Westlaw Journal
GOVERNMENT CONTRACT
Litigation News and Analysis • Legislation • Regulation • Expert Commentary
VOLUME 29, ISSUE 23 / MARCH 14, 2016

EXPERT ANALYSIS

A Government Contractor Wins $20 Million And Sanctions in a Trade Secrets Case: What It Means for You

By Douglas Mishkin, Esq., and Douglas Proxmire, Esq.
Venable LLP

Put yourself in our client's shoes. Your vice president of business development resigns — and the next thing you know, a new business opportunity that would have been yours inexplicably goes to a competitor. Inexplicably, that is, until you learn that the competitor is working with your former vice president in violation of his noncompetition agreement — and is using your trade secrets.

When this happened to our client, we sued the competitor and won a judgment for $20 million plus sanctions consisting of attorney fees and expenses. We proved that the former employee stole a recent successful government contract proposal, statements of work and pricing information (among thousands of stolen files) and gave them to the competitor. The competitor copied them (typos and all) into a proposal that the former vice president helped to prepare. The competitor then submitted the proposal to the U.S. government, knowing that our client's trade secrets would position it to receive the contract award.

The resultant 42-day bench trial was full of issues that every employer, and particularly every government contractor, should learn from to protect their interests and their trade secrets. We will highlight three of those issues here.

METADATA IS META-IMPORTANT

Trade secret cases are largely about unwinding who had what documents, when they had them, who they gave them to, how they were manipulated and what they did with them. No victim of a theft of trade secrets can begin to address these questions without understanding metadata. Metadata can be understood as pieces of information that describe an electronic file. This type of data may reveal who authored a file and when the file was created, opened, edited or printed.

In our case, the defense hinged largely upon one document created in Microsoft Word, which we will call the "sham document," that the competitor claimed exonerated it from misappropriating our client's trade secrets.

The competitor and the former vice president tried to convince the court that the sham document was a proposal the defendant was preparing to submit to a foreign government before the U.S. government contracting opportunity was publicly advertised. The existence of the sham document at the time of the events in question supposedly showed that the competitor was not misappropriating the trade secrets to steal a U.S. government contracting opportunity from our client but rather was engaged in preparing an innocent proposal seeking an opportunity that our client had no plans to pursue.

Metadata proved the sham document was, well, a sham. In fact, the defendant created the sham document only after the litigation began to cover up its misappropriation of our client's trade secrets. How did we prove that?

First, the sham document's metadata contained a "temporal anomaly." This means the metadata revealed a sequence of events that simply could not have happened in that sequence. Specifically, the metadata contained a "last saved date" (the date the document was last saved) that was earlier than the "last printed date" (the date and time the document was last printed).

Experts for both sides agreed that this constituted a temporal anomaly because the last saved date must be on or after the last printed date when Microsoft Word prints a document. The defendant's own computer forensics expert went on to testify that the anomaly "can be indicative of backdating" that can occur "where the system clock associated with the computer is for some reason set to the wrong date, whether it's intentional or not. And then there are tools that are specifically designed for modification of metadata dates."

Second, the sham document bore a "file system created date" on the defendant's server that far postdated the underlying events at issue in the lawsuit and the commencement of the litigation. A file system created date is the date and time the item was created on the file system where it is located. The file system created date was compelling evidence establishing that the defendant was not working on the sham document when it said it was (i.e., the innocent explanation), but instead created the document after it had been sued for misappropriation.

Finally, we used metadata to prove that the defendant had manipulated other files to attempt to raise defenses to our trade secret claims. Litigation-related documents that the defendant received in late September bore "last written dates" in August. These documents included emails that were contained in an .OLM file. The designation OLM file is associated with Microsoft Outlook for Mac; this type of file stores email messages and other data saved by the application from an exchange server.

Odd though it may seem, a collection of information from public sources can constitute a trade secret.

