Acquiring trade secrets through web-scraping: Is it misappropriation?

By R. Mark Halligan, Esq., FisherBroyles LLP

SEPTEMBER 23, 2024

The issue in *Compulife Software, Inc. v. Newman*, No. 21-14074 (11th Cir. Aug. 1, 2024) was whether "scraping" a public website can constitute trade secret misappropriation.

The answer is yes.

Factual background

Compulife Software, Inc. generates life insurance quotes on the Internet. One product it sold was an Internet-quote engine called the "web quoter." The web-quoter allowed licensees to embed a feature on the licensees' own website that connects with Compulife's database server. Prospective life-insurance purchasers visiting one of the licensed websites could then enter their demographic information and receive a responsive quote retrieved from Compulife's proprietary database.

The issue on appeal was whether there was misappropriation of the trade secret by defendants using web-scraping to acquire the Compulife insurance data on a public website and a publicly web-accessible database.

Compulife also maintains a website at www.term4sale.com that allows visitors to obtain life insurance quotes at no cost. Term4Sale.com generates life insurance quotes using Compulife's web-based HTML code, host-based software, and a database of information.

The defendants were direct competitors, involved in the identical business of generating life-insurance quotes through their own website called the "Life Insurance Quote Engine." The defendants obtained life insurance data from web-scraping the Compulife website.

The Compulife insurance data was a trade secret. The issue on appeal was whether there was misappropriation of the trade secret by defendants using web-scraping to acquire the Compulife insurance data on a public website and a publicly web-accessible database.

Misappropriation by acquisition occurs when a person acquires a trade secret and knows or has reason to know that it was acquired by *improper means*. Id. Misappropriation by use occurs when a person uses a trade secret without consent and either: (1) used *improper means* to acquire the trade secret; (2) at the time of use knew or had reason to know that it was (a) derived from a person who used *improper means*, (b) acquired in a manner giving rise to a duty to maintain secrecy, or (c) derived from a person who owed a duty to maintain secrecy to the owner; or (3) before a material change in his position, knew or had reason to know that it was a trade secret and had been acquired by accident or mistake.

Scraping a public website is now a regular business practice. It involves using bots or web crawlers to automatically access and extract data from websites. The data is then exported into a format that is more useful such as a spreadsheet or API. Unlike screen scraping, which only copies pixels displayed onscreen, web scraping extracts underlying HTML code and data that can be used to replicate an entire website content elsewhere.

Proper means/improper means

Acquisition of a trade secret by "proper means" does not constitute trade secret misappropriation.

Acquisition of a trade secret by "improper means" constitutes trade secret misappropriation.

"Proper means" includes:

(1) Discovery by independent invention;

(2) Discovery by "reverse engineering",

(3) Discovery under a license from the owner of the trade secret;

(4) Observation of the item in public use or on public display;

(5) Obtaining the trade secret from published literature.

"Improper Means" includes:

(1) Theft,

(2) Bribery,

(3) Misrepresentation,

(4) Breach or inducement of a breach of a duty to maintain secrecy,

(5) Espionage through electronic or other means.

'Christopher v. DuPont'

Improper means can also include otherwise lawful conduct which is improper under the circumstances. The most famous example is *E. I. du Pont de Nemours & Co., Inc. v. Christopher*, 431 F.2d 1012 (CA5, 1970), cert. den. 400 U.S. 1024 (1970).

The 11th Circuit agreed with the lower court's ruling that the defendants were liable for trade secret misappropriation because they had used "improper means" to acquire Compulife's trade secrets.

An airplane — in public airspace — took aerial photographs of a competitor's plant layout during construction of the plant. The Christophers argued that their actions were lawful in a public airspace, and they did not violate any government aviation standard, did not breach any confidential relationship, and did not engage in any fraudulent or illegal conduct. Under these circumstances, defendants argued there was no misappropriation of a trade secret.

The 5th U.S. Circuit Court of Appeals disagreed. The Court held that "improper means" includes not only illegal acts such as theft, but also fraudulent misrepresentations to induce disclosure, tapping of telephone wires, eavesdropping or other espionage. "Our tolerance of the espionage game must cease when the protections required to prevent another's spying cost so much that the spirit of inventiveness is dampened."

Citing the *Christopher* case, the 11th U.S. Circuit Court of Appeals compared the deceptive behavior of the defendants in *Compulife* to the "surreptitious aerial photography" in *Christopher*.

Conclusion

The district court found that the defendants stole from 3 million to 43.5 million insurance quotes. The evidence established that Compulife's revenue declined after the scraping attack, that it lost business it otherwise expected to receive, that the number of customers looking for free trials declined, that the number of free trials that converted to four-month subscriptions declined, and that the number of four-month subscriptions that converted to annual subscriptions declined. Further, quotes generated from Compulife's software continued to appear on the defendants' website.

The 11th Circuit agreed with the lower court's ruling that the defendants were liable for trade secret misappropriation because they had used "improper means" to acquire Compulife's trade secrets.

The district court entered judgment for Compulife for $184,225.87 in compensatory damages and $368,451.74 in punitive damages.

R. Mark Halligan is a regular contributing columnist on trade secrets law for Reuters Legal News and Westlaw Today.

About the author

R. Mark Halligan is a partner at **FisherBroyles LLP** and is based in Chicago. He focuses his practice on intellectual property litigation and is recognized as a leading practitioner in the development of automated trade secret asset management blockchain systems. He teaches advanced trade secrets law in the LLM program at University of Illinois Chicago School of Law and is the lead author of the "Defend Trade Secrets Act Handbook," 3rd Edition, published by Wolters Kluwer. He can be reached at rmark.halligan@fisherbroyles.com.

This article was first published on Reuters Legal News and Westlaw Today on September 23, 2024.