

Chicago-Based Garrett Popcorn Shops' Parent Company Sues Ex-Employee for Stealing Trade Secrets

MAY 2, 2019

On April 22, 2019, CaramelCrisp LLC, the parent company of Chicago-based Garrett Popcorn Shops, filed a complaint in the U.S. District Court for the Northern District of Illinois against ex-employee, Aisha Putnam, for stealing proprietary trade secrets. See *CaramelCrisp LLC v. Aisha Putnam*, No. CV-02699 (N.D. Ill. filed Apr. 22, 2019). According to the complaint, Putnam, CaramelCrisp's former director of research and development, was one of only three people with access to the company's most confidential information and trade secrets. She allegedly stole over 5,400 files from the company.

Putnam, who began working for CaramelCrisp in March 2014, entered into two Confidentiality Agreements and one Non-Compete Agreement with CaramelCrisp that prohibited her from disclosing any confidential company information, including ingredients, recipes, formulae, and methods. According to the complaint, after Putnam became aware that CaramelCrisp planned to terminate her, she began surreptitiously copying company data to a personal external USB drive that she proceeded to take home. She also allegedly sent herself emails to her personal email account with CaramelCrisp documents attached. CaramelCrisp's IT team discovered the alleged trade secret theft during an analysis of Putnam's work computer after her termination, even though Putnam attempted to hide her tracks by deleting nearly all of the data on her computer, including the trash and recovery folders.

CaramelCrisp suffered the alleged theft despite utilizing confidentiality agreements; limiting access to their confidential information through enhanced network security, user-specific credentials for every computer terminal, file and folder level permissions; and, for the most critical data that can only be given to specific individuals, requiring biometric thumbprint access. CaramelCrisp seeks temporary, preliminary and permanent injunctive relief under the federal Defend Trade Secrets Act (DTSA) for Putnam's alleged trade secret theft.

TIP: Termination is a high-risk time for trade secret theft and companies should be on the lookout for red flags of potential theft at this time so that they can respond promptly.

1 Min Read

Author

[Christopher M. Parker](#)

Related Locations

Chicago

Related Topics

Trade Secret

Data Breach

Biometrics

Related Capabilities

Privacy & Data Security

Trade Secrets, Non Competes & Restrictive Covenants

Compliance Programs

Privacy: Regulated Personal Information (RPI)

Related Regions

North America

Related Professionals



Christopher M. Parker

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.