secret."

Beware of How You Share

There are many times that a company may need to disclose trade secret information with third-party business partners, such as for sales or development purposes. But the fact that there is a legitimate reason to disclose the information does not mean the disclosure is without risk. This is underscored by a recent decision by the Sixth Circuit.

In the case, the plaintiff had shared trade secret information regarding a potential new financial product with an unrelated party, an insurance carrier. The plaintiff had asked the insurance company to sign a nondisclosure agreement as part of the pitch, but it refused to do so. Two of the insurance company's employees later joined the defendant, another insurance carrier, and the plaintiff learned that the defendant was marketing what the plaintiff called an eerily similar product. The plaintiff filed suit for misappropriation of trade secrets.

The district court, however, granted summary judgment to the defendant, holding that the plaintiff did not show misappropriation because it had shared the information in a relationship that was not confidential. The Sixth Circuit agreed, finding that the unrelated insurance company had not entered into a confidential relationship with the plaintiff when the alleged trade secret information was shared. To the contrary, the insurance company had explicitly rejected signing an NDA. The information was shared without establishing a confidential relationship, and its trade secret status was destroyed.

This case is a harsh reminder that companies must always insist on enforceable agreements to protect their sensitive information before sharing it with even their most trusted business partners.

New Year, New Review

Trade secret cases in the last few years have highlighted an increased focus on how companies identify their trade secrets and what measures are implemented to protect them. Once an ex-employee steals trade secrets, it is too late to correct those issues. Companies are well served to conduct an annual audit of trade secret protections, including how trade secrets are identified, what agreements are in place to protect them, what procedures are in place to protect them, and what protocols are implemented to assess a trade secret threat when a key employee leaves the organization. Thompson Hine can provide a comprehensive trade secret audit to bolster those policies and procedures, mitigate the risk of trade secret theft, and prosecute instances of theft.

The FTC Noncompete Ban: Is It or Isn't It?

A year ago, the Federal Trade Commission (FTC) published a proposed rule that would create a federal nationwide prohibition on noncompete employment agreements. The public comment period for the proposed rule closed on March 20, 2023, and commentators expected a final rule shortly following that deadline. However, after a robust public comment period and spirited public debate, the FTC tabled its decision on a final rule and is now expected to take a vote on a final rule this April. The FTC had sought comments on such alternatives as permitting the use of noncompetes for key employees or employees above a certain salary threshold. Whatever rule comes out is expected to face immediate legal challenges.

FOR MORE INFORMATION

For more information, please contact:

Deborah S. Brenneman
513.352.6638
Deborah.Brenneman@ThompsonHine.com

Debbie represents management in all areas of employment law, with a focus on trade secret and non-compete cases. She has a wealth of experience in successfully litigating and resolving these matters in state and federal courts across the country.