

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
----- X

UNITED STATES OF AMERICA

- against -

HUAWEI TECHNOLOGIES CO., LTD.,
HUAWEI DEVICE CO., LTD.,
HUAWEI DEVICE USA INC.,
FUTUREWEI TECHNOLOGIES, INC.,
SKYCOM TECH CO., LTD.,
WANZHOU MENG,
also known as “Cathy Meng” and
“Sabrina Meng,”



Defendants.

----- X

THE GRAND JURY CHARGES:

INTRODUCTION

At all times relevant to this Superseding Indictment, unless otherwise indicated:

I. The Defendants

1. The defendant HUAWEI TECHNOLOGIES CO., LTD. (“HUAWEI”) was a global networking, telecommunications and services company headquartered in Shenzhen, Guangdong, in the People’s Republic of China (“PRC”). As of the date of the filing of this Superseding Indictment, HUAWEI was the largest telecommunications

SUPERSEDING
INDICTMENT

Cr. No. 18-457 (S-3) (AMD)
(T. 18, U.S.C., §§ 371, 981(a)(1)(C),
982(a)(1), 982(a)(2), 982(b)(1), 1343,
1344, 1349, 1512(k), 1832(a)(5),
1832(b), 1956(h), 1962(d), 1963(a),
1963(m), 2323(b)(1), 2323(b)(2), 2 and
3551 et seq.; T. 21, U.S.C., § 853(p);
T. 28, U.S.C., § 2461(c); T. 50, U.S.C.,
§§ 1702, 1705(a) and 1705(c))

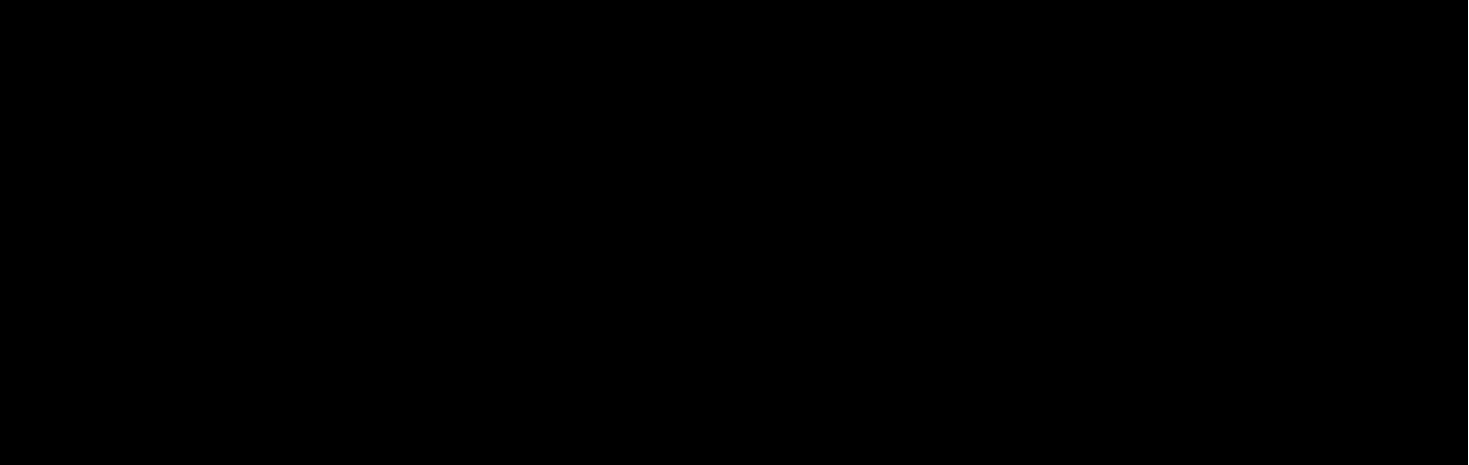
equipment manufacturer in the world. HUAWEI was owned by its parent company, Huawei Investment & Holdings Co., Ltd. (“Huawei Holdings”), which was registered in Shenzhen, Guangdong, PRC, and predecessor entities of that company.

2. The defendant HUAWEI DEVICE CO., LTD. (“HUAWEI DEVICE”) was a company in the PRC that designed and manufactured wireless phones. HUAWEI DEVICE was a subsidiary of HUAWEI.

3. The defendant HUAWEI DEVICE USA INC. (“HUAWEI DEVICE USA”), a manufacturer of communication products whose headquarters was in the United States, and the defendant FUTUREWEI TECHNOLOGIES, INC. (“FUTUREWEI”), a research and development company whose headquarters was in the United States, were both subsidiaries of HUAWEI and Huawei Holdings.

4. The defendant SKYCOM TECH CO., LTD. (“SKYCOM”) was a corporation registered in Hong Kong whose primary operations were in Iran. SKYCOM functioned as HUAWEI’s Iran-based subsidiary. As of 2007, Huawei Holdings owned SKYCOM through a subsidiary (“Huawei Subsidiary 1”), an entity the identity of which is known to the Grand Jury. In or about November 2007, Huawei Subsidiary 1 transferred its shares of SKYCOM to another entity (“Huawei Subsidiary 2”), an entity the identity of which is known to the Grand Jury, which was purportedly a third party in the transaction but was actually controlled by HUAWEI. Following this transfer of SKYCOM shares from Huawei Subsidiary 1 to Huawei Subsidiary 2, HUAWEI falsely claimed that SKYCOM was one of HUAWEI’s local business partners in Iran, as opposed to one of HUAWEI’s subsidiaries or affiliates.

5. The defendant WANZHOU MENG, also known as “Cathy Meng” and “Sabrina Meng,” was a citizen of the PRC. From at least in or about 2010, MENG served as Chief Financial Officer of HUAWEI. Between approximately February 2008 and April 2009, MENG served on the SKYCOM Board of Directors. More recently, MENG also served as Deputy Chairwoman of the Board of Directors for HUAWEI.



II. The Scheme to Misappropriate Intellectual Property

8. Since at least in or about 2000 through the date of this Superseding Indictment, the defendants HUAWEI, FUTUREWEI, HUAWEI DEVICE and HUAWEI DEVICE USA (the “IP Defendants”) and others executed a scheme to operate and grow the worldwide business of HUAWEI and its parents, global affiliates and subsidiaries through the deliberate and repeated misappropriation of intellectual property of companies headquartered or with offices in the United States (the “Victim Companies”) for commercial use. By misappropriating the intellectual property of the Victim Companies, the IP Defendants received income directly and indirectly, including by benefitting from the sale of products containing stolen intellectual property and saving on research and development costs, which income the IP Defendants agreed to use to establish and operate the worldwide

business of Huawei and its parents, global affiliates and subsidiaries, including in the United States.

9. The misappropriated intellectual property of the Victim Companies comprised or included trade secret information, as defined by Title 18, United States Code, Section 1839(3), and other confidential and nonpublic intellectual property. To protect trade secret information and other intellectual property from disclosure, the Victim Companies each employed reasonable measures, including but not limited to physical, electronic and network security, company policy and training, and legal agreements and contracts. The IP Defendants believed that the misappropriated intellectual property comprised or contained trade secret information, and knew and intended that such misappropriation would injure the Victim Companies.

10. The misappropriated intellectual property of Victim Companies consisted of 10 or more copies of copyrighted works with a value greater than \$2,500 within a period of 180 days, as defined and described within Title 18, United States Code, Section 2319. The IP Defendants knew and intended that the misappropriation of copyrighted works would injure the Victim Companies.

11. To obtain the intellectual property of the Victim Companies, the IP Defendants sometimes entered into confidentiality agreements with the owners of the intellectual property and then violated the terms of the confidentiality agreements by misappropriating the intellectual property for the IP Defendants' own commercial use. The IP Defendants also tried to recruit employees of the Victim Companies in order to gain access to intellectual property of their former employers, and the IP Defendants directed and incentivized their own employees to steal intellectual property from other companies.

12. On other occasions, the IP Defendants used proxies such as professors working at research institutions or third party companies, purporting not to be working on behalf of the IP Defendants, to gain access to the Victim Companies' nonpublic intellectual property. Those proxies then impermissibly provided the Victim Companies' nonpublic proprietary information to the IP Defendants.

13. In another effort to gain access to the nonpublic intellectual property of the Victim Companies, in 2013, HUAWEI launched a formal policy instituting a bonus program to reward employees who obtained confidential information from competitors. Under the policy, HUAWEI established a formal rewards schedule to pay employees of HUAWEI affiliates for stealing information from competitors based upon the value of the information obtained. Employees were directed to post confidential information obtained from other companies on an internal HUAWEI website, or, in the case of especially sensitive information, to send an encrypted email to a special huawei.com email mailbox. A "competition management group" was tasked with reviewing the submissions and awarding monthly bonuses to the employees who provided the most valuable stolen information. Biannual awards also were made available to the top "Huawei Regional Divisions" that provided the most valuable information. A memorandum describing this program was sent to employees in the United States.

14. To avoid and minimize the costs of potential civil and criminal liability in the United States, and therefore more easily establish and operate HUAWEI's U.S. business, the IP Defendants engaged in a pattern of obstruction. In advance of and during civil proceedings regarding the IP Defendants' alleged misappropriation of intellectual property, the IP Defendants provided false information in the form of affidavits or reports of

internal investigations, to minimize potential liability for the misappropriation of intellectual property. Similarly, the IP Defendants instructed employees to conceal information from law enforcement. For example, an official HUAWEI manual labeled “Top Secret” instructed certain individuals working for HUAWEI to conceal their employment with HUAWEI during encounters with foreign law enforcement officials.

15. To prevent civil and criminal liability, as well as reputational harm, when confronted with evidence of their wrongdoing, the IP Defendants publicly blamed the wrongdoing on purportedly rogue low-level employees of HUAWEI and its subsidiaries and affiliates.

