AO 91 (Rev. 08/09) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Northern District of California

United States of America)
v.)
Jizhong Chen) Case No. CR 19 70117 MAG
)
)
)

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of June 20, 2018 in the county of Santa Clara in the Northern District of California, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. § 1832	Theft of Trade Secrets

This criminal complaint is based on these facts:

Please see attached affidavit of S/A Adelaida Hernandez
PENALTIES: 10 years imprisonment. $250,000 fine, $100 special assessment, and 3 years' supervised release

☐ Continued on the attached sheet.

Complainant's signature

S/A Adelaida Hernandez, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: January 22, 2019

Judge's signature

City and state: San Jose, California

Virginia K, DeMarchi, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT PRESENTED IN SUPPORT FOR A CRIMINAL COMPLAINT

I, Adelaida Hernandez, Special Agent of the Federal Bureau of Investigation ("FBI"), being duly sworn, hereby declare as follows:

INTRODUCTION AND AGENT BACKGROUND

1. This affidavit is presented in support of a criminal complaint charging JIZHONG CHEN ("Chen") with the crime of theft of trade secrets, in violation of Title 18, United States Code, Section 1832.

2. I am an "investigative or law enforcement officer of the United States" within the meaning of Section 2510(7) of Title 18, United States Code, that is, an officer of the United States who is empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Title 18, United States Code, Section 1832.

3. I have been employed as a Special Agent of the FBI since February 2016 and am currently assigned to the San Francisco Division. While employed by the Federal Bureau of Investigation, I have investigated federal criminal violations related to intellectual property crime, as well as other white collar crimes. I have gained experience through training at the Federal Bureau of Investigation and everyday work relating to conducting these types of investigations. As a federal agent, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States.

4. The facts set forth in this affidavit are based upon the following: my own investigation; information obtained from other law enforcement agencies; legal process; my review of documents and records related to this investigation; oral and written communications with others who have personal knowledge of the events and circumstances described herein; review of public information, including information available on the Internet; and my experience and background as a Special Agent of the FBI. Because this affidavit is being submitted for the limited purpose of securing a criminal complaint, I have not included every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that violations of U.S. law occurred. Also, where I refer to conversations and events, I often refer to them in substance and in relevant part rather than in their entirety or verbatim, and figures and calculations set forth in this affidavit are approximate, unless otherwise noted.

APPLICABLE STATUTE

5. The FBI is investigating alleged violations of Title 18, United States Code, Section 1832, Theft of Trade Secrets, which states in part:

(a) Whoever, with intent to convert a trade secret, that is related to a product or service used in or intended for use 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—

(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;

(2) without authorization copies, duplicates, ... photographs, downloads, uploads, … photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;

(3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

(4) Attempts to commit any offense described in paragraphs (1) through (3); or

(5) conspires with one or more other persons to commit any offense described in paragraphs (1) through (3), and one or more of such persons, do any act to effect the object of the conspiracy,

shall ... be fined under this title or imprisoned not more than 10 years, or both.

SUMMARY

6. Based upon the information below, my training and experience, and the training and experience of agents and investigators involved in this investigation, I believe that there is probable cause to believe that Chen committed the crime of theft of trade secrets in violation of Title 18, United States Code Section 1832, when he took Apple, Inc. ("Apple") trade secrets from Apple's efforts to develop an autonomous vehicle (the "Project").

FACTS SUPPORTING PROBABLE CAUSE

The Project

7. Although Apple has made general statements to the press about being interested in autonomous vehicle development and obtained relevant permits from the State of California for the testing of autonomous vehicles on public roads, the details of Apple's research and development for the Project is a closely guarded secret that has never been publicly acknowledged by Apple.[1] The Project is developing products and services that will be used and are intended to be used in interstate and foreign commerce. Apple derives independent economic value, actual and potential, from the fact that the trade secrets contained in the Project are not readily ascertainable through proper means by another person.

