ORIGINAL

Approved: _____
Benjamin Allee/Ilan Graff
Assistant United States Attorneys

Before: HONORABLE JUDITH C. McCARTHY
United States Magistrate Judge
Southern District of New York

- X
                                :

UNITED STATES OF AMERICA   :
- v. -   :

JIAQIANG XU,   :

             Defendant.   :

                                :
- X

15 mag 4388

COMPLAINT

Violation of
18 U.S.C. § 1832

COUNTY OF OFFENSE:
WESTCHESTER

SOUTHERN DISTRICT OF NEW YORK, ss.:

JOSEPH M. ALTIMARI, 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

1.   From in or about November 2014, through on or about December 7, 2015, in the Southern District of New York and elsewhere, JIAQIANG XU, the defendant, with intent to convert a trade secret that is related to a product and service used in and intended for use in interstate and foreign commerce, to the economic benefit of others than the owner thereof, and intending and knowing that the offense would injure the owner of that trade secret, knowingly did steal, and without authorization appropriate, take, carry away, and conceal, and by fraud, artifice and deception obtain such information; and without authorization did copy, duplicate, sketch, draw, photograph, download, upload, alter, destroy, photocopy, replicate, transmit, deliver, send, mail, communicate, and convey such information; and attempted to do so, to wit, XU stole and converted to his own use the source code for a piece of proprietary software, which source code was a trade secret of a company for which XU previously worked.

(Title 18, United States Code, Section 1832.)

The bases for my knowledge and for the foregoing charges are, in part, as follows:

2.   I am a Special Agent with the FBI. I am currently assigned to the FBI's White Plains Resident Agency, where I investigate a variety of crimes related to counter-intelligence, including espionage and the theft of trade secrets. I have participated in an investigation of the

theft of trade secrets, as set forth below. I am familiar with the facts and circumstances set forth below from my personal participation in the investigation, including my review of pertinent documents, and from my conversations with others, including other Special Agents with the FBI, and representatives of a particular U.S. company (the "Victim Company") with expertise regarding the relevant software (the "Proprietary Software") and its source code. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

The Proprietary Software

3.   Based on my review of FBI reports, information provided by the Victim Company, publicly available information, and my participation in this investigation, I have learned the following about the Proprietary Software: the Proprietary Software is a clustered file system developed and marketed by the Victim Company in the United States and other countries. A clustered file system facilitates faster computer performance by coordinating work among multiple servers. The Victim Company produces the Proprietary Software for use in high-performance computer systems. Customers include government agencies and private corporations.

4.   According to open source information, the Proprietary Software is a key component of some of the world's largest scientific supercomputers, as well as commercial applications requiring rapid access to large volumes of data. Industries that use the Proprietary Software include digital media, engineering, design, business intelligence, financial analytics, seismic data processing, geographic information systems, and scalable file serving.

5.   According to a representative of the Victim Company, the source code underlying the Proprietary Software (the "Proprietary Source Code")—that is, the computer instructions and commands that can be compiled or assembled into the Proprietary Software—is itself proprietary information, which the Victim Company does not sell or otherwise make available to customers.

6.   According further to a representative of the Victim Company, the Victim Company takes significant precautions to protect the Proprietary Source Code as a trade secret. Among other things, the Proprietary Source Code is stored behind a company firewall and can only be accessed by a small subset of the Victim Company's employees. Before receiving Proprietary Source Code access, Victim Company employees must first request and receive approval from a particular Victim Company official. Victim Company employees must also agree in writing at both the outset and the conclusion of their employment that they will maintain the confidentiality of any proprietary information. The Victim Company takes these and other precautions in part because the Proprietary Software and the Proprietary Source Code are economically valuable, which value depends in part on the Proprietary Source Code's secrecy. The Victim Company invests millions of dollars in the Proprietary Software each year for research and development, and the Proprietary Software generates tens of millions of dollars in revenue each year for the Victim Company.

