Articles + Publications | July 19, 2021

Supreme Court Limits Claims Under Computer Fraud and Abuse Act

Labor & Employment Workforce Watch

WRITTEN BY

Kathleen Grossman | Jeffrey M. McPhaul

The Computer Fraud and Abuse Act (CFAA) creates liability for anyone who "intentionally accesses a computer without authorization or exceeds authorized access." The CFAA defines "exceeds authorized access" to mean "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled to so obtain or alter."

In recent years, the U.S. Circuit Courts of Appeals have been split in their interpretation of this definition. Some circuits interpreted the "exceeds authorized access" clause broadly, extending liability to circumstances when an individual misuses his or her otherwise authorized access to obtain or alter information for improper purposes. Other circuits subscribed to a more narrow interpretation, limiting liability to the instances where the individual uses his or her authority to access or obtain information outside of the scope of what the individual is authorized to access.

On June 3, 2021, the Supreme Court of the United States resolved the circuit split in *Van Buren v. United States*, ?141 S. Ct. 1648, 1662. It took the narrower interpretation of what it means to exceed "authorized access." According to the Court in *Van Buren*, liability exists under the CFAA when an individual accesses a computer with authorization and then obtains information—such as files, folders, or databases—to which the user lacks privileges to access. The Court reasoned that a broader interpretation of the "exceeds authorized access" clause would criminalize use of a work computer to send personal emails, check sports scores, or pay bills where an employer policy prohibits computer use for personal purposes.

Employers previously used the CFAA to bring federal claims against employees who obtained sensitive or confidential company information for improper purposes, such as intellectual property theft or trade secret misappropriation, when the employee is otherwise authorized or entitled to access or obtain such information. The Supreme Court's unanimous holding in *Van Buren* now precludes most of these claims under the CFAA. As a result, employers should carefully consider the scope of access afforded to each of its employees and whether the scope of that access can or should be more narrowly tailored.

The *Van Buren* decision did not explicitly address what types of barriers an employee must breach to exceed "authorized access"—for example, whether breach of a written policy is sufficient, or whether technological barriers blocking access must have been breached. As a result, as an additional precaution, employers should ensure company policies and confidentiality agreements are clear regarding the authorized scope of employees' access to, use of, and alteration to sensitive or confidential information. Even if these policies and confidentiality agreements do not, standing alone, create liability under the CFAA, they can serve to establish the employer's

expectations, further preserve the confidential nature of the information at issue, and offer additional avenues for recourse in the event they are breached.

Although the Supreme Court limited companies' use of the CFAA against employees, there are many laws which employers can effectively use in response to misappropriation of confidential information and trade secrets, including the federal Defend Trade Secrets Act and state trade secrets laws, as well as the common law duty of loyalty.

RELATED INDUSTRIES + PRACTICES

- Labor + Employment