16. HUAWEI, HUAWEI DEVICE USA and FUTUREWEI agreed to use the proceeds derived from the theft of intellectual property to establish and operate the business of HUAWEI and its parents, global affiliates and subsidiaries in the United States and abroad. Similarly, HUAWEI, HUAWEI DEVICE USA and FUTUREWEI agreed to benefit from cost savings generated by stolen intellectual property to innovate more quickly and thus to also establish and operate the business of HUAWEI and its parents, and global affiliates and subsidiaries in the United States and abroad.

17. As part of the scheme to establish and operate the business of HUAWEI and its parents, global affiliates and subsidiaries in the United States and elsewhere, and to avoid interference in their scheme by U.S. governmental bodies or other private actors, HUAWEI, HUAWEI DEVICE USA and FUTUREWEI repeatedly made material misrepresentations as to the misappropriation and subsequent commercial use of intellectual property, as well as other criminal activity, including the nature and extent of business in high-risk jurisdictions such as Iran, to U.S. governmental bodies from whom

HUAWEI, HUAWEI DEVICE USA and FUTUREWEI sought regulatory authorization that would help grow the IP Defendants' U.S.-based business. HUAWEI, HUAWEI DEVICE USA and FUTUREWEI made similar material misrepresentations to financial institutions from whom the defendants sought banking services.

A. Company 1

18. Beginning in or about 2000, the defendants HUAWEI and FUTUREWEI misappropriated operating system source code for internet routers, command line interface (a structure of textual commands used to communicate with routers) and operating system manuals from a U.S. technology company headquartered in the Northern District of California ("Company 1"), an entity the identity of which is known to the Grand Jury, and incorporated the misappropriated source code into HUAWEI internet routers that FUTUREWEI sold in the United States from approximately April 2002 until December 2002. Toward this end, HUAWEI and FUTUREWEI hired or attempted to hire Company 1 employees and directed these employees to misappropriate Company 1 source code on behalf of the defendants. Company 1 had registered as copyrighted the material misappropriated by HUAWEI and FUTUREWEI.

19. HUAWEI and FUTUREWEI publicly marketed their internet routers in the United States as lower cost versions of Company 1 internet routers; HUAWEI and FUTUREWEI's routers featured model numbers, user interfaces and operating manuals similar to those of routers sold by Company 1. In actuality, HUAWEI and FUTUREWEI's internet routers were essentially direct copies of routers sold by Company 1.

20. In or about December 2002, representatives of Company 1 notified senior HUAWEI executives, including the founder of HUAWEI ("Individual-1"), an

individual whose identity is known to the Grand Jury, of the misappropriation. After approximately one month of negotiation, the defendants HUAWEI and FUTUREWEI agreed to replace the original versions of some of the misappropriated source code and to recall from the U.S. market products that included misappropriated source code.

21. In or about 2003, Company 1 filed suit against the defendants HUAWEI and FUTUREWEI in federal court in the Eastern District of Texas for infringement of intellectual property. At the outset of the litigation, HUAWEI and FUTUREWEI claimed to have already removed Company 1's source code from products and recalled routers containing any stolen source code in early 2003. However, as part of this recall effort and to obstruct the civil litigation, HUAWEI and FUTUREWEI erased the memory drives of recalled HUAWEI routers and then sent those routers to the PRC before Company 1 could access them, thus destroying evidence of HUAWEI and FUTUREWEI's illicit conduct. Also, in an effort to destroy evidence, FUTUREWEI attempted to remotely access HUAWEI routers that had already been sold in the United States and erase the misappropriated source code contained therein.

22. In the litigation against Company 1, a HUAWEI executive vice president, an individual whose identity is known to the Grand Jury, filed a declaration on behalf of the defendants HUAWEI and FUTUREWEI falsely claiming that the defendants had received Company 1's source code from a third party. HUAWEI and FUTUREWEI submitted this false declaration to minimize potential civil damages in the pending litigation by making it appear that HUAWEI had not knowingly misappropriated Company 1's source code but rather benefitted from a munificent third party.

23. As part of the litigation, the parties agreed that a neutral expert would examine the source code used by Company 1 and HUAWEI in internet routers from which HUAWEI and FUTUREWEI had purportedly removed copied source code. In a limited examination of small portions of the source code at issue, the neutral expert found that source code for two sequences of HUAWEI program instructions (“routines”) were substantially similar to or developed or derived from Company 1’s source code: “It is clear that there was Substantial Similarity in portions of the Huawei . . . code and that there has been copyright infringement.” In particular, the neutral expert found “the conclusion is unescapable” that one routine of HUAWEI source code is “Substantially Similar to [Company 1]’s [source code] and has been misappropriated.” With respect to four other programming routines, the neutral expert agreed with Company 1 that portions of those routines “were copied from [Company 1] source code,” and one routine “was copied in its entirety and modified slightly.”

24. From approximately April 2002 until December 2002, FUTUREWEI sold HUAWEI routers containing Company 1’s source code in the United States. The efforts by FUTUREWEI and HUAWEI to obstruct civil litigation with Company 1, including by filing a declaration with false information and destroying evidence of misappropriation, were designed to save costs from litigation and avoid possible regulatory or law enforcement action.

B. Company 2

25. In or about and between 2000 and 2003, an engineer (“Engineer-1”), an individual whose identity is known to the Grand Jury, engaged in efforts to misappropriate the intellectual property of a U.S. technology company headquartered in the Northern

District of Illinois (“Company 2”), an entity the identity of which is known to the Grand Jury, and provide the intellectual property to HUAWEI. Engineer-1 was employed by Company 2.

26. No later than October 2001, HUAWEI had identified Engineer-1 as a target for recruitment in light of his employment with Company 2. In an October 9, 2001 email, which subject read “[Company 2] [Engineer-1] visit in Huawei,” a HUAWEI employee wrote that Engineer-1 worked for Company 2, and that:

[He] has more than 40 patents. Last year, when [Engineer-1] had a meeting with [Individual-1] and [Huawei’s Chief Strategy Marketing Officer (“Individual-2”, an individual whose identity is known to the Grand Jury)] in Huawei, [Individual-1] asked [Engineer-1] to join Huawei. Considering his team members (more than 10 people), he refused the proposal. Now he is coming to seek opportunity to cooperate with Huawei in a few products. He will come to China around October 20 and wishes to meet Individual-2 and Huawei people from relevant business departments.

The recipient of the email responded, “At present, we can communicate with him to see whether he has any primary plan or proposal for cooperation and cooperation in what products.” As part of this recruitment effort, between in or about 2000 and 2003, Engineer-1 met personally with Individual-1 and other HUAWEI executives multiple times in the PRC.

27. For example, in or about February 2003, Engineer-1 met with Individual-1 in the PRC. On or about March 3, 2003, Engineer-1 wrote an email to Individual-1 and another HUAWEI employee stating, “Attached please find those document [sic] about [Company 2 base station technology] specification you asked.” The email attached a 50-page document with technical specifications for a base station, designed for use

in wireless network, manufactured by Company 2. Each page of the document bore the marking “[Company 2] Confidential Property.” The cover page of the document stated, “This document and the information contained in it is Confidential Information of [Company 2] and shall not be used, published[,] disclosed, or disseminated outside of [Company 2].”

C. Company 3

28. In or about July 2004, at a trade show in Chicago, Illinois, a HUAWEI employee (“Individual-3”), an individual whose identity is known to the Grand Jury, was discovered in the middle of the night after the show had closed for the day in the booth of a technology company (“Company 3”), an entity the identity of which is known to the Grand Jury, removing the cover from a networking device and taking photographs of the circuitry inside. Individual-3 wore a badge listing his employer as “Weihua,” HUAWEI spelled with its syllables reversed. In official correspondence with Company 3 shortly after this incident, HUAWEI claimed that Individual-3 attended the trade show in his personal capacity and that his attempted misappropriation occurred “without Huawei’s authorization.” According to a purported official statement published in Reuters, HUAWEI claimed, “This is a junior engineer who had never traveled to the United States before. His actions do not reflect the culture or values of Huawei.” Notably, a resume that Individual-3 submitted to the U.S. government in approximately 2012 stated that he had been a “senior R&D Engineer” at HUAWEI from 1997 until July 2004, the time of the incident.

29. The efforts to misappropriate the intellectual property of Company 3 were designed to permit HUAWEI to save on research and development costs in the development of its own networking device.

D. Company 4

30. In or about 2009, HUAWEI and FUTUREWEI devised a scheme to misappropriate technology related to antennas that provide cellular telephone and data services. The technology was developed by a technology company operating in the Northern District of California and the Western District of New York (“Company 4”), an entity the identity of which is known to the Grand Jury.

31. In or about September 2009, FUTUREWEI entered into a non-disclosure agreement (“NDA”) with Company 4, which prevented FUTUREWEI from using confidential information provided by Company 4 for FUTUREWEI’s own benefit or to the competitive disadvantage of Company 4.

32. On or about September 21, 2009, Company 4 provided a presentation to HUAWEI and FUTUREWEI regarding Company 4’s proprietary technology to improve reception between cellular telephones and the antennas that provide cellular telephone and data services, which was a trade secret of Company 4. Each slide was marked “Commercial In Confidence.” Thereafter, in response to questions from a FUTUREWEI engineer (“Engineer-2”), Company 4 provided additional information regarding the technology.

33. While expressing outward enthusiasm for a potential partnership with Company 4, HUAWEI and FUTUREWEI secretly worked to misappropriate the Company 4 technology provided pursuant to the NDA. On or about September 21, 2009, the same day that Company 4 provided the presentation to HUAWEI and FUTUREWEI, a HUAWEI employee wrote an email to Engineer-2 at FUTUREWEI expressing interest in the technology on which Company 4 had presented. On or about October 23 and October 26, 2009, Engineer-2 wrote two emails to his colleagues indicating that he was very interested in

the Company 4 technology and had some ideas on how to implement the technology. On or about October 30, 2009, FUTUREWEI filed a provisional patent application with the U.S. Patent and Trademark Office that used and relied in large part upon the Company 4 intellectual property.

