Employers' Rights Under the Computer Fraud and Abuse Act (CFAA) Narrowed after Supreme Court Decision in *Van Buren*

Amundsen Davis Data Privacy & Security and Labor & Employment Alert
November 8, 2021

In today's digital age, employers store immense amounts of information, including confidential and proprietary information, on their on-premises systems, cloud-servers and other data storage solutions. With this collection of data, companies are increasingly worried about cyber-attacks by outside threat actors. In fact, the news is replete with stories detailing the latest ransomware attack or phishing scam.

At the same time, however, employers must safeguard against insider threats. A "data breach" can occur when a disgruntled employee utilizes his access to a company's databases and systems to inflict revenge or harm.

Beyond the more traditional civil and criminal legal remedies employers could seek, until this past summer, one of the few, federal regulations addressing data security, the Computer Fraud and Abuse Act (CFAA), could have been employed to prosecute an employee-turned-insider-cyber-threat-actor.

However, this past summer the Supreme Court, in *Van Buren v. U.S.*, removed CFAA as a readily available, remedial tool for employers. The Court found that this federal law does not provide recourse against an employee who had authorized access to the employer's database but used it for an improper purpose. Instead, the access, itself, must be unauthorized in the first place.

What is the Computer Fraud and Abuse Act?

The CFAA was enacted in 1986 to help combat against the increase in cyber-attacks sweeping the nation at that time. The law provided criminal, and later civil, penalties against hackers. The CFAA had three key provisions in that it (1) prohibited unauthorized access with the intent to defraud, (2) prohibited computer access without authorization and the altering, damaging, or destroying of information, and (3) prohibited trafficking in computer passwords.

PROFESSIONALS

Molly A. Arranz
Partner

Sofia Valdivia
Associate

RELATED SERVICES

Cybersecurity & Data Privacy

Labor, Employment & Immigration

Over the years, as technology advanced, so did hackers. To keep up, Congress began expanding the CFAA to cover more types of data incidents. The law was amended to impose liability against a person who "exceeds authorized access." 18 U.S.C. §1030(a)(2). The CFAA was then used by employers against employees (typically departing employees) who accessed company servers and stole, misappropriated or otherwise misused data.

For many years, the federal courts were split as to whether the CFAA applied when an employee, who had authorized access to an employer's computer systems, misused that access (accessed the information for an improper purpose). Some circuits (including the Seventh Circuit) adopted a broad interpretation of the law, finding that the CFAA covered instances where a person misused information they were otherwise allowed to access. Other circuits limited CFAA applicability to instances in which a person accessed data that was not permitted or authorized in the first place.

What did the Supreme Court decide?

This past summer, the Supreme Court put an end to the debate, but, in doing so, stripped away a legal remedy for employers. The Court limited the scope of CFAA's coverage; it ruled that the language of the statute—both "unauthorized access" and "exceeds authorized access"—requires that the employee (current or former) must have obtained data that was *off-limits* to them. The Court was concerned that if it interpreted the CFAA more broadly it would be used for "every violation of a computer-use policy" causing "millions of otherwise law-abiding citizens" to become criminals. As an example, the Court discussed how if an employer had a policy that a work issued computer is to be used only for business purposes, but an employee sent a personal email or shopped online using his work computer, that would violate the CFAA. Finding this to be too harsh, the Court instead interpreted the law more narrowly and to only cover incidents when an employee improperly accesses information beyond the employee's granted permissions.

The Court, however, did not address or explain what steps an employer must take in order to establish that an employee accessed files that were off-limits, causing the CFAA to be triggered. In other words, employers are left to decipher how they can establish data that is off limits – whether they need to take the step to limit employee access through code-based technology, such as password protected files or firewalls, or whether they can simply provide guidelines on what's prohibited in employee handbooks.

Given the Supreme Court's ruling, how do employers protect their business?

While it may be tougher to use the CFAA to go after employees who misuse the employer's computer systems, data, software or networks, employers still have other protections and remedies. For instance, employees may be liable under

the federal Defend Trade Secrets Act (depending upon the information at issue), as well as state computer trespass or other laws and common law torts. Moreover, the decision does not impact an employer's right to terminate an employee who violates an employer's policies, rules or procedures that govern employee use of the company's computer systems or data. But as with all things cybersecurity, the best approach is making sure your business has proper policies and procedures, including limiting employee access based upon job function, in place *before* the "attack." Consider the following to protect your company:

- Have clear **confidentiality** policies and procedures.
- **Limit access to employees in sensitive positions or when necessary for their roles.** While it may seem easier to allow data access to all employees, consider whether and what information is necessary for employees and establish purpose-based restrictions on access to information and use of computer systems. Include password-protection or encryption for confidential or highly sensitive information and only allow access to employees who have a legitimate business reason for it.
- **Consider who is holding your passwords.** Companies maintain a list of passwords for their different programs. This master password list should not be accessible to all employees. Who has access to what passwords and why?
- **Manage mobile and other electronic devices used for company business (whether personal or company owned).** Have clear policies and procedures in place, including allowing you to remotely wipe devices upon the occurrence of certain events, including termination of employment.
- **Closely monitor employees who resign or are terminated.** Employees who leave their employers (regardless of the reason) often take sensitive or confidential information belonging to their employer. Consider the information to which they had access and examine whether there was any suspicious activity before or after the departure, including downloading or deletion of information. It is also important to have a plan in place to immediately cut off access to the company's computer networks/systems upon termination.