

Presented to the Court by the foreman of the
Grand Jury in open Court, in the presence of
the Grand Jury and FILED in the U.S.
DISTRICT COURT at Seattle, Washington.

Judge Lasnik

January 31, 2018
WILLIAM M. McCOOL, Clerk
By [Signature] Deputy

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA,

Plaintiff,

v.

MUHAMMAD FAHD and
GHULAM JIWANI,

Defendants.

NO. CR17-0290RSL

SUPERSEDING INDICTMENT

The Grand Jury charges that:

INTRODUCTION

At all times material to this Superseding Indictment:

1. AT&T Mobility LLC (hereinafter, AT&T), was a company with headquarters in Atlanta, Georgia, and offices throughout the United States, including a customer service call center in Bothell, Washington.

2. AT&T sold cellular telephones and offered monthly voice and data plans for use with the phones on the AT&T wireless network. AT&T phones and wireless services were sold through authorized AT&T dealers and retailers across the country.

3. AT&T offered subsidies to its customers by selling phones for less than the cost of the phones. AT&T recouped this subsidy investment through profits earned on the sale of AT&T wireless services by entering into service contracts with its customers.

1 4. Manufacturers that produced cellular telephones for AT&T installed
2 proprietary locking software onto AT&T phones that prevented the phones from being
3 used on any wireless network other than the AT&T network unless and until the phones
4 were "unlocked."

5 5. "Unlocking" a phone disabled the proprietary locking software and thereby
6 allowed the phone to be used on multiple carrier systems rather than exclusively with
7 AT&T.

8 6. The Wireless Customer Agreement between AT&T and each of its
9 customers provided that AT&T would unlock the customer's phone upon the satisfaction
10 of certain criteria, such as when the customer had completed his or her contract or
11 installment plan or paid off an installment plan early. Other circumstances in which
12 AT&T might unlock a phone for a customer included when the customer wished to use
13 the phone for international travel.

14 7. Unlocked phones were a valuable commodity because they could be resold
15 and used on any other compatible network around the world. When telephone customers
16 switched to networks other than AT&T's network, the customers stopped paying AT&T
17 for services, including, in some cases, before AT&T had recouped the costs of subsidies
18 provided by AT&T on phones it had sold to the customers for less than the cost of the
19 phones.

20 8. When phones were unlocked fraudulently without AT&T's authorization
21 and customers switched service to other carriers, the fraudulent transactions deprived
22 AT&T of its subsidy investment in phones and of the stream of contract payments that
23 customers no longer remitted because they had switched service to another carrier.

24 9. AT&T employees at AT&T's Mobility Customer Care call center in
25 Bothell, Washington, had access to AT&T's computer systems to assist AT&T customers
26 with service and billing issues. Among other things, AT&T employees at the call center
27 had the ability to submit unlock requests on behalf of eligible customers.
28

1 10. AT&T employees used a variety of internal computer programs at AT&T
2 to process unlock requests including, at different times, a system called "Fat Albert," and
3 a system called "Torch." Access to the systems was limited to authenticated users
4 connected to AT&T's internal and protected corporate network.

5 11. AT&T's unlocking systems permitted AT&T employees with proper
6 authorization and network credentials to, in appropriate circumstances, send requests to
7 unlock the phones of AT&T customers.

8 12. Malware was malicious computer code running on a computer that was not
9 authorized by the owner/authorized user of that computer. Malware could be designed to
10 do a variety of things, including logging every keystroke on a computer, stealing
11 information or "user credentials" (passwords or usernames), and executing unauthorized
12 commands without the consent of the authorized user.

13
14 **COUNT 1**
15 **(Conspiracy to Commit Wire Fraud)**

16 13. The allegations contained in Paragraphs 1 through 12 of this Superseding
17 Indictment are re-alleged and incorporated as if fully set forth herein.

