Reinhart

Misusing Information from Company Computer Systems Does Not Violate Computer Fraud and Abuse Act

On June 3, 2021, the U.S. Supreme Court issued a decision in *Van Buren v. United States* that will make it harder for employers to recover damages against current and former employees who misuse information stored on company computer systems.

The Computer Fraud and Abuse Act (CFAA) prohibits individuals (including employees) from accessing computer systems without authorization (e.g., hackers who lack authorization to access a company's computer system at all). But the statute also prohibits individuals *with authorized access* (like current employees) from exceeding their authorization to those computer systems.

The issue before the Supreme Court in *Van Buren v. United States* was whether an individual violates the CFAA by using their authorization to access information on a computer system for an improper purpose. Ultimately, the Supreme Court decided no.

Employers can no longer rely on the CFAA to deter employees from misusing confidential information they have permitted their employees to access. If an employee has authorization to access all areas within the employer's computer system, the employee does not violate the CFAA by taking and using that information for an improper purpose. The Court was clear on this point: an improper motive to misuse otherwise accessible information does not, by itself, violate the CFAA.

In light of the Supreme Court's ruling, employers should consider walling-off trade secrets and other proprietary or sensitive information so that they are only accessible to employees who need access to those materials for their jobs. Employers should also review their employee handbooks and policies to see whether they are clearly communicating to employees what portions of the employer's computer system they are authorized to access. By doing so, employers will better position themselves to retain the protection of the CFAA. Employees can still violate the CFAA by accessing information they are not authorized to access.

POSTED:

Jun 23, 2021

RELATED PRACTICES:

Banking and Finance
https://www.reinhartlaw.com/practices/banking-and-finance

Health Care
https://www.reinhartlaw.com/practices/health-care

Labor and Employment
https://www.reinhartlaw.com/practices/labor-and-employment

Litigation
https://www.reinhartlaw.com/practices/litigation

Corporate Law
https://www.reinhartlaw.com/practices/corporate-law

RELATED PEOPLE:

Michael J. Gentry
https://www.reinhartlaw.com/people/michael-j-gentry

Christopher K. Schuele
https://www.reinhartlaw.com/people/christopher-schuele

Employers have other ways to protect themselves from employee theft of sensitive information, including the use of confidentiality and return of company property agreements. Employers can also invoke federal and state trade secret protections and state claims for breach of an employee's duty of loyalty.

If you have any questions about your organization's response to the recent Supreme Court decision or its impact on employers' computer authorization processes and procedures for employees, please contact Christopher Schuele, Michael Gentry or your Reinhart attorney.