

USDC SDNY DOCUMENT ELECTRONICALLY FILED DOC #: _____ DATE FILED: 4/5/2018
---

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

----- X  
 :  
 AUA PRIVATE EQUITY PARTNERS, LLC, :  
 :  
 :  
 Plaintiff, :  
 :  
 -v- :  
 :  
 ASTRID SOTO, :  
 :  
 Defendant. :  
 ----- X

1:17-cv-8035-GHW

MEMORANDUM OPINION AND  
ORDER

GREGORY H. WOODS, United States District Judge:

Sensing that her employment with Plaintiff AUA Private Equity Partners, LLC (“AUA”) was nearing its end, Ms. Astrid Soto uploaded AUA trade secrets from her work laptop to her personal Google Drive account. She wiped the laptop clean of any work-related files and cleared her browsing history. When Ms. Soto returned to the office the next business day, her premonition proved well-founded—she was terminated effective immediately. Nonetheless, Ms. Soto continued to represent herself as an AUA employee and refused to return AUA trade secrets in her possession. AUA brought this action, asserting claims against Ms. Soto under the Defend Trade Secrets Act (“DTSA”), 18 U.S.C. § 1836(b), and under New York state law for breach of contract and misappropriation. Ms. Soto has moved to dismiss the complaint in its entirety. Because the complaint plausibly alleges that Ms. Soto misappropriated AUA’s trade secrets by acquiring them through improper means, her motion to dismiss is DENIED.

## I. BACKGROUND

### A. Factual Background<sup>1</sup>

AUA, a Delaware limited liability company with its principal place of business in Manhattan, is a registered private equity firm that specializes in leveraged and management buyouts, growth equity investments, recapitalizations, and buy-and-build/roll-up investments in operationally focused lower-middle-market companies. Complaint, ECF No. 1 (“Compl.”) ¶¶ 3, 7. In March 2014, AUA hired Ms. Soto as the company’s Vice President of Business Development and Investor Relations. *Id.* ¶ 8 & Ex. A.

In connection with her employment, Ms. Soto agreed to abide by various confidentiality policies in place at AUA. Compl. ¶¶ 11-15. First, Ms. Soto agreed to the confidentiality provisions contained in her offer of employment. *Id.* ¶ 11. In signing that letter, Ms. Soto specifically agreed to the following:

By accepting employment with AUA, you understand and agree that you will be privy to certain confidential and proprietary information regarding transactions, investors and other valuable financial and other information regarding the Firm and its employees. In consideration of your employment and access to such confidential information, you agree that you will not during or after your employment with AUA use such information for any reason other than to further the business of AUA and its affiliates.

Compl. ¶ 11 & Ex. A at 2. Ms. Soto also executed an “Employee Acknowledgement of Receipt” of the AUA Supervisory Procedures and Compliance Manual (the “Compliance Manual”), acknowledging that she understood the Compliance Manual’s content and “agree[d] to the policies and procedures set forth therein.” Compl. ¶ 12 & Ex. B at 40. Among the provisions of the

---

<sup>1</sup> Unless otherwise noted, the facts are taken from the complaint and the documents attached thereto and are accepted as true for the purposes of this motion. *See, e.g., Chambers v. Time Warner, Inc.*, 282 F.3d 147, 152 (2d Cir. 2002). However, “the tenet that a court must accept as true all of the allegations contained in a complaint is inapplicable to legal conclusions.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009).

Compliance Manual by which Ms. Soto agreed to abide was AUA's email policy. As set forth in the Compliance Manual, that policy reads:

**8.2 Email Retention Policy.** AUA has implemented an "Email Retention Policy" whereby AUA will attempt to retain all emails and instant messages through the use of Global Relay, a third-party email archiving system. The Firm's Email Retention Policy is comprised of several factors:

- The [Chief Compliance Officer] is responsible for supervision of the policy;
- Employees must refrain from conducting business through any communications network not maintained by the investment adviser (e.g., outside email, instant messaging, or text messaging not provided by the Firm to the Employee or which cannot be captured under the email retention system);
- All electronic communications that fall within the applicable record keeping requirements are identified and preserved in the appropriate manner;
- The disposal of emails must be carried out in a way that protects confidentiality; and
- Training on the Email Retention Policy must be given upon employment and annually thereafter.

