The Metropolitan
Corporate Counsel®

www.metrocorpcounsel.com

Volume 20, No. 11 November 2012

Trends In Trade Secret Litigation

The Editor interviews ***Michael Bunis*** *and* ***Paul Popeo,*** *Co-Leaders of the Trade Secret Group at Choate, Hall & Stewart LLP in Boston.*

Editor: Tell us a little bit about Choate's trade secret practice.

Bunis: Most trade secret disputes arise from an employee taking trade secrets from a former employer or a joint technology venture gone awry. These situations require the immediate attention of lawyers who understand the technology involved and the full scope of the questions presented by these problems.

Choate's trade secrets practice draws on our firm's collective experience in intellectual property litigation, technology law and trial strategy. Through our combined expertise and years of experience handling trade secrets litigation, Choate has developed a critical "play book" for navigating the early stages of litigation to lay the groundwork for success to recover stolen trade secrets and to protect defendants against costly fishing expeditions.

Editor: Why have trade secrets become such a hot topic recently?

Popeo: The stakes are higher than ever. Over the last year, numerous juries have returned multi-million dollar verdicts in trade secret cases. For example, in May 2012 a Utah jury awarded USA Power LLC $134 million for a joint venture partner's misappropriation of trade secrets and unjust enrichment. In August 2012, Brocade Communications Systems, Inc. was awarded $112 million in a California case involving patent infringement and trade secrets. In 2011, St. Jude Medical was awarded $2.3 billion in damages against a Chinese company for theft of trade secrets.

Michael Bunis

Paul Popeo

Trade secrets often consist of information that may not be eligible for patent protection, yet the information is critically valuable and important to the lifeblood of the company. Trade secrets are particularly vulnerable to theft because they are often made available to a relatively large number of people. A trade secret describing a unique manufacturing process may be exposed to all members of the production team that actually builds the device. Trade secrets consisting of computer code may unavoidably be shared among many different programmers.

Editor: What should an employer do to prevent theft of trade secrets in the first place?

Bunis: The most effective way to prevent theft of trade secrets is to keep trade secrets under lock and key, literally or electronically. But, for many businesses, perfect protection of trade secrets is commercially impractical or impossible. Allowing a range of employees relatively unfettered access to sensitive information is frequently necessary to conduct business efficiently. Nonetheless, the business must engage in *reasonable* efforts to preserve the confidentiality of the trade secrets.

Trade secret defendants are often employees who took information that they believed to be non-confidential, or which they believed they could take with impunity because they helped develop it or had not been expressly warned not to. To prevent this type of trade secret theft, companies must set clear expectations for any employee who has access to sensitive information, including: requiring all employees to sign non-disclosure agreements; establishing a culture of secrecy by regularly reminding employees that the competitive success or financial well-being of the company depends on maintaining the secrecy of information and, therefore, they must not share any information; and requiring that departing employees seek permission before taking any information or materials off the premises, whether secret or not.

Editor: What should a joint venturer do to prevent theft of trade secrets?

Popeo: For joint venture partners, information sharing is an inevitable and fundamental element of innovation. Programmers and engineers also often operate in a culture of open-exchange, even across companies. There have been instances where a seemingly innocuous bar room conversation has led to long, drawn-out, but eminently preventable, trade secrets litigation.

At the end of the day, if an idea is worth sharing then each company must sign a comprehensive non-disclosure agreement and must be disciplined to limit their shared disclosures to the technology being jointly developed. Joint venture partners should also maintain careful records of their lawful developments, which can prove useful in the event that allegations of misappropriation arise down the road.

Please email the interviewees at mbunis@choate.com and ppopeo@choate.com with questions about this interview.

Editor: What is the first thing a company should do if it thinks it is a victim of trade secret theft?

Bunis: If a company has any inkling that a trade secret has been stolen, it must act quickly and thoroughly to prevent further dissemination of that trade secret. Once a trade secret becomes a matter of general knowledge in the industry, secrecy is destroyed and the property rights to that trade secret vanish.

A company who believes a secret has been taken, therefore, must contact the alleged thief immediately and demand total cessation of use of the trade secret. Where applicable, the company should demand physical return of the secret information. If the thief does not acquiesce immediately, moving swiftly to court and seeking preliminary injunctive relief can be the difference between maintaining the trade secret and losing it forever.

