

10-17-96

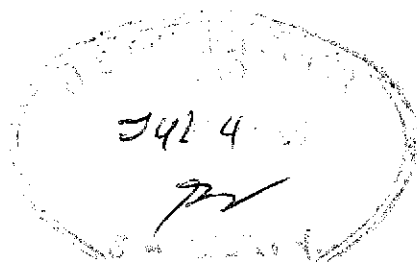
09 MAG 1553

Approved:

*J.P. Facciponti*  
JOSEPH P. FACCIPONTI  
Assistant United States Attorney

Before:

HONORABLE KEVIN NATHANIEL FOX  
United States Magistrate Judge  
Southern District of New York



----- x

UNITED STATES OF AMERICA : Violations of  
-v.- : 18 U.S.C. §§ 1832(a)(2),  
: 2314, & 2

SERGEY ALEYNIKOV, : COUNTY OF OFFENSE:  
Defendant. : NEW YORK

----- x

**DOC #** 1

SOUTHERN DISTRICT OF NEW YORK, ss.:

MICHAEL G. McSWAIN, being duly sworn, deposes and says that he is a Special Agent with the Federal Bureau of Investigation ("FBI"), and charges as follows:

COUNT ONE  
(Theft of Trade Secrets)

1. From at least on or about June 1, 2009, up to and including July 3, 2009, in the Southern District of New York and elsewhere, SERGEY ALEYNIKOV, the defendant, unlawfully, willfully, and knowingly, without authorization, copied, duplicated, sketched, drew, photographed, downloaded, uploaded, altered, destroyed, photocopied, replicated, transmitted, delivered, sent, mailed, communicated, and conveyed, a trade secret that is related to and included in a product that is produced for and placed in interstate and foreign commerce, with the intent to convert that trade secret to the economic benefit of someone other than the owner thereof, and intending and knowing that the offense would injure the owner of that trade secret, to wit, ALEYNIKOV, while in New York, New York and elsewhere, copied, without authorization, proprietary computer code belonging to a financial institution in the United States and then uploaded the code to a computer server in Germany.

(Title 18, United States Code, Sections 1832(a)(2) & 2.)

COUNT TWO

(Transportation of Stolen Property in Foreign Commerce)

2. From at least on or about June 1, 2009, up to and including July 3, 2009, in the Southern District of New York and elsewhere, SERGEY ALEYNIKOV, the defendant, unlawfully, willfully, and knowingly, transported, transmitted, and transferred in interstate and foreign commerce goods, wares, merchandise, securities, and money, of the value of \$5,000 and more, knowing the same to have been stolen, converted and taken by fraud, to wit, ALEYNIKOV, while in New York, New York and elsewhere, copied, without authorization, proprietary computer code, the value of which exceeds \$5,000, belonging to a financial institution in the United States and then uploaded the code to a computer server in Germany.

(Title 18, United States Code, Sections 2314 & 2.)

The basis for my knowledge and for the foregoing charges are as follows:

3. I am a Special Agent with the FBI assigned to the New York Field Office, and have been employed as a Special Agent by the FBI for approximately two and one-half years. I am currently assigned to the FBI's Securities Fraud squad, which investigates, among other things, crimes involving financial institutions. I have received training in, among other things, the means and methods by which individuals use computers and the internet to commit federal offenses, including the theft of trade secrets and the interstate transfer of stolen property. Because this affidavit is being submitted for a limited purpose, I have not included in it everything I know about this investigation. Where the contents of documents and the actions, conversations, and statements of others are related herein, they are related in substance and in part.

The Proprietary Computer Code

4. Based on my investigation, I know that an entity that I shall refer to hereinafter to as the "Financial Institution" is headquartered in New York, New York, and provides a wide range of financial services throughout the world. Based on my conversations with the Financial Institution's representatives, I know the following:

a. Over the past several years, the Financial Institution has devoted substantial resources to developing and

maintaining a computer platform (the "Platform")<sup>1</sup> that allows the Financial Institution to engage in sophisticated, high-speed, and high-volume trades on various stock and commodities markets. Among other things, the Platform is capable of quickly obtaining and processing information regarding rapid developments in these markets. The speed and efficiency by which the Platform obtains and processes market data allows the Financial Institution to employ additional programs that use sophisticated mathematical formulas to place automated trades in the markets based, among other things, on the latest market conditions. The trades made through the Platform typically generate many millions of dollars of profits per year for the Financial Institution. The Financial Institution estimates that it has spent many millions of dollars on the acquisition and development of the Platform and its accompanying programs.