8. To maintain confidentiality, Apple limits the number of employees with knowledge about the Project. Specifically, Apple grants employees "disclosure" for the Project. Disclosure status allows an employee to receive information for the Project and is solely granted on a strict "need to know" basis. Only around 5,000 of Apple's over 140,000 full time employees are disclosed on the Project. Of those 5,000, approximately 1,200 are "core" employees, described as the employees that are directly working on the development of the Project.

9. Apple maintains multiple confidential databases, whose names and categories are known to the government, which contain proprietary and confidential information about the Project (the "Databases"). Not all employees disclosed on the Project have access to the Databases.

Apple's Steps to Protect Intellectual Property

10. Apple goes to great lengths to protect data and intellectual property regarding the Project. Apple's Databases are only accessible with Apple employee credentials and password. Access to Project information on the Databases is further limited and not all disclosed employees have access to Project related Databases. Apple uses an internal software tool to manage requests for project disclosure and maintains a record of all disclosures. An administrator reviews the

[1] In an unrelated case, the FBI arrested another Apple employee on July 7, 2018, who worked on the Project, and the July 9, 2018 Complaint in the matter contained limited information about the Project.

request and approves or denies it. Chen was a core employee on the electrical engineering team and had full access to a subset of the Databases related to his job function on the Project.

11. In addition, Apple limits access to the building where the Project is developed (the "Building"). Access to the Building is limited to core Project employees. As a result, about 1,200 Apple employees have access to the Building. Physical access to the Building is limited by badge access. Further, even within Apple's operations, the Project's development in the Building is not listed; accordingly, only disclosed employees know about the Project's development in the Building.

12. Apple also goes to great lengths to communicate the importance of confidentiality in all aspects of Apple's business as it relates to its employees. Before starting at Apple, employees must sign an Intellectual Property Agreement ("IPA"). The IPA specifies that an employee may not use Apple's intellectual property except as authorized by Apple, including a prohibition against transfer and transmission of intellectual property without Apple's consent. Chen signed an IPA in 2018.

13. Employees disclosed on the Project must also attend an in-person secrecy training for the Project. Chen attended the secrecy training on June 13, 2018. The training covered the importance of keeping the nature and the details of the Project secret and avoiding intentional or unintentional information leaks. The training reviewed methods for ensuring information about the Project is only provided to individuals disclosed on the project, the fact that family members should not have access to information about the Project, as well as possible consequences for providing information or confirmation of information to non-disclosed individuals, including employment termination. The training also covered Apple's policy prohibiting employees from storing Apple's intellectual property on devices over which they do not have personal control, and requirements for storing and transmitting Project documents using secure mechanisms.

Chen and the Apple Investigation

14. Chen was hired by Apple in June 2018 to work as a Hardware Developer Engineer on the Project. Chen worked on the technical system design and hardware integration, as well as optics, on the Project. According to Chen's LinkedIn profile, Chen earned a Masters in Electronics and Communications Engineering and a Ph.D. in Optics and Fine Mechanics in China.

15. In December 2018, Chen was placed on a Performance Improvement Plan ("PIP"). A PIP is a structured plan for an employee to improve work performance within a set period of time. Consequences of not fulfilling PIP criteria may result in termination of employment.

16. According to Apple Global Security employees, on January 11, 2019, an Apple employee reported that they saw Chen taking photographs within the Apple work space. The employee reported Chen because they witnessed Chen taking wide angled photographs of the Project in the Building, which the employee found "suspicious".

17. As a result, an Apple investigation team (composed of Employee Relations and Global Security employees known to me) spoke to Chen. According to the Apple's Global Security employees that I spoke with, Chen admitted to taking photographs in Apple's workspace. In addition, Chen acknowledged that he had backed-up his Apple work computer to a personally- owned hard-drive. After Apple requested to examine Chen's personally-owned devices that contained Apple materials, Chen provided Apple with a personally-owned computer and a personally-owned hard-drive. Chen provided consent for Apple to review those devices. In addition, Chen allowed, with Chen present, Apple to review his personally-owned phone.

