Establishing the "Without Authorization" Element Under the Computer Fraud & Abuse Act

Insights
7.09.10

Since the addition of civil remedies in 1994, the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 ("CFAA"), has evolved into a potentially powerful claim in the departing employee context.In addition to the often-included claims for breach of restrictive covenant, misappropriation of trade secrets and/or unfair competition, CFAA claims are being alleged against more and more employees who transfer employment to a competitive firm.The likelihood of success on CFAA claims against departing employees, however, varies by jurisdiction.Recently, numerous courts have debated, and issued divergent rulings, on the enforceability of CFAA claims against departing employees.

The debate surrounding the application of CFAA claims against departing employees often focuses on the statute's "without authorization" or "in excess of one's authorization" requirement.In 2000, the United States District Court for the Western District of Washington issued a ruling holding that an employee's "authorization" to access his or her employer's computer systems ends when the employee begins to act as another employer's agent.*See Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*, 199 F. Supp. 2d 1121 (W.D. Wash. 2000) ("the authority of an agent terminates if, without knowledge of the principal, he acquired adverse interests or if he is otherwise guilty of a serious breach of loyalty to the principal").Subsequent to the *Shurgard* opinion, two distinct schools of thought on the CFAA's "authorization" requirement have emerged.The majority of courts considering the issue, including the 1st and 7th Circuit Courts of Appeal, have followed the *Shurgard* Court's analysis, holding that an employee exceeds the scope of his or her authorized access to an employer's computer systems by acting for a purpose against the employer's best interests, acting for a competitive purpose and/or acting as someone else's agent – even if such action takes place when the employee is still employed and technically has "authorization" to utilize the company's computer systems.*See EF Cultural Travel BV, EF v. Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2001); *International Airport Centers, LLC v. Citrin*, 440 F. 3d 418 (7th Cir. 2006).Numerous district courts have accepted this legal theory, concluding that if an employee breaches his or her duty of loyalty to an employer, the employee's authorization to access the employer's computer systems terminates and subsequent access may gives rise to a CFAA violation.*See, e.g., Caylon v. Mizuho Securities USA, Inc.*, No. 07-Civ. 2241, 2007 U.S. Dist. LEXIS (S.D.N.Y. Sept. 5, 2007) ("the plain language of the [CFAA] seems to contemplate that, whatever else, 'without access' and 'exceed authorized access' would include an employee who is accessing documents on a computer system which that employee had to know was in contravention of the wishes and interests of his employer"); *Hub Group, Inc. v. Clancy*, No. 05-2046, 2006 WL 208684 (E.D. Pa. Jan. 25, 2006) (finding the employee exceeded the scope of his

authorization into his employer's electronic database of customer information by taking the employer's information for use at a competitive company).

The diverging school of thought on the CFAA's "authorization" requirement believes that the statute was enacted to protect against the unauthorized access (i.e. procurement or alteration) of computerized information – not to protect against any subsequent use or misuse of information.The 9th Circuit Court of Appeals, in analyzing the CFAA's "authorization" requirement, has held that if an employee accesses his or her employer's computer systems during employment and, therefore, with the employer's authorization, subsequent disloyal treatment of the information accessed does not give rise to a CFAA violation.*See LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009).A recent decision from the United States District Court for the Western District of Pennsylvania, *Consulting Professional Resources, Inc. v. Concise Technologies LLC*, Civ. A. No. 09-1201, 2010 WL 1337723 (W.D. Pa., Mar. 9, 2010), follows the *Brekka* Court's analysis, dismissing an employer's CFAA claim against a departing employee and stating: "[t]his court likewise declines to construe the CFAA by reliance upon agency principles where the defendant's intent governs whether the access was without authorization or exceeded authorized access."

It does not appear that this debate regarding the CFAA's "authorization" requirement will be resolved any time soon.As recently as May 27, 2010, a Motion to Dismiss was filed in the United States District Court for the Southern District of New York based, in part, on an argument that the reach of the CFAA does not extend to instances where the employee was authorized to access the information he later transferred and utilized to the detriment of his former employer.*See Aon Risk Services Northeast Inc. v. Kornblau et al.*, Case No. 10-cv-2244(RMB)(JCF) (Document 31).If the *Aon* Court accepts the former employer's arguments regarding the CFAA's authorization requirement, the decision would represent another rejection of the enforcement-friendly agency theory of departing employee violations of the CFAA that was the basis of the opinions *Shurgard, EF Cultural Travel* and *Citrin*.Stayed tuned to further blog updates regarding the *Aon* Court's decision and further debate among the district courts regarding the CFAA's "authorization" requirement.

Related People

Heather Zalar Steele
Partner
610.230.2134
Email