Nick Akerman
(212) 415-9217 ▪ akerman.nick@dorsey.com

Nick is a partner in the New York office of Dorsey & Whitney.

For additional articles like this one go to http://computerfraud.us

DORSEY
DORSEY & WHITNEY LLP

Computer Fraud and Abuse Act Count Dismissed Against Goldman Sachs Computer Programmer Charged with Stealing Source Code

A New York federal Judge dismissed the Computer Fraud and Abuse Act ("CFAA") count charging Sergey Aleynikov, a former computer programmer for Goldman Sachs & Co., with stealing the computer source code used in Goldman's high-frequency trading system. *U.S. v. Aleynikov*, 2010 WL 3489383 *14-17 (S.D.N.Y. Sept. 3, 2010). The reasoning underlying this opinion underscores the need for the U.S. Supreme Court to resolve the conflict between the 9th Circuit and the 1st, 5th, 7th and 11th Circuits on the applicability of the CFAA to employees who steal data from their employers.

As described by the court, "Aleynikov was responsible for developing and maintaining some of the computer programs used to operate Goldman's high-frequency trading system. Aleynikov resigned in June 2009 to work for Teza Technologies, LLC ("Teza"), a company founded earlier that year. Teza offered Aleynikov the title of 'Executive Vice President, Platform Engineering,' in which position he would be responsible for developing Teza's own high-frequency trading business that would compete with Goldman." *Id*. at 1.

Based on his theft of Goldman's source code, Aleynikov was charged with one count of violating the Economic Espionage Act for theft of trade secrets, Title 18, U.S.C. §§ 1832(a)(2) and (4), one count of violating the Interstate Transportation of Stolen Property Statute, Title 18 U.S. C. §2314, and one count of violating the CFAA, Title 18 U.S.C. §1030(c)(2)(B)(i)-(iii). The court granted the motion to dismiss the CFAA count while denying Aleynikov's motion to dismiss the other two counts.

In dismissing the CFAA the count court relied on *LVRC Holdings LLC v. Brekka,* 581 F.3d 1127, 1130-31 (9th Cir.2009) for its proposition 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." *Id.* at 13. Thus, the court concluded that the ordinary meaning of the statute outlawing unauthorized access cannot apply to employees who are provided access to the company computers and that "[w]hat use an individual makes of the accessed information is utterly distinct from whether the access was authorized in the first place." *Id.* at 15.

The court rejected the premise of the Seventh Circuits opinion in *Int'l Airport Ctrs., LLC v. Citrin*, 440 F.3d 418, 420-21 (7th Cir. 2006) that an employee's authorization to access the company computer is predicated on the agency relationship with his employer and the First and Fifth Circuits which allow the employer to place limits on the scope of the employee's authorization to access the company computers. *U.S. v. John*, 597 F.3d 263, 271 (5th Cir. 2010) and *EF Cultural Travel BV v. Explorica, Inc*., 274 F.3d 577, 582-84 (1st Cir. 2001).

The court faults these three circuit cases because "they identify no statutory language that supports interpreting the CFAA to reach misuse or misappropriation of information that is lawfully accessed, but that "[i]nstead, they improperly infer that "authorization" is automatically terminated where an individual "exceed[s] *the purposes* for which access is 'authorized.' " *Id*. at 17. Other than point out the obvious that these "cases would require an analysis of an individual's subjective intent" (Id.) in accessing the computer (a requirement in every criminal statute for determining whether a defendant's actions amounted to a crime), the court does not address why the First Circuit is incorrect in its view that 'the CFAA permits computer owners to "spell out explicitly what is forbidden" on its computers, *EF Cultural Travel B.V. v. Zefer Corp*., 318 F.3d 58, 63 (1st Cir. 2003).

Indeed, if the ordinary meaning of "authorization," as the court explains is to "to grant authority or permission to do something," why cannot an employer set out the scope of an employee's permissions to access the computer? That such employer generated permissions may form the basis for a criminal violation of the CFAA is totally proper and is no different than the long established principle that a "No Trespass" sign can form the predicate for criminal trespass in some jurisdictions.

In *U.S. v. Salum*, 257 Fed. Appx, 225, 230-31 (11th Cir. 2007), a case not discussed by the court, a police officer with the Montgomery, Alabama Police Department was convicted for violating the CFAA for providing information from the FBI's criminal record database to a private investigator. Although Salum, as an employee, "had authority to access the [National Crime Information Center] database," the court held that there was sufficient evidence for the jury to conclude that Salum had accessed the computer "without authorization" because at the time he accessed the computer Salum knew that he was accessing the information "for an improper purpose" that was contrary to the work rules governing how the database was to be used. *Id*. at 230.

Second, the court held 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" and that "[t]his would convert an ordinary violation of the duty of loyalty or of a confidentiality agreement into a federal offense." *Id* at 17. This statement by the court ignores the Supreme Court's holding in *Carpentaer v. United States*, 484 U.S. 19, 27 (1987) which has already approved converting an ordinary violation of a duty of loyalty to a federal offense. In *Carpenter* the Court relied upon the Restatement (Second) of Agency to affirm the mail and wire fraud convictions of a *Wall Street Journal* reporter who prior to publication had provided his upcoming financial columns to his confederates who bought or sold stock "based on the probable impact of the column on the market." *Id*. at 23.

The defendant columnist argued that that his "conduct in revealing prepublication information was no more than a violation of workplace rules and did not amount to fraudulent activity that is prescribed by the mail and wire fraud statutes." *Id*. 27. Based on the Restatement, the Court

held that "an employee has a fiduciary obligation to protect confidential information obtained during the course of his employment" and that intentionally exploiting that information for his own personal benefit was a scheme to defraud his employer of confidential information outlawed by the mail and wire fraud statutes. *Id.*

If the Restatement can proscribe the duty of an employee in the context of the mail and wire fraud statutes to safeguard his employer's confidential information, there is no sound reason why it cannot also proscribe the scope of an employee's authorization to access his employer's computer in the context of the CFAA. What is remarkable in the *Aleynikov* case is that the court did cite to *Carpenter* in that portion of its opinion dealing with the interstate transportation of stolen property count but ignored its relevance to the CFAA count. *Aleynikov* at *11, n.16.

In short, as the *Aleynikov* decision reflects, the conflict among the Circuits created by the Ninth Circuit's opinion in *Brekka* and the inconsistencies in its reasoning with established Supreme Court precedent can only be resolved by the Supreme Court.