

Florida's Fourth District Gives Protection to an Obvious Secret

May 29, 2020

In *Mapei Corp. and Southeastern Printing Co. v. J.M. Field Marketing Inc.*, Florida's Fourth District Court of Appeal addressed trade secret issues in a dispute among a construction product company (Mapei), its former fulfillment and marketing firm (JM), and Mapei's new construction marketing firm (Southeastern).

The case raises interesting issues of when information that is obvious and known can still find trade secret protection because how the information interacts with other information is a secret. It is also a cautionary tale of why it is critical to closely review the details of confidentiality agreements to clearly identify what categories of information qualify for protection, and, in the event of a business divorce, who has rights to do what with categories of information housed within an electronic system.

For many years, JM provided web-based management and marketing services to Mapei through a proprietary platform called AIV. JM developed specialized aspects of the platform tailored to Mapei's specific needs. The parties' agreements included commitments that Mapei would use the same level of confidentiality for JM's AIV system as it uses for its own confidential business information. In those same agreements, Mapei agreed to prohibit access to the AIV system, except under a non-disclosure agreement, approved by JM, for those individuals and third parties with a need to know the information.

After Mapei terminated its relationship with JM, JM discovered that Mapei employees had scraped data from the AIV system. It also discovered evidence suggesting that login and access credentials to the AIV system had been shared with Mapei's new vendor, Southeastern, which is JM's competitor. JM learned that Southeastern was offering a system to Mapei that mimicked the functions of the AIV system and providing similar AIV services at a lower price. JM sued for violations of the Florida Uniform Trade Secrets Act, among other claims, and sought emergency injunctive relief against Mapei and Southeastern.

The trial court granted JM an injunction against Mapei's access and use of the AIV system. It granted a limited injunction against Southeastern prohibiting it from disclosing, aiding and abetting, or encouraging the use of the misappropriated data. However, the court denied an injunction prohibiting Southeastern from using the data for its own benefit. Mapei appealed the injunction. JM cross-appealed the trial court's denial of the complete injunctive relief it sought against Southeastern.

The Fourth District affirmed the trial court's injunction against Mapei but reversed the denial of complete relief against Southeastern. In doing so, the Fourth District addressed several issues of interest to those practicing trade secret law in Florida.

First, the court rejected the assertion that the description of the AIV system was too vague to qualify as a trade secret. JM had placed into evidence a 51-page screen capture that showed the various components of the system and how they were integrated. The court concluded that such evidence satisfied the Restatement definition of a trade secret where some or all of the components may be known, but how the secret nature of their arrangement creates a competitive advantage.

Second, the court rejected the argument that the components of the AIV system did not constitute trade secrets because they were simply a representation of Mapei's own data used to populate the system. The court concluded that even though Mapei's data was part of the system, the back end of the system, and how the data worked together, was not readily ascertainable to unauthorized users of the system.

Third, the court rejected the argument that the injunction should fail because there was no direct proof of misappropriation. The court noted that in most trade secret cases only circumstantial proof of misappropriation exists. Indeed, it is the rare case that has a smoking gun. Here, JM provided evidence showing the login credentials were shared to allow unauthorized users access to the system. That was sufficient to satisfy the misappropriation prong.

Fourth, the court rejected the argument that the trial court was wrong to rely on the presumption of irreparable harm provided by the statute. It further noted that beyond the mere presumption, there was evidence of harm shown by the fact that the misappropriated information was provided to JM's competitor — Southeastern. Citing its precedent in *Hatfield v. AutoNation, Inc.*, 939 So. 2d 155 (Fla. 4th DCA 2006), the court said that the fact that one can only speculate as to the potential harm of the information being disseminated demonstrates the irreparable harm.

Fifth, the court concluded that the trial court should have extended the injunction to Southeastern to prohibit the competitor from actually using the trade secret information that it should not have received.

This decision highlights risks in a situation that is all too common in a cloud-based economy. Many businesses use third-party cloud-based services to automate business processes from marketing to human resources to manufacturing and beyond. Often this involves a vendor customizing an off-the-shelf system or framework to meet the specific needs of the customer. Problems often arise, however, when the customer later wants to use another vendor or internal system for a similar service. The internal developers or new vendor will need to implement very similar customizations, and often the easiest way to accomplish that is to show the new vendor or developers the old system. If not done carefully, however, that disclosure can be a violation of confidentiality terms in the original agreement, particularly where the new vendor is a competitor of the prior vendor. Businesses are well advised, therefore, to consider transition processes carefully when negotiating services agreements. Understanding how transition will be accomplished, what can and cannot be shown to future developers, and obtaining assurances that business processes, system customizations, and outputs can be replicated freely can help avoid expensive litigation and maintain flexibility.

There are a few takeaways here. Even if components of a trade secret may be open and obvious, aspects not visible to the naked eye can still find protection. It is not a secret that a spreadsheet has data in it. Indeed, the data may be well known. But if you do not know how the cells link together to produce an output, therein a trade secret may lie. Closely study the definitions of what qualifies as a trade secret or confidential information, and what rights and restrictions apply to that information if the parties go their separate ways. And, finally, even with a favorable injunctive order, it may be worthwhile to file an appeal or cross-appeal of the denial of full relief.

Authored By



[Kevin P. McCoy](#)



[William Giltinan](#)

Related Practices

[Appellate & Trial Support](#)

[Intellectual Property](#)

[Litigation and Trials](#)

[Trade Secrets / Noncompete Litigation and Consulting](#)

©2024 Carlton Fields, P.A. Carlton Fields practices law in California through Carlton Fields, LLP. Carlton Fields publications should not be construed as legal advice on any specific facts or circumstances. The contents are intended for general information and educational purposes only, and should not be relied on as if it were advice about a particular fact situation. The distribution of this publication is not intended to create, and receipt of it does not constitute, an attorney-client relationship with Carlton Fields. This publication may not be quoted or referred to in any other publication or proceeding without the prior written consent of the firm, to be given or withheld at our discretion. To request reprint permission for any of our publications, please use our Contact Us form via the link below. The views set forth herein are the personal views of the author and do not necessarily reflect those of the firm. This site may contain hypertext links to information created and maintained by other entities. Carlton Fields does not control or guarantee the accuracy or completeness of this outside information, nor is the inclusion of a link to be intended as an endorsement of those outside sites.