18 **I. THE OFFENSE**

19 14. Beginning at a date unknown, but no later than April 2012, and continuing
20 through in or about September 2017, at Bothell, within the Western District of
21 Washington, and elsewhere, MUHAMMAD FAHD, aka Frank Zhang, GHULAM
22 JIWANI, and others known and unknown to the Grand Jury, did knowingly and
23 intentionally, agree and conspire to devise and execute and attempt to execute, a scheme
24 and artifice to defraud, and for obtaining money and property by means of materially
25 false and fraudulent pretenses, representations, and promises; and in executing and
26 attempting to execute this scheme and artifice, to knowingly cause to be transmitted in
27 interstate and foreign commerce, by means of wire communication, certain signs, signals
28

1 and sounds as further described below, in violation of Title 18, United States Code,
2 Section 1343.

3 **II. THE OBJECT OF THE CONSPIRACY**

4 15. The object of the conspiracy was to gain access to AT&T's protected
5 internal computers without authorization, and in excess of authorization, by bribing
6 AT&T employees to submit fraudulent and unauthorized cellphone unlocking requests
7 through AT&T's internal protected computer network through, among other means, the
8 installation of malware and unauthorized hardware on AT&T's internal network. The
9 object further was to sell to members of the public the resulting ability fraudulently to
10 unlock phones, so that the members of the public could stop using AT&T wireless
11 services and thereby deprive AT&T of its subsidy investment in customer cell phones
12 and the value of the wireless service contracts AT&T sold to members of the public.

13 **III. MANNER AND MEANS OF THE CONSPIRACY**

14 **A. Overview of the Conspiracy**

15 16. It was part of the conspiracy that MUHAMMAD FAHD, GHULAM
16 JIWANI and others known and unknown to the Grand Jury, gained unauthorized access
17 to AT&T's internal protected computers through a variety of methods, including by
18 bribing AT&T employees (hereinafter "insiders") at AT&T's call center in Bothell,
19 Washington, to use their network credentials and exceed their authorized access to
20 AT&T's computers to submit large numbers of fraudulent and unauthorized unlock
21 requests on behalf of the conspiracy and to install malware and unauthorized hardware on
22 the AT&T systems.

23 17. From in or about April 2012 to in or about April 2013, MUHAMMAD
24 FAHD, and others known and unknown to the Grand Jury, transmitted instructions to the
25 insiders via the wires in interstate and foreign commerce, including lists of cellular
26 telephone international mobile equipment identity (IMEI) numbers for the insiders to
27 submit for fraudulent and unauthorized unlocking.
28

1 18. From in or about April 2013 to in or about October 2013, MUHAMMAD
2 FAHD, GHULAM JIWANI and others known and unknown to the Grand Jury, bribed
3 insiders to plant malware on AT&T's internal protected computers for the purpose of
4 gathering confidential and proprietary information on how AT&T's computer network
5 and software applications functioned.

6 19. Using information gathered by this malware about AT&T's computer
7 network and software applications, MUHAMMAD FAHD, and others known and
8 unknown to the Grand Jury, created additional malware designed to interact with
9 AT&T's internal protected computers and automatically process fraudulent and
10 unauthorized unlock requests submitted over the wires in interstate commerce from
11 remote servers controlled by members of the conspiracy.

12 20. The malware MUHAMMAD FAHD, and others known and unknown to
13 the Grand Jury, planted on AT&T's internal protected computers used network
14 credentials that belonged to actual AT&T employees, including co-conspirators and
15 others, to allow MUHAMMAD FAHD, and others known and unknown to the Grand
16 Jury, to log into AT&T's internal protected computers under false pretenses and
17 automatically to process fraudulent and unauthorized unlock requests.

18 21. From in or about November 2014 to in or about September 2017,
19 MUHAMMAD FAHD, GHULAM JIWANI and others known and unknown to the
20 Grand Jury, bribed insiders to use their access to AT&T's physical work space to install
21 unauthorized computer hardware devices, including wireless access points designed to
22 provide the conspiracy with unauthorized access to AT&T's internal protected computers
23 and facilitate the automated process of submitting fraudulent and unauthorized unlock
24 requests on behalf of the conspiracy.