Compl. ¶ 13. Ms. Soto further agreed that she would not "engage in any activity that would increase the likelihood that AUA or the Clients of the Firm would be at risk for a cybersecurity event. *Id.* ¶ 14.

In addition to the Compliance Manual, Ms. Soto also agreed to "maintain the confidentiality of any information concerning the Firm . . . in a manner consistent with the confidentiality obligations detailed in" AUA's Employee Policies and Procedures Handbook ("Policies and Procedures"). *Id.* ¶ 14 & Ex. C. at 43. The Policies and Procedures prohibited "[d]isclosure of the Firm's confidential information to anyone outside the Firm and use of the Firm's intellectual property for matters unrelated to the Firm's business." Compl. ¶ 15 & Ex. C at 35. The Policies and Procedures also forbid employees from "commingl[ing] personal property with Firm property," from "download[ing] or transfer[ring] work product or sensitive business content to [the

employee's] device,” and from “back[ing] up [the employee's] device locally or to cloud-based storage or services without the Firm's consent.” Compl., Ex. C. at 27, 34-35.

During the course of Ms. Soto's employment with AUA, she was given access to “high level” confidential information, AUA trade secrets, and other proprietary information, including confidential internal strategic information, confidential investor information, and other confidential information related to AUA's business. Compl. ¶ 9. That information, if improperly disseminated, was capable of harming AUA's business, including by depriving the company of its competitive advantage and by damaging AUA's “position and credibility in the marketplace.” *Id.* ¶ 17.

At some point during her employment, Ms. Soto forwarded emails from her AUA email account to her personal email address. *Id.* ¶ 20. Some of those emails included copies to Karen Kulaga, a former AUA employee now employed by a competitor. *Id.* ¶ 21.

On Friday, September 8, 2017, seemingly in anticipation of her termination, Ms. Soto accessed her Google Drive account for what AUA alleges on information and belief to be the purpose of uploading proprietary AUA files from Ms. Soto's laptop to her personal Google account. *Id.* ¶¶ 29-30. Ms. Soto then deleted all local files contained on her laptop computer, as well as her browser history prior to September 7, 2017. *Id.* ¶ 29.<sup>2</sup>

On the following Monday, September 11, 2017, AUA terminated Ms. Soto's employment. *Id.* ¶ 18. On the same date, AUA ended Ms. Soto's access to her AUA email account and instructed her to return all AUA property, including her building pass and office and restroom keys. *Id.* Ms. Soto, however, did not return all of her AUA property and continued to represent herself as an AUA employee, including on her LinkedIn profile page. *Id.* ¶ 19.

---

<sup>2</sup> The complaint does not allege the date on which Ms. Soto deleted the files and browser history from her laptop. The complaint does allege, though, that Ms. Soto uploaded files from the laptop to her Google Drive account on September 8, 2017, prior to deleting the files from the computer. Compl. ¶ 30. The complaint also alleges that it was the browser history prior to September 7, 2017 that was deleted. *Id.* ¶ 29. Based on these allegations, it is reasonable to infer that the files and browsing history were deleted on or around September 8, 2017.

On September 19, 2017, AUA sent Ms. Soto a letter asking that she immediately cease holding herself out to be an AUA employee and that she return all company property no later than the following day. *Id.* ¶ 22 & Ex. E. In that letter, AUA also reminded Ms. Soto of her confidentiality obligations. Compl. ¶ 23.

