MORRISON | FOERSTER

Legal Updates & News

Bulletins

Court Rejects Computer Fraud and Abuse Act Claim

October 2007

Privacy Bulletin, October 17, 2007

On July 13, 2007, the U.S. District Court for the Eastern District of Pennsylvania ("District Court") ruled that an accountant who used his computer to copy information about a previous employer's clients to share with his new employer did not violate the Computer Fraud and Abuse Act ("CFAA") (*Brett Senior & Assocs. v. Fitzgerald*, No. 06-1412, 2007 WL 2043377 (E.D. Pa. July 13, 2007)).

The plaintiff required all of its employees, including the defendant, to sign a confidentiality agreement. In January 2005, the defendant accountant interviewed with the defendant firm and in November 2005, the defendant accountant notified the plaintiff that he had accepted a job with the defendant firm. Both the defendant accountant and the plaintiff contacted clients and informed them of the defendant accountant's decision to work elsewhere. The defendant accountant managed to get 15 of 20 clients to go with him to the defendant firm.

Prior to leaving the plaintiff, the defendant accountant made copies of information in his files—tax information for clients with whom he had signed engagement letters, clients for whom he was the contact person, and clients whom he brought to the plaintiff. The defendant accountant also e-mailed the defendant firm the engagement letters and financial statements of clients with whom he had signed engagement letters.

According to the District Court, there is no evidence that the information copied by the defendant accountant and e-mailed to the defendant firm was ever used by either defendant. After the plaintiff warned the defendant accountant not to use information taken, the defendant accountant obtained client information from his work papers and the clients themselves. Among other things, the plaintiff claimed that both defendants violated the CFAA.

The CFAA provides that whoever "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 . . . shall be punished . . . ." Thus, the District Court explained that to show a violation of the CFAA, the plaintiff must prove that the defendant has accessed a "protected computer," has done so without authorization or by exceeding such authorization as was granted, has done so "knowingly" and with the "intent to defraud," and, as a result, has "further[ed] the intended fraud and obtain[ed] anything of value."

The plaintiff claimed that the defendant accountant violated the CFAA by accessing its computer system to transfer files to the defendant firm. Specifically, the plaintiff claimed that the defendant accountant violated section 1030(a)(4) of the CFAA when he copied the plaintiff's client files, created a list of the clients he serviced while working with the plaintiff, transformed plaintiff's files to certain formats for the purpose of transferring them to the defendant firm, and e-mailed information relating to four clients of the plaintiffs to the defendant firm.

According to the District Court, the parties agreed that the question presented by the CFAA claim is whether the defendant accountant's actions satisfy the second element of a section 1030(a)(4) claim. In other words, did the defendant accountant access a computer "without authorization" or "exceed" his "authorized access"?

Under the CFAA, "exceeds authorized access" is defined as accessing "a computer with authorization" and using "such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." According to the District Court, this does not apply to the defendant accountant's conduct because he

did not obtain any information that he was not entitled to obtain or alter any information that he was not entitled to alter. In addition, the District Court noted that the plaintiff testified that the defendant accountant was allowed full access to information contained in the plaintiff's computer system until his departure.

The District Court also noted that the plaintiff did not argue that the defendant accountant's action of converting his files to a certain format, making a list of his clients, or copying client information to an external hard drive was actionable per se. Instead, the plaintiff alleged that the use of this "appropriately-obtained information was improper." The District Court found, however, that the conduct under section 1030(a)(4) of the CFAA is the unauthorized procurement or alteration of information, not its misappropriation or misuse. Because there was no allegation that the defendant accountant lacked authority to view any information in the plaintiff's computer system, the District Court ruled that the CFAA claim failed.