
Federal Circuits Split on Computer Fraud and Abuse Act

By Brian Zemel, *Litigation News* Associate Editor

A Middle District of Tennessee decision highlights the federal circuits' split over whether an individual who has been granted access to his employer's computers, but who uses that access for an improper purpose, is liable under the Computer Fraud and Abuse Act (CFAA). *ReMedPar, Inc. v. AllParts Med., LLC*.

At the heart of the controversy is CFAA's prohibition on access "without authorization." Some courts, including the Ninth Circuit, have held that a CFAA cause of action is reserved for clear-cut situations akin to hacking, where an individual clearly never had "authorization" to access the computer or information.

Other courts, such as the First and Seventh Circuits, permit recovery if the individual misuses it in a manner inconsistent with the employer's interests or in a manner

that violates a contractual obligation.

Recognizing that the Sixth Circuit has not yet ruled on this issue, the U.S. District Court for the Middle District of Tennessee followed the Ninth Circuit and dismissed a plaintiff's federal trade secret claim.

The plaintiff, ReMedPar, provided one of its independent contractors (a former employee) with extensive access to its proprietary computer system. The plaintiff later discovered that another company had developed a computer system very similar to its system. It also discovered circumstances suggesting that the contractor provided the other company with the confidential information necessary to develop that system.

ReMedPar filed suit against the other company and the independent contractor. Among other things, ReMedPar sought damages under CFAA, which permits recovery from persons who knowingly access a "protected computer" used in interstate or foreign communication and intentionally or recklessly cause damage.

The defendants moved to dismiss the CFAA claim, arguing that the contractor could not have accessed the protected system "without authorization" or in excess of

the authorization provided and that the dismissal of the sole federal claim in the case deprived the federal court of jurisdiction.

The district court ruled that ReMedPar could not prove unauthorized access or loss and dismissed the case without prejudice. The court reasoned that the phrase "without authorization" only refers to persons who do not have permission to access the company's computers in the first place.

That reasoning contrasts with the interpretation of the First and Seventh Circuits, which permit a CFAA claim where a defendant misuses information he or she is authorized to access.

The *ReMedPar* decision "should motivate companies to revisit employment policies and consider drafting specific language setting forth the scope of authorized computer access for employees," suggests Brian Koji, Tampa, vicechair of the Section of Litigation's Employment & Labor Relations Law Committee.

Until there is some clear consensus, "we know that in certain circuits the CFAA will not provide a cause of action against an employee given access to the company's computer," says Koji. 