25 22. The unauthorized computer hardware devices, like the malware, used
26 network credentials that belonged to actual AT&T employees, including co-conspirators
27 and others, and allowed MUHAMMAD FAHD, and others known and unknown to the
28

1 Grand Jury, to log into AT&T's internal protected computers under false pretenses and
2 automatically to process fraudulent and unauthorized unlock requests.

3 23. During the course of the conspiracy, MUHAMMAD FAHD, GHULAM
4 JIWANI, and other co-conspirators who were not associated with AT&T, paid more than
5 \$1,000,000 in bribes to AT&T insiders who joined the conspiracy. MUHAMMAD
6 FAHD, GHULAM JIWANI, and other co-conspirators paid these bribes to induce the
7 AT&T insiders to unlock cellular phones without authorization, including by installing
8 malware and unauthorized hardware on AT&T's computer systems.

9 24. During the course of the conspiracy, the conspirators caused more than
10 2,000,000 cellular telephones fraudulently to be unlocked by AT&T through the AT&T
11 insiders' submission of fraudulent unlocking requests and through the conspirators' use
12 of malware and hardware installed on AT&T's systems by the AT&T insiders to conduct
13 unauthorized unlocks.

14 **B. Defendant MUHAMMAD FAHD's Participation in the Conspiracy**

15 25. It was part of the conspiracy that MUHAMMAD FAHD, doing business as
16 Endless Trading FZE (aka Endless Trading FZC), Endless Connections Inc., and
17 iDevelopment Co. recruited insiders at AT&T who were willing to take bribes to work on
18 behalf of the conspiracy.

19 26. MUHAMMAD FAHD contacted the insiders at AT&T via telephone,
20 Facebook, and other communication channels in interstate and foreign commerce and
21 offered to pay them to unlock cell phones. MUHAMMAD FAHD instructed the insiders
22 to obtain pre-paid cellular phones and anonymous online email accounts to communicate
23 with him.

24 27. MUHAMMAD FAHD also instructed the insiders to create shell
25 companies and open business banking accounts in the names of the shell companies to
26 receive payments for their work on behalf of the conspiracy.
27
28

1 28. MUHAMMAD FAHD obtained lists of IMEI numbers for cellular
2 telephones from co-conspirators, and others, who operated businesses that offered
3 unlocking services to customers for a fee.

4 29. Beginning in or about August 2012, MUHAMMAD FAHD sent lists of
5 IMEI numbers for cellular telephones via the wires in interstate and foreign commerce to
6 the insiders with instructions to submit unauthorized unlock requests for the IMEIs using
7 their access to AT&T's protected internal computer network.

8 30. Beginning in or about April 2013, MUHAMMAD FAHD sent malware to
9 the insiders via the wires in interstate and foreign commerce and instructed them to install
10 the malware on AT&T's computer network. The malware was designed to gather
11 confidential and proprietary information regarding the structure and functioning of
12 AT&T's internal protected computers and applications.

13 31. Using information collected by the malware, MUHAMMAD FAHD, and
14 others known and unknown to the Grand Jury, created additional malware designed to
15 facilitate the transmission of commands via the wires in interstate and foreign commerce
16 from a remote server to AT&T's protected internal computer network and automatically
17 to submit unauthorized unlock requests.

18 32. MUHAMMAD FAHD sent the insiders multiple versions of the unlocking
19 malware to test and perfect the malware on behalf of the conspiracy. Once the malware
20 was perfected, MUHAMMAD FAHD instructed the insiders to plant the unlocking
21 malware on AT&T's internal protected computers and to run the unlocking malware
22 while they were at work. The unlocking malware used valid AT&T network credentials
23 that belonged to co-conspirators and others, without authorization, to interact with
24 AT&T's internal protected computer network and process automated unauthorized
25 unlock requests submitted from an external server.

