May 8, 2012

On April 11, 2012, the United States Court of Appeals for the Second Circuit issued a much anticipated opinion explaining the reasons that it vacated the conviction of former Goldman Sachs' programmer, Sergey Aleynikov, under the federal National Stolen Property Act[1] ("NSPA") and the federal Economic Espionage Act[2] ("EEA"). As a result of the Second Circuit's decision in *United States v. Aleynikov,* companies that have developed proprietary software that they use to run their business, but that do not offer to sell or license this software to third parties, will no longer be able to seek federal criminal enforcement under the NSPA or the EEA when such software is stolen, at least in the Second Circuit (New York, Connecticut and Vermont). It is possible, perhaps even likely, that this case will also apply to SaaS companies that offer their software as a part of a service to customers, but do not make their software directly available to those customers. Although the case only affects federal cases arising in the Second Circuit, it may be applied by analogy in other federal courts.

Facts

Sergey Aleynikov, a computer programmer employed by Goldman Sachs, was involved in the development of Goldman's proprietary high-frequency trading ("HFT") system for making large volumes of trades in securities and commodities based on trading decisions effected in fractions of a second. Aleynikov encrypted and uploaded more than 500,000 lines of source code for the HFT system to a server in Germany and then deleted the encryption program as well as the history of his computer commands from the Goldman network, before he left the company to work for Teza Technologies, where he had been hired to develop an HFT system.

Holding

The Second Circuit rejected the district court holding that the HFT source code constituted "goods" that were "stolen" within the meaning of the NSPA because the source code "contains highly confidential trade secrets related to the Trading System" that "would be valuable for any firm seeking to launch, or enhance, a high-frequency trading business."[3] Chief Judge Dennis Jacobs acknowledged that the HFT code was "highly valuable," but cited a long line of cases interpreting the NSPA that have held that the theft and subsequent interstate transmission of purely intangible property is beyond the scope of the NSPA. He concluded that Aleynikov stole purely intangible property when he uploaded Goldman's proprietary source code to a computer server in Germany and therefore there was no violation of the NSPA.

The Court then rejected the district court's finding that Aleynikov's conduct violated the EEA. The Court noted that Section 1832 of the EEA imposes the following limitation:

> 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, injury 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.] *(italics added)*

The district court held that a product is "produced for" interstate commerce if its purpose is to facilitate or engage in such commerce. As a result, it concluded that the HFT system was "produced for" interstate commerce because, "the sole purpose for which Goldman purchased, developed, and modified the computer programs that comprise the Trading System was to engage in

interstate and foreign commerce" and because, "Goldman uses the Trading System to rapidly generate high volumes of trades in various financial markets," which in turn generate many millions of dollars in annual products.

The Second Circuit, however, concluded that the phrase "produced for" interstate or foreign commerce should not have been given such a broad interpretation. Noting that the EEA was enacted the year after the Supreme Court issued its landmark decision in *United States v. Lopez,* which held that Congress's Commerce Clause authority is limited to those activities that "substantially affect interstate commerce,"[4] the Court concluded that the term "produced for" should be interpreted narrowly. The Court reasoned that the words "produced for" had likely been intended to cover only products that had not yet been "placed in" commerce, but were under development or being readied to be placed in commerce. Applying this interpretation, the Court concluded that Goldman's HFT system was neither "produced for" nor "placed in" interstate or foreign commerce because Goldman had no intention of selling or licensing it to anyone. Because the HFT system was not designed to enter or pass in commerce, or to make something that does, Aleynikov's theft of source code related to that system did not violate Section 1832 of the EEA.

Conclusion

The decision does not leave such companies without remedies against those who steal valuable proprietary software which is not sold or licensed to others. Aleynikov's actions likely violated the Uniform Trade Secret Act, some form of which has been enacted into law in 47 states, and which provides civil remedies for misappropriation of trade secret information, as well as federal copyright law. His actions may also have violated state penal laws.[5] In addition, as Chief Judge Jacobs noted, Aleynikov's actions violated Goldman's confidentiality policies that required him to keep in strict confidence all of the firm's proprietary information, including any intellectual property created by Aleynikov, and barred him from taking it or using it when his employment ended.

Recommendation

We recommend that companies review the forms of agreements that they use with their employees and contractors to ensure that they include robust provisions prohibiting the theft of any confidential information, whether in tangible or non-tangible form. These provisions should include, at a minimum:

1. A prohibition against disclosure or use of the company's confidential information, except in connection with work for the company, both during the term of the agreement and at any time thereafter.
2. An obligation to return, on termination of employment or at the company's request at any other time, all of the company's property, equipment and documents, together with all copies thereof, and any other material containing or disclosing company's confidential information, and at company's request, an obligation to certify in writing that the employee or contractor has complied with the foregoing.
3. An acknowledgement that any breach of the foregoing obligations by the employee or contractor would cause irreparable injury to the company for which monetary damages would not be adequate and therefore will entitle the company to injunctive relief.

Notes

1 18 U.S.C. §2314.

2 18 U.S.C. §1832.

3 *United States v. Aleynikov,* No. 11-1126, 2012 WL 1193611 (2nd Cir., April 11, 2012)

4 514 U.S. 549, 558-59 (1995).

5 For example, California law may impose criminal penalties for stealing trade secrets. See Cal. Penal Code 499c, 502.

Key Contacts

Adam Ruttenberg Washington, DC	aruttenberg@cooley.com +1 202 842 7804