EMPLOYMENT & LABOR ALERT

ROBINSON BRADSHAW & HINSON

SEPTEMBER 2009

THE CFAA – A Way To Take the Traitorous Employee to Federal Court

By Julian H. Wright, Jr. and Jonathan H. Ferry

Few situations trigger an employer's visceral reaction like a disloyal employee who steals or damages sensitive information or computer systems for personal gain or to benefit a competitor. Add to this volatile mix that the employee probably violated explicit agreements to protect that information, and moral outrage can find an outlet in legal action. Often, however, the employer will have to go to state court to assert a state law claim for breach of contract or misappropriation of trade secrets, and will be denied the advantages of litigating in the federal courts. These advantages include a single judge typically handling all proceedings from start to finish, life-tenured judges with full-time law clerks to assist in legal research, and a simpler appeals system.

The near universal use of computers in the modern business environment, however, may provide employers a way to go after traitorous employees in federal court while still being able to assert state law claims. The Computer Fraud and Abuse Act (the "CFAA") allows federal claims against an employee who improperly accesses and utilizes or damages a company's information. Once a case gets into federal court under the CFAA, the court can also hear related state law claims under a doctrine called supplemental jurisdiction. Employers can take specific actions when hiring and training employees to increase the likelihood that relief under the CFAA will be available to them.

THE CFAA

An employer may pursue a disloyal employee under the CFAA in several situations. Most importantly, an employer can assert a CFAA claim for the misappropriation of a company's electronically stored information for personal use or the use of a competitor as well as for the deletion of company information or other damage to a company's computer systems. The backbone of any civil claim under the CFAA is a showing that the employee was either not authorized to access the computer system or exceeded the access for which he or she was authorized.

Plaintiffs must also show one of six additional effects of the employee's misconduct. The first possible effect – and the one that will most often be present in employment cases – is that the violation results in the loss to one or more persons of $5,000 during any one-year period. Less relevant in most employer-employee cases are the five other

possible results (any one of which can give rise to a CFAA claim): 1) the modification or impairment of the medical examination, diagnosis, treatment or care of one or more individuals; 2) physical injury to any person; 3) threat to public health or safety; 4) damage affecting a computer system used by or for a government entity in furthering the administration of justice, national defense, or national security; or 5) damage affecting ten or more computers during any one-year period. Again, although any of these five effects might be present in some circumstances, the $5,000 loss provision will be the most likely basis for a claim against a disloyal employee. Employers can reach the $5,000 loss threshold by including the amounts the employer incurs in investigating what was done on its computer system, so the threshold is a relatively easy one to reach. If an employer can also show "damage" to its computer system, it may have additional claims under the CFAA. Damage under the CFAA includes any impairment to the integrity or availability of data, a program, a system or information.

Access to the Computer Must be Unauthorized or Exceed Authorized Access

Proving the threshold fact that an employee was unauthorized to access a computer system or exceeded authorized access can be the most challenging – and is so far the most litigated – element in a CFAA claim. Usually the employee or former employee was authorized to access the company's computer system and very often had access to the very information he or she damaged or misappropriated. Instead of accessing the information for legitimate work purposes, however, the employee sought to damage the information or obtain it for his or her own gain and to the employer's detriment. Luckily for employers, the court decisions provide some guidance on steps employers can take to clarify what access by an employee is authorized and what access is not.

Some courts have found unauthorized access by an employee or former employee whenever the employee breaches his or her duties as an agent of the employer. In other words, if an employee accesses information for a purpose detrimental to the employer (*i.e.*, to steal it or copy it for a competitor), that access is automatically deemed unauthorized. *See, e.g., International Airport Centers, LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006); *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp.2d 1121 (W.D. Wash. 2000). This approach is highly favorable to employers, and it requires little advance planning to establish that a disloyal employee's access to the computer system was unauthorized. If an employee just acts as a "rogue agent" in accessing the employer's computer system, the access is unauthorized. Under this approach, an employer need not also prove that an employee breached any specific agreements or policies to establish that access was unauthorized.

A significant number of courts, however, explicitly reject this agency analysis and hold that employers typically grant employees access to the employer's computer system. Under these courts' analysis, even a "rogue agent" was only doing what he or she was permitted to do – accessing the employer's computer system – even if for an ulterior purpose. These courts look for documents like employment agreements and employee handbooks that establish the scope of authorized access to the employers' computer systems. *See Lockheed Martin Corp. v. L-3 Communications Corp.*, 2006 WL 2683058 (M.D. Fla. 2006); *Int'l Ass'n of Machinists and Aerospace Workers v. Werner-Masuda*, 390 F. Supp.2d 479 (D. Md. 2005); *Alliance International, Inc. v. Todd*, 2008 WL 2859095 (E.D. N.C. 2008); *America Online, Inc. v. Nat'l. Health Care Discount, Inc.*, 121 F. Supp.2d 1255, 1272 (N.D. Iowa 2000). If an employer finds itself in a court that focuses on employee agreements, access that violates a carefully designed data access policy is much more likely to be found to be unauthorized or to exceed what is authorized.

Employers should therefore develop computer access policies that explicitly limit the scope of authorized use of the company's computers. The policy should specifically state that accessing any information on, or the use of, the company's computers for personal gain, for purposes that would damage the company, or for any other purpose beyond the scope of the employment are prohibited. Further, an employer should seek signed agreements from every employee acknowledging the policy and agreeing to abide by it. Additionally, employers should seek non-disclosure and confidentiality agreements from every employee who has access to sensitive information. If practicable, an employer also should consider access control lists and limiting access to certain sensitive information to only those employees who need it to do their jobs.

Although some courts have denied causes of action under the CFAA, the weight of the legal authority supports a private cause of action under the CFAA for employee misconduct in misappropriating or damaging information on an employer's computer system to which the employee otherwise had access. Taking precautions early to develop computer access and data control policies will increase an employer's chances of successfully maintaining such a CFAA claim in federal court.