The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

MEMO# 26244

June 15, 2012

2nd Circuit Court Finds That Theft of Proprietary Trading Programs by Former Employee Does Not Violate National Stolen Property or Economic Espionage Acts

[26244]

June 15, 2012

TO: PRIVACY ISSUES WORKING GROUP No. 1-12
TECHNOLOGY COMMITTEE No. 10-12
SEC RULES MEMBERS No. 52-12
COMPLIANCE MEMBERS No. 9-12
SMALL FUNDS MEMBERS No. 20-12 RE: 2nd CIRCUIT COURT FINDS THAT THEFT OF PROPRIETARY TRADING PROGRAMS BY FORMER EMPLOYEE DOES NOT VIOLATE NATIONAL STOLEN PROPERTY OR ECONOMIC ESPIONAGE ACTS

The U.S. Court of Appeals for the Second Circuit recently overturned the criminal conviction of a computer programmer who had been found guilty of two counts of stealing and transferring proprietary computer source code used in his employer's high frequency trading system. [1] The facts of this case and the reasoning behind the court's decision are summarized below.

Background

The Defendant-Appellant was a computer programmer who had been employed by an investment banking firm from May 2007-2009. His work involved helping develop computer source code for his employer's proprietary high-frequency trading (HFT) system, including infrastructure programs to facilitate the flow of information throughout the firm's trading system and monitor the system's performance. According to the court, the employer closely guarded the secrecy of each component of its system and does not license the system to anyone. The employer's confidentiality policies bound the Defendant-Appellant to keep in strict confidence all of the employer's proprietary information, including any intellectual property he created. The employer's policies also barred him from taking such property or using it when his employment ended.

In 2009, he left the investment banking firm to work for a Chicago-based startup that was looking to develop its own HFT system. The Defendant-Appellant was hired to develop the market connectivity and infrastructure components of the startup's HFT system. Just before the Defendant-Appellant's going away party at the investment banking firm, he encrypted and uploaded to a server in Germany more than 500,000 lines of source code for the firm's HFT system, including code for a substantial part of the infrastructure and some of the algorithms and market data connectivity programs. Some of this code pertained to programs that could operate independently of the rest of the investment banking firm's system and be integrated into a competitor's system. After uploading the source code, the Defendant-Appellant deleted the encryption program as well as the history of his computer commands. When he returned to his home in New Jersey, he downloaded the code from the German server to his home computer and copied some of the files to other computer devices he owned, including to a flash drive and laptop. He subsequently took the flash drive and laptop with him to Chicago when he met with representatives of the startup.

In July 2009, when he was returning to New Jersey from Chicago, he was arrested by the FBI and indicted on three counts:

- Count One charged him with violating the Economic Espionage Act of 1996 (EEA) by downloading a trade secret "that is related to or included in a product that is produced for or placed in interstate or foreign commerce with the intent to convert such trade secret and to injure its owner to the economic benefit of anyone other than the owner."
- Count Two charged him with violating the National Stolen Property Act (NSPA), which makes it a crime to transport, transmit, or transfer in interstate or foreign commerce any goods, wares, merchandise, securities or money, of the value of $5,000 or more, knowing the same to have been stolen, converted, or taken by fraud.
- Count Three charged him with unauthorized computer access and exceeding authorized access in violation of the Computer Fraud and Abuse Act.

Lower Court's Decision

In the lower court, the Defendant-Appellant moved to dismiss the indictment for failure to state an offense. The district court dismissed Count Three of the indictment but otherwise denied the motion. After a jury trial on the remaining two counts, the Defendant-Appellant was convicted of both counts and sentenced to 97 months imprisonment, followed by a three-year term of supervised release, and ordered to pay a $12,500 fine. He was denied bail pending appeal because, as a dual citizen of the United States and Russia, he was feared to be a flight risk.

Appellate Court's Decision

On appeal, the Defendant-Appellant renewed his challenge to the sufficiency of the indictment on Counts One and Two. According to the Court of Appeals for the Second Circuit, this challenge required the court to determine the scope of the two federal statutes at issue, the EEA and the NSPA.

The NSPA

As noted above, the NSPA makes it a crime to transport, transmit, or transfer in interstate or foreign commerce any "goods, wares, merchandise, securities or money, of the value of $5,000 or more, knowing the same to have been stolen, converted or taken by fraud." Inasmuch as the statute does not define the terms "goods," "wares," or "merchandise," the issue before the court was whether the source code the Defendant-Appellant downloaded to his computer devices in New Jersey, and later transferred to Chicago, constituted stolen goods, wares, or merchandise within the meaning of the NSPA. According to the court, theft of the source code did not fall within the NSPA's prohibitions because there were no "tangible objects" taken or transported. In the words of the court:

> By uploading [the investment firm's] proprietary source code to a computer server in Germany, [the Defendant-Appellant] stole purely intangible property embodied in a purely intangible format. There was no allegation that he physically seized anything tangible [from the firm], such as a compact disc or thumb drive containing source code, so we need not decide whether that would suffice as physical theft. . . . The later storage of intangible property on a tangible medium does not transform the intangible property into a stolen good. . . . Because the [Defendant-Appellant] did not 'assume physical control' over anything when he took the source code, and because he did not 'deprive [the firm] of its use,' [the Defendant-Appellant] did not violate the NSPA. [2]

The EEA

The court next turned to the sufficiency of the indictment as to the EEA. The court noted that the Defendant-Appellant was charged with violating the section of the EEA that provides as follows:

> Whoever, with intent to convert a trade secret, that is related to or included in a product that is produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly . . . without authorization . . . downloads, uploads, . . . transmits, . . . or conveys such information is guilty of a federal offense, and may be imprisoned for up to 10 years. [Emphasis in original.]

The court began its analysis by noting that the EEA's scope is limited to products that are "produced for" or "placed in" interstate or foreign commerce. It also noted that the words of a statute must be read in their context and with a view to their place in the overall statutory scheme. The court noted that the investment firm's HFT system

> . . . was neither 'produced for' nor 'placed in' interstate or foreign commerce. [The firm] had no intention of selling its HFT system or licensing it to anyone. It went to great lengths to maintain the secrecy of its system. The enormous profits the system yielded for [the firm] depended on no one else having it. Because the HFT system was not designed to enter or pass in commerce, or to make something that does, [the Defendant-Appellant's] theft of source code relating to that system was not an offense under the EEA. [3]

The court added that the "conduct found by the jury is conduct that [the Defendant-

Appellant] should have know was in breach of his confidentiality obligations [to the firm], and was dishonest in ways that would subject him to sanctions; but he could not have known that it would offend this criminal law or this particular sovereign." [4]

Based on the above, the district court's judgment was reversed and the Defendant-Appellant's conviction overturned.

Tamara K. Salmon
Senior Associate Counsel

endnotes

[1] See United States of America v. Sergey Aleynikov (2nd Cir. April 11, 2012) ("Decision"), which is available on the court's website at: http://www.ca2.uscourts.gov/decisions/isysquery/cbfa450b-2707-489e-ab97-a2572d4636e8/1/doc/11-1126_complete_opn.pdf#xml=http://www.ca2.uscourts.gov/decisions/isysquery/cbfa450b-2707-489e-ab97-a2572d4636e8/1/hilite/.

[2] Decision at pp. 17-18. The court distinguished a case in which photocopied documents outlining manufacturing procedures for pharmaceuticals that were transported across state lines were found to be the taking of a tangible good in violation of the NSPA.

[3] Decision at p. 27.

[4] Decision at p. 28.