34. In or about and between approximately 2009 and 2016, HUAWEI received approximately \$22 million in income derived from the sale of products that incorporated intellectual property misappropriated from Company 4.

E. Company 5

35. In or about 2012 and 2013, HUAWEI, HUAWEI DEVICE and HUAWEI DEVICE USA devised a scheme to misappropriate robot technology from a U.S. wireless network operator headquartered in the Western District of Washington (“Company 5”), an entity the identity of which is known to the Grand Jury. In May 2012, HUAWEI DEVICE USA asked Company 5 to sell or license its proprietary robotic system for testing phones to HUAWEI DEVICE USA; Company 5 declined. Thereafter, HUAWEI and HUAWEI DEVICE began to develop their own robotic phone-testing system, and directed HUAWEI DEVICE USA employees to provide detailed information about Company 5’s technology to support that effort.

36. Beginning in or about August 2012, HUAWEI DEVICE USA and Company 5 executed a series of confidentiality agreements allowing select HUAWEI DEVICE USA employees access to a Company 5 robot laboratory. HUAWEI, HUAWEI DEVICE and HUAWEI DEVICE USA employees abused this restricted access in order to misappropriate Company 5 technology. In a November 6, 2012 email, a HUAWEI engineer directed a HUAWEI DEVICE USA employee, “[T]his email is just a kindly reminder for the

information we need to build our own robot system and kindly feedback the information we need in the attachment . . .” Attached to the email was a file requesting information about the technical specifications of the robot hardware components and software systems. The HUAWEI DEVICE USA employee responded, “[HUAWEI DEVICE USA engineers] have accessed the [Company 5] robot lab They know how [Company 5] robot work and system info. I asked them to write down the info in detail and then send to [HUAWEI and HUAWEI DEVICE].”

37. In or about and between November 2012 and January 2013, in response to technical questions from HUAWEI and HUAWEI DEVICE, HUAWEI DEVICE USA employees sent HUAWEI and HUAWEI DEVICE multiple photographs of the Company 5 robot and its software interface system taken from inside the secure Company 5 laboratory, in violation of the confidentiality agreements. In or about January 2013, HUAWEI DEVICE USA suggested that HUAWEI and HUAWEI DEVICE send their own engineer to Company 5’s laboratory in Seattle, Washington: “You will learn a lot in knowledge and experience.” In or about and between March and April 2013, HUAWEI and HUAWEI DEVICE continued to develop their own robot while directing HUAWEI DEVICE USA employees to provide more information about Company 5’s robot.

38. In or about May 2013, HUAWEI sent an engineer working on the robot project (“Engineer-3”), an individual whose identity is known to the Grand Jury, to the United States. Engineer-3 wrote to HUAWEI DEVICE USA, describing his trip as follows: “go to the [Company 5] laboratory for reconnaissance and obtain measurement data.”

39. On or about and between May 13 and 14, 2013, HUAWEI DEVICE USA employees allowed to access the Company 5 laboratory improperly used their badges to

allow Engineer-3 access. Once inside, Engineer-3 photographed and gathered technical information about the robot before Company 5 personnel discovered the breach and escorted him out of the facility. Engineer-3 then emailed HUAWEI, HUAWEI DEVICE and HUAWEI DEVICE USA personnel the photographs and technical information he had improperly gathered.

40. On or about May 29, 2013, a HUAWEI DEVICE USA employee accessed the laboratory and surreptitiously placed a robot arm into a laptop bag and removed the robot arm from the laboratory. Before the robot arm was returned to Company 5—which had discovered the theft—Engineer-3 took measurements of the robot arm and emailed photographs and measurements to HUAWEI and HUAWEI DEVICE engineers.

41. On or about August 13, 2013, HUAWEI DEVICE USA issued an “Investigation Report,” which purported to summarize the findings of an internal investigation into the above-described misconduct in the Company 5 robot laboratory. HUAWEI DEVICE USA subsequently provided a copy of the report to Company 5. The report falsely described the actions of Engineer-3 and HUAWEI DEVICE USA in May 2013 as “isolated incidents,” and characterized Engineer-3’s actions as a “moment of indiscretion.” Additionally, a HUAWEI DEVICE USA employee falsely informed Company 5 that there were “not a lot of emails” discussing the Company 5 robot, when, in fact, there was extensive email correspondence among HUAWEI, HUAWEI DEVICE and HUAWEI DEVICE USA in which HUAWEI and HUAWEI DEVICE employees directed HUAWEI DEVICE USA employees to misappropriate information from Company 5.

42. On or about May 19, 2014, HUAWEI sent a letter to Company 5 describing disciplinary measures taken in response to the actions of Engineer-3 and

HUAWAI DEVICE USA, and claiming that HUAWEI did not condone those actions and that respect for intellectual property rights was one of HUAWEI's "core principles."

43. Company 5 ultimately filed a civil lawsuit against HUAWEI, HUAWEI DEVICE and HUAWEI DEVICE USA.

44. The efforts to misappropriate the intellectual property of Company 5 were designed to permit HUAWEI DEVICE to save on research and development costs in the development of its own testing robot for use on HUAWEI DEVICE prototypes. The efforts to obstruct civil litigation with Company 5, such as misstatements regarding the quantity of relevant email correspondence, were designed to save litigation costs and to avoid scrutiny by regulators and law enforcement.

F. Company 6

45. In or about and between 2013 and 2018, HUAWEI devised a scheme to misappropriate technology from a U.S. developer of architecture for memory hardware headquartered in the Northern District of California ("Company 6"), an entity the identity of which is known to the Grand Jury.

46. Not long after the corporate formation of Company 6—which was a direct competitor of HUAWEI in the field of memory hardware architectural design—HUAWEI devised a corporate strategy to misappropriate proprietary technology from Company 6. An internal HUAWEI presentation from in or about 2015 articulated the "countermeasures" planned against Company 6, including "continuously recruit[ing] people from [Company 6]" in order to cause "internal turmoil" at Company 6. The same document included an organizational chart for Company 6, listing the names and compensation information for Company 6 employees located both in the United States and in the PRC.

47. As part of its scheme to misappropriate Company 6's technology, HUAWEI invited principals of Company 6 to make a presentation in Shenzhen, PRC in or around June 2015 about Company 6's technology regarding architecture for solid state drives, a kind of data storage device. After the presentation, HUAWEI sought a copy of the slide deck that Company 6 had used in its presentation; in the course of these communications, HUAWEI falsely expressed interest in developing a commercial relationship with Company 6. After receiving HUAWEI's oral promises that it would maintain the confidentiality of the information contained in the slide deck, including that HUAWEI would not share this information with HUAWEI's subsidiary that at the time was developing competing technology, Company 6 sent a copy of the slide deck to HUAWEI. Immediately upon receipt of the slide deck, each page of which was marked "Proprietary and Confidential" by Company 6, HUAWEI distributed the slide deck to HUAWEI engineers, including engineers in the subsidiary that was working on technology that directly competed with Company 6's products and services. These engineers discussed developments by Company 6 that would have application to HUAWEI's own prototypes then under design. Such actions were inconsistent with HUAWEI's previously stated intent to develop a commercial relationship with Company 6.

48. Acting at the direction of the Rotating Chairman of HUAWEI, a HUAWEI engineer ("Engineer-4"), an individual whose identity is known to the Grand Jury, visited Company 6's headquarters in the Northern District of California during the summer of 2016. According to a message sent to Company 6, Engineer-4 sought the meeting because "We are choosing . . . your company or [a competitor] to develop the [solid state drive] disc for our next generation of hard discs." After a meeting with a principal of

Company 6, an individual whose identity is known to the Grand Jury, where the principal provided an oral overview of Company 6's plans for architectural design, Engineer-4 wrote an internal HUAWEI email attaching a slide presentation detailing some of Company 6's intellectual property. The email stated, "Our idea of [solid state drive] and controller coordination is good but we acted a bit late."

49. HUAWEI did not follow up on Engineer-4's representations to Company 6 that HUAWEI intended to consider purchasing Company 6's products or services. Rather, HUAWEI made efforts to obtain Company 6's nonpublic technology without directly engaging Company 6. For example, two HUAWEI employees, individuals whose identities are known to the Grand Jury, including a principal of HUAWEI's chip design team, wrote to Company 6's generic email address, without concealing their affiliation with HUAWEI, requesting samples of Company 6's products, which were not then publicly available. Company 6 did not respond to these email requests, which were considered unusual business practice and possible efforts to misappropriate Company 6's protected intellectual property.

50. HUAWEI used a proxy to obtain information about Company 6's proprietary technology. Specifically, a professor of a PRC research university (the "Professor"), an individual whose identity is known to the Grand Jury, gained access to Company 6's proprietary technology on HUAWEI's behalf. An internal HUAWEI document from in or about early 2017 detailed the need to use such proxies to assist HUAWEI's goal of reverse engineering Company 6's nonpublic technology: "The internal information of [Company 6's] controller chip is not open to us, and the public information from [Company 6] is relatively limited; We lack effective engineering methods for reverse

analysis.” The document called for the creation of “reverse analysis engineering teams and laboratories” and reliance on “external resources,” such as the Professor, who could provide “third-party analysis materials,” as well as “external information.”

51. In or about December 2016, HUAWEI and the Professor entered into a contract calling for the Professor to develop prototype software for memory hardware. That same month, the Professor contacted Company 6 seeking access to a prototype board containing Company 6’s proprietary chip (the “Board”) for research purposes. At no time did the Professor disclose to Company 6 the existence of his contract or his relationship with HUAWEI.

52. In or about February 2017, Company 6 agreed to license a Board to the Professor. Company 6 would not have agreed to provide a Board to the Professor had the Professor disclosed the existence of his relationship with HUAWEI, because HUAWEI was a direct competitor of Company 6 in the field of memory architecture.