26 33. In or about October 2013, AT&T discovered the unlocking malware and
27 fired several insiders who were operating the unlocking malware at MUHAMMAD
28 FAHD's direction.

1 34. As a result, beginning in or about November 2014, MUHAMMAD FAHD
2 recruited new insiders at AT&T willing to accept bribes to work on behalf of the
3 conspiracy.

4 35. MUHAMMAD FAHD and others known and unknown to the Grand Jury,
5 began programming hardware devices designed to facilitate unauthorized access to
6 AT&T's internal protected network for the purpose of processing automated
7 unauthorized unlock requests.

8 36. MUHAMMAD FAHD provided the hardware devices to co-conspirators
9 including current and former AT&T insiders who tested the devices. Upon perfecting the
10 operation of the devices, MUHAMMAD FAHD provided the devices to insiders who
11 plugged the devices into AT&T's internal protected network without authorization to
12 facilitate the unlocking of phones in furtherance of the conspiracy.

13 37. MUHAMMAD FAHD continued to pay insiders at AT&T to gain and
14 maintain unauthorized access to AT&T's internal protected computer network, and
15 exceed their authorized access to AT&T's protected internal computer network, plant
16 malware, install unauthorized hardware, and operate malware and unauthorized hardware
17 on AT&T's protected internal computer network on behalf of the conspiracy through in
18 or about September 2017.

19 **C. Defendant GHULAM JIWANI's Participation in the Conspiracy**

20 38. It was part of the conspiracy that GHULAM JIWANI received lists of
21 thousands of IMEIs from customers of the conspiracy and from co-conspirators that those
22 customers wanted to have unlocked. The customers and co-conspirators who provided
23 GHULAM JIWANI such lists included customers and co-conspirators that sold cellular
24 phone unlocking services to the public.

25 39. GHULAM JIWANI caused the lists of IMEIs to be submitted to the AT&T
26 insiders so that the AT&T insiders could unlock the cellular phones. GHULAM JIWANI
27 subsequently received reports from the AT&T insiders showing which IMEIs had been
28

1 unlocked, and forwarded these to customers and co-conspirators. GHULAM JIWANI
2 also negotiated and obtained payments from customers of the conspiracy.

3 40. GHULAM JIWANI made payments of bribes to insiders at AT&T.
4 GHULAM JIWANI did so by causing payments to be transmitted by Western Union to
5 the insiders. GHULAM JIWANI also did so by flying from Pakistan to the United States
6 and delivering cash payments to the insiders or to persons who received the cash
7 payments on behalf of the insiders.

8 41. GHULAM JIWANI facilitated, and attended, a meeting between
9 MUHAMMAD FAHD and one of the AT&T insiders. GHULAM JIWANI did so by
10 arranging for the insider to travel from the State of Washington to Dubai, United Arab
11 Emirates, in order to meet with MUHAMMAD FAHD and to receive payment of a bribe
12 from MUHAMMAD FAHD.

13 All in violation of Title 18, United States Code, Section 1349.
14

15 **COUNT 2**
16 **(Conspiracy to Violate the Travel Act and**
17 **the Computer Fraud and Abuse Act)**

18 42. The allegations set forth in Paragraphs 1 through 41 of this Superseding
19 Indictment are re-alleged and incorporated as if fully set forth herein.

