Court Rules Misuse of Company Data Not Actionable under CFAA

Sep 11, 2020

Categories:

Publications

Authors:

David A. Skidmore, Jr.
Simon Y. Svirnovskiy

Imagine that just before resigning and going to work for a competitor, a group of your employees takes confidential company information from their company-issued computer and cell phone and use that information on behalf of the competitor. Congress passed the Computer Fraud and Abuse Act (CFAA) to combat computer hacking and theft of information stored on computers. Can you sue these former employees under the CFAA? The Sixth Circuit just answered: "No."

The Sixth Circuit Court of Appeals, which covers federal courts in Kentucky, Michigan, Ohio, and Tennessee, ruled in *Royal Truck & Trailer Sales & Serv., Inc. v. Kraft,* No. 19-1235 (6th Cir. Sept. 9, 2020) that the CFAA was only meant to penalize those who breach cyber barriers without permission, rather than those who overstep or misuse their otherwise legitimate access to a cyber system. In doing so, though, the Sixth Circuit acknowledged a nationwide circuit split. We anticipate that this issue will ultimately be resolved in the coming years by the United States Supreme Court.

What Happened?

Two of Royal Truck & Trailer's employees abruptly resigned to join a competitor. The company discovered that shortly before leaving, the employees: (i) forwarded Royal's customer price quotes from their Royal email accounts to their personal emails; (ii) contacted Royal's customers through their Royal emails and asked the customers to send "new vendor info" to their personal emails; and (iii) deleted and reinstalled the operating systems on their company-issued laptops, rendering the data on those laptops unrecoverable. Royal sued under the CFAA, claiming that the employees "intentionally accesse[d] a computer without authorization or exceed[ed] authorized access, and thereby obtain[ed] . . . information from any protected computer . . . [and] shall be punished." 18 U.S.C. § 1030(a)(2)-(a)(2)(C).

FBT Gibbons

What Did the Court Decide and How Did it Get there?

To succeed on its CFAA claim, Royal had to prove that the employees (1) intentionally accessed a computer; (2) the access was unauthorized or exceed the employees' authorized access; (3) the employees obtained information from a protected computer through that access; and (4) the conduct caused damages in excess of $5,000. Only the second element was at issue on appeal. Since Royal admitted the employees had authorization to access the confidential company information on their Royal email accounts, the Court only had to determine if the employees' access was unauthorized or whether they exceeded their authorized access when they sent Royal's confidential information from their work devices to their personal email accounts.

The Court ruled that based on how the CFAA defined "exceeds authorized access" ("to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter"), the Act had a limited purpose to penalize external (think computer hackers) or internal actors (think employees who access parts of the company database where they should not be) who over-step cyber barriers, rather than police internal actors who misuse data they were authorized to obtain in the first place.

What Does This Mean?

The Sixth Circuit joins the Second (New York and part of the Northeast), Fourth (mid-Atlantic), and Ninth (west coast) Circuits in deciding that one who is authorized to access a computer does not exceed her authorized access by violating an employer's restrictions on the use of that information after the information is validly accessed. In contrast, the First (Massachusetts and part of the Northeast), Fifth (South), Seventh (Illinois and northern Midwest), Eighth (central Midwest), and Eleventh (Southeast) Circuits all determined that various kinds of misuse of otherwise lawfully-accessed information constitutes "exceed[ing] authorized access" in violation of the CFAA. In sum, the federal appellate judges disagree with one another on this issue.

FBT Gibbons

It is worth noting that the person who steals information from the computer on the way out the door may not be liable under the CFAA, but may still be liable for breach of a confidentiality agreement, the tort of conversion (theft), and misappropriation of trade secrets. In this era where information is power, your business should expect more, not less, of these types of issues.

FBT Gibbons