Trade Secrets – a Fragile Web

By ALAN S. WERNICK, ESQ.

Of all the various types of intellectual capital assets, trade secrets are the most fragile. As this article explores, the Internet (also known as the "web") is not a fertile ground in which to plant one's trade secrets and that protection of trade secrets among other things requires constant vigilance.

Trade secrets are rooted typically in the common law or state statute. A "trade secret" is defined in the Uniform Trade Secret Act ("USTA") – the basis of many state trade secret statutes – as:

> …information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (1) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use; and (2) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

Companies owning trade secrets that follow best practices in obtaining, preserving, and managing trade secrets reflect the significant value of those trade secrets in their bottom line profitability. Perhaps the "classic" example of a trade secret is the secret formula for Coca-Cola® which has been successfully maintained as a trade secret for many years. When properly protected as trade secrets, other examples include computer programs, customer lists, business plans, and so forth. Famous trade secrets, in addition to the secret formula for Coca-Cola, include the chemical formula for WD-40, Google's proprietary search algorithms, the New York Times "Best Seller List" rating system, and the recipes for such famous foods as Twinkies, Thomas' English Muffins, and Mrs. Field's chocolate chip cookies.

A report from the President of the United States recognized the importance of trade secrets to the national economy (See, "Administration Strategy on Mitigating the Theft of U.S. Trade Secrets," Executive Office of the President of the United States, February 2013). Trade secrets are valuable assets. Every CEO, CFO, CIO, and GC, as well as every audit and risk committee member of the board of directors, should be questioning the business' ability to protect the trade secret assets, and other digital assets, from risks of theft or a data breach.

One case example is that of an otherwise successful online retailer who failed to successfully protect its trade secrets. Although the online retailer prevailed in obtaining a preliminary injunction in the trial court enjoining the defendant from violating the online retailer's "trade secrets," the Court of Appeals disagreed and reversed, thereby removing the preliminary injunction and returning the case to the lower court. A brief review of the facts and the Court's analysis is instructive regarding the fragile nature of trade secrets.

The Court of Appeals of Indiana had occasion to address these legal aspects of trade secrets on the web in Ivan Paramanandam D/B/A Scorpion Consultants, Mall88.Com, and Scaleablescales.Com, et al., vs. Victoria Herrmann D/B/A Dynamicscales.Com (Case No. 84A01-0408-CV-345, May 24, 2005). In October 2002 Victoria Herrmann ("Victoria") began Dynamic Scales and the next month hired Ivan Paramanandam D/B/A Scorpion Consultants ("Ivan") to develop a website for Dynamic Scales' online retail store. According to the Court, in addition to developing the web site, "…Ivan registered approximately four hundred domain names, among them Mall88.com, and developed six thousand corresponding keywords, all of which would direct potential customers to Dynamic Scales' online store via internet search engines such as Yahoo! and Google. Customers would call Dynamic Scales' toll-free number to receive a quote; in the event of a sale, the manufacturer would ship the scale directly to the customer. Eventually, Dynamic Scales developed the largest online retail store in the scale industry." (Paramanandam, *supra*, at page 3.)

In December 2003 Ivan and Victoria terminated their business relationship. At the end of December 2003 Ivan started a competing online retail operation using the domain name "ScaleableScales.com" which was substantially similar to Victoria's Dynamic Scales' website. In addition it appears that Ivan also used the "Mall88.com" domain name for his own business and directed Internet searches for Dynamic Scales' name and toll-free number to the Mall88.com website.

In February 2004 Victoria sued Ivan, *et al.*, alleging, among other things, "[t]he information contained on [its] website" and "domain names developed, created, and maintained by and for Dynamic Scales" were trade secrets under the Uniform Trade Secrets Act … and that Appellants [Ivan, et al.] had misappropriated those secrets." After a hearing, the trial court in May 2004 issued a preliminary injunction enjoining Ivan, et al., from "…using or appropriating any of the information copied from plaintiff's website, domain names, trade names, content,

images, key words and other information supplied by the plaintiff to the defendants or received by the defendants or Ivan during his period of employment by the plaintiff…"

The Court of Appeals, in reversing the lower court, noted that it is plaintiff's burden to prove the existence of the trade secrets in what typically is a fact-specific inquiry. The applicable law, Indiana Code § 24-2-3-2, follows the USTA and in sub-part (2) requires that the trade secret "…is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."