53. In the licensing agreement executed in or about February 2017 (the “Agreement”), the Professor and Company 6 agreed that the Professor’s access to a Board was conditioned on, among other requirements, the following prohibitions: (1) the direct or indirect transfer of rights or usage in the Board to third parties; (2) the modification or creation of derivative works based on the Board; and (3) the disclosure, divulgence or publication of the Board and its underlying technology. Pursuant to the Agreement, Company 6 provided the Professor with a specific product number and the identity of its PRC-based distributor of the Board (the “Distributor”), both of which were considered sensitive proprietary information.

54. Supply chain issues ultimately prevented Company 6 from delivering a Board to the Professor immediately after execution of the Agreement. In or about April 2017, approximately two months after execution of the Agreement, the Professor contacted Company 6 and claimed that he/she needed the Board immediately because of the availability of students to assist with research. In actuality, the Professor sought immediate delivery of the Board because of a pending project that the Professor had with HUAWEI. Indeed, that same month, the Professor wrote HUAWEI that “[t]he current dilemma is that the equipment [from Company 6] is not yet available”—thus making the Professor’s research impossible.

55. In or about April 2017, after obtaining a Board from Company 6, the Professor provided HUAWEI with the product number for the Board, as well as the identity of the Distributor, in violation of the Agreement. HUAWEI used this information to try on at least two occasions to acquire a Board from the Distributor without first contacting Company 6, but the Distributor refused to sell a Board to HUAWEI without Company 6’s consent. After the Distributor informed Company 6 about these efforts by HUAWEI, Company 6 contacted the Professor, who falsely denied providing the product number and the identity of the Distributor to HUAWEI. Company 6 also contacted HUAWEI, which refused to answer Company 6’s query as to how HUAWEI obtained information regarding the product number and the identity of the Distributor.

56. Also in violation of the terms of the Agreement, the Professor provided HUAWEI with performance results of the Professor’s testing of the Board. This information would have assisted in HUAWEI’s efforts to reverse engineer Company 6’s proprietary technology.

57. In or about July 2017, HUAWEI requested a high-level meeting with Company 6 to discuss Company 6's proprietary technology, ostensibly to develop a commercial relationship with Company 6. However, an internal HUAWEI email indicated that HUAWEI's actual motivation for the meeting was to "[o]btain the [Board] and support the development of our two projects" with the Professor. During the meeting, HUAWEI requested several samples of the Board, but Company 6 responded that it would not release a Board to HUAWEI without a nondisclosure agreement. At no time during these negotiations did HUAWEI disclose its relationship with the Professor or that it was seeking samples of the Board in connection with the Professor's work or its collaboration with the Professor. HUAWEI never established a commercial partnership with Company 6.

58. The efforts to misappropriate the intellectual property of Company 6 were designed to permit HUAWEI to save on research and development costs in the development of its own architecture for memory hardware.

III. False Statements to the U.S. Government

59. As part of the efforts by the defendant HUAWEI to establish and operate its business, particularly in the United States, the IP Defendants and their agents and representatives made repeated false statements to the U.S. government about their efforts to misappropriate the intellectual property of the Victim Companies, as well as the nature and the scope of HUAWEI's business activities related to sanctioned countries such as Iran and North Korea, to avoid the economic and regulatory consequences of making truthful statements, including the restriction of HUAWEI from U.S. markets and business opportunities.

60. In or about July 2007, agents with the Federal Bureau of Investigation (“FBI”) interviewed Individual-1 in New York, New York.

a. During the interview, among other things, Individual-1 falsely stated, in substance and in part, that HUAWEI did not conduct any activity in violation of U.S. export laws and that HUAWEI operated in compliance with all U.S. export laws. Individual-1 also falsely stated, in substance and in part, that HUAWEI had not dealt directly with any Iranian company. Individual-1 further stated that he believed HUAWEI had sold equipment to a third party, possibly in Egypt, which in turn sold the equipment to Iran.

b. During the same interview, Individual-1 falsely stated, in substance and in part, that HUAWEI “won” the lawsuit with Company 1 and that the FBI should consult with the Chief Executive Officer (“CEO”) of Company 1, who would “testify” that HUAWEI did not engage in intellectual property rights violations.

61. In or about 2012, the U.S. House of Representatives’ Permanent Select Committee on Intelligence (the “HPSCI”) conducted an investigation (the “HPSCI Investigation”) and hearings related to “National Security Threats from Chinese Telecommunications Companies Operating in the United States.” The purpose of the investigation was to consider, in relevant part, potential threats posed by HUAWEI as it sought to expand its business in the United States.

62. On or about September 13, 2012, a “corporate senior vice president under the chief Huawei representative to the United States” who also claimed to have the title of “President of Huawei North America” (the “Senior Vice President”), an individual whose identity is known to the Grand Jury, testified before the HPSCI. At the start of his testimony, the Senior Vice President identified the economic importance of the hearing for

HUAWEI, explaining that HUAWEI's "U.S. business has been damaged by unsubstantiated, non-specific concerns suggesting that Huawei poses a security threat."

a. During his testimony, in response to questions about HUAWEI's theft of trade secrets from Company 1, the Senior Vice President falsely testified that "Huawei provided our source code [for] our product to [Company 1] for review. And the result is there was not any infringement found." The Senior Vice President further falsely testified that the "source code" was "actually from a third party partner . . . already available and opened on the Internet."

b. Also during his testimony, the Senior Vice President falsely testified that HUAWEI's business in Iran had not "violated any laws and regulations including sanction-related requirements," and that "We have never provided any equipment to the Iranian government. All that we have provided are only for commercial civilian use." In fact, HUAWEI's business in Iran did violate laws and regulations, including sanction-related requirements, and included the provision of goods and services to the Iranian government, including surveillance technology used to monitor, identify and detain protestors during anti-government demonstrations in Tehran, Iran in or about 2009.

63. To supplement the testimony of the Senior Vice President, HUAWEI submitted, among other documents, a chart falsely reflecting "No Huawei Entities or Affiliates involved in Business activities" in North Korea and approximately \$19 million in "sales by distributors and resellers" to North Korea in 2008 and 2009. The chart did not reflect any activity in North Korea after 2009. In fact, HUAWEI was involved in business activities in North Korea, including numerous telecommunications projects, beginning no later than 2008. The chart also listed several HUAWEI clients in Iran, but omitted other

large HUAWEI clients with connections to the Government of Iran being served by SKYCOM.

IV. The Scheme to Defraud Financial Institutions

A. The Victim Financial Institutions

64. Financial Institution 1, an entity the identity of which is known to the Grand Jury, was a multinational banking and financial services company that operated subsidiaries throughout the world, including in the United States and in Eurozone countries. Its United States-based subsidiary (“U.S. Subsidiary 1”), an entity the identity of which is known to the Grand Jury, was a federally chartered bank, the deposits of which were insured by the Federal Deposit Insurance Company (“FDIC”). Among the services offered by Financial Institution 1 to its clients were U.S.-dollar clearing through U.S. Subsidiary 1 and other financial institutions located in the United States, and Euro clearing through Financial Institution 1 subsidiaries and other financial institutions located in Eurozone countries. Between approximately 2010 and 2014, Financial Institution 1 and U.S. Subsidiary 1 cleared more than \$100 million worth of transactions related to SKYCOM through the United States. In or about 2017, Financial Institution 1 verbally communicated to HUAWEI representatives that it was terminating its banking relationship with HUAWEI.

65. Financial Institution 2, an entity the identity of which is known to the Grand Jury, was a multinational banking and financial services company that operated subsidiaries throughout the world, including in the United States and in Eurozone countries. Among the services offered by Financial Institution 2 to its clients were U.S.-dollar clearing through a Financial Institution 2 subsidiary and other financial institutions located in the

United States, and Euro clearing through Financial Institution 2 subsidiaries and other financial institutions located in Eurozone countries.

66. Financial Institution 3, an entity the identity of which is known to the Grand Jury, was a multinational banking and financial services company that operated subsidiaries throughout the world, including in the United States and in Eurozone countries. Among the services offered by Financial Institution 3 to its clients were U.S.-dollar clearing through Financial Institution 3 subsidiaries and other financial institutions located in the United States, and Euro clearing through Financial Institution 3 subsidiaries and other financial institutions located in Eurozone countries.

67. Financial Institution 4, an entity the identity of which is known to the Grand Jury, was a multinational banking and financial services company that operated subsidiaries throughout the world, including in the United States and in Eurozone countries. Among the services offered by Financial Institution 4 to its clients were U.S.-dollar clearing through Financial Institution 4 subsidiaries and other financial institutions located in the United States, and Euro clearing through Financial Institution 4 subsidiaries and other financial institutions located in Eurozone countries. A subsidiary of Financial Institution 4 (“U.S. Subsidiary 4”), an entity the identity of which is known to the Grand Jury, was a financial institution organized in the United States offering banking and financial services throughout the world. U.S. Subsidiary 4 offered HUAWEI and its affiliates banking services and cash management services, including for accounts in the United States.

B. HUAWEI's Business in Countries Subject to Sanctions

68. As part of its international business model, HUAWEI participated in business in countries subject to U.S., E.U. and/or U.N. sanctions, such as Iran. This business, which included arranging for shipment of HUAWEI goods and services to end users in sanctioned countries, was typically conducted through local affiliates in the sanctioned countries, such as SKYCOM in Iran.

69. Reflecting the inherent sensitivity of conducting business in jurisdictions subject to U.S., E.U. and/or U.N. sanctions, internal HUAWEI documents referred to such jurisdictions with code names. For example, the code "A2" referred to Iran, and "A9" referred to North Korea. HUAWEI internal documents sometimes referred to those countries solely by code name, rather than by country name. HUAWEI internal documents did not refer to countries that were not subject to sanctions, such as the United States or Canada, by similar code names.