20 **I. THE OFFENSE**

21 43. Beginning at a date uncertain, but no later than April 2013, and continuing
22 through in or about September 2017, at Bothell, within the Western District of
23 Washington, and elsewhere, MUHAMMAD FAHD, aka Frank Zhang, GHULAM
24 JIWANI, and others known and unknown to the Grand Jury, did knowingly and
25 intentionally agree and conspire to:

26 a. use a facility in interstate and foreign commerce, namely the wires,
27 with the intent to promote, manage, establish, carry on and facilitate the promotion,
28 management, establishment and carrying on of an unlawful activity, that is, Commercial

1 Bribery, in violation of the Revised Code of Washington Section 9A.68.060, and
2 thereafter performed and attempted to perform an act to distribute the proceeds of such
3 unlawful activity, and to promote, manage, establish and carry on, and to facilitate the
4 promotion, management, establishment and carrying on of, such unlawful activity in
5 violation of Title 18, United States Code, Section 1952(a)(1) and (3);

6 b. knowingly and with intent to defraud, access a protected computer
7 without authorization and exceed authorized access to a protected computer, and by
8 means of such conduct further the intended fraud and obtain anything of value exceeding
9 \$5,000.00 in any 1-year period, in violation of Title 18, United States Code, Sections
10 1030(a)(4) and (c)(3)(A); and

11 c. knowingly cause the transmission of a program, information, code,
12 and command, and as a result of such conduct, intentionally cause damage without
13 authorization to a protected computer, and the offense caused loss to 1 or more persons
14 during any 1-year period aggregating at least \$5,000 in value and damage affecting 10 or
15 more protected computers during a 1-year period, in violation of Title 18, United States
16 Code, Sections 1030(a)(5)(A) and (c)(4)(B)(i).

17 **II. THE OBJECT OF THE CONSPIRACY**

18 44. The object of the conspiracy is set forth in Paragraph 15 of this Superseding
19 Indictment and is re-alleged and incorporated as if fully set forth herein. Through their
20 conduct, the conspirators caused damages to AT&T's protected computers, including
21 impairment to the integrity and availability of data, programs, systems, and information,
22 and caused losses to AT&T for the costs of responding to the offense, conducting damage
23 assessments, restoring data, programs, systems and information and lost revenue during
24 any 1-year period in excess of \$5,000.00.

25 **III. THE MANNER AND MEANS OF THE CONSPIRACY**

26 45. The manner and means of the conspiracy are set forth in Paragraphs 16
27 through 41 of this Superseding Indictment and are re-alleged and incorporated as if fully
28 set forth herein.

1 **IV. Overt Acts**

2 46. In furtherance of the conspiracy, and to achieve the objects thereof,
3 defendants MUHAMMAD FAHD, GHULAM JIWANI and others known and unknown
4 to the Grand Jury, did commit and cause to be committed, the following overt acts, at
5 Bothell, within the Western District of Washington and elsewhere:

6 a. On or about April 11, 2013, MUHAMMAD FAHD opened a Yahoo
7 account with the email address unlockoutlet@ymail.com;

8 b. In or about April 2013, MUHAMMAD FAHD provided two AT&T
9 insiders (CC-2 and CC-3) who were employed at AT&T in Bothell, Washington, with
10 malware;

11 c. In or about April 2013, each of those AT&T insiders (CC2 and
12 CC-3) installed the malware on AT&T's internal protected network;

13 d. On or about April 15, 2013, a co-conspirator wired bribe payments
14 in the amount of \$11,000.00 to each of the two AT&Ts insiders (CC-2 and CC-3) from
15 California to Marysville, Washington;

16 e. On or about November 12, 2014, MUHAMMAD FAHD sent a
17 WhatsApp message to GHULAM JIWANI instructing him to send a \$4,000 bribe by
18 Western Union to one AT&T insider (CC-2) and a \$1,000 bribe by Western Union to
19 another AT&T insider (CC-5);

20 f. On or about November 25, 2014, MUHAMMAD FAHD sent a
21 router to an AT&T insider (CC-2) via Federal Express from Dubai, United Arab
22 Emirates, to Lynnwood, Washington;

23 g. In or about November 2014, the AT&T insider (CC-2) provided a
24 router configured to provide unauthorized access to AT&T's internal protected network
25 to another AT&T insider (CC-5) to install on AT&T's network;

26 h. On or about August 9, 2015, MUHAMMAD FAHD and GHULAM
27 JIWANI traveled to Dubai, United Arab Emirates, from Karachi, Pakistan, to meet an
28 AT&T insider (CC-2) and to deliver a bribe payment to him;

1 i. On or about February 26, 2015, GHULAM JIWANI traveled to
2 Houston, Texas, to deliver a bribe for an AT&T insider (CC-5).