In reaching its decision to reverse the preliminary injunction, the Court of Appeals examined Dynamic Scales' complaint which stated that the alleged trade secrets consist of "[t]he information contained on [its] website" and the "domain names developed, created, and maintained by and for Dynamic Scales[.]" Focusing on sub-part (2) of the Indiana Code § 24-2-3-2, the Court concluded that regardless of whether or not the subject items were "trade secrets," Dynamic Scales failed to establish that any efforts were made to maintain its secrecy. The Court stated: "By definition, information is a trade secret only if it is the subject of reasonable efforts to maintain its secrecy." … Here, Dynamic Scales made no efforts to maintain secrecy of the information contained on its website or its domain names."

One lesson from the Paramanandam case is that trade secret owners must proactively properly and appropriately identify and protect their trade secret assets. While some courts have recognized certain items as potentially trade secret by their statutory treatment (e.g., customer lists), the risk increases that trade secret items will not be treated as trade secrets by the courts if the trade secret owner fails to properly treat the items as trade secrets. The facts in Paramanandam indicate that the trade secret owner, Victoria, did not properly identify and treat the purported trade secret assets as trade secrets. Another lesson learned from the Paramanandam case is that attempts to characterize and protect items as trade secrets after the fact (i.e., after the misappropriation) rarely succeed.

Illustrative of the point concerning the risks of after the fact efforts to protect trade secrets is the case nClosures Inc. v. Block & Co. 770 F.3d 598 (USCA 7th Cir. 2014). In nClosures the plaintiff ("nClosures"), the purported trade secrets owner, alleges to have developed a proprietary design for enclosures for electronic tablets. nClosures had a confidentiality agreement signed by the defendant ("Block") which was general in nature as the parties pursued negotiations for the manufacture and sale of the nClosures design of tablet

enclosures. While those negotiations continued, nClosures allowed Block to manufacture (under an oral agreement) some units which nClosures sold.

The Court of Appeals observed that nClosures did not follow through with other reasonable steps that the Court expected of a trade secrets owner to keep its proprietary information confidential (e.g., nClosures did not require other Block employees or engineers to sign additional agreements in order to access the trade secret design files, nClosures did not mark its drawings as "confidential" or "contains proprietary information," nClosures' drawings were not kept under lock and key nor were they stored on a computer with limited access).

Trade secret owners have essentially three obligations when protecting their trade secret assets:

A. **INTERNAL**. How is the trade secret owner handling the trade secrets assets within the trade secret owner's own organization? Are all employees trained in understanding and identifying the trade secrets and the employees' responsibilities to protect these valuable corporate assets? Is the training done on a recurring basis or only one-time? Are proprietary notices used consistently and only where appropriate? Are systems in place to monitor access to the trade secrets? Are the employees "tested" with regards to their understanding of trade secrets?

B. **EXTERNAL**. How is the trade secret owner handling the trade secrets assets when third parties need to access the trade secrets? Do all agreements with third parties appropriately address the trade secrets protections? Are proprietary notices used consistently and only where appropriate? Are systems in place to monitor access to the trade secrets? Are access controls in place and regularly tested?

C. **ETERNAL**. In order to protect and preserve trade secrets, the trade secret owner must be constantly vigilant in maintaining and managing the best practices for legal, technical, and physical procedures needed to protect these valuable assets.

There are several steps in the best practices of trade secret ownership. These include, without limitation:

1. Proper identification of the trade secret assets.
2. Proper proprietary markings or legends (e.g., not marking everything as proprietary and a trade secret when only some things really are properly categorized as trade secret).
3. Limited and secure access to the trade secrets.
4. Attention to best practices for cybersecurity.
5. Execution of non-disclosure agreements with all third parties for whom it is necessary to access the trade secrets.
6. Inclusion of non-disclosure provisions in employee agreements.
7. Training of all employees regarding the use and handling of the trade secret assets.
8. Sign in and sign out logs regarding access to the trade secrets.
9. Periodic audit of trade secrets handling procedures.
10. Proper destruction of physical and digital copies of the trade secret materials.

The above is not meant to be exhaustive of all the things a trade secret owner must do in order to properly protect and preserve trade secret rights. Preventive measures by the trade secret owner can go a long way towards providing a firm foundation upon which to manage and grow and protect the value of the trade secret assets. The bottom line is that trade secret owners need to be eternally vigilant in protecting their trade secrets through proper means and training of individuals responsible for handling of those trade secret assets.