What to Do When a Departing Employee Downloads Information

Prepared by:
William R. Sylvester, Esq. and Timothy Wagner
Baker, Donelson, Bearman, Caldwell & Berkowitz, PC

LORMAN®

Published on www.lorman.com - June 2022. "This article was originally published by Foley & Lardner LLP - https://www.foley.com/en/insights/publications/2021/06/what-to-do-when-departing-employee-downloads-info on 6/14/21. It is republished here with permission."

LORMAN®

Lorman Education Services is a leading provider of online professional learning, serving individuals and teams seeking training and CE credits. Whether you're looking for professional continuing education or an enterprise-wide learning and development solution, you will find what you need in Lorman's growing library of resources.

Lorman helps professionals meet their needs with more than 100 live training sessions each month and a growing collection of over 13,000 ondemand courses and resources developed by noted industry experts and professionals.

Learn more about Lorman's individual programs, economical All-Access Pass, and Enterprise Packages:

www.lorman.com

What to Do When a Departing Employee Downloads Information

Author(s): Bennett L. Epstein

The day after an employee's last workday, you get around to checking his email and learn that he has downloaded and transmitted company and client documents to his personal cloud storage account. What weapons do you have in your legal quiver to compel the employee to return or delete those documents? Until recently, employment and data security lawyers would tell you that the employee is at risk of violating the federal Computer Fraud and Abuse Act (CFAA), which provides both criminal penalties and a civil cause of action. Among other things, the CFAA prohibits persons who are authorized to access computer files from exceeding their authority. It appears that your former employee clearly exceeded his authority when he downloaded documents on the way out the door. However, the U.S. Supreme Court begs to differ.

In a case decided last week (*Van Buren v. United States*), the Court held that persons who were authorized to access computer files do not necessarily violate the CFAA by accessing the information for a purpose that exceeds their authority. In that case, the Court decided that a police officer who was permitted to access the department's data files for law enforcement purposes did not violate the CFAA when he received $6,000 from an undercover police officer to check whether another person

was also an undercover police officer. The majority of the justices expressed concern that the broad application of the CFAA could lead zealous law enforcement officers to prosecute otherwise law-abiding citizens who make trivial personal use of computer data that they were otherwise authorized to access.

While the *Van Buren* case was decided in the context of a criminal appeal, limitations imposed by the Court also significantly reduce the scope of the CFAA in a civil case. No longer will employers confidently be able to rely on the CFAA when suing employees who misappropriate trade secrets or proprietary information to which they have access, by downloading them from the company's server.

However, rest assured that companies are not left without recourse. There are other actions to be taken, provided that companies take the appropriate precautions. Companies should enter into agreements requiring employees to return or delete company information upon demand or upon termination of employment. They also should require employees to sign a confidentiality or nondisclosure agreement upon the commencement of employment. HR departments should regularly audit personnel files to make sure that each employee who has access to company information has a signed nondisclosure agreement in his file. An even better practice is to require employees to install software on their cell phones enabling the employer to delete company information remotely.

In addition to confidentiality and deletion of information agreements, companies should have policies and agreements

clearly defining what areas of the computer system particular employees are authorized to access. Remember – the *Van Buren* decision applies to circumstances in which an employee is otherwise authorized to access certain information; when an employee does not have such access, CFAA remedies may still apply.

At exit interviews, HR should require employees to sign a form confirming that they did not take any company information and that they have deleted or returned any information that they legitimately have on personal data storage devices or in their cloud accounts. By taking such steps, employers can enforce contractual rights.

Even in the absence of a confidentiality agreement or a computer usage policy, most states have enacted the Uniform Trade Secrets Act, which provides claims and remedies for the misappropriation of trade secrets. In 2016, Congress enacted the Defend Trade Secrets Act, which for the first time created a federal claim against persons who misappropriate trade secrets, provided that the company maintains policies and agreements required by the statute.

While the Supreme Court significantly limited the use of the CFAA as a means of punishing employees who wrongfully use their employer's computer systems to take information that they are not authorized to take, many potential claims remain.

LORMAN®

2510 Alpine Road Eau Claire, WI 54703
www.lorman.com 866-352-9539 customerservice@lorman.com