Insights

INSIGHT: Stolen Info Is Not Trade Secret If It Can Be Reverse Engineered

Posted:

A recent court decision offers an important lesson for companies considering bringing a trade secret claim: before filing suit, companies should ensure that their confidential information—even if it was stolen by the defendant—is actually a trade secret.

Joshua Fowkes
Arent Fox

Jake Christensen
Arent Fox LLP

A recent court decision offers an important lesson for companies considering bringing a trade secret claim: before filing suit, companies should ensure that their confidential information—even if it was stolen by the defendant—is actually a trade secret. Although a plaintiff whose confidential information was stolen can establish some required elements of a trade secret claim (and tell a powerful story), the plaintiff must also establish that its confidential information is an actionable trade secret. Determining whether the confidential information is a trade secret turns in part on whether the information could be ascertained by proper means. That analysis includes considering whether *any* member of the public—not just the *particular defendant* that may have admitted to misappropriating the information—could ascertain it. The Nevada Supreme Court recently addressed that important distinction and emphasized that a company that admitted that it stole information from its rival had not stolen a trade secret because the information could be ascertained by the public through reverse

engineering. MEI-GSR Holdings, LLC v. Peppermill Casinos, Inc. (Nev. 5/3/18)2018 BL 158574.

The Case

In *Peppermill*, an employee of Peppermill Casino visited the rival Grand Sierra Resort and Casino to determine the "par value" of Grand Sierra's slot machines. A slot machine's par value measures the amount that the machine keeps for the house and the amount that it pays out to players. A Peppermill employee used a manufacturer's key without authorization to open Grand Sierra's machines and learn their par values. Grand Sierra caught Peppermill's employee in the act and reported Peppermill and its employee to the Nevada Gaming Control Board. The Board found that the Peppermill employee improperly accessed Grand Sierra's machines to learn their par values and that Peppermill executives had condoned the employee's misconduct at Grand Sierra and other casinos for several years. Peppermill later stipulated to a $1 million fine imposed by the Board.

Later, Grand Sierra sued Peppermill and its employee in Nevada state court, alleging that Peppermill had violated Nevada's Trade Secrets Act ("NTSA"). But at trial, multiple expert witnesses testified that members of the public could learn a slot machine's par value by using permissible methods that did not involve opening the machine. These methods included using reverse engineering, which involves starting with a known, honestly obtained product and working backward to determine the method by which it was developed.

At trial, Grand Sierra proposed a jury instruction that focused the definition of a trade secret on the *means* by

which the defendant actually ascertains the information and stated that resorting to immoral means (such as theft) to obtain the information meant that the information was not reasonably ascertainable:

"A trade secret is not readily ascertainable when the means of acquiring the information falls below the generally accepted standards of commercial morality and reasonable conduct .... Even if the information which is asserted to be a trade secret could have been duplicated by other proper means, the information is not readily ascertainable if in fact it was acquired by improper means."

Peppermill Casinos, Inc., 2018 WL 2090872, at *1. But the court rejected Grand Sierra's proposed instruction, instead instructing the jury that "'[i]f the information is in fact obtained through reverse engineering ... the actor is not subject to liability, because the information has not been acquired improperly' and (2) '[a] trade secret may not be readily ascertainable by proper means,'" which includes reverse engineering.

The jury returned a verdict in Peppermill's favor, finding that the par values that Peppermill stole were not trade secrets because Grand Sierra failed to prove that the par values could not be ascertained by proper means. In the jury's view, even if Peppermill learned the par values by theft or other improper means, a member of the public could reverse engineer the par values by openly observing the machines and tracking the money put into the machines by, and paid out to, players. As a result, they found that Grand Sierra's par values were not trade secrets.

The Nevada Supreme Court agreed. It noted that Grand Sierra's proposed jury instruction was improper because it contravened the NTSA's definition of a trade secret as "not being readily ascertainable by proper means by the public or other persons … ."

Lessons Learned

Companies considering initiating trade secret litigation must carefully assess whether their confidential information is a trade secret at all. Many state trade secret statutes define a trade secret as information that derives independent value from "not being readily ascertainable by proper means by the public or any other persons who can obtain commercial or economic value from its disclosure or use." Grand Sierra focused on the strong evidence of Peppermill's theft of its par values, but overlooked whether the public could learn its par values by proper means like reverse engineering. For the jury and the Nevada Supreme Court, it did not matter that the Peppermill employee used improper means to obtain Grand Sierra's par value information; rather, it mattered that *any member of the public* could use *proper* means to obtain it.

Josh focuses on complex commercial litigation, particularly contract actions, fraud, breach of fiduciary duties and other business torts, intra-company disputes, trade secret cases, and derivative and class action claims.

Jake's practice focuses on complex litigation matters, including commercial contract disputes, healthcare fraud, patent litigation, commercial payer disputes, and OFAC sanctions and AML compliance.