C. The SKYCOM Fraudulent Scheme

70. Even though the U.S. Department of the Treasury's Office of Foreign Assets Control's ("OFAC") Iranian Transactions and Sanctions Regulations ("ITSR"), 31 C.F.R. Part 560, proscribed the export of U.S.-origin goods, technology and services to Iran and the Government of Iran, HUAWEI operated SKYCOM as an unofficial subsidiary to obtain otherwise prohibited U.S.-origin goods, technology and services, including banking services, for HUAWEI's Iran-based business while concealing the link to HUAWEI. HUAWEI could thus attempt to claim ignorance with respect to any illegal act committed by SKYCOM on behalf of HUAWEI, including violations of the ITSR and other applicable U.S. law. In addition, HUAWEI assisted the Government of Iran by installing surveillance

equipment, including surveillance equipment used to monitor, identify and detain protestors during the anti-government demonstrations of 2009 in Tehran, Iran. Moreover, contrary to U.S. law, SKYCOM, on behalf of HUAWEI, employed in Iran at least one U.S. citizen (“Employee-1”), an individual whose identity is known to the Grand Jury.

71. Since in or about July 2007, HUAWEI repeatedly misrepresented to the U.S. government and to various victim financial institutions, including Financial Institutions 1, 2, 3 and 4, and their U.S. and Eurozone subsidiaries and branches (collectively, the “Victim Institutions”), that, although HUAWEI conducted business in Iran, it did so in a manner that did not violate applicable U.S. law, including the ITSR. In reality, HUAWEI conducted its business in Iran in a manner that violated applicable U.S. law, which includes the ITSR. Had the Victim Institutions known about HUAWEI’s repeated violations of the ITSR, they would have reevaluated their banking relationships with HUAWEI, including their provision of U.S.-dollar and Euro clearing services to HUAWEI.

72. Additionally, HUAWEI repeatedly misrepresented to Financial Institution 1 that HUAWEI would not use Financial Institution 1 and its affiliates to process any transactions regarding HUAWEI’s Iran-based business. In reality, HUAWEI used U.S. Subsidiary 1 and other financial institutions operating in the United States to process U.S.-dollar clearing transactions involving millions of dollars in furtherance of HUAWEI’s Iran-based business. Some of these transactions passed through the Eastern District of New York.

73. In or about 2011 and early 2012, news reports in The Wall Street Journal and Reuters claimed that HUAWEI assisted the Government of Iran to perform domestic surveillance, including providing equipment to track persons’ locations and a

surveillance system to monitor landline, mobile and internet communications. In response to the claims in The Wall Street Journal, HUAWEI issued an official press release in or about December 2011 through its website titled “Statement Regarding Inaccurate and Misleading Claims about Huawei’s Commercial Operations in Iran.” In the press release, HUAWEI claimed it “is not capable of ‘overseeing’ the network as reported in the article and we have no involvement in any type of monitoring and filtering activities.”

74. Similarly, in or about late 2012 and early 2013, various news organizations, including Reuters, reported that SKYCOM had sold and attempted to sell embargoed U.S.-origin goods to Iran in violation of U.S. law, and that HUAWEI in fact owned and operated SKYCOM. In December 2012, Reuters published an article purporting to contain a HUAWEI official statement addressing and denying those allegations. In January 2013, Reuters published a second article purporting to contain a HUAWEI official statement, again addressing and denying the Iran allegations. The purported statements by HUAWEI in these articles were relied on by the Victim Institutions in determining whether to continue their banking relationships with HUAWEI and its subsidiaries

75. Following publication of the December 2012 and January 2013 Reuters articles, various HUAWEI representatives and employees communicated to the Victim Institutions and to the public that the allegations regarding HUAWEI’s ownership and control of SKYCOM were false and that, in fact, HUAWEI did comply with applicable U.S. law, which includes the ITSR. Based in part on these false representations, the Victim Institutions continued their banking relationships with HUAWEI and its subsidiaries and affiliates.

76. For example, in or about June 2013, the defendant WANZHOU MENG requested an in-person meeting with a Financial Institution 1 executive (the “Financial Institution 1 Executive”), an individual whose identity is known to the Grand Jury. During the meeting, which took place on or about August 22, 2013, MENG spoke in Chinese, relying in part on a PowerPoint presentation written in Chinese. Upon request by the Financial Institution 1 Executive, MENG arranged for an English-language version of the PowerPoint presentation to be delivered to Financial Institution 1 on or about September 3, 2013.

77. In relevant part, the PowerPoint presentation included numerous misrepresentations regarding HUAWEI’s ownership and control of SKYCOM and HUAWEI’s compliance with applicable U.S. law, including that (1) HUAWEI “operates in Iran in strict compliance with applicable laws, regulations and sanctions of UN, US and EU”; (2) “Huawei has never provided and will never provide any technology, product, or service for monitoring communications flow, tracking user locations, or filtering media contents in the Iranian market”; (3) “HUAWEI’s engagement with SKYCOM is normal business cooperation”; (4) the defendant WANZHOU MENG’s participation on the Board of Directors of SKYCOM was to “help HUAWEI to better understand SKYCOM’s financial results and business performance, and to strengthen and monitor SKYCOM’s compliance”; and (5) “HUAWEI subsidiaries in sensitive countries will not open accounts at [Financial Institution 1], nor have business transactions with [Financial Institution 1].” These statements were all false.

78. In early 2014, several months after the meeting with Financial Institution 1 Executive, the defendant WANZHOU MENG traveled to the United States,

arriving at John F. Kennedy International Airport, which is located in the Eastern District of New York. When she entered the United States, MENG was carrying an electronic device that contained a file in unallocated space—indicating that the file may have been deleted—containing the following text:

Suggested Talking Points

The core of the suggested talking points regarding Iran/Skycom: Huawei's operation in Iran comports with the laws, regulations and sanctions as required by the United Nations, the United States and the European Union. The relationship with Skycom is that of normal business cooperation. Through regulated trade organizations and procedures, Huawei requires that Skycom promises to abide by relevant laws and regulations and export controls. Key information 1: In the past — ceased to hold Skycom shares 1, With regards to cooperation: Skycom was established in 1998 and is one of the agents for Huawei products and services. Skycom is mainly an agent for Huawei.

Other text in the same file appeared to refer to a document announcing the appointment of Huawei employees that was “signed by MENG Wanzhou,” the defendant.

79. Based in part on the false representations made by the defendant WANZHOU MENG and others, Financial Institution 1 continued its banking relationship with HUAWEI and its subsidiaries and affiliates.

D. The North Korea Fraudulent Scheme

80. Some of the Victim Institutions asked HUAWEI about HUAWEI's business presence in North Korea to better understand the risk, both reputational and legal, in processing HUAWEI transactions.

81. HUAWEI representatives and employees repeatedly denied to some of the Victim Institutions that HUAWEI was involved in numerous projects in North Korea. For example, in or about March 2013, HUAWEI employees told representatives of Financial

Institution 4 that, in sum and substance, HUAWEI had no business in North Korea. These representations were false.

82. In fact, HUAWEI was involved in numerous projects in North Korea beginning no later than 2008. Indeed, internal HUAWEI documents referred to the geographic location of projects in North Korea with the code “A9”—HUAWEI’s code for North Korea. HUAWEI employees took steps to conceal HUAWEI’s involvement in projects in North Korea. For example, shipping instructions provided by HUAWEI to a supplier in 2013 included the instruction that, for shipments to “A9/NK/NORTH KOREA,” there should be “No HW [HUAWEI] logo,” indicating that HUAWEI’s corporate logo should not be included on shipments destined for North Korea.

E. HUAWEI’s Continued Scheme to Defraud Financial Institutions

83. In or about 2017, Financial Institution 1 decided to terminate its global relationship with HUAWEI because of risk concerns regarding HUAWEI’s business practices. During a series of meetings and communications, Financial Institution 1 repeatedly communicated to HUAWEI that the decision to terminate its banking relationship with HUAWEI had been made by Financial Institution 1 alone, and was not a mutual decision with HUAWEI.

84. After learning of Financial Institution 1’s decision to terminate its relationship with HUAWEI, HUAWEI took steps to secure and expand its banking relationships with other financial institutions, including U.S. Subsidiary 4. In doing so, HUAWEI employees made material misrepresentations to U.S. Subsidiary 4, among other financial institutions, regarding the reason for the termination of its relationship with Financial Institution 1 and the party responsible for the termination, claiming that HUAWEI,

not Financial Institution 1, had initiated the termination. Specifically, in meetings and correspondence with representatives of U.S. Subsidiary 4, HUAWEI employees, [REDACTED] [REDACTED] falsely represented that HUAWEI was considering terminating its relationship with Financial Institution 1 because HUAWEI was dissatisfied with Financial Institution 1's level of service. HUAWEI's misrepresentation that it had decided to terminate its relationship with Financial Institution 1 was communicated to various components of U.S. Subsidiary 4, including in the Eastern District of New York.

85. Based in part on these false representations and omissions made by the defendants HUAWEI, [REDACTED], among other HUAWEI employees, U.S. Subsidiary 4 undertook to expand its banking relationship with HUAWEI and its subsidiaries and affiliates, and continued to maintain its existing banking relationship with HUAWEI globally, including in the United States. Had the defendants told U.S. Subsidiary 4 the truth about Financial Institution 1's decision to terminate its relationship with HUAWEI, U.S. Subsidiary 4 would have reevaluated its relationship with HUAWEI and its subsidiaries and affiliates.

86. By avoiding the termination of HUAWEI's relationship with Financial Institution 4 and U.S. Subsidiary 4, HUAWEI received income indirectly in the form of cost savings and the value of continued banking services, the proceeds of which income were used to operate and grow HUAWEI's business.

