LAW360

Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

2nd Circ. Ruling Highlights Risks In Trade Secret Licenses

By **Jill McWhirter, Kevin Duffy and Zev Beeber** (May 5, 2022, 5:55 PM EDT)

Jill McWhirter

Kevin Duffy

Zev Beeber

Owners of intellectual property often monetize the fruits of their innovative labors by licensing out their confidential know-how or trade secrets. Whether the trade secret remains a trade secret during the license depends, in part, on the licensee taking reasonable measures to keep it secret from third parties.

But what happens when the licensee is not explicitly obligated to do so? The U.S. Court of Appeals for the Second Circuit recently issued its decision on that question in Turret Labs USA Inc. v. CargoSprint LLC.[1]

The case is a cautionary tale for licensors and licensees of trade secrets. It illustrates how an IP asset holder, despite having taken certain measures to limit third-party access, can still become subject to the loss of a precious trade secret — and marketplace advantage. Both licensors and licensees should prepare for critical changes to the contractual landscape in response.

Background

Plaintiff Turret Labs is the proprietor of a logistics-management software program called Dock EnRoll, which facilitates the ground handling control of air cargo. Dock EnRoll's trade secret lies in its functionality. The first program of its kind, it allows for the payment of fees and scheduling of shipments based on synchronized real-time U.S. Customs release notifications.

In 2008, Turret Labs entered into a licensing agreement with Deutsche Lufthansa AG's Lufthansa Cargo Americas for the use of Dock EnRoll. The agreement contemplated that Lufthansa would have exclusive authority to extend program access to third parties. Such third parties included, but were not limited to, freight forwarders, or entities that arrange for the storage and shipping of merchandise on behalf of shippers.

Enter defendant CargoSprint LLC, which accessed Dock EnRoll vis-à-vis the licensing agreement with Lufthansa. Upon gaining access, CargoSprint allegedly reverse engineered Dock EnRoll to create its own competing program. Turret Labs sued CargoSprint under Section 1836(b) of the Defend Trade Secrets Act of 2016 and common law misappropriation of a trade secret.

The Court's Ruling

Affirming the dismissal by the U.S. District Court for the Eastern District of New York, the Second Circuit rejected Turret Labs' claims of trade secret misappropriation.

Despite having implemented certain restrictions on user access to Dock EnRoll's servers, the court determined that these fell short of "reasonable measures" to keep Turret Labs' valuable information secret, a threshold issue for alleging misappropriation under the DTSA and common law.

The court came to this decision based on deficiencies in the licensing agreement, namely that neither Lufthansa nor its third-party freight forwarders were under any specific contractual obligation to Turret Labs to maintain the confidentiality of Dock EnRoll.

Absent such obligations, Turret Labs failed to take reasonable measures to maintain confidentiality of Dock EnRoll's functionality, and so Dock Enroll did not qualify for trade secret protection. Accordingly, the Second Circuit refused to find CargoSprint's allegedly unscrupulous and "unfettered access" to Dock EnRoll a misappropriation of a trade secret.

A Warning for Intellectual Property Licensors and Licensees

Turret Labs is a critical case for trade secret licensors, offering guidance on what constitutes reasonable measures of trade secret protection. Licensees, in turn, should anticipate new postures in contract negotiations. Key takeaways and considerations include the following:

Understand Who Needs Access

Licensee disclosure of confidential know-how to third parties does not necessarily spoil overwise valid trade secret protection. So long as the information was provided in conjunction with restrictions on the third party mandating confidentiality, the trade secret may remain intact.

Trade secret licensors must therefore ask the threshold question: Who requires access? Although the named licensee may hold the license to the trade secret, the intended end user is often the representatives, affiliates or third parties of the licensee.

Confidentiality provisions must extend to such other parties via the primary licensing agreement to hedge against trade secret loss.

Here, Turret Labs produced Dock EnRoll for freight forwarders, yet the licensing agreement granted Lufthansa unlimited authority to extend access to third parties. By first identifying the universe of parties permitted access to the licensed trade secret, the licensor can then work diligently to circumscribe information flow beyond the identified set, ensuring greater trade secret protection.

Licensees face a new contracting environment, in which licensors urgently seek to define end-user access as rigorously as possible. In turn, licensees must ensure that they receive the breadth of license required for their business objectives.

Following the same process described above, licensees should identify third parties at the outset of the license relationship and secure their access upfront when negotiating the licensing agreement.