18. Apple's review of Chen's personally-owned hard-drive showed that Chen conducted a backup of his entire work computer onto a personally-owned hard-drive, in violation of Apple policy, since Chen's Apple work computer had Apple's confidential and proprietary materials.

19. In addition, Chen's personally-owned computer had over two thousand files containing confidential and proprietary Apple material, including manuals, schematics, and diagrams. Further, hundreds of the files on Chen's personally-owned computer were photographs of computer screens with Apple information on the screen. Some of these photographs showed a laptop with the name "Jizhong" on a label near the screen. According to Apple Global Security

employees, taking a photograph of the computer screen with Apple's information would circumvent Apple's internal monitoring of activity on its network. Initial investigation by Apple indicated that the photographs were taken within Apple's Building, and at an unknown location(s) while logged in through Apple's Virtual Private Network to the Project related Databases.

20. When Apple's investigation team went through Chen's personally-owned phone, with Chen present, they discovered that it had about 100 photographs taken within the interior of Apple's Building. Apple deleted these photographs with Chen's permission. Chen subsequently kept his personally-owned cellphone.

21. When asked by Apple, Chen stated that he downloaded the work computer onto his personally-owned hard-drive as an "insurance policy" to support his job applications after being placed on a PIP. Chen told Apple that he was applying for jobs within Apple. However, Apple subsequently learned that Chen had applied for two external jobs, including one at a China-based autonomous vehicle company – a direct competitor of the Project. Additionally, even though Chen was placed on a PIP in December 2018, Apple located photographs of Apple's confidential and proprietary material on Chen's personally-owned computer taken in June 2018.

22. After speaking to Chen on January 11, 2019, Apple immediately suspended Chen, with pay, and revoked his access to the Building, the Databases, and all other Apple physical and network access.

23. Apple considered the Apple material on Chen's personally-owned computer and personally-owned hard-drive confidential and proprietary and said the disclosure of it would to be "enormously damaging" to Apple.

Files on Chen's Personally-owned Computer

24. Apple investigators provided the FBI with a sample of photographs that Apple identified as images of Apple intellectual property and recovered from Chen's personally-owned computer, along with technical descriptions of the photograph. Although the information included photographs were taken on an Apple iPhone 6s Plus, which according to Apple Global Security, was Chen's personally-owned cellphone, the photographs themselves were located on Chen's personally-owned computer.

25. One photograph was date-stamped December 19, 2018, 09:28:51. The image is a diagram of autonomy architecture, which shows input from sensors and output to actuators. The diagram includes input from the sensors and the output to the actuators. Further, this appears to be a photograph of the employee's computer based on the login that shows his name at the bottom of the image. The image originated in Apple's secure databases and was found on Chen's personally-owned computer.

26. Another photograph was date-stamped June 20, 2018, 17:10:07. The image depicts a photograph of an assembly drawing of a wire harness for an autonomous vehicle. The item is an Apple-designed wiring harness custom-built to meet Apple's signaling requirements. Further, the image appears to be from Chen's Apple-provided computer screen, based on the appearance of his name at the bottom of the image. The image originated in Apple's secure databases and was found on Chen's personally-owned computer.

27. The files shown in the photographs were only accessible to certain Apple employees that were "disclosed" and were granted Databases access, as described above. These two photographs serve as the basis for the instant criminal charges.

Travel

28. On or around January 18, 2019, Chen told Apple that he was traveling to China to visit his ill father on January 19, 2019. Apple requested that Chen delay his travel. Chen told Apple he agreed to delay his travel until January 22, 2019. Later, Chen told Apple that he was leaving for China on January 23, 2019 and planned to stay in China for one month. As of January 22, 2019, Chen told Apple he has airplane reservations for a direct flight to China on January 23, 2019.

CONCLUSION

29. Through my training and experience as an FBI Agent, I believe that Chen used his employment as an Apple employee, working on a highly confidential program, to obtain intellectual property containing trade secrets from Apple. Apple took reasonable measures to protect its intellectual property. Chen signed an agreement about Apple's intellectual property as well as attended specialized training designed to educate Chen on the importance of protecting confidential and proprietary Apple information.