F. The Scheme to Obstruct Justice

87. In or about 2017, HUAWEI and HUAWEI DEVICE USA became aware of the U.S. government's criminal investigation of HUAWEI and its affiliates. In

response to the investigation, HUAWEI and HUAWEI DEVICE USA made efforts to move witnesses with knowledge about HUAWEI's Iran-based business to the PRC, and beyond the jurisdiction of the U.S. government, and to destroy and conceal evidence in the United States of HUAWEI's Iran-based business. By impeding the government's investigation, HUAWEI and HUAWEI DEVICE USA sought to avoid criminal prosecution with respect to HUAWEI's Iran-based activities, which would subject HUAWEI and its U.S. affiliates and subsidiaries, including HUAWEI DEVICE USA, to the threat of economic harm.

COUNT ONE
(Racketeering Conspiracy)

88. The allegations contained in paragraphs one through 87 are realleged and incorporated as if fully set forth in this paragraph.

89. At all times relevant to this Superseding Indictment, HUAWEI and its parents, global affiliates and subsidiaries, including HUAWEI DEVICE, HUAWEI DEVICE USA, FUTUREWEI and SKYCOM, constituted an "enterprise," as defined in Title 18, United States Code, Section 1961(4), that is, a group of legal entities associated in fact (hereinafter, the "Huawei Enterprise"). The Huawei Enterprise was engaged in, and its activities affected, interstate and foreign commerce.

90. The principal purpose of the Huawei Enterprise was to grow the global "Huawei" brand into one of the most powerful telecommunications equipment and consumer electronics companies in the world by entering, developing and dominating the markets for telecommunications and consumer electronics technology and services in each of the countries in which the Huawei Enterprise operated.

91. The Huawei Enterprise operated in the Eastern District of New York, the Central District of California, the District of Columbia, the District of Delaware, the District of New Jersey, the Eastern District of Texas, the Northern District of California, the Northern District of Illinois, the Northern District of Texas, the Southern District of California, the Southern District of New York, the Western District of New York, the Western District of Washington and elsewhere, including overseas.

92. In or about and between 1999 to the present, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants HUAWEI, HUAWEI DEVICE USA and FUTUREWEI, together with others, did knowingly and intentionally conspire to violate Title 18, United States Code, Section 1962(a), that is, to use and invest, directly and indirectly, a part of income and the proceeds of income, to wit: income received by HUAWEI, HUAWEI DEVICE USA and FUTUREWEI and derived, directly and indirectly, from a pattern of racketeering activity, in which HUAWEI, HUAWEI DEVICE USA and FUTUREWEI participated as principals within the meaning of Title 18, United States Code, Section 2, in the establishment and operation of the Huawei Enterprise, an enterprise that engaged in, and the activities of which affected, interstate and foreign commerce.

93. The pattern of racketeering activity, as defined in Title 18, United States Code, Sections 1961(1) and 1961(5), consisted of multiple acts indictable under Title 18, United States Code, Sections 1343 (relating to wire fraud), 1344 (relating to financial institution fraud), 1503 (relating to obstruction of justice), 1512 (relating to tampering with a witness, victim or an informant), 1832 (relating to theft of trade secrets), 1956 (relating to the

laundering of monetary instruments), and 2319 (relating to criminal infringement of a copyright). The manner and means of the above-described conspiracy include the allegations set forth in paragraphs one through 87, which are realleged and incorporated as if fully set forth in this paragraph.

(Title 18, United States Code, Sections 1962(d) and 3551 et seq.)

COUNT TWO
(Conspiracy to Steal Trade Secrets)

94. The allegations contained in paragraphs one through three and eight through 63 are realleged and incorporated as if fully set forth in this paragraph.

95. In or about and between 2000 and the present, both dates being approximate and inclusive, in the Eastern District of New York and elsewhere, the defendants HUAWEI, HUAWEI DEVICE, HUAWEI DEVICE USA and FUTUREWEI, together with others, knowingly, and with intent to convert one or more trade secrets that were related to a product used in or intended for use in interstate and foreign commerce, conspired to (a) steal, and without authorization appropriate, take, carry away and conceal, and obtain by fraud, artifice and deception such trade secrets, (b) without authorization copy, duplicate, sketch, draw, photograph, download, upload, alter, destroy, photocopy, replicate, transmit, deliver, send, mail, communicate and convey such trade secrets, (c) receive, buy and possess such trade secrets, knowing the same to have been stolen and appropriated, obtained and converted without authorization, to the economic benefit of HUAWEI, HUAWEI DEVICE, HUAWEI DEVICE USA and FUTUREWEI, and intending or knowing that the offense would injure any owner of those trade secrets, to wit: the trade secrets of the

Victim Companies, all contrary to Title 18, United States Code, Sections 1832(a)(1), 1832(a)(2) and 1832(a)(3).

96. In furtherance of the conspiracy and to effect its objects, within the Eastern District of New York and elsewhere, the defendants HUAWEI, HUAWEI DEVICE, HUAWEI DEVICE USA and FUTUREWEI, together with others, committed and caused the commission of, among others, the following:

OVERT ACTS

a. In or about March 2002, an employee of FUTUREWEI, an individual whose identity is known to the Grand Jury, contacted an employee of Company 1, an individual whose identity is known to the Grand Jury, regarding potential employment with FUTUREWEI, in an attempt to misappropriate trade secret information of Company 1.

b. On or about March 3, 2003, at the request of HUAWEI, Engineer-1, an employee of Company 2, wrote an email to Individual-1 and Individual-2, both employed by HUAWEI, and attached a Company 2 document, which comprised and included trade secret information, bearing the markings “HIGHLY CONFIDENTIAL” and “[Company 2] Confidential Property.”

c. On or about July 11, 2007, Individual-1 stated to FBI agents that HUAWEI had “won” the lawsuit with Company 1 and that the CEO of Company 1 would “testify” that HUAWEI did not engage in intellectual property rights violations.

d. On or about October 30, 2009, FUTUREWEI filed a provisional patent application with the U.S. Patent and Trademark Office that used and relied upon in large part misappropriated Company 4 trade secret information.

e. On or about September 13, 2012, the Senior Vice President falsely testified before U.S. Congress that “As specifically to the source code [allegedly stolen from Company 1], the source code of the issues was actually from a third party partner . . . already available and open on the internet.”

f. On or about May 29, 2013, a HUAWEI DEVICE USA employee accessed a Company 5 laboratory and surreptitiously placed a robot arm, which comprised and included trade secret information of Company 5, into a laptop bag and secreted the robot arm from the laboratory.

g. In or about July 2013, HUAWEI and HUAWEI DEVICE launched a formal policy to encourage employees to steal confidential information from competitors.

h. On or about June 9, 2015, Company 6 emailed a presentation marked “Proprietary and Confidential” to HUAWEI describing Company 6’s architecture for solid state drives, which HUAWEI personnel distributed internally, notwithstanding oral promises to maintain confidentiality and not to distribute the information to HUAWEI engineers.

i. On or about June 18 and 21, 2017, HUAWEI tried unsuccessfully to purchase Company 6’s nonpublic proprietary technology directly from the Distributor without Company 6’s permission and without informing Company 6.

j. On or about August 2, 2017, the Professor emailed testing results of software run on the Board to HUAWEI, contrary to the Agreement between the Professor and Company 6, which expressly prohibited the direct or indirect transfer of rights or usage in the Board to third parties.

k. In or about 2017, HUAWEI circulated an internal memorandum calling for the use of reverse engineering teams which would rely on external resources to obtain third-party analysis of nonpublic intellectual property belonging to other companies.

(Title 18, United States Code, Sections 1832(a)(5), 1832(b) and 3551 et seq.)

COUNT THREE

(Conspiracy to Commit Wire Fraud)

97. The allegations contained in paragraphs one through three and eight through 63 are realleged and incorporated as if fully set forth in this paragraph.

98. In or about and between 2009 and the present, both dates being approximate and inclusive, in the Eastern District of New York and elsewhere, the defendants HUAWEI, HUAWEI DEVICE, HUAWEI DEVICE USA and FUTUREWEI, together with others, did knowingly and intentionally conspire to devise a scheme and artifice to defraud the Victim Companies, and to obtain money and property from the Victim Companies, by means of one or more materially false and fraudulent pretenses, representations and promises, and for the purpose of executing such scheme and artifice, to transmit and cause to be transmitted by means of wire communication in interstate and foreign commerce, writings, signs, signals, pictures and sounds, contrary to Title 18, United States Code, Section 1343.

(Title 18, United States Code, Sections 1349 and 3551 et seq.)

COUNT FOUR

(Conspiracy to Commit Bank Fraud)

99. The allegations contained in paragraphs one, four, five, and 64 through 79 are realleged and incorporated as if fully set forth in this paragraph.

100. In or about and between November 2007 and May 2015, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants HUAWEI, SKYCOM and WANZHOU MENG, also known as “Cathy Meng” and “Sabrina Meng,” together with others, did knowingly and intentionally conspire to execute a scheme and artifice to defraud U.S. Subsidiary 1, a financial institution, and to obtain moneys, funds, credits and other property owned by and under the custody and control of said financial institution, by means of one or more materially false and fraudulent pretenses, representations and promises, contrary to Title 18, United States Code, Section 1344.

(Title 18, United States Code, Sections 1349 and 3551 et seq.)

COUNT FIVE

(Conspiracy to Commit Bank Fraud)

101. The allegations contained in paragraphs one, six, seven, 64 through 79, and 83 through 86 are realleged and incorporated as if fully set forth in this paragraph.

102. In or about and between August 2017 and January 2019, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants HUAWEI, [REDACTED] together with others, did knowingly and intentionally conspire to execute a scheme and artifice to defraud U.S. Subsidiary 4, a financial institution, and to obtain moneys, funds, credits and other property owned by and under the custody and control of said financial institution, by means of one or more materially false and fraudulent

pretenses, representations and promises, contrary to Title 18, United States Code, Section 1344.

(Title 18, United States Code, Sections 1349 and 3551 et seq.)

COUNT SIX

(Conspiracy to Commit Wire Fraud)

103. The allegations contained in paragraphs one, four, five, and 64 through 79 are realleged and incorporated as if fully set forth in this paragraph.

