Missouri Supreme Court sidesteps whether customer list is a trade secret

by John Vering

In our March 2013 issue, we reported on a decision in which the Missouri Court of Appeals for the Southern District found that the customer information at issue wasn’t a trade secret (see “Customer list is not a trade secret” on pg. 1). The company claiming its trade secrets had been misappropriated appealed the decision to the Missouri Supreme Court, which didn’t decide whether the customer list was a trade secret but did rule that the company failed to prove that its competitor had in fact stolen any trade secrets. Read further to learn how the Missouri Supreme Court reached its decision and what you can do to protect your confidential customer lists and client information.

Facts

Troy Kennedy began working for Springfield Trust and Investment Company (STIC) in 1992. While his role fluctuated somewhat during his time at STIC, his duties included acting as an executive vice president, a shareholder, an officer, and a director. His primary job duty was to develop new business and act as a relationship manager for business already acquired by STIC.

In 2008, Kennedy entered into an employment contract that was to be in effect from January 1, 2008, to December 31, 2013. The contract contained a three-year noncompete agreement that included prohibitions on soliciting STIC’s clients and working for a competing business within 100 miles of Springfield. The agreement also contained a provision stating that it would be void if STIC was sold.

Central Trust and Investment Company began negotiations to purchase STIC in March 2009. Kennedy was aware of the negotiations and began making preparations to leave STIC, including telling clients he intended to leave and even soliciting their potential business upon his departure. In addition, on the advice of his attorney (but before leaving STIC), he placed written client lists and a cell phone containing the contact information of 200 STIC clients in a safety deposit box. The client lists consisted of 39 pages of documents containing information about STIC’s clients, including names, addresses, telephone numbers, e-mail addresses, and confidential financial information. The record was silent on exactly what the “confidential financial information” was.

In July 2009, Kennedy, as an STIC director, signed an “Oath of Director.” The oath, which contained a confidentiality agreement, provided that he wouldn’t use or disclose any confidential information acquired while he was a director. The document defined “confidential information” to include, among other items, “information regarding...”
clients’ personal information[,] including but not limited to . . . contact information, net worth, [and] account balances with [STIC] or any other places of investment.”

Central Trust purchased STIC on November 20, 2009. Kennedy’s employment with STIC ended that day, and the following day, he founded ITI Financial Management LLC to compete directly with Central Trust by providing financial advice and investment management services to investors. He also began soliciting STIC’s customers.

On February 22, 2010, Kennedy signed an agreement with SignalPoint Asset Management, LLC, under which SignalPoint would serve as his registered investment adviser. However, he never provided any of STIC’s or Central Trust’s client lists to SignalPoint.

**Company’s claims**

On January 5, 2010, Central Trust sued Kennedy and ITI, claiming misappropriation of trade secrets, breach of fiduciary duty, tortious (wrongful) interference with business relations, alleged breach of Kennedy’s employment contract, and civil conspiracy. Central Trust later added SignalPoint to the lawsuit, claiming it had (1) interfered with its business relations, (2) misappropriated trade secrets, and (3) engaged in a civil conspiracy with Kennedy and ITI.

Kennedy, ITI, and SignalPoint each asked the trial court to throw out the lawsuit. After a hearing, the trial court ruled (1) the claims against Kennedy and ITI couldn’t be dismissed because there were some questions of fact that needed to be decided by a jury, and (2) the claims against SignalPoint should be thrown out because Central Trust couldn’t prove that STIC protected the confidentiality of its customers’ identities to the extent that they might be considered a trade secret. Central Trust appealed the trial court’s ruling to the Missouri Court of Appeals in Springfield.

**Court of appeals decision**

In determining whether the client lists were a trade secret under the Missouri Uniform Trade Secrets Act (MUTSA), the appeals court looked first at the statute, which talks about whether the information derives independent economic value from not being generally known or readily ascertainable through proper means. Next, the court looked at whether STIC had taken reasonable steps to maintain the secrecy of the information. In doing so, it considered the following six factors:

1. The extent to which the information is known outside the holder’s business;
2. The extent to which it is known by employees and others involved in the holder’s business;
3. The extent of any measures taken by the holder to guard the secrecy of the information;
4. The value of the information to the holder and its competitors;
5. The amount of effort or money expended by the holder in developing the information; and
6. The ease or difficulty with which the information could be properly acquired or duplicated by others.

The appellate court found that customer lists aren’t expressly mentioned in the MUTSA’s definition of a trade secret and don’t qualify as a trade secret under the six-factor test. The court explained its reasoning as follows.

