The Computer & Internet Lawyer

Volume 38 ▲ Number 9 ▲ October 2021

Ronald L. Johnston, Arnold & Porter, Editor-in-Chief

Employees Do Not "Exceed Authorized Access" by Misusing Computer Data They Are Otherwise Authorized to Access, U.S. Supreme Court Rules

By Damien P. DeLaney and Brian M. Noh

The scenario is familiar, and frustrating, to employers: An employee, preparing to leave to join a competitor, accesses sensitive product, customer, and sales data using his or her own credentials, copies it to a flash drive, and takes it to a competing firm. Employers have had a variety of legal tools available to take action in response, but one previously potent tool is now seemingly off the table due to a June 3, 2021 opinion by the U.S. Supreme Court. That decision, *Van Buren v. United States*, reminds employers that litigation, even under expansive anti-hacking statutes such as the Computer Fraud and Abuse Act ("CFAA"), is no substitute for strong preventative actions to protect sensitive competitive information.

Damien P. DeLaney, a partner in the Los Angeles office of Akerman LLP, focuses his practice on employment litigation. **Brian M. Noh**, an associate in the firm's Los Angeles office, focuses his practice on labor and employment counseling and litigation. The authors may be contacted at *damien.delaney@akerman.com* and *brian.noh@akerman.com*, respectively.

Background

Although *Van Buren* was a criminal case, its facts will be familiar to many employers. Nathan Van Buren was a police sergeant in the Cumming, Georgia, police department. His job provided him access to the state law enforcement computer database, which contained license plate information that Van Buren was authorized to use "for law-enforcement purposes."

When an acquaintance offered Van Buren $5,000 to access the database to determine whether another individual was actually an undercover police officer, Van Buren agreed. As it turned out, however, the acquaintance was cooperating with an FBI investigation.

The government subsequently charged Van Buren with a felony violation of the CFAA, which imposes both civil and criminal liability on anyone who "intentionally accesses a computer without authorization or exceeds authorized access."

The Department of Justice's position was similar to that many employers take in civil CFAA claims: the CFAA prohibits any computer access that violates or exceeds the user's authorization to use the information

accessed. Notwithstanding Van Buren's authorization to access the database, the government claimed that, because he did not have permission to access the database for non-job related purposes, he "exceeded" his authorized access. Based on this reading of the law, Van Buren was convicted.

On appeal, Van Buren argued that the "exceeds authorized access" language of the CFAA only applied to individuals who obtained information to which their computer access did not extend, not to those who access the information for an improper reason.

The U.S. Court of Appeals for the Eleventh Circuit, however, agreed with the government that Van Buren "exceed[ed] his authorized access" by obtaining the information for a nonbusiness reason, and affirmed his conviction.

The Supreme Court's Decision

But the Supreme Court agreed with Van Buren. Writing for a 6-3 majority, Justice Amy Coney Barrett adopted the narrower reading of the CFAA that users do not violate the Act by using their authorized access for unauthorized purposes. Instead, the prohibition on "exceed[ing] authorized access" only applies to users who access a computer, or areas of a computer system, they have not been authorized to access.

The Supreme Court's opinion focused on the statute's scope, noting that the government's broad interpretation would criminalize a "breathtaking amount of commonplace computer activity," including using a work computer to send personal e-mails or read the news, presumably in violation of employment policies that only allow computer use for business purposes.

The Supreme Court thus found that Van Buren did not "exceed[] authorized access" to the Georgia law enforcement database.

Further, in explaining its interpretation of the statute, the majority further explained the meaning of "damage" and "loss" within the civil provisions of CFAA. The Court explained that those terms, as defined within the CFAA, are limited to "technological harms," and are "ill fitted . . . to remediating 'misuse' of sensitive information that employees may access using their computers." While the scope of civil remedies was not before the Court in *Van Buren*, this reasoning indicates clear hostility toward using the CFAA to respond to employees misappropriating data they are otherwise authorized to access.

Implications for Employers

Because the CFAA also provides civil remedies for various computer crimes, the CFAA once presented an important tool for employers seeking to prevent their employees from misappropriating sensitive business data. Particularly in cases where the data at issue could not be easily proven to be protected trade secrets, employers would assert claims under the CFAA against their employees simply for exceeding their authorized access to company information on company equipment (often spelled out in computer use policies).

Van Buren has now taken that tool away; employers can only pursue a claim under the CFAA with a showing that the employee was not authorized to access the data entirely.

Van Buren is an important reminder to employers to take steps they should already be taking to ensure the security of their business data. Proactive preventative steps are a far better means of protecting the business than trying to claw back data through litigation after it has already fallen into the hands of a competitor. Monitoring remote employees' access and use of business data poses additional challenges that employers must also address.

Below are several measures that employers can implement to stay vigilant on this front:

- *Enter into strong confidentiality and non-disclosure agreements with your employees*. The NDA is a powerful tool in protecting your sensitive business data, especially in situations where it may be difficult to prove that the data meets the legal definition of a trade secret. Not only does the NDA impose contractual obligations directly on your employee, but it may also expose your competitor to tort liability for encouraging or assisting a former employee in breaching its terms. NDAs should clearly define the categories of covered data and define what is permissible and impermissible use of that data. The NDA should also define the employee's obligations at the time of departure from the company, including setting parameters for the return of all company data in the employee's possession.

- *Prepare comprehensive computer use policies, and have your employees sign them*. A robust computer use policy can provide employers with more options to monitor, and discipline, employees who violate company policy by accessing confidential files and folders without permission. Having such a policy in place, and periodically updating it, can help you respond appropriately whenever a violation takes place.

- *Consider imposing tiered access restrictions on certain files, folders, or databases*. Instead of opening up your entire system to your workers, consider limiting that access to only those files that are necessary to an employee's

ordinary scope of duties. Many courts view these types of restrictions as "reasonable steps" necessary to establish a trade secret.

But, as *Van Buren* makes clear, an employee will not face liability under the CFAA for accessing information from a computer or files within a computer system he or she has authorization to access. Limiting access to "areas of the computer" the employee does not need to access as part of the employee's position consequently decreases the amount of sensitive data the employee can access with permission.

- *Coordinate and conduct an audit of all computers and company-issued devices used by every executive and high-level manager who leaves*. The risk of compromise is significant when senior employees depart to compete, considering that these employees often have deep knowledge of and access to highly sensitive information acquired through higher levels of access, a long relationship with the company, or both. Departures of employees at this level must be handled carefully with an eye toward identifying and remediating breaches in security or misappropriation of company property early before the damage is done.

  When senior employees depart to compete, it is critical to identify what sensitive data they may have accessed in the weeks or months prior to departure and to take steps, typically with letters to the employee and to the new employer, generally identifying the protected information and reminding the employee and the employer of the employee's obligations not to disclose.

Taking measures now to secure sensitive business information will be the best defense against employees who may plan to take that data to your competitors.