AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Northern District of California

United States of America	)	FILED
v.	)	JUL 09 2018
XIAOLANG ZHANG	)	SUSAN Y. SOONG
	)	CLERK, U.S. DISTRICT COURT
	)	NORTHERN DISTRICT OF CALIFORNIA
	)	SAN JOSE

Case No.

CR 18 70919

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 _____ April 30, 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(a)(1)	Theft of Trade Secrets

This criminal complaint is based on these facts:

See attached affidavit of S/A Eric Proudfoot
PENALTIES: 10 years imprisonment, $250,000 fine, $100 special assessment, and 3 years' supervised release

☑ Continued on the attached sheet.

_____
Complainant's signature

Eric M. Proudfoot, Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: ___July 9, 2018___

_____
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, Eric M. Proudfoot, 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 **Xiaolang Zhang** ("**Zhang**") with the crime of theft of trade secrets, in violation of Title 18, United States Code, Section 1832, Theft of Trade Secrets.

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 Federal Bureau of Investigation since March 2, 2008, 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 high technology/cybercrime, child exploitation, child pornography, foreign counterintelligence, and intellectual property crime. 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. As an FBI agent, I am authorized to investigate violations of United States law and I am a law enforcement officer with the authority to execute warrants issued under the authority of the United States. During my career as a Special Agent of the FBI, I have received training and possess actual experience relating to Federal criminal procedures and Federal statutes. I have

1

also received specialized training and instruction in the field of investigation in computer-related crimes. I have had the opportunity to conduct, coordinate, and participate in numerous investigations relating to computer-related crimes. I have participated in the execution of numerous search warrants conducted by the FBI and have participated in the seizure of email accounts and computer systems.

5.   The facts in this affidavit are based on my personal participation in this investigation, my training and experience, and documents, records, emails, and other types of information obtained during the investigation from other sources and witnesses. The FBI has, thus far conducted interviews and reviewed documentation provided by the victim company, Apple, ("Apple"), which included file listings, closed circuit television images, physical access badge history, and employee agreements. The FBI has also conducted a physical search of ZHANG's residence, authorized on June 22, 2018, by the Honorable Susan van Keulen, Magistrate Judge, United States District Court, Northern District of California, San Jose Disivison. 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 evidence of 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 complaint are approximate, unless otherwise noted.A

APPLICABLE STATUTES

6.   The FBI is investigating alleged violations of Title 18, United States Code, Section 1832, 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, . . . downloads, uploads, . . . 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) . . .

(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.

ENTITIES

7.   Apple, Inc. "Apple" is a technology company headquartered in Cupertino, California with an annual revenue (in 2017) of $229 billion.

8.   Xiaopeng Motors, aka Xpeng Motors, ("XMotors") is an intelligent electric vehicle company with headquarters in Guangzhou, China, and North American offices located in Palo Alto, California.

INDIVIDUALS

9.   **Xiaolang Zhang** ("ZHANG") is a former Apple employee, working as a hardware engineer on their autonomous vehicle development team.

ZHANG BACKGROUND

10.   **ZHANG** was hired at Apple starting on December 7, 2015, to work on a project to develop software and hardware for use in autonomous vehicles (the Project). Although Apple has made general statements to the press about being interested in autonomous vehicle development, the details of Apple's research and development for the Project is a closely

guarded secret that has never been publicly revealed. Most recently, **ZHANG** worked on the Compute Team, where he designed and tested circuit boards to analyze sensor data within the Project. Because of his role on the team, **ZHANG** was granted broad access to secure and confidential internal databases containing trade secrets and intellectual property for the Project. Among these are multiple confidential databases whose names and categories are known to the government (the "Databases").

11.   **ZHANG** took paternity (new parent) leave following the birth of his child from April 1 to April 28, 2018, pursuant to Apple's employee leave policy. While on paternity leave, **ZHANG** traveled with his family to China. On April 30, 2018, shortly after returning from China, **ZHANG** met with his immediate supervisor at Apple, and explained that **ZHANG** would be resigning to move back to China in order to be closer to his mother who he stated was in poor health. As the meeting progressed, **ZHANG** disclosed that he intended to work for XMOTORS – a Chinese start-up company focused on electric automobiles and autonomous vehicle technology.

12.   After hearing **ZHANG's** intentions and feeling that he had been evasive during their meeting, **ZHANG's** supervisor asked a representative from Apple's New Product Security Division to join the meeting with **ZHANG**. At the conclusion of their meeting, **ZHANG** was asked to turn in all Apple-owned devices, and **ZHANG** was advised he would then be walked off the campus.   **ZHANG** turned over to Apple two (2) Apple iPhones and one (1) MacBook laptop computer. Apple security then immediately disabled **ZHANG's** remote network access, badge privileges, network access, and other employee accesses. **ZHANG** was also reminded about Apple's intellectual property policy, and **ZHANG** acknowledged that he understood and would comply.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.

fastcase®
Smarter legal research.