AUA received no response from Ms. Soto and, on September 29, 2017, followed-up with a cease-and-desist letter. *Id.* ¶ 24. The September 29 letter informed Ms. Soto of her ongoing confidentiality breaches, in violation of her offer letter, the Compliance Manual, and the Policies and Procedures. *Id.* ¶ 24 & Ex. F. Five days later, counsel for Ms. Soto responded to the cease-and-desist letter and acknowledged that Ms. Soto “was in possession of” documents and information belonging to AUA. *Id.* ¶ 25. Nonetheless, Ms. Soto never returned the sensitive and confidential information of AUA that she possessed. *Id.* ¶¶ 25, 31. In October 2017, AUA performed a forensic search of Ms. Soto’s work laptop and discovered the emails she had forwarded to her personal accounts, the files deleted from her computer, and her September 8, 2017 access of her Google Drive account. *Id.* ¶¶ 20, 29.

Ms. Soto continues to possess information belonging to AUA, including AUA investor reports, investor contact information, investor commitment amounts, and other documents and information containing AUA trade secrets, all of which is used in connection with AUA’s services that are offered nationally and globally. *Id.* ¶¶ 10, 35. AUA has not authorized Ms. Soto’s possession of this information, nor has AUA consented to her use of the information in her personal email accounts. *Id.* ¶¶ 1, 44. Instead, AUA believes that Ms. Soto “is retaining and using that information to compete with and/or to otherwise harm AUA.” *Id.* ¶ 41.

## **B. Procedural History**

AUA commenced this action on October 18, 2017, bringing claims against Ms. Soto under the Defend Trade Secrets Act (“DTSA”), 18 U.S.C. § 1836(b)(1), and under New York state law for

breach of contract and misappropriation. ECF No. 1. On October 19, 2017, AUA applied for a temporary restraining order and preliminary injunction enjoining Ms. Soto from accessing, disclosing, or in any way using any of the trade secrets and other confidential AUA information that she possessed. ECF No. 5. The Court granted that motion and issued a temporary restraining order against Ms. Soto on October 24, 2017, and a preliminary injunction on November 6, 2017. ECF Nos. 12, 17.

On December 5, 2017, Ms. Soto moved to dismiss the complaint, arguing that AUA has failed to properly plead a violation of the DTSA. ECF No. 29. In that motion, Ms. Soto alternatively moves for summary judgment. *See id.* AUA opposed the motion on January 4, 2018, and Ms. Soto filed a reply on January 12, 2018. ECF Nos. 36, 38.

## **II. LEGAL STANDARD**

### **A. Rule 12(b)(6)**

Under Federal Rule of Civil Procedure 8(a)(2), a complaint must contain “a short and plain statement of the claim showing that the pleader is entitled to relief.” Fed. R. Civ. P. 8(a)(2). Rule 8 “does not require ‘detailed factual allegations,’ but it demands more than an unadorned, the-defendant-unlawfully-harmed-me accusation.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007)). To survive a motion to dismiss under Federal Rule of Civil Procedure 12(b)(6), “a complaint must allege sufficient facts, taken as true, to state a plausible claim for relief.” *Johnson v. Priceline.com, Inc.*, 711 F.3d 271, 275 (2d Cir. 2013) (citing *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555-56 (2007)). To determine plausibility, courts follow a “two-pronged approach.” *Ashcroft v. Iqbal*, 556 U.S. 662, 679 (2009). “First, although a court must accept as true all of the allegations contained in a complaint, that tenet is inapplicable to legal conclusions, and threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice.” *Harris v. Mills*, 572 F.3d 66, 72 (2d Cir. 2009) (alterations and internal

quotation marks omitted) (quoting *Iqbal*, 556 U.S. at 678). Second, a court determines “whether the ‘well-pleaded factual allegations,’ assumed to be true, ‘plausibly give rise to an entitlement to relief.’” *Hayden v. Paterson*, 594 F.3d 150, 161 (2d Cir. 2010) (quoting *Iqbal*, 556 U.S. at 679). Determining whether a complaint states a plausible claim is a “context-specific task that requires the reviewing court to draw on its judicial experience and common sense.” *Iqbal*, 556 U.S. at 679. Rule 8’s pleading standard applies to claims brought under the DTSA. See *Tesla Wall Sys., LLC v. Related Cos., L.P.*, No. 17-cv-5966 (JSR), 2017 WL 6507110, at \*10 (S.D.N.Y. Dec. 18, 2017) (“[T]here is no heightened pleading requirement on actions brought under the DTSA.”); accord *Chubb Ina Holdings, Inc. v. Chang*, No. 16-cv-2354 (BRM) (DEA), 2017 WL 499682, at \*10 (D.N.J. Feb. 7, 2017); *Mission Measurement Corp. v. Blackbaud, Inc.*, 216 F. Supp. 3d 915, 921 (N.D. Ill. 2016).