In our case, post-August emails contained in an OLM file had a "last written date" in August, but again the computer forensics experts for both sides agreed that this was impossible. Two of the defendant's own computer forensics experts conceded that these anomalies suggested that someone had used some kind of software to backdate these files. One testified at trial that "a tool could have been used to change these [last written dates] so that they were, you know, screwy."

Our computer forensics expert testified, "You can set those dates to anything you want. Once you're using tools, all bets are off. You can make the dates dance and sing any way you want."

The judge noted all of this evidence in concluding that the sham document was a fraud. In addition to assessing $20 million in compensatory and exemplary (punitive) damages against the defendant, the judge said the company's law firm should have known from the metadata that the sham document defense was a fraud. As a result, the judge imposed a portion of our client's attorney fees and expenses as sanctions against the law firm for continuing to assert the defense despite the metadata that disproved the authenticity of the sham document.

COMPILATIONS OF PUBLIC INFORMATION MAY BE PROTECTABLE

Odd though it may seem, a collection of information from public sources can constitute a trade secret. Under the Uniform Trade Secrets Act, a "compilation" of information may be a trade secret as long as it:

- Derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use.
- Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

Businesses frequently invest considerable resources in compiling and combining public and proprietary information for all kinds of purposes, such as to enhance marketing campaigns, to respond to requests for proposals for contracts and to improve corporate performance. Any particular piece of that publicly available information is not a trade secret. But when efforts to find, organize and present the information create a work product that provides a competitive advantage and is not easily ascertainable, the end result may well be a trade secret.

In our case, the defendant tried to justify its misappropriation of our client's government contract proposal by saying that it was simply a collection of publicly available information — and thus was not a trade secret. Through the testimony of those who crafted the proposal, we persuaded the judge that the misappropriated material represented six years of our client's effort in developing, improving and refining its proposed product to meet an ongoing need.

Drafting the proposal required finding and reviewing massive amounts of publicly available information, making judgment calls about what information to use, and then distilling that information into proposal-appropriate tidbits that communicated the end product that our client offered. The judge found that our client's investment in compiling this information "provided the company with the competitive advantage necessary for trade secret protection."

PRESERVING DOCUMENTS AND DEVICES IS ESSENTIAL

The judge awarded our client millions of dollars in punitive damages against the defendant and millions of dollars in attorney fees as sanctions against that company and its law firm. Some of the most egregious sanctionable conduct included:

Any particular piece of publicly available information is not a trade secret.

- The defendant "scrubbed" its server and key computers during the trial, shortly before these devices were to be imaged (i.e., forensically copied). The defendant used two evidence deletion tools that not only delete files but also delete evidence that the files have been deleted. The judge wrote that "[t]he court has rarely, if ever in a civil matter, witnessed a party engage in such flagrant misconduct and act with such complete disregard for the truth and such profound disrespect for the law."
- The defendant's law firm mishandled various pieces of electronic evidence. The firm could not identify what laptop, hard drive or thumb drive it received from its client, or when. The firm also opened certain electronic files, thereby altering their all-important metadata, and in so doing erased evidence.
- The defendant's law firm failed to disclose that it had certain pieces of electronic evidence in its possession.
- The defendant repeatedly failed to produce documents in its possession and repeatedly misrepresented to the court that no such documents existed.

CONCLUSION

Employers understandably fear the prospect of seeing their most valuable assets — personnel and intellectual property — march out the door. Prudent employers can address that fear by understanding issues like these, by training their employees as to their obligations and by working with counsel who can guide them through these crises.

Douglas Mishkin is a partner at **Venable LLP** in Washington, where he handles a variety of matters on behalf of government contractors, to whom the misappropriation of trade secrets and intellectual property assets is of significant concern. He has litigated for and advised contractor clients about issues relating to the spoliation of evidence by former employees and misuse of metadata by departing staff. He can be reached at dmishkin@venable.com. **Douglas Proxmire** is a partner in **Venable LLP**'s government contracts group in Tysons Corner, Virginia, and Washington. He advises clients on government and construction contract formation and dispute resolution. He can be reached at dcproxmire@venable.com.