Suing An Employee For Unauthorized Computer Access Reaches a Dead End Under Federal Law

10/20/2025

What should an employer do when an employee violates company policy by taking electronic files that the employee was not permitted to access? A recent Third Circuit decision answered the question by advising what an employer should not do: sue the employee under federal law for unlawful computer access.

The Computer Fraud and Abuse Act of 1986 (CCFA) creates a private cause of action (and makes it a crime) under federal law against a person who "intentionally accesses a computer without authorization or exceeds authorized access," and thereby obtains computer information. 18 U.S.C. § 1030(a)(2), (g). The downloading of electronic files from the company's computer system by an employee, when the employee does not need those files to perform assigned job duties and violates company policy by doing so, would seem to be the classic example of a CCFA violation. Providing access to company electronic systems is not meant to be an invitation for employees to fish around.

Not so fast. The courts have generally been reluctant to treat workplace disputes as federal crimes, highlighted in a 2021 U.S. Supreme Court case, *Van Buren v. United States*, where that court noted that if the CCFA

> criminalizes every violation of a computer-use policy, then millions of otherwise law-abiding citizens are criminals. Take the workplace. Employers commonly state that computers and electronic devices can be used only for business purposes. So on the Government's reading of the statute, an employee who sends a personal e-mail or reads the news using her work computer has violated the CFAA. Or consider the Internet. Many websites, services, and databases . . . authorize a user's access only upon his agreement to follow specified terms of service. If the "exceeds authorized access" clause encompasses

violations of circumstance-based access restrictions on employers' computers, it is difficult to see why it would not also encompass violations of such restrictions on website providers' computers.

The Third Circuit in *NRA Group, LCC v. Durenleau* channeled this reluctance by concluding that the CCFA addresses only third party hacking, not the more commonplace "breach of workplace computer-use policies." If the employee had permission to access the system, the CCFA is not violated even if the employee abuses that permission.

What then may an employer do to protect its computer systems from wayward employees? A lot. Well-crafted workplace policies and written contracts with employees can afford an employer significant ammunition to respond to an employee who takes electronic files without permission.

A word of caution. Some jurisdictions, including New Jersey and Massachusetts, sanction such employee theft in certain circumstances when the documents are used by the employee to vindicate certain employment rights. Whether an employee is protected under this doctrine is highly fact specific, and, at least in New Jersey, does not necessarily immunize the employee against criminal prosecution under state law. When confronted with employee electronic theft, an employer needs to carefully take into account all of these considerations.

For more information about how your organization can protect its computer systems and electronic files, please contact:

Jay Sabin, Esq., *Member*, Labor and Employment Practice at 917.596.8987 or jsabin@bracheichler.com

Authors

The following attorneys contributed to this insight.

Jay Sabin

Member
Labor and Employment, Cannabis Industry

917.596.8987 · 973.618.5907 Fax

jsabin@bracheichler.com