“In considering a motion to dismiss for failure to state a claim pursuant to Rule 12(b)(6), a district court may consider the facts alleged in the complaint, documents attached to the complaint as exhibits, and documents incorporated by reference in the complaint.” *DiFolco v. MSNBC Cable L.L.C.*, 622 F.3d 104, 111 (2d Cir. 2010) (citations omitted). “Where a document is not incorporated by reference, the court may never[the]less consider it where the complaint ‘relies heavily upon its terms and effect,’ thereby rendering the document ‘integral’ to the complaint.” *Id.* (quoting *Mangiafico v. Blumenthal*, 471 F.3d 391, 398 (2d Cir. 2006)). Finally, the Court may also consider “matters of which judicial notice may be taken.” *Goel v. Bunge, Ltd.*, 820 F.3d 554, 559 (2d Cir. 2016) (citation omitted).

### **III. DISCUSSION**

AUA brings claims against Ms. Soto for violations of the DTSA, breach of contract, and misappropriation. Ms. Soto moves to dismiss the DTSA claim and requests that the Court decline to exercise supplemental jurisdiction over the state law claims.

### A. AUA's DTSA Claim

The DTSA, enacted on May 11, 2016, provides a private cause of action to the “owner of a trade secret that is misappropriated.” 18 U.S.C. § 1836(b)(1). This cause of action is available only in connection with those acts of misappropriation that occurred on or after the date of the Act’s enactment. *See* Defend Trade Secrets Act of 2016, Pub. L. 114-153, 130 Stat. 376, 381-82 (“The amendments made by this section shall apply with respect to any misappropriation of a trade secret . . . for which any act occurs on or after the date of the enactment of this Act.”); *RCC Ventures, LLC v. Am. DG Energy, Inc.*, No. 17-cv-3007 (AJN), 2018 WL 1415219, at \*2 (S.D.N.Y. Mar. 19, 2018); *Yager v. Vignieri*, No. 16-cv-9367 (DLC), 2017 WL 4574487, at \*3 (S.D.N.Y. Oct. 12, 2017).

A “trade secret” includes “all forms and types” of information that “derives independent economic value . . . from not being generally known” and that the owner of which took reasonable measures to keep secret. 18 U.S.C. § 1839(3). The DTSA defines “misappropriation” to include “acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means” or “disclosure or use of a trade secret of another without express or implied consent” in specified circumstances. 18 U.S.C. § 1839(5). “Improper means” under the Act includes “theft, bribery, misrepresentation, [and] breach or inducement of a breach of a duty to maintain secrecy,” but excludes “reverse engineering, independent derivation, or any other lawful means of acquisition.” 18 U.S.C. § 1839(6). The DTSA, thus, “contemplates three theories of liability: (1) acquisition, (2) disclosure, or (3) use.” *Cave Consulting Grp., Inc. v. Truven Health Analytics Inc.*, No. 15-cv-2177 (SI), 2017 WL 1436044, at \*4 (N.D. Cal. Apr. 24, 2017); *accord Physician’s Surrogacy, Inc. v. German*, No. 17-cv-718 (MMA) (WVG), 2017 WL 3622329, at \*8 (S.D. Cal. Aug. 23, 2017).

Ms. Soto does not contest AUA’s allegations with respect to whether they sufficiently plead a trade secret, as that term is defined in the DTSA. Therefore, for purposes of this motion, the



Court assumes that the complaint sufficiently pleads that the confidential information at issue constitutes trade secrets.