30. Based upon the foregoing, my training and experience, and the training and experience of agents and investigators involved in this investigation, I believe that there is probable cause to believe that Chen has committed the crime of theft of trade secrets in violation of Title 18, United States Code Section 1832.

REQUEST FOR SEALING

31. Because this investigation is continuing, disclosure of the Complaint, this affidavit, and/or this application will jeopardize the progress of the investigation. Disclosure of the Complaint at this time would seriously jeopardize the investigation; as such, a disclosure would give the target an opportunity to destroy evidence, change patterns of behavior, notify confederates, or flee from prosecution. Accordingly, I request that the Court issue an order that the Complaint and this affidavit in support of application for the Complaint, be filed under seal until further order of this Court.

Adelaida Hernandez
Special Agent
Federal Bureau of Investigation

Sworn to before me this 22 day of January, 2019.

HONORABLE VIRGINIA K. DEMARCHI
United States Magistrate Judge

DEFENDANT INFORMATION RELATIVE TO A CRIMINAL ACTION - IN U.S. DISTRICT COURT

BY: ☒ COMPLAINT ☐ INFORMATION ☐ INDICTMENT ☐ SUPERSEDING

Name of District Court, and/or Judge/Magistrate Location

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

OFFENSE CHARGED

Count 1: 18 U.S.C.§ 1832 - Theft of Trade Secrets

☐ Petty ☐ Minor ☐ Misde-meanor ☒ Felony

PENALTY: Maximum Prison Term: 10 years
Maximum Fine: $250,000
Minimum Supervised Release: 3 years
Special Assessment: $100

SEALED BY ORDER OF COURT

FILED JAN 22 2019 SUSAN Y. SOONG CLERK, U.S. DISTRICT COURT NORTHERN DISTRICT OF CALIFORNIA SAN JOSE

CR 19 70117 MAG

DEFENDANT - U.S

PROCEEDING

Name of Complaintant Agency, or Person (& Title, if any)

S/A Adelaida Hernandez - FBI

☐ person is awaiting trial in another Federal or State Court, give name of court

☐ this person/proceeding is transferred from another district per (circle one) FRCrp 20, 21, or 40. Show District

☐ this is a reprosecution of charges previously dismissed which were dismissed on motion of: ☐ U.S. ATTORNEY ☐ DEFENSE } SHOW DOCKET NO.

☐ this prosecution relates to a pending case involving this same defendant

☐ prior proceedings or appearance(s) before U.S. Magistrate regarding this defendant were recorded under } MAGISTRATE CASE NO.

DEFENDANT

IS *NOT* IN CUSTODY

1) ☒ Has not been arrested, pending outcome this proceeding. If not detained give date any prior summons was served on above charges

2) ☐ Is a Fugitive

3) ☐ Is on Bail or Release from (show District)

IS IN CUSTODY

4) ☐ On this charge

5) ☐ On another conviction } ☐ Federal ☐ State

6) ☐ Awaiting trial on other charges

If answer to (6) is "Yes", show name of institution

Has detainer been filed? ☐ Yes ☐ No } If "Yes" give date filed

DATE OF ARREST Month/Day/Year

Or... if Arresting Agency & Warrant were not

DATE TRANSFERRED TO U.S. CUSTODY Month/Day/Year

Name and Office of Person Furnishing Information on this form: DAVID L. ANDERSON

☒ U.S. Attorney ☐ Other U.S. Agency

Name of Assistant U.S. Attorney (if assigned): MATTHEW A. PARRELLA

☐ This report amends AO 257 previously submitted

ADDITIONAL INFORMATION OR COMMENTS

PROCESS:

☐ SUMMONS ☐ NO PROCESS* ☒ WARRANT Bail Amount: No Bail

If Summons, complete following:

☐ Arraignment ☐ Initial Appearance

Defendant Address:

** Where defendant previously apprehended on complaint, no new summons or warrant needed, since Magistrate has scheduled arraignment*

Date/Time: Before Judge:

Comments: