# The Computer Fraud & Abuse Act: An Overview of Potential Use in the Departing Employee Context

Insights
6.30.10

The Computer Fraud & Abuse Act, 18 U.S.C. § 1030 ("CFAA"), since its amendment in 1994 to include civil provisions, has become a potentially powerful tool that employers can use against departing employees and their new employers.The civil provisions of the CFAA create a private right of action against those who wrongfully access, or exceed their authorized access, to a protected computer (as defined by the CFAA to includes computers used in interstate or foreign commerce or communication), thereby causing the requisite damage or loss.

**Applicable Provisions of the CFAA**

The CFAA includes seven distinct offenses, set forth in section 1030(a)(1) through (a)(7).The sections most relevant to a potential claim by an employer related to departing employee misconduct or unfair competition are set forth at: 18 U.S.C. 1030(a)(2)(C) (unlawful to intentionally access a protected computer without authorization or in excess of one's authorization and thereby obtain information); 18 U.S.C. 1030(a)(4) (unlawful to knowingly, and with the intent to defraud, access a protected computer without authorization or in excess of one's authorization, and by means of such conduct further the intended fraud and obtain anything of value); 18 U.S.C. 1030(a)(5)(A)(i) (unlawful to knowingly cause the transmission of information, and as a result of such conduct, intentionally cause damage without authorization); and 18 U.S.C. 1030(a)(5)(A)(ii)-(iii) (unlawful to intentionally access a protected computer without authorization, or in excess of one's authorization, and as a result of such conduct, cause damage or recklessly cause damage).

In addition to fitting within one of the sections outlined above, an employer attempting to assert a claim under the CFAA must also consider Section 1030(g), which requires that the conduct complained of must involve a "loss to one or more persons during a 1-year period . . . aggregating at least $5,000 in value."

Courts analyzing the CFAA requirements as outlined above have focused on two main hurdles facing employers who attempt to assert CFAA claims against departing employees: (1) establishing that the employee accessed the computer without authorization or in excess of the employee's authorized access; and (2) establishing that the employer sustained a loss aggregating at least $5,000 in value.

**"Authorization" Requirement**

An employer's best argument that a departed employee accessed its computer system without authorization or in excess of the employee's authorized access is that the employee's authorization ended the very moment that the employee began acting as a agent for someone else or began acting against the employer's best interest.Numerous courts have held that once an employee breaches his or her duty of loyalty to the employer, including by operating in competition with the employer, the employee's authorization to access the employer's computer systems terminates.*See, e.g., Hub Group, Inc. v. Clancy*, No. 05-2046, 2006 WL 208684 (E.D. Pa. Jan. 25, 2006) (employee exceeds 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).It is important, however, for employers to know the current state of the law in the jurisdiction where they are seeking to assert a CFAA claim against a departing employee.Recently, some courts have held that an employee does not act without authorization or in excess of his or her authorized access under the CFAA by accessing the employer's computer systems during employment – even if the employee subsequently uses the accessed information to compete with the employer.*See LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009) (holding that disloyal treatment of information accessed by an employee during employment does not give rise to a CFAA violation).

**"Loss" Requirement**

With regard to the "loss" requirement of the CFAA, it is clear that certain expenses – including amounts expended in responding to an unauthorized access or "re-securing" the computer system, salaries paid to individuals for time spent fixing computer problems, and costs associated with hiring consultants to evaluate the integrity of the computer system – may be counted in reaching the $5,000 "loss" threshold.Courts differ, however, on whether employers can count a loss of business or loss of clients toward meeting the $5,000 "loss" threshold. Again, employers need to review the state of the law in the jurisdiction where they plan to allege a CFAA violation against a departed employee in order to evaluate their ability to prove the requisite loss under the statute.

**Potential Benefits of CFAA Claims**

If an employer is able to meet the CFAA's requirements and successfully assert a claim against a departed employee, there are certain benefits to asserting a claim under the Act.For example, because the CFAA is a federal statute, it provides a basis for federal jurisdiction and thereby expands the choice of forums presented to a potential plaintiff.In addition, the CFAA does not require a showing that the information accessed by the employee is confidential or proprietary in nature.Thus, an employer may be entitled to injunctive relief under the CFAA even where a claim for misappropriation of trade secrets may fail based on the alleged confidential status of the information at issue.

In sum, in addition to the often-included claims for breach of restrictive covenant, misappropriation of trade secrets and/or unfair competition in the departing employee context, employers should also consider whether they have a claim under the CFAA.Although the CFAA is a complicated statute, an

employer who is able to evaluate and properly state a claim under the CFAA benefits by adding a powerful tool to its arsenal against defecting employees.

## *Related People*

**Heather Zalar Steele**
Partner
610.230.2134
Email