Ms. Soto's sole attack on the sufficiency of AUA's DTSA claim is made on the grounds that the complaint fails to sufficiently plead that Ms. Soto used or disclosed AUA's trade secrets. This argument, however, ignores the Act's complete and disjunctive definition of "misappropriation." That definition includes acquisition of a trade secret of another by improper means *or* disclosure or use of the trade secret. *See* 18 U.S.C. § 1839(5). Disclosure or use is not a required element of misappropriation, but rather an alternative basis for liability under the Act. *See Yager*, 2017 WL 4574487, at \*3 (explaining that "misappropriation" under the DTSA is "*either* 'acquisition of a trade secret by a person who knows or has reason to know that the trade secret was acquired by improper means,' *or* 'disclosure of use of a trade secret of another without express or implied consent'" (emphasis added)); *Cave Consulting Grp.*, 2017 WL 1436044, at \*4 (noting that misappropriation through acquisition is a separate basis for liability). Therefore, AUA is not required to plead disclosure or use of a trade secret to survive dismissal; the complaint survives a motion to dismiss if it plausibly pleads an improper acquisition of trade secrets occurring on or after the effective date of the DTSA, *i.e.*, May 11, 2016.<sup>3</sup>

---

<sup>3</sup> Ms. Soto argues that improper use or disclosure is a "necessary" element of a DTSA claim. *See* Def.'s Mem. in Supp. of Mot. to Dismiss, ECF No. 31 ("Def.'s Mem.") at 2. Ms. Soto relies in part on a decision from this district in *Free Country Ltd. v. Drennen*. In *Free Country*, however, the court found that the plaintiff failed to show a likelihood of success on the merits of its DTSA claim in the context of a preliminary injunction motion because the plaintiff's allegations failed to plead that the information at issue qualified as a "trade secret" under the Act and failed to plead that the defendant had "stolen" any proprietary information. 235 F. Supp. 3d 559, 566-67 (S.D.N.Y. 2016). The Court does not read *Free Country* to support the proposition that a defendant's use or disclosure of trade secrets is a required element to state a DTSA claim, rather than simply one avenue by which liability may be pleaded.

Similarly, Ms. Soto's reliance on *Singer v. Stuerke* for the same proposition is misplaced. Ms. Soto contends that *Singer* "held improper use or disclosure [is a] necessary element of [a] DTSA claim." Def.'s Mem. at 2. But, again, this is a misleading misreading of the case. The issue in *Singer* was whether the information constituted a "trade secret" under the DTSA. *Singer v. Stuerke*, No. 16-cv-2526 (KJD) (GWF), 2017 WL 2603305, at \*3 (D. Nev. June 14, 2017). The court's focus was on the requirement that a trade secret be subject to "reasonable measures to keep such information secret." *Id.* In discussing the plaintiff's allegations in this regard, the court stated the following:

Petitioners have not alleged provisions in the [ ] Agreement . . . that serve to

The complaint alleges that Ms. Soto signed a variety of confidentiality agreements upon her hiring. By signing those agreements, Ms. Soto was bound by a contractual duty to abide by their terms, including compliance with the Email Retention Policy and with the provisions of the Policies and Procedures that prohibited employees from transferring work-related information to their personal devices and from uploading business information to cloud-based storage. Despite this duty to maintain the secrecy of AUA’s trade secrets, and in direct violation of the confidentiality agreements, Ms. Soto is alleged to have uploaded proprietary AUA files to her personal Google Drive account on September 8, 2017—an act alleged to have occurred after the DTSA was enacted.<sup>4</sup> The complaint also alleges that Ms. Soto has not returned those trade secrets. These allegations plausibly plead that Ms. Soto acquired the trade secrets by improper means.