3 All in violation of Title 18, United States Code, Section 371.
4

5 **COUNTS 3-6**
6 **(Wire Fraud)**

7 47. The allegations set forth in Counts 1 and 2 of this Superseding Indictment
8 are re-alleged and incorporated as if fully set forth herein.

9 **I. THE SCHEME**

10 48. Beginning at a date uncertain, but no later than April 2012, and continuing
11 through in or about September 2017, at Bothell, within the Western District of
12 Washington, and elsewhere, MUHAMMAD FAHD, aka Frank Zhang, GHULAM
13 JIWANI, and others known and unknown to the Grand Jury, devised and intended to
14 devise a scheme to defraud AT&T Mobility LLC, and to obtain money and property by
15 means of materially false and fraudulent pretenses, representations and promises.

16 **II. THE MANNER AND MEANS OF THE SCHEME**

17 49. The manner and means of the scheme are set forth in Paragraphs 16
18 through 41 of this Superseding Indictment and are re-alleged and incorporated as if fully
19 set forth herein.

20 **III. EXECUTION OF THE SCHEME**

21 50. On or about the dates set forth below, at Bothell, within the Western
22 District of Washington, and elsewhere, MUHAMMAD FAHD, GHULAM JIWANI, and
23 others known and unknown to the Grand Jury, having devised a scheme and artifice to
24 defraud, and to obtain money and property by means of materially false and fraudulent
25 pretenses, representations, and promises, did knowingly transmit and cause to be
26 transmitted writings, signs, signals, pictures, and sounds, for the purpose of executing
27 such scheme, by means of wire communication in interstate and foreign commerce,
28

including the following transmissions, with each such transmission constituting a separate count of this Superseding Indictment.

Count	Date(s)	Defendant(s) Charged	Wire Communication
3	April 6, 2013	MUHAMMAD FAHD GHULAM JIWANI	Email from an AT&T insider (CC-3) at Bothell, Washington, to MUHAMMAD FAHD, outside the State of Washington, which then was forwarded by MUHAMMAD FAHD to GHULAM JIWANI, reporting on the status of cellular telephone unlocks for a list of cellular telephone IMEIs
4	April 19, 2013	MUHAMMAD FAHD	Email from MUHAMMAD FAHD from outside the State of Washington, to an AT&T insider (CC-2) at Bothell, Washington, with attached malware and with instructions for installing the malware on AT&T's computer system
5	November 13, 2014	MUHAMMAD FAHD GHULAM JIWANI	Western Union transfer of \$4,052 from outside the State of Washington to Lynnwood, Washington, to pay a bribe to an AT&T insider (CC-2)
6	January 8, 2015	MUHAMMAD FAHD	E-mail from an AT&T insider (CC-5) at Bothell, Washington, to MUHAMMAD FAHD, outside the State of Washington, containing photographs of the AT&T insider's work computer screen

All in violation of Title 18, United States Code, Sections 1343 and 2.

1
2
3
4
5
6
7
8
9
0
1
2
3
4
5
6
7
8
9
0
1
2
3
4
5
6
7
8

51. The allegations set forth in Counts 1 and 2 of this Superseding Indictment are re-alleged and incorporated as if fully set forth herein.

All in violation of Title 18, United States Code, Sections 1030(a)(4) and (c)(3)(A) and 2.

