Will Supreme Court Enforce Law And Order In The Digital Workplace?

Insights
10.30.20

Now entering its ninth month in the United States with no sign of slowing down, the COVID-19 pandemic has forced many employers to make permanent changes to business operations in order to survive. Among the most noticeable of those changes has been the wholesale digitization of many workplaces. For the first time since many businesses were formed, the majority of your information is being stored in a purely electronic format, the majority of your employees are performing some or all of their job responsibilities remotely, and the majority of your sales are coming from internet or app-based transactions.

Accompanying the innovations brought about by the arrival of the electronic workplace have come new types of problems. With record numbers of employees now having access to your computer systems, the potential for them to use that access for improper or illegal purposes – including viewing, copying, and distributing your confidential, trade secret, and propriety business information without authorization – is at an all-time high. But what can you do when your current or former employees engage in such illegal actions? While asserting claims against those employees for breach of contract, misappropriation of trade secrets, or unfair competition can potentially offer some relief, each can be difficult and expensive to prove in a court of law.

Fortunately, employers have powerful weapons at their disposal in the effort to combat digital misconduct, including the United States Computer Fraud and Abuse Act (CFAA). And in the Supreme Court term that is just getting underway, the highest court in the land will be deciding a CFAA case that may in fact amplify the resources you have available to you under that statute to further protect your organization.

A Quick CFAA Primer

The Computer Fraud and Abuse Act has a long history that began well before most employers had entered the digital age. It was a 1986 amendment to the Comprehensive Crime Control Act of 1984 (CCCA) whose primary purpose was to expand the list of computer crimes contained in that statute. While the CCCA merely prohibited individuals from using computers to access classified government information or confidential bank information, the CFAA purported to criminalize the more commonly performed actions of computer fraud, computer hacking, and trafficking in stolen passwords.

What Does The CFAA Prohibit?

Now, 30 years later, the CFAA has been amended to impose both civil and criminal liability on individuals who perform a wide variety of computer related actions. As currently written, the CFAA forbids individuals from causing any loss or damage, or committing any act of fraud, extortion, or trafficking, by knowingly and/or intentionally accessing any "computer" or "protected computer" without authorization or in a way that exceeds their authorization. Actions that potentially violate the statute include downloading or deleting data, using logins or passwords without authorization, and using a computer for an unauthorized purpose.

What Devices Does The CFAA Cover?

Importantly, the CFAA defines the term "computer" as "any high speed data processing device [that performs] logical, arithmetic, or storage functions." Accordingly, the CFAA prohibits not only an employee's unauthorized use of desktop computers and laptops, but also an employee's unauthorized use of cell phones, tablets, point of sale systems, electronic security systems, and other similar devices.

How Can You Prove A CFAA Violation?

In order to prove a violation of the CFAA, an employer needs to have suffered either damage or loss. While there has been significant case law interpretation of these terms, as defined in the CFAA, "damage" means any "impairment to the integrity or availability of data, a program, a system, or information." Alternatively, "loss" means "any reasonable cost to [the] victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service."

What Can You Recover?

Should you be able to prove that an employee violated the CFAA, you may be entitled to actual damages, injunctive relief, and/or other "equitable" relief from that employee. However, you are generally not entitled to either attorneys' fees or punitive damages.

SCOTUS Will Help Determine Meaning Of Authorized Access

Whether an individual has used a computer "without authorization" in order to trigger the CFAA has caused courts great confusion – especially in situations where they are otherwise authorized to use a computer but arguably use it for unauthorized purposes. For example, where a restaurant employee who is authorized to use his employer's computer to make reservations for customers uses it to make reservations for himself, is he subject to imprisonment for committing the crime of computer fraud? Alternatively, where a restaurant manager uses his employer's computer to check his personal email, is his employer permitted to file a civil lawsuit against him for damages and injunctive relief because he acted without authorization?

The U.S. Supreme Court has agreed to consider whether a person who is authorized to access information on a computer for certain purposes violates the CFAA if they access the same information for an improper purpose in the upcoming case of *United States v. Van Buren*. In this case, a police officer in Georgia was charged with violating the CFAA after he accessed a workplace

case, a police officer in Georgia was charged with violating the CFAA after he accessed a workplace computer database. While he was authorized to use the system for work purposes, he instead used it for the non-work-related purpose of running background checks on individuals in exchange for money. Applying the language of the statute as written, the 11th Circuit Court of Appeals held that the police officer violated the CFAA because he used the computer in a way that "exceeded his authorized access" even though he was otherwise authorized to use the relevant computer.

In seeking to overturn that decision at the Supreme Court, organizations such as the Electronic Frontier Foundation and the National Association of Criminal Defense Lawyers have argued that the CFAA was never intended to expose individuals to criminal liability and imprisonment for engaging in behavior that was simply "improper." Rather, they argue, it was intended to prohibit true "computer crimes" like hacking. They further argue that subjecting individuals to criminal liability based on the vague and ambiguous language contained in a website's "Terms of Service" or a business's employee handbook violates those individuals' due process rights.

Written briefs have now been filed by all interested parties, and the Supreme Court has set the case for oral argument on November 30. You should be sure to review the ruling in the *Van Buren* matter when it is issued in early 2021, as it could potentially expand – or limit – the scope of your rights under the CFAA in significant ways.

Service Focus

Privacy and Cyber

Litigation and Trials