United States Supreme Court Limits An Employer's Ability to Protect Trade Secrets Through Violations of the Computer Fraud and Abuse Act

Description

By Michael GamboliÂ andÂ John Ottaviani

A recent United States Supreme Court decision has limited the claims that an employer could assert against departing employees who steal trade secrets and confidential information from the employerâ€™s computer systems.

Background.Â The Computer Fraud and Abuse Act (â€œCFAAâ€•) is a federal law that makes it a crime for a person to: (a) access a computer without authorization; or (b) exceed whatever authorization the person may have had to access the computer. 18 U.S.C. Â§1030(a)(2). The CFAA also creates a private right of action for anyone to bring a civil lawsuit if they were damaged by conduct that violates the CFAA.

Companies often used the CFAA to sue former employees who had, for example, absconded with trade secrets or confidential information such as customer lists, prospect information, financial information, business plans, or virtually any other information contained on the company computer systems. In such circumstances, the companyâ€™s claim is that, while the employee was authorized to access the computer and even to access the information at issue, by essentially stealing the information (to start the employeeâ€™s own business, to provide the information to a future employer, or just to retain the information for possible future use), the employee violated the CFAA byÂ *exceeding*Â such authorization.

The Courts Split of Opinion.Â Over the years, federal Circuit courts have disagreed on what it means to â€œexceed oneâ€™s authorizationâ€• to access information under the CFAA. Some courts, including those in the 1st Circuit (which governs most of the Northeast, including Rhode Island and Massachusetts), defined â€œexceeding oneâ€™s authorityâ€• to include situations in which employees who had authority to access the particular information at issue (e.g. a customer list), nonetheless accessed that particular information for an unauthorized purpose (e.g. to steal it in order to solicit those customers after the person quit). Other courts, including the 2nd Circuit (which governs Connecticut, New York and other states), applied a more narrow reading of the CFAA, opining that it was impossible to violate the statute if the person was authorized to access the information. In other words, the 2nd Circuit would find that the fact that the person accessed the information for an improper purpose is irrelevant, because the only way the statute could be violated was if the person was not authorized to see the information in the first place.

Since almost every employer claim based upon the CFAA involves information the employee was allowed to access (for proper business reasons), claims available to employers in the 1st Circuit were not available to employers in the 2nd Circuit. The United States Supreme Court was asked to take up this issue recently in the case ofÂ *Van Buren v. United States*Â and to harmonize the split among the Circuits on how the CFAA should be interpreted.

The Van Buren Case.Â Van Buren was a police officer in Georgia who used the police computer system to run license plate searches for personal reasons (specifically, he was paid $5000 by a civilian who wanted to run plates of women the civilian met at strip clubs to ensure the women were not undercover police officers). Van Buren was convicted of violating the CFAA by accessing information he was authorized to access, but doing so for reasons outside of his authority. In other words, the court applied the 1st Circuitâ€™s interpretation. Van Buren appealed the conviction to the 11th Circuit, arguing that he did not violate the CFAA because he was

authorized to use the computer system (and the license plate scanner), and the fact that he did so for an inappropriate and unauthorized reason did not matter. In other words, Van Buren wanted to apply the 2nd Circuitâ€™s definition of the CFAA. The 11th Circuit Court of Appeals disagreed with Van Buren, applied the same interpretation as the 1st Circuit, and upheld the conviction. As his last ditch effort to escape jail, Van Buren petitioned the United States Supreme Court to take up his cause. The Supreme Court agreed to hear his case and to set the record straight, one way or another, on the split of opinion with respect to the meaning of â€œunauthorized useâ€• under the CFAA.

SCOTUSâ€™ Decision.Â Sparing readers from the grammatical gymnastics and statutory construction rules the Supreme Court plodded through in order to determine just what Congress was trying to say in the use of the particular language of the CFAA, the Court ultimately agreed with Van Buren. The example given by the Court is clear:Â *[I]f a person has access to information stored in a computer â€" e.g., in â€œFolder Y,â€• from which the person could permissibly pull information â€" then he does not violate the CFAA by obtaining such information, regardless of whether he pulled the information for a prohibited purpose. But if the information is instead located in prohibited â€œFolder X,â€• to which the person lacks access, he violates the CFAA by obtaining such information.*

The Supreme Court thus rejected the existing body of law in the 1st Circuit, which would have found that Van Buren violated the CFAA and would have convicted Van Buren because his action in accessing the informationÂ *for a forbidden or unauthorized reason*Â was illegal under the CFAA.

Takeaways.Â Proponents of the Supreme Courtâ€™s reading of the CFAA believe it is in keeping with the original intent of the law, which was aimed at preventing computer hacking and unauthorized access to computer systems and networks. While this decision eliminates one very powerful and useful claim for employers against departing employees who steal trade secrets and confidential information such as customer lists, business plans or R&D type information, such conduct may still violate other federal and state statutes and/or company confidentiality and computer use and access agreements. Nonetheless, employers should review and consider revising existing computer use and access policies and employee confidentiality agreements to limit the type of information employees are â€œauthorizedâ€• to access in order to deter such conduct.

Partridge Snow & Hahn partnersÂ Michael GamboliÂ andÂ John OttavianiÂ are ready to answer any questions employers may have about this recent decision. For additional information and resources visit the firm'sÂ Employment & Labor Practice GroupÂ page andÂ Intellectual Property Practice GroupÂ page.

Date Created
July 15, 2021