Minor v. Martin: A Memory Game Of Trade Secrets

-- By Jonathan Goins

In 1971, there was a short-lived television game show created by media mogul Merv Griffin called the Memory Game. Each of the five contestants had a certain amount of time to try to memorize a booklet containing questions and answers, the former for which they were asked about during the subsequent competing rounds. The contestant who could answer the most questions won a monetary prize or car.

The Ohio Supreme Court recently created their own trade secrets-version of the Memory Game. In February 2008, the seven-member court unanimously ruled that when a former employee memorizes a client list to compete with a former employer then a trade secrets violation has occurred. *See Al Minor & Assocs. v. Martin*, 881 N.E.2d 850 (Ohio 2008). The court explained that the confidential information of the company was not lost because the former employee memorized 15 clients and solicited them for his own, newly-formed company.

The *Martin* case is in line with a majority of other states (including Arkansas, California, Illinois, Massachusetts, Oklahoma, Pennsylvania, Texas, and Washington among others) recognizing that memorized information of a trade secret can form the basis of a misappropriation claim.

But this decision seems to take trade secrets law involving memory a step further, suggesting that *any* memorization of a trade secret is subject to UTSA protection, intentional or not. It moved the focus away from what reasonable steps Al Minor should have taken in protecting its confidential proprietary information, which were almost none; after all, Martin did not sign any non-disclosure, non-compete, or non-solicitation agreement. And no written confidential policy or employment contact was in place. One could even argue that the case supports applicability of the inevitable disclosure doctrine, or more generally, rises to the level of a company's right to control the use of memory of competing former employees.

Unfortunately, companies seeking redress for trade secret violations in Georgia should not anticipate playing the Memory Game (i.e., applying the *Martin* case) anytime soon. Georgia is in the minority view as only information in written or otherwise tangible form, such as customer lists, is warranted trade secrets protection (merely memorizing is insufficient).[1] And good luck trying to enforce the protection of confidential information by traditional means such as non-compete or non-disclosure agreements. Georgia is notorious for striking down restrictive covenants (based in large part on the underlying principle of the state's constitutional provision mandating that contracts having the effect to "defeat or lessen competition" are "illegal and void").

So make sure that the restrictions are reasonably limited in time, scope, and geography; and try to execute contracts and incorporate choice of forum/law provisions in non-Georgia states.

[1] *See* O.C.G.A. § 10-1-760 *et seq*.

Regardless of whether companies can enforce violations based on misuse of memorized trade secrets under the *Martin* case, companies should continue to employ reasonable safeguards in protecting its confidential information, including as follows:

(i) designate appropriate documents as HIGHLY CONFIDENTIAL;

(ii) limit physical access to areas maintaining any confidential information, use video surveillance, and require security cards or ID badges at all times;

(iii) establish firewalls, filters and other IT-related security systems that minimize cyber-hacking, monitor Internet use, and maintain bulletproof filing storage programs;

(iv) implement a selective security team to manage and enforce compliance, confidential policies and reporting mechanisms for suspected violations; and

(v) most importantly, employ a "prevent defense" strategy and avoid unnecessary distribution or disclosure.

Information relating to trade secrets should be disclosed only on a need-to-know basis! This includes keeping an eye out for low-level employees, a lesson almost learned the hard way when Joya Williams, the secretary to Coca-Cola's global brand director, got her hands on confidential documents and product samples, and conspired to sell them to rival PepsiCo for $1.5 million (one of her co-conspirators actually exchanged info with an undercover FBI agent for 30k; they were convicted in February 2007).

The unregulated, and increasing international, nature of cyber-hacking activity is only getting worse. A recent *New York Times* article[2] reported that as of the end of 2008, Internet spam and malware infect as many as 10 million computers worldwide on a daily basis.

Protecting trade secrets and other confidential proprietary information cannot be under-estimated, and in fact, can be quite costly. A U.S. Chamber of Commerce study, for example, found that from July 2000 to June 2001, Fortune 1000 companies reported stolen IP and proprietary information at a value of almost 60 b-b-b-billon dollars!

So by all means, take steps to enforce trade secrets policies and minimize an employee's ability to play the trade secrets-Memory Game.

Jonathan D. Goins is an IP Attorney associated with Kilpatrick Stockton LLP

[2] John Markoff, *Thieves Winning Online War, Maybe Even In Your Computer*, N.Y. TIMES, Dec. 5, 2008, at A1.