**First,** while the client lists were attached to Kennedy’s employment contract, there was nothing in the contract that stated the lists were confidential. Further, there was evidence that Kennedy could, for the most part, remember the names and personal information associated with each of the clients, so he didn’t need written client lists to recreate his relationships.

**Second,** Central Trust admitted that it and its predecessor, STIC, shared their client lists and related personal information with various affiliates, including local banks. **Third,** Central Trust and STIC allowed all their employees to access the client database without requiring them to sign any type of confidentiality or other privacy agreement. **Fourth,** before Kennedy’s departure, three other employees left STIC for new employment and took lists of clients with them or actively solicited STIC’s clients, but none of those employees was pursued legally.

**Fifth,** Central Trust and STIC had used client names and likenesses in marketing materials and put some client names on their website. **Sixth,** Central Trust admitted that each client could leave at any time and take its business elsewhere.

Missouri Supreme Court decision

By the time the case reached the Missouri Supreme Court, the only parties still involved were Central Trust and SignalPoint. The supreme court rejected each of Central Trust's three claims against SignalPoint: misappropriation of trade secrets, tortious interference with business relations, and civil conspiracy.

The court's basis for finding in favor of SignalPoint was that Central Trust failed to prove that it had misappropriated the client list. SignalPoint denied that it ever received or saw the client list or that it knew which of Kennedy's clients were clients of Central Trust and STIC and which were new clients belonging solely to him. The court then ruled that SignalPoint couldn't be responsible for any misappropriation of the client list by Kennedy because he wasn't its employee or agent; they merely had an independent contractor relationship. Central Trust and Investment Co. v. SignalPoint Asset Management, LLC, Mo. Sup.Ct. (No. SC93182) (February 25, 2014).

How to protect customer lists, related information

Because the Missouri Supreme Court declined to rule on whether the customer lists were trade secrets, Missouri law remains unclear about whether customer lists can be trade secrets in some circumstances. When the Missouri Court of Appeals and the Missouri Supreme Court decisions are read together, however, they do provide some valuable insights into what you can do to protect customer lists and related customer information. We continue to believe that depending on the information and how you protect it, certain customer information can be a trade secret subject to protection under the MUTSA.

It's important to keep in mind that every business is different, and the steps necessary to protect confidential information, including customers' names and related information, vary from business to business. Nevertheless, this case provides some lessons for any organization that wants to maintain the confidentiality of its client lists and related information:

- If possible, get employees to sign a noncompete agreement that contains a provision preventing the disclosure or use of customers' names and confidential information (e.g., their addresses, contact information, and buying preferences).
- Make the noncompete agreement assignable by the company so the right to enforce the noncompete agreement will pass to the new owner if the company or its stock is sold.
- Make sure every confidentiality agreement specifically addresses which information in your organization is confidential and proprietary. For example, if your business has only four customers and they're listed on your website, the customers' names won't be confidential, but their contact information and buying preferences very well may be.
- Don't share customer lists with others, including affiliates, unless you have an agreement with them to keep the information confidential.
- Allow only employees with a "need to know" access to confidential customer information, and require each person who has access to the information to sign a confidentiality/nondisclosure agreement.
- Don't let your guard down. While there is Missouri legal authority to support the proposition that you don't have to sue every former employee who breaches a noncompete agreement, if you regularly allow employees to leave and solicit your customers in violation of applicable noncompetes, you might find it more difficult to persuade a court that you would be irreparably injured if a former employee isn't prevented from competing with your organization.
- If you're going to use client names and information in marketing materials or on your website, don't be surprised if a court finds that you failed to treat the information like a trade secret.
- Explain in your noncompete and nondisclosure agreements why your customer information is important and valuable. If the information has been compiled at great expense over a number of years, state that as well.
- Remember that you typically have to prove that the departing employee or his new employer actually used or disclosed the trade secret information. Contractually requiring the employee to return or destroy any confidential information upon termination of employment is a step in the right direction because it gives you the right to pursue a breach-of-contract claim against the employee for failing to return or destroy customer information.
- Be aware that it will be much easier to sue your competitor under the MUTSA if the departing individual is an employee or agent of your competitor. However, if your former employee has only an independent contractor relationship with your competitor, it will be harder to make a case against the other company.
- Get counsel experienced in drafting noncompete, nonsolicitation, and nondisclosure agreements to audit your policies and practices, including your procedures for protecting customer information and other confidential and proprietary information. And update your agreements to conform to the latest legal requirements, if necessary.

The author may be contacted at jvering@armstrongteasdale.com.