b. The Financial Institution considers the Platform, its accompanying programs, and the underlying computer code,<sup>2</sup> to be confidential and proprietary. The Financial Institution does not license the Platform to any third parties, and does not share the computer code for the Platform with any third parties, except insofar as is necessary to maintain or improve the computer connection between the Platform and the computer systems of the equity and commodities markets with which the Platform interacts. Employees of the Financial Institution who have access to the Platform's computer code are instructed that they are not permitted, without prior authorization, to distribute or transmit that code outside of the Financial Institution's computer network.

c. The Financial Institution has undertaken steps to prevent the unauthorized transfer of the Platform's code to third parties. For example, among other measures, the Financial Institution scans outgoing e-mail messages sent by its employees to prevent the unauthorized transfer of code outside the Financial Institution. The Financial Institution also

---

<sup>1</sup>Typically, a computer "platform" refers to the hardware framework (such as, for example, the physical components of a computer) or software framework (such as, for example, the operating system running on a particular computer) on which other computer programs may operate. In referring to the Platform herein, I am referring primarily to the Platform's software framework.

<sup>2</sup>Computer "code" refers to the computer programming commands that constitute a computer program or platform.

prohibits ftp<sup>3</sup> file transfers outside of its computer network. Within the past few weeks, the Financial Institution began regular monitoring of https<sup>4</sup> transfers made to destinations outside its computer network.

d. The Financial Institution believes that certain features of the Platform, such as the speed and efficiency by which it obtains and processes market data, give the Financial Institution a competitive advantage among other firms that also engage in high-volume automated trading. The Financial Institution further believes that, if competing firms were to obtain the Platform and use its features, the Financial Institution's ability to profit from the Platform's speed and efficiency would be significantly diminished.

#### The Defendant's Employment at the Financial Institution

5. Based upon my conversations with Financial Institution representatives and my review of records provided by the Financial Institution, I know the following:

a. SERGEY ALEYNIKOV, the defendant, was employed by the Financial Institution as a computer programmer from in or about May 2007 until on or about June 5, 2009. ALEYNIKOV was employed in one of the New York, New York, offices of the Financial Institution. While working at the Financial Institution, ALEYNIKOV was part of a team of employees who are responsible for, among other things, developing and improving the Platform. To facilitate the performance of his responsibilities at the Financial Institution, ALEYNIKOV was given access to the computer code for the Platform and its associated programs.

b. Upon the start of his employment with the Financial Institution, ALEYNIKOV was required to review and accept the Financial Institution's standard confidentiality agreement, which provided, among other things, that ALEYNIKOV was

---

<sup>3</sup>"File transfer protocol," or "ftp" refers to a means of transmitting computer files over the internet.

<sup>4</sup>"Https" refers to a secure form of "hypertext transfer protocol," or "http," which is a form of internet communication frequently used to access websites on the internet. Https differs from http because https uses a secure, encrypted connection between the originating and recipient computers in an internet communication, making it less likely that the communication could be intercepted or exploited by a third party.

to hold, "in strict confidence," all non-public information pertaining to, among other things, the Financial Institution's "business and financial affairs" and "operating procedures" and that such non-public information was not to be disclosed, without authorization, to any person or entity, including another Financial Institution employee, "who does not have a need to know or see" the information. In addition, the confidentiality agreement provided that any documents or other materials containing the Financial Institution's non-public information were to be returned to the Financial Institution upon the termination of employment.

c. It is the Financial Institution's policy to regularly instruct all employees who had access to computer code related to the Platform and other proprietary computer programs, such as ALEYNIKOV, to not transfer that code outside of the Financial Institution's computer network.

d. At some point prior to June 2009, ALEYNIKOV notified the Financial Institution that he intended to resign from his employment. ALEYNIKOV's last day of work was on or about June 5, 2009. At the time of his resignation, his annual salary was approximately \$400,000.

6. According to a Financial Institution representative who was responsible for supervising SERGEY ALEYNIKOV, the defendant, and who spoke with ALEYNIKOV regarding his resignation, I have learned that ALEYNIKOV stated that he was leaving the Financial Institution to work for a new company that intended to engage in high-volume automated trading. ALEYNIKOV further reported that the new company was to pay him approximately three times his annual salary at the Financial Institution.

#### The Unauthorized Transfer of the Platform's Code

7. According to representatives of the Financial Institution, within the past few weeks, I have learned that the Financial Institution has begun monitoring the uploads of large amounts of data from the Financial Institution's computer system via https. As a result of that review, the Financial Institution learned that the work desktop<sup>5</sup> of SERGEY ALEYNIKOV, the

---

<sup>5</sup>According to representatives of the Financial Institution, employees of the Financial Institution are each assigned a unique username and password. That username and password allows each employee to access his/her computer desktop, which is maintained

defendant, had been used, on at least four occasions starting on or about June 1, 2009 and ending on or about June 5, 2009, to transfer a total of approximately 32 megabytes of information through https to a certain website (the "Website") outside of the Financial Institution's computer network. Based on this information, the Financial Institution conducted an internal investigation of these uploads.