The DTSA does not define the term “acquisition.” Therefore, to determine whether AUA has plausibly alleged that Ms. Soto’s uploading of the trade secrets to her personal Google Drive was an “acquisition” under the Act, the Court must look to the plain-language meaning of that term. *See Chen v. Major League Baseball Props., Inc.*, 798 F.3d 72, 76 (2d Cir. 2015) (“When construing a statute, we begin with its language and proceed under the assumption that the statutory language, unless otherwise defined, carries its plain meaning . . .”). Black’s Law Dictionary defines “acquisition” as

---

protect proprietary trade secrets from improper disclosure. To allege that trade secrets were misappropriated, requires factual assertions that disclosure or use of a trade secret was without consent by a person who knew of “a duty to maintain the secrecy of the trade secret or limit the use of the trade secret.” On the basis of this deficiency, the Petitioners’ seventh claim for relief is invalid because it fails to allege reasonable measures to keep the information secret.

*Id.* Read in context, the court’s comment regarding the requirement of allegations of use or disclosure was not meant to be a recital of the “necessary” elements of a DTSA claim; rather, it was an explanation of the complaint’s failure in that case to sufficiently plead that the plaintiff had taken reasonable measures to keep the information in question safe.

<sup>4</sup> Although the complaint alleges that Ms. Soto emailed AUA trade secrets to her personal email accounts, also in violation of the confidentiality and other agreements executed by her, the complaint fails to allege the specific dates of those emails. The Court is unable, therefore, to determine whether those emails are alleged to have been sent on or after the effective date of the DTSA.

“the gaining of possession or control over something.” *Acquisition*, Black’s Law Dictionary (10th ed. 2014). “Possession,” in turn, is defined as “the fact of having or holding property in one’s power; the exercise of dominion over property”; “the right under which one may exercise control over something to the exclusion of all others”; or “the detention or use of a physical thing with the intent to hold it as one’s own.” *Possession*, Black’s Law Dictionary (10th ed. 2014). And “control” is “the power or authority to manage, direct, or oversee.” *Control*, Black’s Law Dictionary (10th ed. 2014).

Here, the complaint’s allegations do not plausibly plead that Ms. Soto had possession or exercised control over AUA’s trade secrets prior to her uploading of those secrets to her personal Google account. Rather, the complaint alleges that “AUA gave [Ms. Soto] *access to* its confidential and proprietary information for the sole purpose of performing her job duties.” Compl. ¶ 16 (emphasis added). The confidentiality agreements that Ms. Soto signed also characterize her relationship to the trade secrets as one of mere “access.” The offer letter states that Ms. Soto would be “privy to” and have “access to” confidential information. *Id.* ¶ 11. Similarly, the Policies and Procedures describe the trade secrets as belonging to AUA, despite employees’ use of the information in the course of their employment. *Id.* ¶ 15. These allegations do not suggest that Ms. Soto held the trade secrets as her own, or that she exercised dominion over them and the ability to exclude others from their use, or that she otherwise had the authority to manage, direct, or oversee the information. To the contrary, the complaint alleges that the trade secrets at issue were controlled by AUA and were meant to remain at all times within AUA’s possession and control by being stored exclusively on AUA-registered devices. *See* Compl., Ex. C at 34 (“All devices used for or on behalf of the Firm must be registered with and authorized by Andy Unanue, Managing Partner.”). Thus, as alleged, prior to transferring the data to her own personal Google Drive account, which Ms. Soto impliedly controlled, Ms. Soto had not “acquired” the trade secrets under the plain meaning of that term.

This construction of the term “acquisition” is supported by the DTSA’s legislative history and the case law interpreting the term in other trade secrets statutes. The DTSA “models its definition of ‘misappropriation’ on the Uniform Trade Secrets Act.” H.R. Rep. No. 114-529, at 1 (2016). The Uniform Trade Secrets Act (“UTSA”) defines “misappropriation” based on acquisition of a trade secret in terms identical to those of the DTSA. *See* Unif. Trade Secrets Act § 1(2) (Nat’l Conference of Comms. on Unif. State Law 1985). Therefore, it is instructive to examine the meaning of “misappropriation” as that term is used in the UTSA. The UTSA has been adopted, in one form or another, by nearly every state. *See* Unif. Law Comm., *Trade Secrets Act, Legislative Tracking*, <http://www.uniformlaws.org/Act.aspx?title=Trade%20Secrets%20Act> (last visited Apr. 4, 2018). Courts evaluating claims for misappropriation of trade secrets under the various state UTSA that define “misappropriation” in terms nearly identical to the DTSA have found that liability attaches to employees who, like Ms. Soto, abscond with their employers’ trade secrets, even in the absence of any subsequent use or disclosure of the information.

