Stoel Rives World of Employment
Insight and Commentary on Labor and Employment Law
PUBLISHED BY STOEL RIVES LLP ATTORNEYS AT LAW

Stoel Rives World of Employment

Posted at 6:00 AM on January 11, 2013 by Jamie Kilberg

Circuit Split Remains As To Possible Employer Remedies Under Computer Fraud and Abuse Act (CFAA)

There is a growing divide in the federal circuit courts of appeal over whether the Computer Fraud and Abuse Act (the "CFAA")—a criminal statute that permits victims to bring civil actions against violators—reaches certain conduct by departing employees. The U.S. Supreme Court was poised to potentially resolve the dispute when an employer filed a petition for writ of certiorari stemming from a decision in the U.S. Court of Appeals for the Fourth Circuit. But on January 2, 2012, the parties settled the case and filed a stipulation under the Supreme Court's Rule 46 dismissing the petition. We will have to wait until another case comes along to see if the Supremes will resolve the split. Until then, employers need to pay attention to the decisions coming out of the circuits in which they operate to know whether they may have a claim under the CFAA against departing employees who take proprietary computer information with them upon their departure.

Courts Disagree About What The CFAA Says

The CFAA prohibits accessing and obtaining information from a "protected computer" (i.e., any computer used in or affecting interstate commerce or communication) "without authorization" or in a way that "exceeds authorized access." 18 U.S.C. § 1030(a)(2)(C). Employers often face situations where employees, prior to their departure from employment, copy proprietary files for their own use or to benefit their new employer. Usually, these employees were technically authorized to access the computer system and its files, but certainly were not permitted under company policy to copy those files for the purpose of using them outside of their employment with the company. Besides other causes of action, employers have increasingly sought to bring civil claims under the CFAA, arguing that accessing the files for the purpose of copying them and using them to benefit a competitor was unauthorized in the first instance, or certainly exceeded otherwise authorized access.

Several courts have agreed to a broad reading of the CFAA, and have permitted employers to make CFAA claims against departing employees who attempt to pilfer the company's files. Thus, in the First Circuit (covering Maine, Massachusetts, New Hampshire, and Rhode Island), Fifth Circuit

(covering Louisiana, Mississippi, and Texas), Seventh Circuit (covering Illinois, Indiana, and Wisconsin), and Eleventh Circuit (covering Alabama, Florida, and Georgia), an employee who misuses information obtained from an employer's computer system—that is, an employee who ordinarily is permitted access to the information, but accesses it for the purpose of harming the employer or in violation of the employer's computer use and access policies—can be sued under the CFAA. The theory is that accessing the information in that manner is adverse to the employer's interests, constitutes a serious breach of loyalty, and effectively converts the access into unauthorized access or access that "exceeds authorized access." *See, e.g.*, *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 583 (1st Cir. 2001); *United States v. John*, 597 F.3d 263, 272 (5th Cir. 2010); *Int'l Airport Ctrs., LLC v. Citrin*, 440 F.3d 418, 420-21 (7th Cir. 2006); *United States v. Rodriguez*, 628 F.3d 1258, 1263 (11th Cir. 2010).

Other courts, however, disagree. In particular, the Fourth Circuit (covering Maryland, North Carolina, South Carolina, Virginia, and West Virginia) and the Ninth Circuit (covering the Western U.S. including Alaska, California, Hawaii, Oregon, and Washington)—as well as district courts in New York (the Second Circuit) and Ohio (the Sixth Circuit)—all have taken a narrow view of the CFAA. Those courts have found that the CFAA addresses only ***access*** to information, not ***misuse*** of information once accessed. Thus, if an employee during their employment is within their rights to access proprietary information, the CFAA does not apply even if that employee later misuses that information, or accessed the information in the first place with the intent to misuse it in a way that is detrimental to the employer. That is not to say that employers in those jurisdictions have no remedy for such breaches, but those courts have made clear that any such remedy cannot come from the CFAA. *See, e.g.*, *WEC Carolina Energy Sol'ns LLC v. Miller*, 687 F.3d 199 (4th Cir. 2012); *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (*en banc*); *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009); *Orbit One Commc'ns, Inc. v. Numerex Corp.*, 692 F. Supp. 2d 373, 385 (S.D.N.Y. 2010); *Ajuba Int'l LLC v. Saharia*, 871 F. Supp. 2d 671, 687 (E.D. Mich. 2012).

Clarification May Be On The Way...Or Not

Late last year, it looked as if the U.S. Supreme Court was going to have an opportunity to weigh in. The employer in the Fourth Circuit case filed a petition for writ of certiorari on October 24, 2012. The employer argued that the Court should resolve the circuit split. It also argued that the Fourth Circuit's decision to narrowly construe the CFAA was wrong because "failure to recognize that the purpose for which an employer authorizes access to information is an inseparable component of the authorization itself." The defendants' brief in opposition was due at the end of 2012. Instead, on January 2, 2013, the parties filed a stipulation dismissing the case. We have confirmed that the dismissal was filed because the parties settled the litigation.

Thus, while we wait for the next CFAA case to come along, employers must be mindful of the law that governs their jurisdiction in assessing whether they have a viable CFAA claim against departing employees who take company-owned electronic documents with them.