The Defendant

7.   From my review of FBI reports and information obtained from the Victim Company, I have learned the following:

a.   JIAQIANG XU, the defendant, worked for a branch of the Victim Company in China (the "China Branch") from November 2010 to May 2014.

b.   At the China Branch, XU worked as a software engineer and had full access to the Proprietary Source Code, including the ability to download the Proprietary Source Code to a computer or digital storage device.

c.   On or about November 30, 2010, XU signed a four-page document entitled "Agreement Regarding Confidential Information and Intellectual Property" (the "Confidentiality Agreement"). By signing the Confidentiality Agreement, XU agreed that he would not, among other things, disclose "any confidential information or material of [the Victim Company] or its affiliates." The Confidentiality Agreement specified that "Confidential information . . . shall include but [is] not limited to any information or material . . . generated or collected by or utilized in the operations of [the Victim Company] or its affiliates . . . which has not been made available generally to the public."

d.   In May 2014, XU voluntarily resigned from the Victim Company.

The Investigation

8.   In 2014, the FBI received a report that an individual in China—who, as described below, was later identified as JIAQIANG XU, the defendant—claimed to have access to the Proprietary Source Code and to be using the Proprietary Source Code in business ventures that were not related to the Victim Company's clients. Other Special Agents and I thereafter conducted an investigation, which included the use of undercover law enforcement officers ("UC-1" and "UC-2," and collectively "the UCs").

9.   In or around November 2014, UC-1 contacted JIAQIANG XU, the defendant, via email. For purposes of this investigation, UC-1 posed as a financial investor aiming to start a large-data storage technology company (the "UC Company"). I have reviewed copies of emails that UC-1 exchanged with XU between November 2014 and February 2015. From my review of those emails, I have learned the following:

a.   On or about November 27, 2014, UC-1 wrote to XU, among other things: "I am currently investing in and working with a new technology company which is seeking to develop improved and more secure data storage systems. As you may be aware, there is exciting new development in this area and the opportunities to be involved with cutting edge start up companies are excellent."

b.   On or about November 27, 2014, XU responded, among other things: "Nice to hear from you. I am very interested in opportunities working over the architecture

3

design and code development for cutting edge storage systems. I have several years working experience over this field and spent most of my career in [the Victim Company] working on the development of [the Proprietary Software] which is a largescale parallel storage system used in lots of hyperscale cluster systems in the world. . . . I am looking forward to discuss with you on the project and further opportunities. Thank you very much! Best Regards, Jiaqiang Xu."

        c.   On or about February 19, 2015, XU emailed to UC-1 a copy of XU's resume (the "Xu Resume"). According to the Xu Resume, XU lived in Beijing, China; his skills included "Operating Systems and Parallel File System"; he had received a master of science degree in computer science from a university in the United States; he had worked at the Victim Company from November 2010 through June 2014 ("Job Role: Research & Development of [the Proprietary Software]"); and he thereafter worked at another company as "Architect of the Storage Platform for Cloud Computing".

        10.   I have reviewed additional emails between JIAQIANG XU, the defendant, and the UCs, from in or about March 2015, by which date UC-2 had been brought into the email chain by UC-1. For purposes of this investigation, UC-2 was posing as a project manager, working for UC-1. From my review of those emails, I have learned that on or about March 16, 2015, XU sent an email to UC-1 and UC-2 ("the Source Code Email"). In the Source Code Email, XU described some of his past experience with the Proprietary Software and reported that he had "attached some sample code of [his] previous work in [the Victim Company]." XU also pasted a "short [Proprietary Software]+NFS related patch" directly into the Source Code Email, purportedly for the purpose of showing XU's "coding style."

        11.   After receiving the Source Code Email, other Special Agents and I showed the computer code in it to a representative of the Victim Company ("Employee-1"), who has expertise in the Proprietary Software. Employee-1 confirmed that the Source Code Email included proprietary Victim Company material that related to the Proprietary Source Code.

        12.   On or about April 12, 2015, JIAQIANG XU, the defendant, and UC-2 participated in a recorded audio conversation using a commercial communication service (the "Communication Service"),[1] which had been arranged via emails between XU and the UCs. I have reviewed that recording, as well as a draft transcript of that conversation, which was conducted in English. From my review of those materials, I have learned of the following conversation, in substance and in part:

        a.   XU stated that "[the Proprietary Software] is not open source,"[2] to which UC-2 responded "No I know it isn't."

        b.   UC-2 inquired as to whether XU "was allowed to have this code, since it's [the Victim Company]'s" and clarified that UC-2 was asking if UC-2 should "be a little . . .

---

[1] Based on my training and experience, I know that the Communication Service allows for, among other things, remote voice communication.

