Published on *The National Law Review* https://natlawreview.com

Employees Who Download Trade Secrets As They Head Out the Door Can Be Guilty of TS Theft, Even Before They Make Use of the Information

Article By:

Business Litigation at Womble Bond Dickinson

When a high-level employee leaves the company, downloads sensitive company trade secrets on her way out, but hasn't yet *used* or *disclosed* the info to a new employer, what options does the company have to keep the information confidential?

Before the 9th Circuit's *Nosal* and the 4th Circuit's *WEC Carolina Energy* decisions last year derailed the argument, companies in these situations often asserted Computer Fraud and Abuse Act ("CFAA") violations, claiming the employees were not authorized to download the information for a non-company use. Others asserted claims for breach of confidentiality contracts or utilized the oft-debated inevitable disclosure doctrine. A recent Eastern District of Virginia case reminds us that we should also consider a trade secret misappropriation claim, even if there is little or no evidence of actual use or disclosure yet.

In *Marsteller v. ECS Federal, Inc.*, Electronic Consulting Services ("ECS") terminated Jacqueline Marsteller, a Senior VP and Account Exec. So that Marsteller would remain eligible for a $94,000 end-of-the-year bonus, ECS set the effective date of the termination about 6 weeks after they gave her the notice. During those few weeks, Marsteller allegedly downloaded or emailed to her personal account sensitive company documents regarding company contracts and billing rates, a business development pipeline, internal strategy documents called "Capture Plans," as well as other confidential documents.

ECS asserted claims for trade secret misappropriation under the Virginia Uniform Trade Secret Act ("VUTSA"), computer trespass in violation of the Virginia Computer Crimes Act, breach of contract, conversion, breach of fiduciary duty, and unjust enrichment.

Marsteller moved to dismiss all claims, asserting among other defenses that ECS did not adequately allege facts showing she misappropriated the information by using it. Except for the unjust enrichment claim, the Court denied the motion to dismiss.

On the misappropriation claim, the Court noted that:

> the improper acquisition of a trade secret, even in the absence of allegations of use or disclosure, is sufficient to state a claim

under the Virginia Uniform Trade Secret Act. *See* Va. Code Ann. § 59.1-336. Under the Uniform Trade Secret Act ("UTSA"), misappropriation through acquisition occurs when a person "knows or has reason to know that the trade secret was acquired by improper means." "Improper means" include "theft, bribery, misrepresentation, *use of a computer or a computer network without authority*, breach of a duty or inducement of a breach of duty to maintain secrecy, or espionage through electronic or other means."

On the "improper means" prong, ECS alleged the following in its Counterclaim:

- Marsteller transferred highly sensitive and confidential ECS documents to an external storage device;
- At the time she transferred the information to the devices, Marsteller was not engaged in any work-related activities on behalf of ECS which would have required her to access the information or to transfer it to an external storage device outside of the control of ECS;
- Marsteller was not authorized to transfer the information to any external storage device;
- The stolen documents resided on an ECS password-protected server not shared with or known by the public.

Relying on the definition of misappropriation under the UTSA, the court found these allegations sufficient to state a "plausible claim" for misappropriation through improper acquisition. In full disclosure, the court went on to say that ECS had also presented plausible allegations that Marsteller*used* the info for her new employer to help them obtain ISO certification. The opinion, however, implies that either scenario alone may have been sufficient to state a claim.

Although North Carolina is not one of the 47 states who has officially adopted UTSA, North Carolina's Trade Secret Protection Act shares a lot of similarities with UTSA, including defining misappropriation to include the acquisition of a trade secret without implied or express authority. Specifically, N.C. Gen. Stat. sec 66-152(1) defines a "misappropriation" as an "***acquisition***, disclosure, or use of a trade secret of another without express or implied authority or consent. . . ."

To establish a prima facie case of misappropriation through acquisition in North Carolina, N.C. Gen. Stat. sec. 66-155 requires a claimant to introduce:

> substantial evidence that the person against whom relief is sought both: (1) knows or should have known of the trade secrets; and (2) has had a ***specific opportunity to acquire it for disclosure or use*** or has acquired, disclosed, or used it without the express or implied consent or authority of the owner.

Bridgetree, Inc. v. Red F Marketing LLC, a Western District case decided earlier this year, is a good example of a North Carolina court applying the misappropriation by acquisition definition. The court found the circumstantial evidence presented overwhelmingly supported the jury's verdict finding of misappropriation of trade secrets. The defendant downloaded trade secrets from his employer's servers to a one-terabyte flash drive following his resignation. The downloading coupled with subsequent spoliation of evidence on his company-owned computer and his personal family computer previously used for work provided sufficient circumstantial evidence that defendant "acquired" the trade secrets "for disclosure or use."

These cases demonstrate the importance of performing a forensic analysis on key employees' electronic devices when they depart (or perhaps sooner). Evidence that an employee downloaded any documents containing your trade secrets to an external device when the transfer could not have been for your company's benefit may state a claim for trade secret misappropriation — even before the employee uses that information for a new employer.

National Law Review, Volume III, Number 282