Trade Secret Theft: You're A Victim, Now What?

by Chris Hamilton, CPA, CFE, CVA, DABFA

Trade secrets are defined under the law in varying ways depending on the legal jurisdiction. There are three factors that tend to cut across all definitions: it is information that is generally not known that confers economic benefit on its holder, and is the subject of reasonable efforts to maintain its secrecy. The value of the secret derives specifically from the fact that it is not known, not just from the value of the information itself. If a company takes no steps to protect the information there is a weakened ability to claim trade secret status.

Avenues for Protection

Businesses generally protect secrets through the use of non-compete and non-disclosure contracts with vendors, customers, employees, and others who have access to the information. This places the theft of secrets into a framework of violating a written agreement in addition to the actual misappropriation and misuse of the information. Once a company suspects that its secrets have been stolen there must be an effort to identify not only who took the secrets, but how they are being used. This generally requires an extraordinary effort to obtain (often, secret) communications, data download histories, relationship clues, and interviews/cooperation from individuals (recipients of the secrets) who are not motivated to assist in the investigation.

What To Do When Theft Occurs

The most common case of trade secret theft is when an employee resigns or is terminated. It is common in trade secret cases to discover that the departing employee was recruited by a competitor business and offered employment and compensation for changing employment and bringing secrets with them. Resolving these cases is often dependent on sophisticated data tracking systems that retain emails and date/time stamped records of data dumps from servers and hard drives.

Once the case has been made that secrets were stolen the decision is made whether to pursue criminal prosecution, civil remedies, or both. The criminal penalties are severe and can include jail time for the persons involved. Under federal law, companies involved in theft of trade secrets can be fined up to $10,000,000.

Civil litigation can result in a range of penalties including injunctions, a reallocation of profit earned from the secret by the party who benefitted from the theft, reimbursement of actual damages, and punitive damages. In some jurisdictions, the award can include a multiple of actual damages. Actual damages can be calculated as lost profits or by placing a value on the information that was stolen. To the extent the information was stolen and destroyed (published widely, for example) the extent of damage was the value of the information right before it was destroyed.

Valuation of intellectual property, including trade secrets, is ultimately based on the projected income stream generated by the information discounted to present value at an appropriate risk rate. The valuation of trade secrets is difficult because of the need to isolate the historical income stream associated uniquely with the information that was protected as secret. The valuation expert must be able to identify income, direct expenses, and allocated indirect expenses associated with the information. That data is then used to project future net cash flows. In some cases where the information is stolen, used by a competitor, and cannot be recovered the value of damages is calculated based on the marginal benefit derived by the competitor from the stolen information.

2468 Tapo Canyon Road Simi Valley, CA 93063
Ph: 805.306.7890 Fx: 805.306.7891 www.arxisfinancial.com

Experts Can Make or Break Your Case

As noted above, accurate and relevant estimates of damages are based on reliable historical accounting information. Additionally, the use of an experienced account and valuation expert is required to properly use the historical information as a basis to opine as to the value of the trade secret and/or the damages caused by the theft of the trade secrets. **Arxis Financial, Inc**. has significant expertise in forensic accounting services for trade secret theft. Please contact us with your questions.

About the author:

Chris Hamilton is a partner with the CPA firm of Arxis Financial, Inc., in Simi Valley. He is a member of the California Society of Certified Public Accountants (Litigation Services Committee), and the American Institute of Certified Public Accountants. Mr. Hamilton is a Certified Public Accountant, a Certified Fraud Examiner, a Certified Valuation Analyst, and a Diplomate of the American Board of Forensic Accounting. He can be reached at ph. 805-306-7890 or chamilton@arxisgroup.com.