[2] Based on my training and experience, I know that the term "open-source software" refers to software whose source code is made publicly available.

discreet as to who [UC-2] show[ed] it to." XU replied that "Yes, we signed some, you know, signed some files there but actually I can, um, I can, I, I have all the code."[3]

  c. UC-2 asked, "Oh you do have all the code?" XU replied, "Yeah I have all the [Proprietary Software] code."

  d. UC-2 later said, "I just want to assure you that like, if you started working with us, not only will we pay you for your services but if you brought some of this code, [UC-1 would] be more than willing to pay you for that as well. . . . You, you'll be fully compensated for anything that you can offer to us. . . . [A]t the end of the day, the most important thing is, is we just want a, a good product and that is going to satisfy our needs."

  e. XU replied, among other things, that in his experience, start-up companies often used code obtained from large, established companies, "because no one, ah, no one want to, you know, code from the, the first line." Based on my training, experience, and participation in this investigation, I believe that XU was intimating to UC-2 that XU could provide the Proprietary Source Code to UC-2 to accelerate the development of UC-2's company's product.

  f. XU reported that he had already used a portion of the Proprietary Source Code as part of his then-current employment at a technology startup company.

  13. On or about May 11, 2015, JIAQIANG XU, the defendant, and UC-2 had another recorded audio conversation using the Communication Service. I have reviewed that recording, as well as a draft transcript of that conversation, which was conducted in English. From my review of those materials, I have learned that XU said the following, in substance and in part:

  a. XU again stated that he had used "some of the [Proprietary Software] code" in his work after he left the Victim Company.

  b. XU stated that he was willing to consider providing UC-2's company with the Proprietary Source Code as a platform for UC-2's company to facilitate the development of UC-2's company's own data storage system.

  c. XU informed UC-2 that if UC-2 set up several computers as a small network, then XU would remotely install the Proprietary Software so that the UCs could test it and confirm its functionality.[4]

---

  [3] Based on my training, experience, and participation in this investigation, I believe that XU's reference to having "signed some files" was an acknowledgement that he had signed the Confidentiality Agreement as part of his employment at the Victim Company, see supra ¶¶ 6, 7(c). In addition to the Confidentiality Agreement, XU may also have been referring to an exit affidavit that he completed before leaving the Victim Company's employment. I have reviewed a Victim Company document with the header "Affidavit," which appears to have been completed by XU in Mandarin — which I do not speak — in connection with the conclusion of XU's employment by the Victim Company. Among other things, that document bears XU's identification card number. It also reads, in part, in English "I hereby represent that I have settled/returned or will settle/return all debit/assets due [the Victim Company]."

14.   I have reviewed additional emails exchanged between JIAQIANG XU, the defendant, and UC-2 in or about early June 2015. On or about June 1, 2015, UC-2 emailed XU to confirm that the UCs would set up several computers per XU's specifications. On or about June 2, 2015, XU responded, thanked UC-2, and stated, among other things, that he "ha[d] a lot of thinking about what we can do in storage layer to better support the big-data applications."

15.   In or around early August 2015, I and other FBI agents arranged for a computer network to be set up, consistent with the specifications that JIAQIANG XU, the defendant, had provided (the "UC Network").

16.   On or about August 6, 2015, JIAQIANG XU, the defendant, and UC-2 had another recorded audio conversation using the Communication Service. I have reviewed that recording, as well as a draft transcript of that conversation, which was conducted in English. From my review of those materials, I have learned the following, in substance and in part:

     a.   UC-2 confirmed to XU that UC-2 had set up the network that XU had requested and provided XU with instructions for how to access that network.

     b.   XU stated that "I will have a try and ah try to install it [*i.e.*, the Proprietary Software]. And ah, I think, ah, it will be good."

17.   Based on my conversations with other law enforcement officers and my review of the UC Network's contents, I have learned that in or around early August 2015, files were remotely uploaded to the UC Network (the "Xu Upload"). Thereafter, on or about August 26, 2015, XU and UC-2 exchanged emails confirming that UC-2 had received the Xu Upload.