8. According to representatives of the Financial Institution and documents that I have reviewed, I have learned that the work desktop associated with SERGEY ALEYNIKOV, the defendant, was used on a least four occasions to transfer information, located on the Financial Institution's computer servers in New Jersey, to the Website. The First transfer occurred at or about 5:30 p.m. on or about June 1, 2009. The second and third transfers occurred at or about 11:11 p.m. and 11:14 p.m., respectively, on or about June 4, 2009. The final transfer occurred at or about 5:24 p.m. on or about June 5, 2009. The Financial Institution is presently attempting to recover records related to the files transferred on or about June 1, 2009 and June 4, 2009. As to June 5, 2009, the Financial Institution has recovered a record of a series of commands entered in ALEYNIKOV's desktop, which is known as a "bash history."<sup>6</sup>

---

on the Financial Institution's computer network. The desktop contains the programs each employee needs to perform his/her duties, such as, for example, e-mail, word-processing or spreadsheet applications. For certain employees, such as ALEYNIKOV, the desktop also provides access to the Financial Institution's proprietary computer code. When employees arrive at work, they may log in to the desktop. They may also log out when they leave work. If an employee who is logged into his/her desktop does not use it for a certain amount of time, the desktop locks, so that the employee must re-enter the username and password to regain access to the desktop. The Financial Institution also allows employees to log in and out, again using their unique username and password, to their desktop from their home computers. The Financial Institution instructs all employees to not share their username and password with any other employee.

<sup>6</sup>"Bash" refers to the Unix-based operating system that the Financial Institution uses to edit and maintain the code related to the Platform and its associated programs. "Bash history" is the most recent series of commands executed by a particular bash user.

9. According to representatives of the Financial Institution and records of the bash history, I have learned that, beginning at or about 5:21 p.m. and ending at or about 5:24 p.m. on or about June 5, 2009, the following commands were executed on ALEYNIKOV's desktop:

a. A script<sup>7</sup> was run that appears to have copied, compressed,<sup>8</sup> and merged certain files containing code for the Platform and some of its associated programs. A copy of this script was recovered from another part of ALEYNIKOV's desktop.

b. After the script was run, the copied files were encrypted,<sup>9</sup> were renamed, and then uploaded to the Website.

c. The program used to encrypt the files was then erased. An attempt was also made to erase the bash history, which was unsuccessful, because of a feature of the Financial Institution's computer system that retains a back-up copy of each user's bash history.

10. Based on a search of the Website's URL<sup>10</sup> on a publically-available database, it appears that the Website is registered to an individual with an address in London, United Kingdom, and associated with a computer server located in Germany. Based upon information provided by Financial Institution representatives, it appears that the Website, similar to an electronic document-management system, allows users to

---

<sup>7</sup>A "script" is a series of computer commands.

<sup>8</sup>To "compress" computer code or a computer file means to reduce the size of the file.

<sup>9</sup>Encryption programs typically make computer files unreadable to anyone who does not possess a certain code, or "key," to unlock the encryption.

<sup>10</sup>Uniform Resource Locators ("URLs") are part of an addressing scheme for web pages and other resources on the internet. For websites, a URL is typically comprised of a domain name (e.g., www.cybercrime.gov) and a file location or directory (e.g., ccmanual), and a file name (e.g., index.html). These parts can be assembled together to create a complete URL, which will facilitate the transfer of the web page from the web server to the requesting user's web browsing software (e.g., <http://www.cybercrime.gov/ccmanual/index.html>).

upload, save, and manage different versions of software code that the user is editing.

11. According to Financial Institution representatives and security records provided by the Financial Institution, I have learned the following:

a. The Financial Institution issues to all of its employees an identification card that contains a code that allows the Financial Institution to identify each employee and which also bears the employee's photograph. To enter the building in which SERGEY ALEYNIKOV, the defendant, worked for the Financial Institution, employees are required to "swipe" their identification cards through an electronic reader in the lobby, which recorded and identified the code embedded in the card. Once past the lobby, employees are required to swipe their cards again at various points of entry within each floor of the building. To leave the building, employees were not required to swipe their cards.

b. From on or about June 1, 2009, through on or about June 5, 2009, the identification card issued by the Financial Institution to SERGEY ALEYNIKOV, the defendant, was used to gain access to the office building in New York, New York (the "Building") and to the specific floor where ALEYNIKOV worked for the Financial Institution.

c. Specifically, in addition, on or about June 5, 2009, the card issued to ALEYNIKOV was used on the Building floor on which ALEYNIKOV's workstation was located at or about 4:10 p.m. and at or about 4:44 p.m., approximately 30 minutes before ALEYNIKOV's workstation was used to upload files to the Website. Several minutes after the files were uploaded, ALEYNIKOV's card was used again on the same Building floor on which ALEYNIKOV's workstation was located, specifically, at or about 5:32 p.m., and at or about 5:34 p.m..

