Bryan Benard

Partner
801.799.5833
Salt Lake City
bbenard@hollandhart.com

Utah Supreme Court: Misappropriation of Trade Secrets Presumes Irreparable Harm

Publication — September 3, 2015

A Utah employer has dodged a $229,482 fee award and can continue its lawsuit against a former employee for misappropriation of company trade secrets and violation of a non-disclosure agreement. The Utah Supreme Court recently revived InnoSys, Inc.'s claims against a former engineer, Amanda Mercer, holding that the company established a prima facie case of trade secret misappropriation that gave rise to a rebuttable presumption of irreparable harm. The divided Court reversed the grant of Mercer's summary judgment motion, allowing the company to take its claims to trial. *InnoSys, Inc. v. Mercer*, 2015 UT 80.

Employee Copied Sensitive Company Information to Thumb Drive and Personal Email Account

During her employment as an engineer for InnoSys, Mercer forwarded confidential company emails to her personal Gmail account. On the day that she was terminated for poor performance, Mercer copied the company's confidential business plan onto a thumb drive.

Following her termination, Mercer filed a claim for unemployment benefits with the Utah Department of Workforce Services. After her claim was denied, she appealed, submitting a number of protected documents, including the confidential business plan and protected emails, into the administrative record. At that point, InnoSys began asking for details as to when and how she gained access to the confidential materials. Mercer then deleted all of the emails and InnoSys files. InnoSys filed a complaint in court, alleging that Mercer had breached her non-disclosure agreement (NDA), misappropriated company trade secrets in violation of the Uniform Trade Secrets Act (UTSA), and breached her fiduciary duty to the company.

Employee Changed Her Story But Still Won Judgment From Lower Court

Throughout discovery, Mercer changed her story regarding the use of her Gmail account and the timing of her acquisition of the company's confidential business plan. Despite first claiming that she had IT's permission to transfer company emails to her personal Gmail account, Mercer later admitted that she did not have anyone's permission to do so. As to the business plan, Mercer initially testified in her deposition that she had copied the business plan onto a thumb drive because she had been asked to review the plan the day before her termination and was unable to access it via the company's secure remote network. She later admitted that she copied it on the day of her termination and did not have it in her possession the day before she was fired.

Despite Mercer's inconsistent statements regarding how she obtained the company's confidential information, the district court ruled in Mercer's favor on all of InnoSys's claims. It did so after concluding that “there was no objectively reasonable basis to believe that Mercer had harmed InnoSys or was threatening to do so.” In addition to dismissing all of InnoSys's claims against Mercer, the lower court also granted Mercer's motion for sanctions against InnoSys and to collect attorneys' fees as the prevailing party. The court ordered InnoSys to pay Mercer $229,481.58. InnoSys appealed.

Evidence of Harm

At the crux of the appeal was whether InnoSys needed to provide sufficient evidence of harm or threatened harm as a result of Mercer's misappropriation and/or disclosure of company trade secrets to avoid summary judgment and proceed to trial. The lower court had found that InnoSys had not presented sufficient evidence that it had actually been harmed by Mercer's admitted taking and disclosure of confidential company information and, therefore, could not support its claims.

The Utah Supreme Court disagreed, holding that where a company establishes a prima facie case of misappropriation of trade secrets under the UTSA, it is entitled to a presumption of irreparable harm. The court held InnoSys was not required to produce evidence of financial damages as it also sought an injunction to prevent Mercer from further disclosing or using its confidential information.

The presumption of irreparable harm, as well as affirmative evidence of threatened harm, was also enough to keep alive the company's claim for breach of the NDA. By reversing the grant of summary judgment in Mercer's favor, the Court overturned the award of sanctions and attorneys' fees against InnoSys.

Lessons Learned

First, put procedures in place to retain all signed employee agreements and documents. InnoSys initially could not find the NDA that Mercer had signed when her employment began. The lower court was hard on the company for that failure and did not want to accept a copy of its standard NDA as evidence of what Mercer signed. The company eventually found the NDA signed by Mercer but the turmoil caused by its absence highlights the importance of strict record keeping for important employee agreements. Be certain to keep your signed agreements and acknowledgments in a secure location. You never know when you might need to enforce them.

Second, when employment ends for any reason, take steps to ensure that the departing employee returns all company information and property without retaining any copies. It is unclear from the opinion whether InnoSys asked Mercer for the return of any company materials when she was fired, but it appears that it learned she had confidential company information after she submitted the company documents as part of her unemployment appeal. Don't wait until after there has been a disclosure or further misappropriation; instead, proactively cut off access to company materials

and seek the return of all company property. Also, remind departing employees of their continued obligations under confidentiality policies and NDAs.

Finally, enforce your NDAs to ensure continued protection of your company trade secrets and other proprietary information. Allowing a former employee to retain or disclose confidential information will undermine your future chances of arguing that such information is indeed a trade secret. You must continually guard that information or it will lose its protected status.