18.   On or about September 21, 2015, I made a digital copy of the Xu Upload available to a Victim Company employee who has expertise regarding the Proprietary Software and the Proprietary Source Code ("Employee-2") for Employee-2 to review. Based on my discussions with Employee-2, I have learned the following:

     a.   Based on Employee-2's assessment of the Xu Upload, the Xu Upload appeared to contain a functioning copy of the Proprietary Software.

     b.   The Xu Upload did not appear to be the official Proprietary Software package that the Victim Company provides to licensed customers. Among other irregularities, the Xu Upload appeared to have been built by a "build host" (that is, a computer system) that was not on the Victim Company's network. Additionally, the Xu Upload's version of the Proprietary Software had a "build date" that was inconsistent with the date on which the Victim Company's

---

[4] Based on my training, experience, and conversations with Victim Company employees, I know that source code cannot be completely reverse engineered from software. In other words, it does not appear that XU was agreeing to provide the Proprietary Source Code to the UCs but instead to demonstrate to them that XU himself had access to the Proprietary Source Code and could use it to build the UCs a working version of the Proprietary Software.

developers had created the licensed edition of that same version of the Proprietary Software.

c.   Notwithstanding the irregularities noted in the preceding paragraph, the Xu Upload's version of the Proprietary Software appeared to have been built using coding practices used by the Victim Company's developers for internal development purposes.

d.   Based on the foregoing, among other factors, it appeared to Employee-2 that the Xu Upload had been built by someone with access to the Proprietary Source Code who was not working within the Victim Company or otherwise at the Victim Company's direction.

19.   On or about the morning of December 7, 2015, JIAQIANG XU, the defendant, met with UC-2 at a hotel in White Plains, New York (the "Hotel"). I have listened to a recording of that meeting. Based on my review of that recording and my conversations with UC-2, I have learned that during the meeting, XU said the following in substance and in part:

a.   XU has used the Proprietary Source Code to make software to sell to customers.

b.   XU knew the Proprietary Source Code to be the product of two decades' work on the part of Victim Company engineers.

c.   XU had used the Proprietary Source Code to build a copy of the Proprietary Software, which XU had uploaded and installed on the UC Network (*i.e.*, the Xu Upload).

d.   XU knew that the copy of the Proprietary Software that XU had installed on the UC Network contained information identifying the Proprietary Software as the Victim Company's property, which could reveal the fact that the Proprietary Software had been built with the Proprietary Source Code without the Victim Company's authorization. XU indicated to UC-2 that XU could take steps to prevent detection of the Proprietary Software's origins—*i.e.*, that it had been built with stolen Proprietary Source Code—including writing computer scripts that would modify the Proprietary Source Code to conceal its origins.

e.   UC-2 and XU arranged to meet again in the afternoon.

20.   On or about the afternoon of December 7, 2015, UC-2 and JIAQIANG XU, the defendant, again met, along with UC-1, in the Hotel. I watched and listened to portions of that meeting which was transmitted live to monitoring agents, and audio and video recorded. Based on my monitoring of the meeting as well as my conversations with the UCs, I have learned that the following occurred during that meeting, in substance and in part:

a.   XU showed UC-2 a copy of what XU represented to be the Proprietary Source Code on XU's laptop. XU noted to UC-2 a portion of that code which indicated that it originated with the Victim Company as well as the date on which it had been copyrighted.

b.   XU reiterated to the UCs that he knew the Proprietary Source Code had been the product of extended work on the part of Victim Company employees, which continued to the present day.

7

c. XU stated that XU had previously modified the Proprietary Source Code's command interface to conceal the fact that the Proprietary Source Code originated with the Victim Company.
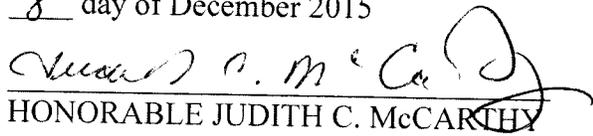
d. XU identified multiple specific customers to whom XU had previously provided the Proprietary Software using XU's stolen copy of the Proprietary Source Code. XU acknowledged that the Proprietary Source Code had considerable value.

WHEREFORE, deponent respectfully requests that JIAQIANG XU, the defendant, be imprisoned, or bailed, as the case may be.
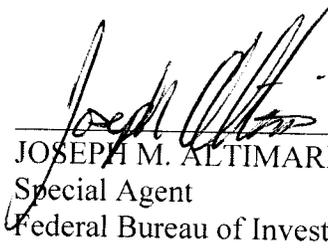
JOSEPH M. ALTIMARI
Special Agent
Federal Bureau of Investigation

Sworn to before me this
_8_ day of December 2015

HONORABLE JUDITH C. McCARTHY
United States Magistrate Judge
Southern District of New York

8