12. As detailed above, Financial Institution employees may use their username and password to access their work desktop remotely, including from their homes. According to representatives of the Financial Institution and Financial Institution records, I learned that the Financial Institution retains logs of its employees' remote access to their work desktops. According to the remote access logs, I learned that, from at or about 10:51 p.m. to at or about 11:44 p.m. on or about June 4, 2009, ALEYNIKOV's username and password were used to log on to ALEYNIKOV's work desktop from a remote computer with IP



address<sup>11</sup> 69.125.178.4. During this same period, at or about 11:11 p.m. and 11:14 p.m., ALEYNIKOV's username and password were used to issue commands to upload data from the Financial Institution's servers to a server in Germany. I have spoken with a representative of Optimum Online, a division of Cablevision and the ISP that controls IP address 69.125.178.4, and learned that during the same time period (at or about 10:51 p.m. to at or about 11:44 p.m. on or about June 4, 2009) IP address 69.125.178.4 was assigned to "Sergey Aleynikov" at an address in New Jersey (the "Address"). Based on information provided by the Financial Institution, it appears that the Address matches ALEYNIKOV's home address. In addition, based upon surveillance conducted on July 2, 2009, by agents with whom I have spoken, I know that a 2006 Honda Odyssey, which has New Jersey license plates and is registered, according to Department of Motor Vehicle records, to "Sergey Aleynikov," was located in the driveway of the Address.

#### Foreign Transfer of Stolen Property

13. According to the Financial Institution's representatives, the code for the Platform that was copied and sent, on or about June 5, 2009, to the server in Germany was

---


<sup>11</sup>An Internet Protocol Address ("IP address") is a unique numeric address used to identify a computer on the internet. An IP address looks like a series of four numbers, each in the range of 0-255, separated by periods (e.g., 121.56.97.178). Every computer connection to the internet must be assigned an IP address so that Internet traffic sent from and directed to that computer is directed properly from its source to its destination. An IP address acts much like a home or business street address - it enables internet sites to properly route traffic to each other. There are two methods of assigning IP addresses - dynamic and static. Most of the larger ISPs (Internet Service Providers) such as Comcast or Time Warner control blocks of IP addresses that they assign to their customers. Although there may be thousands of IP addresses within these blocks, there are not enough to enable larger ISPs to assign a single, permanent IP address to each of their millions of customers. Therefore, these ISPs use dynamic IP addressing: Each time a computer connects to the ISP, the ISP assigns the computer one of the available IP addresses in the range (or block) of IP addresses controlled by the ISP. The computer retains that IP address for the duration of that session alone. Once the computer disconnects from the ISP, the IP address returns to the pool of available IP addresses.

originally located on the Financial Institution's server in New Jersey. The commands to effect this transfer were made from the workstation of SERGEY ALEYNIKOV, the defendant, in the Financial Institution's offices in New York, New York.


The Defendant's Arrest

13. At or about 9:20 p.m. on July 3, 2009, a team of FBI agents and myself arrested SERGEY ALEYNIKOV, the defendant, as he got off a flight at Newark Airport, New Jersey. After his arrest, I advised ALEYNIKOV of his Miranda rights, which he waived orally and in writing. ALEYNIKOV then made a statement, in my presence, which I committed to writing and which ALEYNIKOV signed. Among other things, ALEYNIKOV wrote that, on or about June 5, 2009, he copied and encrypted files from the Financial Institution's server, uploaded those files to the Website, and then deleted the encryption software and bash history. Thereafter, ALEYNIKOV downloaded the files from the Website to his home computer, his laptop computer, and a portable memory device. ALEYNIKOV claimed, however, that he only intended to collect "open source" files on which he had worked, but later realized that he had obtained more files than he intended. ALEYNIKOV also admitted that he has uploaded files from the Financial Institution to the Website while he was logged on to his work desktop from home. ALEYNIKOV claimed that he did not distribute any of the proprietary software that he obtained from the Financial Institution, and further claimed that he has abided by an agreement he entered into with his new employer not to use any unlicensed software.

WHEREFORE, deponent prays that SERGEY ALEYNIKOV, the defendant, be imprisoned or bailed, as the case may be.

  
\_\_\_\_\_  
MICHAEL G. McSWAIN  
Special Agent  
Federal Bureau of Investigation

Sworn to before me this  
4th day of July, 2009

  
\_\_\_\_\_  
HONORABLE KEVIN NATHANIEL FOX  
UNITED STATES MAGISTRATE JUDGE  
SOUTHERN DISTRICT OF NEW YORK