The Northern District of Illinois, for example, found that an employee was liable under the Illinois Trade Secrets Act for misappropriating his employer’s trade secrets when, during his employment, the employee “downloaded, copied, or otherwise transmitted” the trade secrets “for purposes other than serving the interests of” his employer. *RKI, Inc. v. Grimes*, 177 F. Supp. 2d 859, 875 (N.D. Ill. 2001).<sup>5</sup> The court explained that it reached its conclusion in part because of evidence that the employee accessed work computers after business hours from his home computer, and later deleted large quantities of information from his home computer and defragmented his personal

---

<sup>5</sup> The Illinois Trade Secrets Act defines acquisition-based misappropriation in terms very similar to the DTSA. “Misappropriation” is defined as the “acquisition of a trade secret of a person by another person who knows or has reason to know that the trade secret was acquired by improper means.” Ill. Trade Secrets Act, 765 Ill. Comp. Stat. Ann. 10625 (“ITSA”) § 2(b). “Improper means” include “theft, bribery, misrepresentation, breach or inducement of a breach of a confidential relationship or other duty to maintain secrecy or limit use, or espionage through electronic or other means.” ITSA § 2(a).

computer despite the fact that “no mechanical or engineering reason required it.” *Id.* at 875. The court also noted that the employee’s “spoliation of evidence on [his] computer support[ed] a negative inference that [he] destroyed evidence of misappropriation.” *Id.* at 877 (citing *Minnesota Mining & Mfg. Co. v. Pribyl*, 259 F.3d 587, 606 n.5 (7th Cir. 2001)); *see also Liebert Corp. v. Mazur*, 827 N.E.2d 909, 926-27 (Ill. App. Ct. 2005) (finding acquisition by improper means when employee downloaded trade secrets onto his laptop in violation of a confidentiality policy hours before resigning and then “attempted to destroy any indication of his downloading activities”).

Similarly, the Court of Appeals of Maryland found sufficient evidence of acquisition by improper means when an employee, on the last day of his employment, transferred specific, confidential documents of his employer from his work laptop to a CD that the employee “intended to keep for his personal use.” *LeJeune v. Coin Acceptors, Inc.*, 849 A.2d 451, 467 (Md. 2004).<sup>6</sup> Like the employee in *RKI*, the *LeJeune* employee deleted hundreds of files from the laptop, which the court found suggestive of an attempt “to hide [the employee’s] conduct” and also evidence that the employee was “aware that transferring the files was improper.” *Id.* Notably, the *LeJeune* court rejected the employee’s argument that his acquisition of the trade secrets was proper because they had been provided to him by his employer during the course of his employment. *Id.* at 466.

Misappropriation by acquisition has been found under other state UTSA’s in similar circumstances. *See, e.g., Minuteman, Inc. v. Alexander*, 434 N.W.2d 773, 847-49, 854-55 (Wisc. 1989) (finding misappropriation of a trade secret under Wisconsin’s UTSA—which defines

---

<sup>6</sup> The Maryland Uniform Trade Secrets Act defines “misappropriation” to include “acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means.” Md. Unif. Trade Secrets Act, Md. Code Ann., Commercial Law § 11-1201(c). “Improper means” includes theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means.” *Id.* § 11-1201(b).

