Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

A Cloud On The Horizon: Trade Secret Theft In The Cloud

By **Amy Van Zant, Evan Brewer and Margaret Wheeler Frothingham**
(June 29, 2018, 11:07 AM EDT)

Amy Van Zant

Evan Brewer

Margaret Wheeler Frothingham

As cloud services have transformed modern business, they have also changed the way companies protect and enforce their trade secrets. Companies and their employees increasingly store data on cloud-based platforms. While these platforms can provide flexible and cost-effective storage options, they also present unique problems for tracking access to and use of company trade secrets. As a result, companies that allow employees to access company data remotely or from personal devices via cloud platforms should carefully consider the implications and weigh options for protecting company data that makes its way to devices and locations outside the company's direct control.

Although courts and companies have at times struggled to keep pace with the rapidly evolving challenges surrounding the use of cloud-based software, some best practices have emerged from the body of case law addressing claims of cloud-based appropriation of trade secrets.

The Cloud's Risks to Trade Secret Owners

First, the risks: Innumerable companies worldwide use cloud applications like Dropbox, iCloud, Google Drive and Box to enable employees to work more flexibly and efficiently. Often, employers allow access to company cloud applications from employees' personal devices. But when an employee downloads information from the cloud to a personal device that is outside the company's control, the company may lose track of what subsequently happens to that information. In other instances, companies (especially startups) adopt a "bring your own cloud," or BYOC, policy permitting employees to use personal cloud accounts for company business. Under this approach, there is a risk that the employee may ultimately refuse the company access to a personal cloud account, even if it contains company information.

The ease with which data may be transferred in a cloud-centric world compounds the difficulties of maintaining a handle on company data. Because no physical files are at issue in cloud-based transfers, massive amounts of data can be taken without any overtly suspicious behavior (e.g., no employee is seen carrying boxes

of files out of the office).

This has led to an increase in cases alleging cloud-based theft. For example, in Frisco Medical Center LLP v. Bledsoe, two former hospital employees used Dropbox to misappropriate thousands of confidential company documents after accepting employment with another hospital. The plaintiff was alerted to the theft after one of the defendants warned a human resources manager that she "knew where too many bodies were buried," which prompted the plaintiff to undertake a forensic investigation.[1] Absent that defendant's offhand comment to the HR manager, the company may have never discovered the theft.

Without the right security controls, keeping track of data once it has made its way to an employee's personal device or account can be vexingly difficult, and may necessitate an expensive and time-consuming forensic investigation, court proceedings or both. Such was the case in RealPage Inc. v. Enter. Risk Control LLC, which arose after former employees founded a competing venture, allegedly using the plaintiff's source code. Following a discovery dispute, a court-ordered forensic investigation of defendants' devices revealed that one former employee had not deleted the source code from his personal devices following his departure, and that the defendants destroyed thousands of files after the lawsuit was filed. [2] This case illustrates the difficulty in controlling data once it leaves the company's devices and servers, and of proving what data has been taken or used when defendants delete data from their devices.

But the benefits of implementing cloud applications and platforms are such that companies have worked out various tools and methods to ensure they can have their cake and eat it too. While methods of protecting company information in the cloud are almost as numerous as the cloud services themselves, they typically fall into a handful of categories.

Site-Blocking Software

In response to the risks cloud storage poses to trade secrets, some companies utilize third-party software to block access to specific sites, including to cloud services. Among the problems with this approach is that there are too many cloud service applications out there to block. For example, in RLI Ins. Co. v. Elisabeth Banks, the plaintiff, RLI, equipped its computer system with Websense software that blocked access to various websites, including Dropbox.[3] The company alleged that, upon finding that Dropbox was blocked the defendant employee searched for Dropbox alternatives, found a Norwegian cloud service called "Jottacloud," opened a personal account, and proceeded to upload hundreds of company documents.[4] As RLI demonstrates, site-blocking software can only go so far. Moreover, there are other concerns with such an approach, including that it limits employees' abilities to use a diverse range of services for legitimate purposes. Thus, playing "whack-a-mole" by blocking various cloud services is unlikely to be successful on its own, as is any other purely technical solution.

Employee Agreements and Company Policies

Employee agreements and company trade secret and confidentiality policies deserve close attention when crafting a trade secret protection program intended to mitigate the risks created by cloud technologies. Such agreements and policies can serve as a first layer of defense and a basis for investigation and remedial action in cases of suspected trade secret misappropriation.

There is no "one size fits all" best practices for such agreements and policies. But case law has shown that inserting trade secret protection clauses in employee agreements can be key to enforcing trade

secret rights even in circumstances where an employee might argue that he acquired the trade secrets through proper means, such as during the course of work. For example, in Prominence Advisors Inc. v. Dalton, the court dismissed Prominence's claim of trade secret misappropriation, finding the employee had acquired information from the company's cloud-based systems during the course of his official duties.[5] However, because the company's employee agreement required the return of all company policy upon leaving the company, Prominence was still able to pursue a breach of contract claim.[6] The lesson here is clear: Even if a trade secret misappropriation or similar statutory or common law claim fails to protect a company's trade secrets, a well-crafted employee or confidentiality agreement may be a backstop to theft. Such provisions are a low-cost means of ensuring an additional layer of protection beyond what is provided by default under the law, and an important tool in trade secret protection.

