Careful, That Slice Of Pizza May Be Full Of Trade Secrets

Law360, New York (October 11, 2013, 5:10 PM ET) -- Earlier this month, New York Pizzeria Inc., a pizzeria chain with more than 30 restaurants in the United States and the Middle East, filed a complaint in federal court in Texas alleging trade secret misappropriation. In the lawsuit, New York Pizzeria Inc. v. Syal et al, New York Pizzeria alleged that a former employee, as well as several individual restaurant owners, were conspiring to misappropriate trade secrets for the purposes of creating a competing business.

According to New York Pizzeria's complaint, Adrian Hembree, a former employee, and Ravinder Syal, the owner of a competing business, were conspiring to steal and use the company's trade secrets. The two defendants allegedly used this unlawfully obtained information to start a competing chain, Gina's Restaurants.

According to the complaint, Hembree and another man, Robert Salcedo, previously owned a New York Pizza franchise. Hembree's employment with the company was terminated in March 2011, and in October of that same year, the company sought to terminate the franchise as well.

The parties agreed that New York Pizzeria would assume ownership of the restaurant and would buy Hembree out. However, Hembree allegedly failed to honor certain obligations from this contract, and sued for breach of contract. In response, New York Pizzeria filed a counterclaim, alleging misappropriation of trade secrets.

The suit eventually settled; however, after the settlement, Hembree allegedly continued to steal New York Pizzeria's product, and the company filed a second lawsuit, asserting independent claims of trade secret misappropriation.

According to the complaint, as vice president of New York Pizzeria, "Hembree had access to ... confidential, proprietary information, including NYPI's recipes, 'plate specifications,' supplier and ingredient lists, and training and restaurant operations manuals ... Hembree provided that information to the Syal defendants, without privilege to do so."

Additionally, plaintiffs allege that Hembree and Syal illegally accessed New York Pizzeria's online portal by using one of New York Pizzeria's company usernames and passwords. This login information allegedly enabled defendants to obtain New York Pizzeria's confidential and proprietary information, including special recipes and concepts for pizza, eggplant parmesan and baked ziti.

How Should Employers/Franchisors Protect Themselves From Situations Like This?

From a legal standpoint, it remains to be seen whether the factual allegations have merit and to what extent New York Pizzeria has a protectable interest in the recipes and other proprietary data. However, the case serves as a reminder that those in the restaurant industry must closely guard their cooking secrets and employ effective nondisclosure and confidentiality agreements.

Trade secrets, such as financial, structural, technical, engineering, marketing, distribution techniques, formulas and recipes can be the life blood of the franchise, and parties must use caution to ensure this valuable information is protected.

Franchisors must be careful to make sure that they use effective nondisclosure and confidentiality agreements, including noncompete and nonsolicitation provisions as permitted,

with their franchisees. Additionally, franchisors should ensure that their franchisees use similar provisions with their employees. However, such a reminder is broadly applicable to other industries as well.

Employers should assume their employees may work for a competitor following their departure from their current employer, and based on this assumption, ought to take steps in order to minimize harm associated with a former employee's employment with a competitor.

First, employers should require their employees to sign proprietary information or confidentiality agreements, as the employees in New York Pizzeria Inc. v. Syal et al did, as well as noncompete and nonsolicitation provisions as permitted. Furthermore, employers should limit the accessibility of confidential, proprietary and trade secret information to those employees who require such information in order to perform their jobs.

Following an employee's departure, companies should take steps to ensure the departing employee has complied with nondisclosure and noncompete agreements, and that steps are taken to ensure the departing employee does not have continued access to confidential and proprietary information.

Prior to an employee's departure from the company, employers should review and retain all records and files in the departing employee's control. Employers should also collect all company property issued to the departing employee, including laptops, cell phones, flash drives and other devices, as well as ensure that electronic documents have been returned or deleted from any cloud-storage application.

The departing employee's office and files should be inspected to ensure nothing is missing, and his or her office should be photographed in order to create a record of the office's state at the time of the employee's departure.

Additionally, the departing employee's ongoing access to confidential, proprietary and trade secret information should be terminated, unlike in New York Pizzeria Inc. v. Syal et al, where the defendants retained access to the company's login information. Furthermore, the employee should be reminded of previously signed agreements regarding confidential, proprietary and trade secret information.

In addition to these precautionary steps, employers ought to consider whether confidential and proprietary information has actually been taken by a departing employee. Following an employee's departure, employers should confirm that no unauthorized information, file, document or email transfers have occurred.

Email folders, computer access and print logs should be reviewed for unusual or unauthorized use, and employers should confirm that all confidential, proprietary and trade secret information has been returned prior to the employee's departure.

Employers may also want to have their employees sign a statement acknowledging that he or she has not retained or forwarded any document, writing, email, voicemail or text message containing confidential or proprietary information. If there is suspicious activity, an employer would be wise to preserve the departing employee's computer and not assign it to another employee as important evidence could be destroyed.

Finally, employers ought to take steps to ensure that their former employees continue to protect the company's confidential and trade secret information following their departure from the company.

At the time of his or her departure, a departing employee should sign a statement acknowledging that he or she understands what constitutes confidential, proprietary and/or trade secret information belonging to the company, and that there is a continuing obligation to keep this information confidential.

The departing employee should also sign a statement acknowledging that he or she no longer has access in any manner (electronic, dial-in or otherwise) to any company email or documents.

Ultimately, New York Pizzeria Inc. v. Syal et al reminds us that employers should be careful to ensure the use of enforceable confidentiality agreements, and that plans are in place to identify and protect against misappropriation of confidential, proprietary and trade secret information. Such plans can help employers avoid costly litigation down the road.

--By Jessica Mendelson, Seyfarth Shaw LLP