

## **HNRK OBTAINS FIRST SEIZURE ORDER UNDER THE DEFEND TRADE SECRETS ACT**

Until passage of the federal Defend Trade Secrets Act (the “DTSA”), previously discussed in this blog, employers had limited access to the federal courts when their trade secrets were misappropriated. We pointed out that the DTSA allows employers to file a civil suit in federal court for theft of trade secrets and obtain injunctive relief against the misuse of those secrets as well as damages and attorneys’ fees. In extraordinary circumstances, the DTSA allows for the *ex-parte* seizure of trade secrets by law enforcement to prevent their propagation or dissemination.

Our article proved most prescient for in late July 2016, we were called by a NYC real estate finance company that suspected that an employee had misappropriated its trade secrets. We confirmed those suspicions via forensic examination and soon thereafter obtained the very *first* DTSA *ex-parte* seizure order in the US in the United States District Court for the Southern District of New York. (*Mission Capital Advisors LLC v. Romaka*, Case No. 16 civ. 5878 (LLS)).

### **The Facts**

The employee in the case, Romaka, a debt and equity finance specialist, was accused of downloading confidential company files including contacts and deal documents. Originally cooperative, Romaka allowed a forensic examination of his personal desktop. That review revealed that he had downloaded a multitude of company files. Thereafter the employee, who lived in Manhattan, went to ground, thus thwarting Mission’s efforts to obtain the return of the misappropriated data. Mission Capital, Romaka’s employer, needing to protect the integrity of its trade secrets, quickly filed a complaint in the Southern District seeking both an injunction against disclosure and seizure under the DTSA.

The case was tailor-made for the DTSA because its facts satisfied the statute’s elements. The misappropriated information constituted trade secrets, the defendant had wrongfully taken and downloaded the material by improper means through electronic espionage, and the employer had suffered economic loss as a result. As a result the court granted the employer emergency *ex-parte* relief.<sup>1</sup> After a temporary restraining order hearing, the court granted Mission injunctive relief (barring Romaka from accessing, disclosing, copying or otherwise conveying plaintiff’s

---

<sup>1</sup> Of course, that took some lawyering for this was the first time the court was faced with an action under the brand new DTSA and there was absolutely no precedent. Knowing this, and to make the court’s job easier, we were sure to bring with us copies of the statute and the Congressional Bill Report (No. 114-529, 114<sup>th</sup> Congress, 2d Sess) to distribute to the judge and his law clerks.

contact list) which, given his disappearance, was served on him via email. When Romaka did not acknowledge service or the TRO, and subsequently failed to respond to us or appear in court on the TRO hearing date, thereby ignoring the court's directive that he appear, the matter became ripe for seizure so as to protect disclosure or misuse of Mission's trade secrets.

We demonstrated to the court that any form of equitable relief other than seizure would be inadequate because Romaka's own actions showed that he was likely to misuse the purloined data and would evade, avoid or otherwise not comply with the court's directive, and that Mission was at risk of immediate and irreparable injury should the misappropriated materials be disseminated. While the court was concerned about protecting Romaka's privacy and the integrity of Romaka's non-Mission related computer content, we addressed those concerns, identifying with specifics the exact computer files that needed to be seized, their location, and a reasonable method for seizure. As a result the court issued a seizure order directing the US Marshals Service to "as soon as possible" seize "i.e., copy onto a storage medium and delete the file on Defendant's computer..."

On August 4, 2016, five days after the Seizure Order and three days after the court approved a computer expert, the defendant was woken in his apartment by three US Marshals in bulletproof vests. The "seizure" took almost all day as appropriate files were copied and then deleted from the employee's computer. But that did not end the matter because the DTSA requires the court to hold a post-seizure hearing to give the defendant an opportunity to further challenge, modify or dissolve the seizure. Again, neither Romaka, nor a lawyer acting on his behalf, attended the hearing so the Order remained in place.

## **Conclusion**

The DTSA gave the employer in this case a new forum and set of tools to obtain the return of misappropriated trade secrets. The court and the Marshals Service moved quickly to establish protocols intended to give effect to the statute and at the same time protect the interests of the defendant employee. To maximize the chances that an employer will prevail in a DTSA action our experience in *Romaka* suggests that a party seeking DTSA injunctive relief that may result in seizure be armed with the following:

1. Evidence of misappropriation or misuse of trade secrets.
2. An improper taking of those trade secrets.
3. Proof that what was taken is indeed a trade secret.
4. Evidence that a defendant, absent seizure, is likely to misuse or propagate the seized material or will evade the court. E.g.: defendant intends to leave the country or sell or disclose the misappropriated material.
5. The ability to identify with specificity what is to be seized.

6. The location of misappropriated material.
7. Ability to post a bond.
8. Ability to pay the Marshals' fee.
9. The identity of an expert who may need to accompany the Marshals.
10. Information that will be helpful to the Marshals about the nature and location of the property to be seized and the plaintiffs who may be in possession of the misappropriated material.