# U.S. Loses Argument that the Computer Fraud & Abuse Act Applies to Employees Who Access Work Computers

Insights
11.10.10

The recent developments in the criminal prosecution of Sergey Aleynikov for his alleged misappropriation Goldman Sach's high-frequency trading platform provide more interesting insights in the ongoing debate within the federal judiciary concerning the scope of the federal Computer Fraud and Abuse Act ("CFAA"). Specifically, federal courts continue to debate whether the CFAA applies to the misappropriation of an employer's electronic trade secrets by departing employees. In United States v. Aleynikov, the United States District Court for the Southern District of New York said the statute does not apply in this context. In reaching this conclusion and dismissing the CFAA-based count against Aleynikov, the federal court cited the civil interpretations of the CFAA offered by some recent courts that reached this same conclusion and rejected the holdings taking the opposite interpretation.

Count Three of the Indictment charged Aleynikov with unauthorized computer access and exceeding authorized access in violation of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030(a)(2)(C). Specifically, Count Three alleged that Aleynikov "unlawfully, intentionally, and knowingly ... accessed a computer server maintained by Goldman and copied Goldman's proprietary computer source code ... and then downloaded it to his home computer, all with the intent to use that source code for the economic benefit of himself and his new employer, Teza."

Aleynikov argued that Section 1030(a)(2) does not encompass an employee's misuse or misappropriation of information that the employee has authority to access. In response, the United States conceded that Aleynikov was authorized to access the source code for the High-Frequency Trading Platform System that he allegedly stole, but argued that a defendant's purpose or intention is a necessary component of the violation. According to the Government, the CFAA is therefore violated whenever an individual accesses information with authorization, but does so in violation of a confidentiality agreement or policies or other obligations that the individual owes to the information's owner.

The disagreement between Aleynikov and the United States turns on Section 1030(a)(2) of the CFAA. It provides that anyone who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer" commits a crime. 18 U.S.C. § 1030(a)(2)(C). The CFAA defines "exceeds authorized access" 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." Id. § 1030(e)(6). The CFAA does not, however, define the term "access without authorization" or "authorization."

In order to resolve the dispute and define "authorization," the court looked to its ordinary meaning as provided by dictionaries. The court concluded that "a person who "accesses a computer without authorization" does so without any permission at all. By contrast, a person who "exceeds authorized access" has permission to access the computer, but not the particular information on the computer that is at issue." Interestingly, the court also noted that this interpretation of § 1030(a)(2)(C) was supported by holdings in civil actions by U.S. Court of Appeals for the 9th Circuit, district courts in the United States 2nd Circuit and in other circuits, which recently held that an employee with authority to access his employer's computer system does not violate the CFAA by using his access privileges to misappropriate information.

In dicta, but important to the ongoing debate over the scope of the CFAA, the Court specifically rejected the reasoning of other courts such as in Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 420-21 (7th Cir. 2006) and EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582-84 (1st Cir. 2001). In its pointed disagreement with the reasoning underlying these cases, the court concluded that:

"an interpretation of the CFAA based upon agency principles would greatly expand the reach of the CFAA to any employee who accesses a company's computer system in a manner that is adverse to her employer's interests. This would convert an ordinary violation of the duty of loyalty or of a confidentiality agreement into a federal offense. An employee does not lose "authorization" by accessing a computer with an improper purpose; rather, authorization is controlled by the employer, who may or may not terminate or restrict an employee's access privileges."

This holding could have important implications for employers who want to use the CFAA as an enforcement tool against departing employees. If this interpretation and reasoning were to become the consensus, then it would foreclose use of the CFAA in cases where employees only misappropriated electronic trade secrets. A copy of the Court's Opinion is available in pdf format below.

*Brent Cossrow is a member of Fisher Phillips' Employee Defection & Trade Secrets Practice Group. Mr. Cossrow's practice focuses on e-discovery and other electronically stored information issues. As always, please feel free to share your thoughts and questions in the comment space below. Mr. Cossrow has written previously about the Aleynikov prosecution in Risk Management Magazine (pdf copy below) and has been interviewed about it as well.*

US v. Aleynikov.pdf (112.71 kb)

Risk Management Magazine -- Jan-Feb 2010.pdf (1.28 mb)

### *Related People*

**Brent A. Cossrow**
Regional Managing Partner
610.230.2135
Email