MAYNARDNEXSEN

U.S. Supreme Court Confirms Narrow Scope of Federal Computer Fraud Claim Often Used in Trade Secret Litigation

Practices

Employees & Technology

Employment & Labor Law

Article

06.09.2021

On June 3, the U.S. Supreme Court held that the federal Computer Fraud and Abuse Act ("CFAA"), a cybercrime statute providing civil claims against someone who "exceeds authorized access" to a computer system to obtain trade secrets or other information, does not apply to employees or others who steal information from computer systems to which they had legitimate, technical access. This ruling sharply curtails the CFAA's effectiveness as a litigation option against employees who violate employers' computer use policies or confidentiality restrictions to divert company information for themselves or a prospective competing employer.

The case, *Van Buren v. United States*, involved a Georgia police officer who was charged with a felony CFAA violation after he improperly obtained license plate information from a law enforcement database in exchange for money from someone he did not yet know to be an FBI informant. The question on appeal was whether the CFAA applied here—that is, whether the officer "exceeded authorized access" to the law enforcement database—when he used his own, valid credentials to obtain the information, from a database to which he had legitimate access to perform his job.

Before this decision, federal circuit courts had long been split on the CFAA's scope. Some courts, including the Eleventh Circuit Court of Appeals from which this case arose, held that the CFAA's "exceeds authorized access" language applied even where, as here, the employee was authorized to access information for certain purposes, but misused that information for unauthorized purposes (such as the bribe in this case). Other courts, including the Fourth Circuit Court of Appeals (which covers the Carolinas), held that someone "exceeds authorized access" to a computer network only when he wrongfully obtains information from portions of a computer network to which he

had no authorized access at all.

In a 6-3 decision split among historically "conservative" and "liberal" justices, the Court's majority confirmed that an employee or other insider "exceeds authorized access" to a computer network for purposes of CFAA liability only when he "obtains information located in particular areas of the computer—such as files, folders, or databases—that are off-limits to him." Specifically here, the Court reversed the lower court and held that the police officer did not violate the CFAA because he had legitimate access to the computer database from which he improperly obtained license plate information in exchange for money.

Although its decision focused primarily on the CFAA's statutory language, the Court also noted the troubling policy implications of a broader reading of the CFAA. The Court reasoned that, if the CFAA's "exceeds authorized access" language applied to any conduct in violation of employer policies, it would create criminal and civil liability for "a breathtaking amount of commonplace computer activity," such as an employee who sends a personal email or reads the news from a work computer or on working time. The Court held that such a result was both unmanageable and inconsistent with the CFAA's legislative history, which reflects Congress' purpose of mitigating damage arising from outsider or insider computer "hacking," not mere computer misuse.

The decision has practical implications for trade secret litigation, as CFAA claims are often among those considered by employers who discover that a departing employee has stolen information from computer networks to use on behalf of a competing subsequent employer. This case makes clear that the CFAA is unlikely to be a viable claim in that common scenario, unless the employee somehow accessed and stole information from parts of the employer's network to which the employee did not have access to perform his or her job. In other words, CFAA liability generally does not turn on the scope of the employer's policies, but on the scope of technical access provided to employees.

This case also reinforces the importance to employers, from both an information security and trade secret protection standpoint, of carefully limiting each employee's access to employer computer databases to only that information or those portions of the network that the employee needs to access to perform his or her job. The failure to limit electronic access to information on a "need to know" basis risks losing protections under the CFAA as well as trade secret statutes. For assistance and strategies on protecting company information, consult with your Nexsen Pruet employment and labor counsel.