Bloomberg Law®

Privacy and Security Law Report®

Trade Secrets

Can Companies Sue Employees Under CFAA for Misusing Rightfully Accessed Information?

Trade Secrets

Courts have split over whether employees who misuse company information can run afoul of the Computer Fraud and Abuse Act. Joshua Fowkes of Arent Fox discusses how courts have approached the issue and suggests why companies should consider raising claims under the CFAA in addition to under trade secret laws.

BY JOSHUA FOWKES

A company's trade secrets are often its most valuable assets. Because trade secrets are typically stored electronically, they are vulnerable to computer hackers. Hacking is prohibited by and subject to criminal and civil liabilities under the Computer Fraud and Abuse Act (CFAA). 18 U.S.C. Section 1030. But trade secrets are also vulnerable to theft by employees and business partners. When trade secrets are stolen by an employee, a company has several remedies, including claims for misappropriation of trade secrets, breach of employment contract, and conversion. But companies sometimes overlook the option of adding claims under the CFAA, particularly now that federal courts have jurisdiction over most trade secret cases under the Defend Trade Secrets Act. The CFAA prohibits a person from obtaining information by accessing a computer without authorization or by exceeding his authorized access. But what if an employee who is authorized to access a company's information used it in violation of a corporate policy or to harm the company? Courts around the country have answered that question differently. In fact, two courts within two weeks reached opposite results.

Joshua Fowkes is a partner in the litigation group at Arent Fox LLP in Washington.

The U.S. District Court for the Southern District of Florida held that a person with authorization to access data ''exceeds authorized access'' if he uses the data to contravene a corporate policy. There, an employee who had full access to his employer's computer system was supposed to help his employer in a lawsuit, but undermined his employer's legal defense by sending key evidence to his employer's adversary. *Hamilton Group Funding v. Basel*, S.D. Fla., 16-cv-61145, 4/12/18. The

 ISSN 1538-3423

district court noted that the Eleventh Circuit had ruled that a defendant violated CFAA's prohibition of ''exceeding authorized access'' when he ''obtained personal information for a nonbusiness reason.'' As a result, the Florida district court broadly interpreted the phrase ''exceeding authorized access'' so that the employee's misuse of this information violated the CFAA and awarded judgment to the company on its CFAA claim.

But the U.S. District Court for the District of Columbia interpreted the phrase ''exceeds authorized access'' much differently. *Sandvig v. Sessions*, D.D.C., 16-cv-01368, 3/30/18. There, researchers and a media organization planned to use computer programs that, among other things, adopt a technique called scraping to collect large amounts of data from corporate websites and then analyze that data to assess whether the websites had engaged in discrimination. But those websites include terms of use that bar scraping and other practices that the researchers plan to use. The researchers challenged the CFAA by claiming that its criminal penalties for people who ''exceed authorized access'' while visiting a website violated the Constitution. In reviewing the government's motion to dismiss the researchers' claims, the court interpreted whether the CFAA's penalty against people who ''exceed authorized access'' applied to the researchers' planned activities. The court noted that the D.C. Circuit has never interpreted that phrase, but added that several circuit courts significantly differ in how to interpret it — first in whether it bars only ''unauthorized access to information'' or whether it also bars ''unauthorized use of information that a defendant was authorized to access for specific purposes,'' and second, ''whether violating a website's [terms of service] exceeds authorized access for purposes of CFAA.'' The court found that the phrase bars a person's unauthorized access of information, but does not stop a person's unauthorized use of information to which a person had authority to access. Because most of the researchers' activities at issue collected a website's data that is publicly accessible but used it in a way that is barred by that website's terms of use, the court ruled that those activities were not prohibited by the CFAA.

These two contrasting rulings are just the latest examples of a circuit split on this issue. The First, Seventh, and Eleventh Circuits interpret the phrase ''exceeds authorized access'' broadly and conclude that an employee exceeds his authorized access to information whenever he acquires information with a subjective intent that is contrary to his employer's interest, even if the employee had authorization to access the information. In other words, these courts have held that the CFAA bars unauthorized use of information that a person was authorized to access only for particular purposes. *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2001); *Int'l Airport Centers, LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006); *U.S. v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010). In contrast, the Second, Fourth, and Ninth Circuits interpret that same phrase narrowly and conclude that an employee or business partner does not exceed authorized access in violation of the CFAA by acting with an improper subjective intent or by violating corporate policies restricting use of that information. *U.S. v. Valle*, 807 F.3d 508 (2d. Cir. 2015); *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199 (4th Cir. 2012); *Nosal v. U.S.*, 676 F.3d 854 (9th Cir. 2012). The U.S. Supreme Court may need to resolve this split of authority, but it has refused requests to do so. And people have complained for years that the CFAA is an outdated statute that was implemented before the internet existed, and that Congress should replace or revise it.

In the meantime, companies whose employees misuse corporate information should consider complementing their claims for misappropriating trade secrets with CFAA claims. First, while a claim for trade secret theft generally permits a company to recover greater damages, a claim under the CFAA in some ways is easier to win. For instance, a company pursuing a claim for trade secret misappropriation frequently must spend significant time and money to prove that the stolen information was a trade secret, and that it took adequate measures to guard the trade secret's confidentiality. But a company pursuing a CFAA claim must prove only that its adversary intentionally accessed a computer, lacked authorization or exceeded its authorized access, obtained the information, and caused a loss of at least $5,000. Second, the Supreme Court may ultimately resolve the current circuit split by ruling that an employee exceeds his authorized access to information whenever he obtains it with an intent that is contrary to his employer's interest, even if the employee initially had authorization to access it. Third, even if a company's CFAA claim against an employee who had authorization to access the trade secret may fail, it might learn in discovery that another person who *lacked* authorization violated the CFAA by directing the employee to access the computer. Fourth, a CFAA claim will provide additional leverage to use in settlement discussions. Consequently, even though courts are resolving this issue by issuing competing rulings, companies should not overlook the option of raising CFAA claims against disloyal partners and employees.