104. In or about and between November 2007 and May 2015, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants HUAWEI, SKYCOM and WANZHOU MENG, also known as “Cathy Meng” and “Sabrina Meng,” together with others, did knowingly and intentionally conspire to devise a scheme and artifice to defraud the Victim Institutions, and to obtain money and property from the Victim Institutions, by means of one or more materially false and fraudulent pretenses, representations and promises, and for the purpose of executing such scheme and artifice, to transmit and cause to be transmitted by means of wire communication in interstate and foreign commerce, writings, signs, signals, pictures and sounds, contrary to Title 18, United States Code, Section 1343.

(Title 18, United States Code, Sections 1349 and 3551 et seq.)

COUNT SEVEN

(Bank Fraud)

105. The allegations contained in paragraphs one, four, five, and 64 through 79 are realleged and incorporated as if fully set forth in this paragraph.

106. In or about and between November 2007 and May 2015, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the

defendants HUAWEI, SKYCOM and WANZHOU MENG, also known as “Cathy Meng” and “Sabrina Meng,” together with others, did knowingly and intentionally execute a scheme and artifice to defraud U.S. Subsidiary 1, a financial institution, and to obtain moneys, funds, credits and other property owned by, and under the custody and control of said financial institution, by means of one or more materially false and fraudulent pretenses, representations and promises.

(Title 18, United States Code, Sections 1344, 2 and 3551 et seq.)

COUNT EIGHT
(Bank Fraud)

107. The allegations contained in paragraphs one, six, seven, 64 through 79, and 83 through 86 are realleged and incorporated as if fully set forth in this paragraph.

108. In or about and between August 2017 and January 2019, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants HUAWEI, [REDACTED] together with others, did knowingly and intentionally execute a scheme and artifice to defraud U.S. Subsidiary 4, a financial institution, and to obtain moneys, funds, credits and other property owned by, and under the custody and control of said financial institution, by means of one or more materially false and fraudulent pretenses, representations and promises.

(Title 18, United States Code, Sections 1344, 2 and 3551 et seq.)

COUNT NINE
(Wire Fraud)

109. The allegations contained in paragraphs one, four, five, and 64 through 79 are realleged and incorporated as if fully set forth in this paragraph.

110. In or about and between November 2007 and May 2015, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants HUAWEI, SKYCOM and WANZHOU MENG, also known as “Cathy Meng” and “Sabrina Meng,” together with others, did knowingly and intentionally devise a scheme and artifice to defraud the Victim Institutions, and to obtain money and property from the Victim Institutions, by means of one or more materially false and fraudulent pretenses, representations and promises, and for the purpose of executing such scheme and artifice, did transmit and cause to be transmitted by means of wire communication in interstate and foreign commerce, writings, signs, signals, pictures and sounds, to wit: the defendants HUAWEI, SKYCOM and MENG, together with others, (a) made, and caused to be made, a series of misrepresentations through email communications, written communications otherwise conveyed through the wires, and oral communications made with knowledge that the oral communications would be memorialized and subsequently transmitted through the wires, about, among other things, the relationship between HUAWEI and SKYCOM, HUAWEI’s compliance with U.S. and U.N. laws and regulations, and the kinds of financial transactions in which HUAWEI engaged through the Victim Institutions; and (b) as a result of the misrepresentations, caused a series of wires to be sent by financial institutions from outside of the United States through the United States.

(Title 18, United States Code, Sections 1343, 2 and 3551 et seq.)

COUNT TEN
(Conspiracy to Defraud the United States)

111. The allegations contained in paragraphs one, four, and 64 through 87 are realleged and incorporated as if fully set forth in this paragraph.

112. In or about and between July 2007 and January 2019, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants HUAWEI and SKYCOM, together with others, did knowingly and willfully conspire to defraud the United States by impairing, impeding, obstructing and defeating, through deceitful and dishonest means, the lawful governmental functions and operations of OFAC, an agency of the United States, in the enforcement of economic sanctions laws and regulations administered by that agency and the issuance by that agency of appropriate licenses relating to the provision of financial services.

113. In furtherance of the conspiracy and to effect its objects, within the Eastern District of New York and elsewhere, the defendants HUAWEI and SKYCOM, together with others, committed and caused the commission of, among others, the following:

OVERT ACTS

a. On or about July 11, 2007, Individual-1 stated to FBI agents that HUAWEI did not conduct any activity in violation of U.S. export laws, that HUAWEI operated in compliance with all U.S. export laws, that HUAWEI had not dealt directly with any Iranian company and that he believed HUAWEI had sold equipment to a third party, possibly in Egypt, which in turn sold the equipment to Iran.

b. On or about September 13, 2012, the Senior Vice President testified before U.S. Congress that HUAWEI's business in Iran had not "violated any laws and regulations including sanction-related requirements."

c. On or about September 17, 2012, the Treasurer of HUAWEI met with a principal of U.S. Subsidiary 4, an individual whose identity is known to the Grand

Jury, in New York, New York, and informed U.S. Subsidiary 4 that HUAWEI and its global affiliates did not violate any applicable U.S. law.

d. On or about July 24, 2013, SKYCOM caused U.S. Subsidiary 1 to process a U.S.-dollar clearing transaction of \$52,791.08.

e. On or about July 24, 2013, SKYCOM caused a bank located in the Eastern District of New York (“Bank 1”), an entity the identity of which is known to the Grand Jury, to process a U.S.-dollar clearing transaction of \$94,829.82.

f. On or about August 20, 2013, SKYCOM caused Bank 1 to process a U.S.-dollar clearing transaction of \$14,835.22.

g. On or about August 28, 2013, SKYCOM caused Bank 1 to process a U.S.-dollar clearing transaction of \$32,663.10.

h. On or about April 11, 2014, SKYCOM caused a bank located in the United States (“Bank 2”), an entity the identity of which is known to the Grand Jury, to process a U.S.-dollar clearing transaction of \$118,842.45.

i. In or about April 2018, HUAWEI made efforts to move an employee (“Individual-4”), an individual whose identity is known to the Grand Jury, with knowledge about HUAWEI’s Iran-based business to the PRC, and beyond the jurisdiction of the U.S. government.

(Title 18, United States Code, Sections 371 and 3551 et seq.)

COUNT ELEVEN
(Conspiracy to Violate IEEPA)

114. The allegations contained in paragraphs one, four, 64 through 67, 70 through 79 are realleged and incorporated as if fully set forth in this paragraph.

115. Through the International Emergency Economic Powers Act (“IEEPA”), the President of the United States was granted authority to address unusual and extraordinary threats to the national security, foreign policy or economy of the United States. 50 U.S.C. § 1701(a). Under IEEPA, it was a crime to willfully violate, attempt to violate, conspire to violate or cause a violation of any license, order, regulation or prohibition issued pursuant to the statute. 50 U.S.C. §§ 1705(a) and 1705(c).

116. To respond to the declaration by the President of a national emergency with respect to Iran pursuant to IEEPA, which was most recently continued in March 2018 (83 Fed. Reg. 11,393 (Mar. 14, 2018)), OFAC issued the ITSR. Absent permission from OFAC in the form of a license, these regulations prohibited, among other things:

a. The exportation, reexportation, sale or supply from the United States, or by a U.S. person, wherever located, of any goods, technology or services to Iran and the Government of Iran (31 C.F.R. § 560.204);

b. Any transaction by a U.S. person, wherever located, involving goods, technology or services for exportation, reexportation, sale or supply, directly or indirectly, to Iran or the Government of Iran (31 C.F.R. § 560.206); and

c. Any transaction by a U.S. person, or within the United States, that evaded or avoided, had the purpose of evading or avoiding, attempted to violate, or caused a violation of any of the prohibitions in the ITSR (31 C.F.R. § 560.203).

117. The ITSR prohibited providing financial services, including U.S. dollar-clearing services, to Iran or the Government of Iran. 31 C.F.R. §§ 560.204, 560.427. In addition, the prohibition against the exportation, reexportation, sale or supply of services applied to services performed on behalf of a person in Iran or the Government of Iran, or

where the benefit of such services was otherwise received in Iran, if the services were performed (a) in the United States by any person; or (b) outside the United States by a United States person, including an overseas branch of an entity located in the United States. 31 C.F.R. § 560.410.

118. In or about and between November 2007 and November 2014, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants HUAWEI and SKYCOM, together with others, did knowingly and willfully conspire to cause the export, reexport, sale and supply, directly and indirectly, of goods, technology and services, to wit: banking and other financial services from the United States to Iran and the Government of Iran, without having first obtained the required OFAC license, contrary to Title 31, Code of Federal Regulations, Sections 560.203, 560.204 and 560.206.

(Title 50, United States Code, Sections 1705(a), 1705(c) and 1702; Title 18, United States Code, Sections 3551 et seq.)

COUNT TWELVE
(IEEPA Violations)

119. The allegations contained in paragraphs one, four, 64 through 67, and 70 through 79, and 115 through 118 are realleged and incorporated as if fully set forth in this paragraph.

120. In or about and between November 2007 and November 2014, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants HUAWEI and SKYCOM, together with others, did knowingly and willfully cause the export, reexport, sale and supply, directly and indirectly, of goods,

technology and services, to wit: banking and other financial services from the United States to Iran and the Government of Iran, without having first obtained the required OFAC license, contrary to Title 31, Code of Federal Regulations, Sections 560.203, 560.204 and 560.206.

(Title 50, United States Code, Sections 1705(a), 1705(c) and 1702; Title 18, United States Code, Sections 2 and 3551 et seq.)

COUNT THIRTEEN
(Conspiracy to Violate IEEPA)

121. The allegations contained in paragraphs one, four, 64 through 67, and 70 through 79, and 115 through 118 are realleged and incorporated as if fully set forth in this paragraph.