Drafting employee agreements to protect trade secret information is all the more important because it remains unsettled what improper "acquisition" entails under the Computer Fraud and Abuse Act, or CFAA. The Second, Fourth and Ninth Circuits have held that the CFAA prohibits only unauthorized access to information. In these circuits, a defendant can use information however he chooses without CFAA liability as long as his access was authorized. By contrast, the First, Fifth and Eleventh Circuits have held that the CFAA may also cover the unauthorized use of information, even if the defendant was authorized to access it. Depending on the circuit in which a company resides, its claims could meet different outcomes under the CFAA.

For example, in Teva Pharmaceuticals USA Inc. v. Sandhu, an employee copied Teva files to her personal cloud and downloaded them to USBs. The Teva court found that a CFAA claim could not survive because the employee was authorized to access the information at the time that she made the copies.[7] Conversely, in Aquent LLC v. Stapleton, the court found that a CFAA claim could survive where the defendant began working for a competitor while still employed at Aquent, and downloaded Aquent data for subsequent use by the competitor. The defendant's Aquent offer letter expressly limited use of company confidential information within the scope of company duties. Consequently, the court found the allegations that she had exceeded her authorization by downloading company data for nonbusiness purposes to be a viable CFAA claim.[8]

Best Practices for Avoiding Cloud-Based Theft

Employers should employ an array of solutions to combat theft through cloud technology, taking a comprehensive approach that considers the particular character of the business and its employees. Some companies may be in a place to implement a more lenient, "trust but verify" type approach that provides more flexibility. Others, such as those with highly sensitive trade secrets (for example, the proverbial "recipe for Coca-Cola") may need to take a more restrictive approach that locks down access and limits flexibility for the sake of absolute security. In striking the appropriate balance, companies should consider the following tools and procedures:

1. Implement technical solutions when feasible. Blocking access to particular domains or services, or restricting access to certain files and repositories may be appropriate depending on the individual circumstances of the business.

2. Employ surveillance and monitoring tools to the extent appropriate for the business. Search out and monitor unusual download or computer behavior, especially when an employee has given notice of intent to work for a competitor or has been terminated.

3. Verify compliance with company confidential information and computer use policies (see below). After an employee departs, companies should assess the risks of potential theft and

consider investigating the employee's recent computer activity for illicit use of a personal cloud. While it is not practical to investigate every departing employee, suspicion of wrongdoing should trigger some level of investigation. Often, trade secret theft that goes undiscovered until too late could have been found by a prompt review of a departing employee's devices. In addition, upon employee departure or termination, company-owned employee cloud accounts should be promptly disabled and companies should verify that company data stored on employees' personal cloud accounts has been destroyed.

4. Implement and require employees to sign acknowledgement of a comprehensive written company policy that defines the scope of the company's and the employees' rights and obligations regarding trade secrets. This should contain both standard provisions regarding the company's trade secrets and specific provisions governing the use of cloud storage, company-issued devices and personal devices. Not only will such policies place employees on notice of their responsibilities, but they will place the company on firm footing when and if it ever must investigate or litigate trade secret theft.

5. Include trade secret provisions in employee agreements. Companies should consider incorporating the following into the company's standard employment agreement, its written company policies or both:

- Require employees to maintain company trade secret information as confidential, and prohibit disclosure of company trade secrets to third parties.
- Identify what company data can and cannot be transferred to the cloud.
- State whether employees are permitted to use personal devices to access company cloud services and whether use of personal cloud storage services to store company information is prohibited.
- Define the company's right to access, retain, destroy and/or delete data or information from an employee's personal devices and cloud accounts.
- Require employees to identify and provide login information for any personal cloud solutions used for work purposes.
- Specify a process for preserving and producing data from personal clouds.
- Require the return of all company information at the end of employment.

Because of the sheer number of cloud-storage applications available, combined with the many ways of using and accessing such applications, companies should implement policies that will provide multiple alternative remedies should data theft ever become a reality. A multiprong strategy that is tailored to the specific needs of a company is the best method for combating theft through cloud-storage services. As Benjamin Franklin famously said, "An ounce of prevention is worth a pound of cure."

Amy Van Zant is a partner and Evan Brewer and Margaret Wheeler Frothingham are managing associates at Orrick Herrington & Sutcliffe LLP.

[1] Frisco Med. Ctr. LLP v. Bledsoe, 147 F. Supp. 3d 646, 651 (E.D. Tex. 2015).

[2] RealPage Inc. v. Enter. Risk Control LLC, No. 4:16-CV-00737, 2017 WL 3313729 at *2-3 (E.D. Tex. Aug. 3, 2017).

[3] RLI Ins. Co. v. Banks, No. 1:14-CV-1108-TWT, 2015 WL 400540, at *2 (N.D. Ga. Jan. 28, 2015).

[4] Id.

[5] Prominence Advisors Inc. v. Dalton, No. 17 C 4369, 2017 WL 6988661 at *4 (N.D. Ill. Dec. 18, 2017).

[6] Id. at *3.

[7] Teva Pharm. USA Inc. v. Sandhu, 291 F. Supp. 3d 659, 671 (E.D. Pa. 2018).

[8] Aquent LLC v. Stapleton, 65 F. Supp. 3d 1339, 1346 (M.D. Fla. 2014).