A Cautionary Tale: Don’t Wait Until There Is A Problem To Protect Your Trade Secrets

Thursday, May 2, 2019

A federal decision recently reminded businesses about the importance of taking appropriate measures to protect their proprietary information before any misappropriation occurs. In *Abrasic 90 Inc. v. Weldcote Medals, Inc.*\(^{[1]}\), the court denied the plaintiff’s motion for a preliminary injunction “largely because [the plaintiff] did not protect its supposedly secret information.” The court’s order underscores that businesses may be unable to enforce as a trade secret their valuable information unless they have taken adequate steps to protect its secrecy.

In that case, a manufacturer of grinding and sanding disks sought to enjoin its former employees and their new employer from operating in the abrasives industry and from using its trade secrets. The defendants took information about the plaintiff’s pricing, customers and suppliers when they left the company to start a competing business. Yet, the court declined to issue an injunction on the ground that Abrasic had failed to protect its supposedly trade secret information.

The court explained that there are two basic elements to the analysis: (1) the information must have been “sufficiently secret to impart economic value because of its relative secrecy” and (2) the plaintiff must have made “reasonable efforts to maintain the secrecy of the information.” The court concluded that the plaintiff failed to establish the second element because it “did virtually nothing to protect that information to preserve its status as a trade secret.”

The court criticized “[the plaintiff’s] almost total failure to adopt even fundamental and routine safeguards for the information at issue[,]” pointing to the following conduct by the plaintiff:

- Failing to confine access to the alleged trade secret information to those who had a need to access it (aka “need to know” access).
- Permitting employees to access the confidential information without requiring them to sign non-disclosure agreements (NDAs).
- Using employment policies that do not require employees to maintain the confidentiality of the company’s confidential information after the employment ends.
- At termination of employment, failing to ask the employee if she possesses any of the company’s confidential information and failing to ask the employee to delete or return it.
- Failing to admonish employees at termination of an on-going obligation to protect the company’s confidential information.
- Using confidentiality employment policies that are vague and do not give employees sufficient guidance about what information they are to treat as confidential to the company.
- Doing nothing to train or educate employees about their obligations to protect the company’s confidential information.

---

*Sheppard Mullin, Richter & Hampton LLP*  
*Intellectual Property Law Blog*  
*Corporate & Business Organizations*  
*Intellectual Property*  
*Litigation / Trial Practice*  
*7th Circuit (incl. bankruptcy)*
• Failing to require suppliers and distributors who had access to the information to execute NDAs.
• Failing to password-protect and encrypt the company’s trade secrets.
• Permitting employees unfettered ability to download, save elsewhere (e.g., a USB drive), print, and email files containing the company’s confidential information.
• Allowing employees to share passwords.
• Failing to label “proprietary” or “confidential” documents or files containing the company’s confidential information.
• Disclosing publicly supposedly confidential information.
• Using an IT Manager who has no training in data security or is otherwise unqualified.
• Not implementing security measure recommendations of its IT Manager, such as requiring employees to remove company data from their personal devices when their employment ends.
• Taking no measures to protect supposedly confidential information that are different than measures taken to protect non-confidential information.

There is no single set of protection measures that automatically qualifies as reasonable efforts. What are reasonable efforts depends on the circumstances, such as the nature of the information to be protected. For example, reasonable measures to protect a trade secret recipe may not be appropriate to protect trade secret customer pricing terms. Other circumstances affecting reasonableness may include the trade secret holder’s sophistication, size and resources. A “mom and pop” operation likely would not be held to the same standard as a Fortune 500 company. As a business grows and become more sophisticated and its trade secrets change, it should periodically revisit its protection measures to attempt to ensure that they are appropriate and commensurate to those taken by businesses in similar circumstances.

We stand ready to assist you to identify and implement measures that are reasonable to protect the confidentiality of your business’ trade secrets. Not only should such measures reduce the risk that your trade secrets will be misappropriated, but also they should put your business in a better position if it needs to litigate against a competitor which has misappropriated or threatens to misappropriate your trade secrets.


Copyright © 2019, Sheppard Mullin Richter & Hampton LLP.

Source URL: https://www.natlawreview.com/article/cautionary-tale-don-t-wait-until-there-problem-to-protect-your-trade-secrets