122. In or about and between 2008 and 2014, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants HUAWEI and SKYCOM, together with others, did knowingly and willfully conspire to cause the export, reexport, sale and supply, directly and indirectly, of goods, technology and services, to wit: telecommunications services provided by Employee-1, a U.S. citizen, to Iran and the Government of Iran, without having first obtained the required OFAC license, contrary to Title 31, Code of Federal Regulations, Sections 560.203, 560.204 and 560.206.

(Title 50, United States Code, Sections 1705(a), 1705(c) and 1702; Title 18, United States Code, Sections 3551 et seq.)

COUNT FOURTEEN
(IEEPA Violation)

123. The allegations contained in paragraphs one, four, 64 through 67, and 70 through 79, and 115 through 118 are realleged and incorporated as if fully set forth in this paragraph.

124. In or about and between 2008 and 2014, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants HUAWEI and SKYCOM, together with others, did knowingly and willfully cause the export, reexport, sale and supply, directly and indirectly, of goods, technology and services, to wit: telecommunications services provided by Employee-1, a U.S. citizen, to Iran and the Government of Iran, without having first obtained the required OFAC license, contrary to Title 31, Code of Federal Regulations, Sections 560.203, 560.204 and 560.206.

(Title 50, United States Code, Sections 1705(a), 1705(c) and 1702; Title 18, United States Code, Sections 2 and 3551 et seq.)

COUNT FIFTEEN
(Money Laundering Conspiracy)

125. The allegations contained in paragraphs one, four, 64 through 67, and 70 through 79, and 115 through 118 are realleged and incorporated as if fully set forth in this paragraph.

126. In or about and between November 2007 and November 2014, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants HUAWEI and SKYCOM, together with others, did knowingly and intentionally conspire to transport, transmit and transfer monetary instruments and funds, to wit: wire transfers, from one or more places in the United States to and through one or more places outside the United States and to one or more places in the United States from and through one or more places outside the United States, with the intent to promote the carrying on of specified unlawful activity, to wit: conspiracy to violate IEEPA, in violation of Title

50, United States Code, Section 1705, all contrary to Title 18, United States Code, Section 1956(a)(2)(A).

(Title 18, United States Code, Sections 1956(h) and 3551 et seq.)

COUNT SIXTEEN
(Conspiracy to Obstruct Justice)

127. The allegations contained in paragraphs one, three, 64 through 82, and 87 are realleged and incorporated as if fully set forth in this paragraph.

128. In or about and between January 2017 and January 2019, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants HUAWEI and HUAWEI DEVICE USA, together with others, did knowingly, intentionally and corruptly conspire to obstruct, influence and impede an official proceeding, to wit: a Federal Grand Jury investigation in the Eastern District of New York, contrary to Title 18, United States Code, Section 1512(c)(2).

(Title 18, United States Code, Sections 1512(k) and 3551 et seq.)

CRIMINAL FORFEITURE ALLEGATION AS TO COUNT ONE

129. The United States hereby gives notice to the defendants charged in Count One that, upon their conviction of such offense, the government will seek forfeiture in accordance with Title 18, United States Code, Section 1963(a), which requires any person convicted of such offense to forfeit: (a) any interest the person acquired or maintained in violation of Title 18, United States Code, Section 1962; (b) any interest in, security of, claim against, or property or contractual right of any kind affording a source of influence over any enterprise which the person has established, operated, controlled, conducted or participated in the conduct of, in violation of Title 18, United States Code, Section 1962; and (c) any

property constituting, or derived from, any proceeds which the person obtained, directly or indirectly, from racketeering activity in violation of Title 18, United States Code, Section 1962.

130. If any of the above-described forfeitable property, as a result of any act or omission of the defendants:

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third party;
- c. has been placed beyond the jurisdiction of the court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which cannot be

divided without difficulty;

it is the intent of the United States, pursuant to Title 18, United States Code, Section 1963(m), to seek forfeiture of any other property of the defendants up to the value of the forfeitable property described in this forfeiture allegation.

(Title 18, United States Code, Sections 1963(a) and 1963(m))

CRIMINAL FORFEITURE ALLEGATION AS TO COUNT TWO

131. The United States hereby gives notice to the defendants charged in Count Two that, upon their conviction of such offense, the government will seek forfeiture in accordance with Title 18, United States Code, Section 2323(b)(1), of (a) any article, the making or trafficking of which is prohibited under Title 17, United States Code, Section 506; Title 18, United States Code, Section 2318, 2319, 2319A, 2319B or 2320; or Chapter 90 of Title 18 of the United States Code; (b) any property used, or intended to be used, in any manner or part to commit or facilitate the commission of such offense; or (c) any property

constituting, or derived from, any proceeds obtained directly or indirectly as a result of such offense.

132. If any of the above-described forfeitable property, as a result of any act or omission of the defendants:

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third party;
- c. has been placed beyond the jurisdiction of the court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which cannot be divided without difficulty;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 2323(b)(2), to seek forfeiture of any other property of the defendants up to the value of the forfeitable property described in this forfeiture allegation.

(Title 18, United States Code, Sections 2323(b)(1) and 2323(b)(2); Title 21, United States Code, Section 853(p))

CRIMINAL FORFEITURE ALLEGATION
AS TO COUNTS THREE THROUGH NINE

133. The United States hereby gives notice to the defendants charged in Counts Three through Nine that, upon their conviction of such offenses, the government will seek forfeiture in accordance with Title 18, United States Code, Section 982(a)(2), which requires any person convicted of such offenses to forfeit any property constituting, or derived from, proceeds obtained directly or indirectly as a result of such offenses.

134. If any of the above-described forfeitable property, as a result of any act or omission of the defendants:

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third party;
- c. has been placed beyond the jurisdiction of the court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which cannot be

divided without difficulty;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 982(b)(1), to seek forfeiture of any other property of the defendants up to the value of the forfeitable property described in this forfeiture allegation.

(Title 18, United States Code, Sections 982(a)(2) and 982(b)(1); Title 21, United States Code, Section 853(p))

CRIMINAL FORFEITURE ALLEGATION
AS TO COUNTS TEN THROUGH FOURTEEN AND SIXTEEN

135. The United States hereby gives notice to the defendants charged in Counts Ten through Fourteen and Sixteen and that, upon their conviction of such offenses, the government will seek forfeiture in accordance with Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c), which require any person convicted of such offenses to forfeit any property, real or personal, constituting, or derived from, proceeds obtained directly or indirectly as a result of such offenses.

136. If any of the above-described forfeitable property, as a result of any act or omission of the defendants:

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third party;
- c. has been placed beyond the jurisdiction of the court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which cannot be

divided without difficulty;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), to seek forfeiture of any other property of the defendants up to the value of the forfeitable property described in this forfeiture allegation.

(Title 18, United States Code, Section 981(a)(1)(C); Title 21, United States Code, Section 853(p); Title 28, United States Code, Section 2461(c))

CRIMINAL FORFEITURE ALLEGATION
AS TO COUNT FIFTEEN

137. The United States hereby gives notice to the defendants charged in Count Fifteen that, upon their conviction of such offense, the government will seek forfeiture in accordance with Title 18, United States Code, Section 982(a)(1), which requires any person convicted of such offense to forfeit any property, real or personal, involved in such offense, or any property traceable to such property.

138. If any of the above-described forfeitable property, as a result of any act or omission of the defendants:

- a. cannot be located upon the exercise of due diligence;

- b. has been transferred or sold to, or deposited with, a third party;
- c. has been placed beyond the jurisdiction of the court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which cannot be

divided without difficulty;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 982(b)(1), to seek


forfeiture of any other property of the defendants up to the value of the forfeitable property described in this forfeiture allegation.

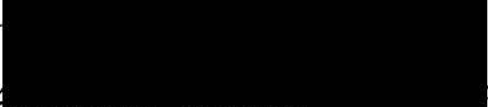
(Title 18, United States Code, Sections 982(a)(1) and 982(b)(1); Title 21,


United States Code, Section 853(p))

A TRUE BILL


FOREPERSON


RICHARD P. DONOGHUE
UNITED STATES ATTORNEY
EASTERN DISTRICT OF NEW YORK


DEBORAH L. CONNOR
CHIEF
MONEY LAUNDERING AND ASSET RECOVERY SECTION
CRIMINAL DIVISION
U.S. DEPARTMENT OF JUSTICE


CHIEF
COUNTERINTELLIGENCE AND EXPORT CONTROL SECTION
NATIONAL SECURITY DIVISION
U.S. DEPARTMENT OF JUSTICE

F. # 2017R05903
FORM DBD-34
JUN. 85

No.
UNITED STATES DISTRICT COURT
EASTERN *District of* NEW YORK
CRIMINAL DIVISION

THE UNITED STATES OF AMERICA

vs.

HUAWEI TECHNOLOGIES CO., LTD., HUAWEI DEVICE CO., LTD.,
HUAWEI DEVICE USA INC., FUTUREWEI TECHNOLOGIES, INC.,
SKYCOM TECH CO. LTD., WANZHOU MENG, also known as "Cathy
Meng" and "Sabrina Meng," [REDACTED]

Defendants.

SUPERSEDING INDICTMENT

(T. 18, U.S.C., §§ 371, 981(a)(1)(C); 982(a)(1), 982(a)(2), 982(b)(1),
1343, 1344, 1349, 1512(k), 1956(h), 1962(d), 1963(a), 1963(m),
2323(b)(1), 2323(b)(2), 2 and 3551 *et seq.*; T. 21, U.S.C., § 853(p); T. 28,
U.S.C., § 2461(c); T. 50, U.S.C., §§ 1702, 1705(a) and 1705(c))

A true bill.

[REDACTED]
Foreperson

Filed in open court this _____ day of _____ A.D. 20 ____

Clerk

Bail, \$ _____

*Alexander A. Solomon, Julia Nestor, David K. Kessler, and Sarah
Evans, Assistant U.S. Attorneys (718) 254-7000*