

# THE NATIONAL LAW JOURNAL

DAILY UPDATES AT NLJ.COM

THE NEWSPAPER FOR THE LEGAL PROFESSION

Monday, March 5, 2007

ALM

## BUSINESS INFORMATION

# E-Discovery Under CFAA

**T**HE COMPUTER Fraud and Abuse Act, 18 U.S.C. 1030, a federal criminal statute outlawing various computer crimes, provides a civil remedy for companies victimized by a violation of the statute. The CFAA expressly permits a private company to sue for compensatory damages and injunctive relief. 18 U.S.C. 1030(g). In this new digital age, the CFAA is fast becoming recognized as a proactive tool that can be used by companies to retrieve stolen data, prevent its dissemination in the marketplace and obtain compensatory damages resulting from its theft, use and malicious destruction.

### Court applied the new rules in 'Ameriwood Industries'

By its nature, a CFAA civil action is almost exclusively dependent on electronic evidence. For that reason, the newly enacted amendments to the Federal Rules of Civil Procedure governing electronic discovery, which became effective on Dec. 1, 2006, will undoubtedly define how discovery is conducted whenever CFAA claims are filed. Indeed, it took less than a month after the effective date of the e-discovery rules for the first federal court in *Ameriwood Industries Inc. v. Liberman*, No. 4:06CV524, 2006 WL 3825291 (E.D. Mo. Dec. 27, 2006), to apply these new rules to a discovery

By Nick Akerman



dispute in a CFAA case. The thrust of the complaint alleged that the “defendant former employees forwarded plaintiff’s customer information and other trade secrets from plaintiff’s computers to defendants’ personal email accounts.” Id. at \*3.

In the course of discovery, the plaintiff served upon the defendants a document request for all of the mirror images (exact bit-for-bit copies) of their entire business and personal hard drives. When the defendants objected to producing their hard drives, claiming that the requests were “overbroad, vague, and burdensome and [called] for irrelevant information,” the plaintiffs moved to compel. Id. at \*2. This article will review how the court decided that motion in the context of the new e-discovery rules and its implications for discovery under the CFAA.

Initially, the court cited to Fed. R. Civ. P. 34(a), which now expressly permits a party to request another party to produce “electronically stored information—including...data compilations stored in any medium from which information can be obtained.” Id. at \*2. The court recognized that Rule 34(a) “does not give the requesting

party the right to search through all of the responding party’s records,” citing to concerns “of confidentiality and privacy.” Id. In addition, the *Ameriwood* court was required under newly enacted Fed. R. Civ. P. 26(b)(2) to engage in a “burden-shifting analysis” to decide whether to order the production of the hard drives sought by the plaintiff.

Rule 26(b)(2) provides: “[T]he party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause....The Court may specify conditions for discovery.”

The court concluded that the defendants met their burden of showing that the electronic evidence sought from the hard drives is not “reasonably accessible” because of undue cost. The court relied upon affidavits submitted by the defendants “describing the significant costs of copying the hard drives, recovering deleted information, and translating the recovered data into searchable and reviewable formats.” Id. at \*3.

Having found that the requested discovery was not reasonably accessible, the court still ordered the discovery because the plaintiff showed “good cause” for the production of the electronic evidence residing on the hard drives. In reaching that conclusion, the court analyzed the factors enumerated in the advisory note to Fed. R. Civ. P. 26(b)(2): “(1) the specificity of the discovery request; (2) the quantity of information available from other and more easily accessed sources; (3) the failure to produce relevant information that seems likely to have existed

**Nick Akerman** is a partner in the New York office of *Dorsey & Whitney* who specializes in the protection of trade secrets and computer data.

but is no longer available on more easily accessed sources; (4) the likelihood of finding relevant, responsive information that cannot be obtained from other, more easily accessed sources; (5) predictions as to the importance and usefulness of the further information; (6) the importance of the issues at stake in the litigation; and (7) the parties' resources."

In essence, the court found that Rule 34(e) electronic discovery was justified based on "the close relationship between plaintiff's claims and defendants' computer equipment." Id. at \*1. These were the allegations in the complaint that the defendants had "used the computers, which are the subject of the discovery request, to secrete and distribute plaintiff's confidential information," creating a factual issue for discovery as to "[h]ow and whether defendants handled those documents and what defendants did with the documents." Id. at \*5.