misappropriation as “acquiring the trade secret of another by means which the person knows or has reason to know constitute improper means”—when employee resigned from his employment and took without using his employer’s secret formula without employer’s permission); Jane Osborne McKnight, *Disloyal Employees and Trade Secrets: What We Can Learn from Barbies and Bratz*, 34 Vt. B.J. 38 (2008) (“If the employee takes trade secret materials with him at the time of his departure from employment, he has acquired the trade secrets, ‘by improper means.’”); *cf. Gallagher Benefit Servs., Inc. v. De La Torre*, 283 F. App’x 543, 545 (9th Cir. 2008) (concluding that district court abused its discretion in finding a likely misappropriation of trade secrets under California’s Uniform Trade Secrets Act, despite allegations that former employee “accessed and likely copied a large volume of computer files from his [employer]-issued laptop before he resigned,” only because there was no evidence that the computer files were trade secrets).

Because Ms. Soto is alleged to have uploaded AUA trade secrets from her work laptop to her personal cloud-based storage without AUA’s permission and in direct violation of the confidentiality agreements that she signed, the complaint plausibly alleges that she acquired the trade secrets by improper means, *i.e.*, theft and in breach of her duty to maintain secrecy. *See RKI*, 177 F. Supp. 2d at 875-77 (finding sufficient evidence of acquisition by theft when employee downloaded or copied trade secrets from work computer to home computer). Therefore, the complaint states a claim for misappropriation under the DTSA.<sup>7</sup>

---

<sup>7</sup> Ms. Soto is correct in that the allegations regarding emails sent by Ms. Soto with copies to AUA’s former employee are by themselves insufficient to state a claim under the DTSA under a disclosure-liability theory. Those allegations contain no information regarding the dates on which the emails were sent. Drawing all reasonable inferences in favor of AUA, the only conclusion that the Court may draw with respect to the dates of those emails is that they were sent on or before Ms. Soto’s termination, given that her email access was also terminated at that time. *See* Compl. ¶ 18. However, because Ms. Soto was hired in 2014, it is plausible that all of the emails at issue were sent well before the DTSA’s effective date. In the absence of more specific allegations, the complaint fails to state a claim under the DTSA predicated on Ms. Soto’s improper disclosure of the alleged trade secrets.

## **B. AUA's State Law Claims**

Because the Court has not dismissed AUA's federal claim, and Ms. Soto has not moved to dismiss the state law claims on any basis other than her request that the Court decline to exercise pendent jurisdiction over them, AUA's state law claims survive.

## **C. Motion for Summary Judgment**

Ms. Soto asserts that this case may appropriately be decided on summary judgment as an alternative to a disposition on the pleadings. The record that Ms. Soto claims has been sufficiently developed thus far includes the submissions and arguments made in connection with AUA's preliminary injunction motion.

It is true that "a party may file a motion for summary judgment at any time until 30 days after the close of all discovery." Fed. R. Civ. P. 56(b). However, "[t]he nonmoving party must have 'had the opportunity to discover information that is essential to his opposition' to the motion for summary judgment." *Trebor Sportswear Co., Inc. v. The Limited Stores, Inc.*, 865 F.2d 506, 511 (2d Cir. 1989). The Court declines at this time to decide Ms. Soto's motion for summary judgment. The motion was filed prior to the close of discovery, and it is unlikely that AUA had sufficient opportunity at that time to discover the information relevant and essential to its opposition.<sup>8</sup> The Court expects to consider any summary judgment motions brought by the parties on the basis of the record as fully developed through the discovery process.

## **IV. CONCLUSION**

For the reasons stated herein, Defendant's motion to dismiss the complaint is DENIED.

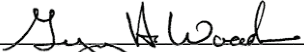
---

<sup>8</sup> Rule 2(C) of the Court's Individual Rules of Practice in Civil Cases also requires that a party who intends to bring a summary judgment motion file a pre-motion submission. Ms. Soto's pre-motion letter did not address an anticipated summary judgment motion, but requested leave only to file a motion to dismiss the complaint. *See* ECF No. 19.

The Clerk of Court is directed to terminate the motion pending at Dkt. No. 29.

SO ORDERED.

Dated: April 5, 2018  
New York, New York

  
\_\_\_\_\_  
GREGORY H. WOODS  
United States District Judge