

The Legal Intelligencer

THE OLDEST LAW JOURNAL IN THE UNITED STATES 1843 - 2009

PHILADELPHIA

An **ALM** Publication

THE LEGAL INTELLIGENCER

EMPLOYMENT LAW

Can the CFAA Protect Your Business Data?

By Carolyn M. Plump
December 9, 2009

The economic issues facing many companies have resulted in large numbers of employee terminations and resignations. This job reshuffling has brought a variety of employment issues to the forefront for management. One such issue is how best to safeguard business data once employees are asked to leave or elect to resign.

Under the Computer Fraud and Abuse Act, or CFAA, employers can pursue civil claims against former employees if such individuals seek a competitive advantage through the wrongful use of information from their employer's computer system. This article will address what constitutes a civil violation of the CFAA, the two lines of cases interpreting the CFAA's phrase "unauthorized access" and what steps companies can take -- short of filing a lawsuit -- to safeguard their computer information.

ELEMENTS OF A CFAA VIOLATION

Civil liability attaches to an individual under the CFAA if he or she knowingly and with intent to defraud accesses a protected computer without authorization or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, as noted at 18 U.S.C. § 1030. If a court finds there is a civil violation of the CFAA, it may award compensatory damages, injunctive relief or other equitable relief. The statute of limitations for an action under the CFAA is two years from the date of the act complained of or the date of discovery of the damage.

As outlined above, a prerequisite to a claim under the CFAA is proof that a party accessed a protected computer "without authorization" or "exceeded authorized access." The phrase "without authorization" is not defined in the CFAA. The phrase "exceeded authorized access" is defined as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter" at 18 U.S.C. § 1030(e)(6).

CONFLICT REGARDING 'UNAUTHORIZED ACCESS'

In interpreting the meaning of the term "authorization," two distinct lines of cases have evolved. The first line espouses a narrow interpretation of the CFAA and holds that the phrase "without authorization" only reaches conduct by outsiders who do not have permission to access the computer system at issue. (See *Lockheed Martin Corp. v. Speed*, explaining that employees who were granted access to the information at issue did not exceed authorized access.)

In other words, the mere misuse of information to which a defendant has authorized access is not enough to sustain a claim. For example, see *LVRC Holdings LLC v. Brekka*, where an employee in charge of marketing who, among other things, allegedly sent e-mails to his personal computer with company financial and marketing information did not violate the CFAA because he had initial authority to access the computer and the employer never rescinded such permission; *Bridal Expo Inc. v. Van Florestein*, where a court declined to equate authorization with a duty of loyalty to an employer where two employees allegedly downloaded business information on their final day of employment and then used such information to advertise and to solicit business for their competing entity; and *Condux Int'l Inc. v. Haugum*, where a court refused to read the CFAA expansively to allow a claim against a former vice president who allegedly used his authorized access for improper purposes because it would equate a breach of duty of loyalty to an employer with a violation of the CFAA.

By contrast, the second line utilizes a more expansive view and finds unauthorized access whenever the employee, without the employer's knowledge, acquires an interest that is adverse to that of his or her employer or commits a serious breach of loyalty. For example, in *Int'l Airport Ctrs. v. Citrin*, an employee allegedly acted without authorization when he accessed a computer with intent to destroy company information because a breach of his duty of loyalty terminated his authority to access the laptop. Also see *Shurgard Storage Centers Inc. v. Safeguard Self-Storage Inc.*, where employees allegedly acted without authorization when they obtained and sent proprietary information to the defendant.

Under these cases, an employee accesses a computer without authorization if the employee acquires an interest that is adverse to the employer or is guilty of a serious breach of loyalty. For example, see *Guest Tek Interactive Entm't Inc. v. Pullen*, where a company alleged sufficient facts to state a claim under the CFAA based on a former vice president's surreptitious transposing of thousands of company files onto his personal USB device before launching a competing company and in *EF Cultural Travel BV v. Explorica Inc.* a court upheld a CFAA claim against employees who allegedly collected pricing information from their former employer's website in order to develop a competing entity with lower prices.

STEPS TO PROTECT AGAINST UNAUTHORIZED ACCESS

Given the need to provide employees with access to certain information on their work computer systems, what can employers do to protect their business information? At a minimum, companies should take the following affirmative measures to help protect their business property:

- Conduct a comprehensive review of current computer policies -- or develop such policies if none exist -- to evaluate and to define acceptable and unacceptable use of data on the computer system.

- Review computer security protections to flag any unauthorized use of data or unauthorized access to data.
- Require new employees to sign confidentiality agreements that contain language to protect business data.
- Consider whether it is feasible and advisable to prohibit employees from transmitting all (or certain) business data to personal computers or personal devices.
- Revise telecommuting policies to delineate what type of remote access is authorized by the company.
- Hire a company to conduct an audit of all computer systems and security protocols to verify the necessary safeguards are operational and suggest additional methods to protect business information.
- In addition to a written policy, educate employees on what constitutes acceptable use of and access to data on the company's computer system.
- Limit access to sensitive business information such as customer lists, pricing information and business plans only to employees with a legitimate need to know.
- Monitor all access to sensitive business information.
- Investigate potential computer violations and, if warranted, discipline employees for such violations.
- Revise all termination notices and exit letters to include language rescinding any previous authorization for computer access.
- If practical, immediately upon an employee's termination (or upon learning of an employee's resignation), revoke any and all login privileges to prohibit any access to the computer system and the contained therein.

Carolyn M. Plump is a partner in Mitts Milavec's labor and employment law practice group. Plump has successfully negotiated labor contracts, counseled clients regarding regulatory compliance, prepared corporate employment policies and handbooks, conducted investigations and advised companies regarding the hiring, firing and disciplining of employees. She has represented clients in litigation, mediation and arbitration matters in federal court and before administrative agencies.