Require Obligations to Licensor

The licensed trade secret tautologically originates from the licensor. It follows that whoever is granted access — both the licensee and third parties alike—should be contractually obligated to the licensor to maintain the information's secrecy. Absent explicit obligations, the receiving party is under no obligation to maintain secrecy, and trade secret protection ceases.

Turret Labs cautions that a licensor cannot expect to secure end-user confidentiality with general understandings of their IP constituting confidential or proprietary information. Nor can the licensor rely on the licensee's internal guidelines obligating third parties to secrecy.

Although Turret Labs expected Lufthansa to restrict third-party access to legitimate freight forwarders bound by confidentiality agreements, the Dock EnRoll licensing agreement did not explicitly condition disclosure based on these criteria.

Licensors must take reasonable measures to maintain the secrecy of their trade secret, and this duty extends to all those who receive the trade secret. Licensors can bolster the asset's secrecy by defining the confidentiality obligations of each recipient of the asset.

Licensees may be resistant to new and nonstandard confidentiality obligations. They can reduce this potential burden by establishing a uniform third-party confidentiality provision for use across their licensing agreements.

By doing so, licensees can ensure that their third-party partners are comfortable with the applicable confidentiality language, while building a means to counteract licensors proposing unique or complex confidentiality provisions.

Not Just Any Reasonable Measures

While the licensor is obligated to take reasonable measures to maintain secrecy, not just any measures will suffice. Whether the measures are reasonable will depend on their nexus with the nature or type of the trade secret itself.

In Turret Labs, the alleged trade secret consisted entirely of Dock EnRoll's functionality, which became obvious upon use. Turret Labs could have protected Dock EnRoll's functionality as a trade secret, in part, by requiring end users maintain its functionality in confidence.

However, Turret Labs took other protective measures, such as physical barricades enclosing the servers. The district court responded that Turret Labs seemingly "locked all the upstairs windows of [their] house, while remaining silent on whether the front and back doors were left opened."[2]

Turret Labs' control of their physical servers was not a reasonable measure to ensure the secrecy of its program's functionality. Licensors of similar assets, in which the trade secret is as intangible and vulnerable as program functionality, must employ context-appropriate protections, including confidentiality provisions on the use of the software itself.

Licensees can support their licensors through this process by surveying the applicable industry standards. Armed with this information, licensees can both suggest best practices and mitigate the risk of agreeing to nonstandard measures.

Tighten Up the Terms

The Second Circuit indicated that tighter license contractual provisions could have resulted in a different outcome. As a baseline, the licensor and licensee must have a common understanding of confidentiality when agreeing to the provision of the trade secret information.

Further, third parties should receive the information on an explicit, common understanding of confidentiality, and downstream users' obligations should arise from a contractual duty owed to the licensor.

In practice, the licensor may consider prescribing the disclosure of confidential information to the licensee and a limited group of third parties, where applicable. The license can be conditioned on the licensee agreeing to disclose confidential information:

- Only to the limited group of third parties, and
- Only to the extent that the limited group is subject to confidentiality obligations that are no less restrictive than the license.

The license may include additional terms that define the rights and obligations of the licensee, which the licensor and licensee must negotiate. For example, to promote compliance, the license can be further conditioned on the licensee assuming liability for any breach of confidentiality by the end users.

Alternatively, licensees may insist on a disclaimer of liability for third-party end users' copying the functional ideas of the trade secret. Parties must assess the impact of specific contract terms and consult with knowledgeable advisors.

Conclusion

Turret Labs is consistent with recent decisions of other U.S. circuit courts, including the U.S. Courts of Appeals for the Eighth Circuit[3] and the Ninth Circuit.[4]

Although Turret Labs focuses on the importance of confidentiality provisions in license agreements, licensors and licensees face an open question regarding how best to protect their trade secrets while maintaining practicable third-party access.

Jill A. McWhirter is a partner, Kevin J. Duffy is a senior associate and Zev G. Beeber is an associate at King & Spalding LLP.

[1] No. 21-952, 2022 U.S. App. LEXIS 6070, 2022 WL 701161 (2d Cir. 2022).

[2] Turret Labs USA, Inc. v. CargoSprint, LLC, No. 19-CV-6793, 2021 U.S. Dist. LEXIS 27838, 2021 WL 535217, at *17 (E.D.N.Y. Feb. 12, 2021).

[3] See Farmers Edge Inc. v. Farmobile, LLC, 970 F.3d 1027 (8th Cir. 2020).

[4] See InteliClear, LLC v. ETC Glob. Holdings, Inc., 978 F.3d 653 (9th Cir. 2020).