The court also disposed of the defendants' argument that "the requested information has already been disclosed" in paper documents with the recognition that data, unlike paper documents, contain metadata that describe "the history, tracking, or management of" the electronic file that "is usually not apparent to the reader viewing a hard copy or a screen image." Id. at \*3. Finally, the court emphasized the defendants' failure to produce an e-mail created by a defendant that had only been produced by a third-party recipient of the e-mail, concluding "that other deleted or active versions of emails may yet exist on defendants' computers." Id. at \*3.

Given that the type of wrongdoing upon which the CFAA is premised can best be proven through electronic evidence, "good cause" for electronic discovery in a CFAA case should almost always be a foregone conclusion. For example, in *Physicians Interactive v. Lathian Systems Inc.*, No. CA 03-1193-A, 2003 WL 23018270, at \*1 (E.D. Va. Dec. 5, 2003), a case decided three years before the effective date of the new rules, the plaintiff sued a competitor for violations of the CFAA, alleging that the defendants' "information technology employee...secretly hacked Physicians Interactive's website and stole their confidential customer lists and computer software code." The court ordered discovery because the data sought were unquestionably relevant to the alleged computer attacks. Id. at \*10.

Upon finding "good cause" for the production of the hard drives, the *Ameriwood* court directed a "three-step imaging, recovery, and disclosure process" to provide the "requesting party sufficient access to information that is not reasonably accessible

and ensures the process does not place an undue burden on the responding party." First, the court ordered that the plaintiff choose "a computer forensics expert of its choice...that has been trained in the area of data recovery" to obtain the mirror images of the defendants' hard drives at their premises pursuant to a confidentiality agreement. Id. at \*5.

Second, the expert was charged with recovering "from the mirror images all available word-processing documents, incoming and outgoing e-mail messages, PowerPoint or similar presentations, spreadsheets, and other files included but not limited to those files that were 'deleted.'" Id. at \*6. A full report of the documents found "in a reasonably convenient and searchable form" was then to be provided to defendants' counsel. Id.

## A federal court applied the new e-discovery rules in a Computer Fraud and Abuse Act case shortly after their effective date.

Third, "[w]ithin twenty days of the receipt of the recovered documents and data, defendants' counsel" was required to "review the records for privilege and responsiveness, appropriately supplement defendants' responses to discovery requests, and send to plaintiff's counsel all responsive and non-privileged documents and information." Id. at \*6. The defendants were also ordered to supply the plaintiff's counsel with a privilege log.

The court ordered the plaintiff to pay for the imaging of the computers, recovering the data from the computers and preparing it in readable format for the defendants. While the plaintiff did not object to incurring these costs, it is highly likely that in the balancing process, courts will be strongly influenced by the parties' resources in deciding who pays for the production of the electronic discovery. It is a fair assumption that in most situations the courts will order a large plaintiff company to bear the cost over an individual defendant.

## 'Ameriwood' three-step process could be a model

The three-step process established in *Ameriwood* can be used as a model in the early stages of a CFAA case. Newly amended Fed. R. Civ. P. 26(f) requires the parties to confer as soon as practicable after the case is filed, and certainly prior to the first scheduling conference, about "preserving discoverable information," "any issues relating to disclosure or discovery of electronically stored information, including the form or forms in which it should be produced" and "any issues relating to claims of privilege or of protection as trial-preparation material" including "a procedure to assert such claims after production."

Thus, a plaintiff filing a CFAA case is well advised at the Rule 26(f) conference to propose some variation of the three-step *Ameriwood* process as the basis for a proposal for conducting electronic discovery. Prior to the conference, it is important for the plaintiff's counsel to identify an appropriate computer forensic expert to be assigned the task of reviewing the defendant's computers and the type and sources of data the plaintiff's counsel will need to prove his or her case. A big company suing individuals should be prepared to offer to pay the cost of the forensic expert. Because electronic discovery can involve the production of a huge volume of data, particularly e-mail, this is also the juncture at which a procedure should be agreed upon pursuant to new Rule 26(b)(5)(B) to return inadvertently produced privileged documents.