3 Ways to Protect Your Trade Secrets

Published: April 2018

By: Noah Webster, ACCDocket.com, Litigation Columnist, and General Counsel for Mobility Solutions at BlackBerry, and Brian Bianco, partner in the Intellectual Property Group of Akerman LLP

Original content: http://www.acc.com/docket/articles/ip-law-3-ways-to-protect-your-trade-secrets.cfm

150-Character summary: Avoid losing control of your confidential information with the IRAC - Issue, Rule, Application, and Conclusion - method.

Article:

The scale of the Waymo v. Uber trade secrets case surprised me: An employee took 14,000 documents containing sensitive data resulting in a US$1.859 billion claim and a settlement of around US$245 million. Waymo claimed it had instituted sufficient security precautions to protect trade secrets, such as encryption, security cameras, and confidentiality agreements.

But a competitor potentially obtained access to Waymo’s information and, to protect its rights, Waymo had to explain in court how the measures it had taken were reasonable under the Defend Trade Secrets Act (DTSA). The situation highlights the need for in-house counsel to re-examine the trade secrets policy that protects their own company’s innovation.

To get a refresher on the basics of trade secrets, I consulted my law school classmate Brian Bianco. He advises clients on building intellectual property portfolios and has a litigation practice. In the spirit of our law school connection, we decided to go back to our roots: the IRAC (Issue, Rule, Application, and Conclusion) method of first-year law school legal writing.

Issue

How can a company take “reasonable measures” in an effort not only to satisfy DTSA requirements, but also to protect against theft of trade secrets?

Rule

Consistent with prevailing authority, the court in Dichard v. Morgan held that a DTSA claim must allege how reasonable measures were taken to keep secret any misappropriated information. “Reasonable measures” requires some
affirmative step beyond merely intending to keep the information secret. However, what constitutes reasonable measures to maintain secrecy is not well defined. Courts have typically examined the specific facts of the case, the nature of the trade secrets at issue, and even the type or size of the business.

**Application**

Here are a few suggestions for affirmative steps you can take:

**1. Identify and mark your trade secrets**

The first step in protecting a company’s trade secrets is to know what information is considered to be (and is best protected as) a trade secret. The type of intellectual property protection that is being sought (i.e., patents vs. trade secrets) will lead to different steps. For example, patenting can result in exclusive rights to commercialize an invention for a limited time in exchange for public disclosure. Trade secret protection can last indefinitely, but requires secrecy.

Thus, for information that is deemed to be a trade secret, the information should be identified and marked as confidential. Some companies take a step of distinguishing trade secrets over-and-above other confidential information with additional marking that indicates that the material is a trade secret proprietary to the company.

**2. Limit and track access to trade secret information**

Once trade secrets are identified, access to the trade secrets should be restricted. Efforts should be made to limit the disclosure of the information only to individuals who “need to know” to perform their duties. Access control can be achieved through steps like physical security, passwords, encryption, and data segregation. For example, Waymo employees working on projects unrelated to self-driving cars were prohibited from accessing the sensitive information they did not need to know. Similarly, the networks hosting Waymo’s confidential and proprietary information were encrypted and required passwords and dual-authentication for access.

In addition to these technology-related security measures, Waymo’s physical facilities were monitored with security cameras and guards. Further, not only did Waymo require outside vendors to execute non-disclosure agreements, Waymo purchased its components from a number of different vendors so that no single vendor would have full knowledge of Waymo’s proprietary systems.

Despite all these safeguards, Waymo apparently had a gap. For individuals who are allowed to access trade secret information, their interactions with the information can be monitored. For example, access logs and tracking mechanisms can be maintained as well as alerts if bulk file transfers occur. Waymo either did not know of the mass download of documents in real time or
did not comprehend its significance, as Waymo partly discovered the
misappropriation of its trade secrets by happenstance due to a misdirected email
from a vendor.

Done manually, it is challenging to implement these types of controls across a
large organization. However, technology makes the task much easier and
safeguards can be built into the collaboration tools that your business will likely
need to use anyway [Link to: https://accounsel.realмагнет.land/lex-ManageRisk].

3. Actively manage secret information

After taking initial, proactive steps to protect trade secret information, you must
be mindful to continually manage its secret nature. For example, in Art & Cook,
Inc. v. Haber, the court recognized that the plaintiff took some steps to secure its
information, including using password-protected servers and folders, and
employing a third-party internet security company to protect its servers from
outside hacking.

However, the court concluded the plaintiff’s further actions constituted a failure to
take reasonable measures. Specifically, despite the fact that the defendant
refused to sign an employee handbook and a non-disclosure agreement, the
plaintiff nonetheless granted the defendant access to the confidential information.
Thus, the court denied a motion for a preliminary injunction under the DTSA.

Art & Cook v. Haber demonstrates the importance of being consistent in how you
care for trade secret information since the uncontrolled release of the information
can result in a loss of protection. Training employees and developing a culture
around protecting secrets is important to ensure your information will be cared for
properly.

Conclusion

You will be less likely to lose control of your confidential information and a court
will be more likely to support your claim for trade secret protection if you take the
types of steps identified above.

While the legal issue fits nicely into an IRAC format, the practical application of
trade secret management is complex and has gotten the better of several
companies. Planning and consistent diligence are required to protect your most
sensitive information.

As in-house counsel, you know how quickly today’s business landscape is
changing - from cybersecurity breaches to shifting international regulations. The
Association of Corporate Counsel is here to help you navigate these new
challenges and opportunities. Download an exclusive compilation of fifteen of the
most popular ACC Docket articles on risk management authored by in-house
counsel, for in-house counsel, and gain complimentary access to tools to do your
job better, easier and faster in 2018. [Link to https://accounsel.realmagnet.land/lex-ManageRisk]