Editor: What should a trade secrets plaintiff do to make sure the defendant doesn't destroy evidence before the plaintiff can get discovery?

Popeo: Someone who is likely to become a trade secrets defendant is not necessarily a scrupulous person and may be inclined to destroy evidence if accused of misappropriation. Seeking preliminary injunctive relief, including requesting an order of preservation (and potentially imaging any computer hard drives), is typically the most advantageous course.

Editor: What discovery should a defendant accused of taking trade secrets seek?

Bunis: Since disclosure of alleged trade secrets to a competitor normally destroys secrecy, a defendant who is accused of taking trade secrets should consider subpoenaing their accuser's competitors to find out what information was shared with those entities.

A plaintiff's customers should also be subpoenaed. Companies often claim as trade secrets ideas that they initially derived from soliciting requirements from customers. Courts have been reluctant to extend trade secret protection to ideas that originated as an improvement suggestion by a customer.

Editor: Why has the identification of trade secrets become such a critical aspect of trade secrets litigation?

Popeo: Increasingly, plaintiffs are required to define trade secrets with particularity before they are allowed to proceed with discovery in trade secret cases. Most courts now refuse to allow a plaintiff discovery concerning what a defendant allegedly stole before the plaintiff articulates with particularity what it believes was stolen. A few courts have gone much further, refusing to allow a plaintiff any discovery at all before defining its trade secrets.

This limitation on discovery derives from the competing fears of the parties to a trade secret litigation: the defendant fears that a plaintiff has alleged trade secrets misappropriation merely to harass the defendant or, worse yet, as a cover for an attempt at industrial espionage to discover the defendant's own trade secrets. Meanwhile, the plaintiff fears that a defendant will simply withhold or destroy critical information once it knows what the plaintiff is looking for. The plaintiff can address this concern by seeking preliminary injunctive relief early on to ensure a defendant preserves critical evidence.

If a plaintiff defines the allegedly stolen trade secrets early in litigation, then learns during discovery that the defendant took additional, undefined trade secrets, the plaintiff usually can amend its description of trade secrets as long as it can show it did not have reason to know of the newly discovered theft at the outset of litigation.

Editor: What are the jurisdictional considerations for a plaintiff about to file a trade secret case?

Bunis: Despite the fact that trade secrets are a state law issue, the law is broadly similar across the states. Forty-seven states have adopted the Uniform Trade Secrets Act and courts in the states that have not (Massachusetts, Texas and New York) frequently rely on decisions applying the Act. Therefore, where a plaintiff initiates a trade secret case normally depends more on the convenience of the parties than on the substantive law of the jurisdiction. However, a company considering bringing a complaint under the Computer Fraud and Abuse Act may want to think carefully about where to file the action, because the courts are currently split regarding the scope of actions covered by the Act.

The Computer Fraud and Abuse Act assesses civil and criminal penalties against someone who accesses a non-public computer "without authorization or access." The Seventh Circuit has found a violation of the Act when an employee who is authorized to access information did so for an unauthorized purpose. The First, Fifth, and Eleventh Circuits have each taken a similar broad approach. The Fourth and Ninth Circuits, on the other hand, have read the statute more literally to find that an employee has not violated the statute as long as the employee is authorized to access the information, whether or not the employee accessed the information for an authorized purpose. District courts in the Second, Third, Sixth, Eighth, and Tenth Circuits have taken a similarly narrow approach to the Act, limiting it to true hackers, rather than employees engaging in acts against their employer's interest.

If the employee in question was authorized to access the computer, but did so for an unauthorized purpose, the employer should consider the benefits and availability of filing suit in a circuit that has adopted the broader reading of the Act.

Editor: How is trade secret litigation different from other types of litigation?

Popeo: Trade secret litigation is not ordinary commercial litigation. Just as patent litigation has become increasingly standardized over the last two decades, with claim constructing dominating the early stages of litigation, trade secret litigation has begun to follow familiar patterns, particularly during the early stages.

Lawyers who have handled many of these critically important trade secret cases know what to expect from the outset of a case. Speed is the critical element in these cases. Companies must act very quickly from the time they learn about a theft, so they need integrated trade secret counsel on board from the beginning. They must think about it before problems occur, be prepared, and be ready to act aggressively to deal with this threat when needed.