(Intentional Damage to a Protected Computer)

54. Beginning at a date uncertain, but no later than in or about April 2013, and continuing until in or around October 2013, at Bothell, within the Western District of Washington and elsewhere, MUHAMMAD FAHD, aka Frank Zhang, and others known and unknown to the Grand Jury, knowingly caused the transmission of a program, information, code, and command, specifically malicious code that was downloaded and installed on AT&T Mobility LLC's protected computers without AT&T Mobility LLC's

1 knowledge or consent, and as a result of such conduct, intentionally caused damage
2 without authorization to protected computers, which damage caused losses to 1 or more
3 persons during any 1-year period of at least \$5,000.00 and affected 10 or more protected
4 computers during a 1 year period.

5 All in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and
6 (c)(4)(B)(i) and 2.

7
8 **COUNT 9**
9 **(Accessing a Protected Computer in Furtherance of Fraud)**

10 55. The allegations set forth in Counts 1 and 2 of this Superseding Indictment
11 are re-alleged and incorporated as if fully set forth herein.

12 56. Beginning at a date uncertain, but no later than in or about November 2014,
13 and continuing until in or around September 2017, at Bothell, within the Western District
14 of Washington and elsewhere, MUHAMMAD FAHD, aka Frank Zhang, and others
15 known and unknown to the Grand Jury, knowingly and with intent to defraud accessed
16 protected computers without authorization and exceeded authorized access and by means
17 of such conduct furthered the intended fraud and obtained something of value,
18 specifically, the defendant and others downloaded and installed malware onto AT&T
19 Mobility LLC's protected computers and executed the malware programs designed to
20 facilitate fraudulent and unauthorized unlocking transactions on AT&T Mobility LLC's
21 wireless network and by means of such conduct furthered the intended fraud and obtained
22 things of value exceeding \$5,000.00 in any 1-year period.

23 All in violation of Title 18, United States Code, Sections 1030(a)(4) and (c)(3)(A)
24 and 2.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

COUNT 10

(Intentional Damage to a Protected Computer)

57. The allegations set forth in Counts 1 and 2 of this Superseding Indictment are re-alleged and incorporated as if fully set forth herein.

58. Beginning at a date uncertain, but no later than in or around November 2014, and continuing until in or around September 2017, at Bothell, within the Western District of Washington and elsewhere, MUHAMMAD FAHD, aka Frank Zhang, and others known and unknown to the Grand Jury, knowingly caused the transmission of a program, information, code, and command, specifically malicious code that was downloaded and installed on AT&T Mobility LLC's protected computers without AT&T Mobility LLC's knowledge or consent, and as a result of such conduct, intentionally caused damage without authorization to protected computers, which damage caused losses to 1 or more persons during any 1-year period of at least \$5,000.00 and affected 10 or more protected computers during a 1 year period.

All in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and (c)(4)(B)(i) and 2.

COUNTS 11-14
(Travel Act)

59. The allegations set forth in Counts 1 and 2 of this Superseding Indictment are re-alleged and incorporated as if fully set forth herein.

60. On or about the dates below, at Bothell, within the Western District of Washington, and elsewhere, MUHAMMAD FAHD, aka Frank Zhang, GHULAM JIWANI, and others known and unknown to the Grand Jury, used a facility in interstate and foreign commerce with the intent to distribute the proceeds, and to promote, manage, establish, carry on and facilitate the promotion, management, establishment and carrying on, of an unlawful activity, that is: Commercial Bribery in violation of Revised Code of Washington Section 9A.68.060, and thereafter performed and attempted to perform an act

1 to distribute the proceeds, and to promote, manage, establish and carry on and facilitate
2 the promotion, management, establishment and carrying on, of such unlawful activity.
3

Count	Date(s)	Defendant(s) Charged	Act Performed
11	April 15, 2013	MUHAMMAD FAHD	Payment of \$11,000, by wire transfer, from an account outside the State of Washington to an account at Chase Bank within the State of Washington to pay a bribe to an AT&T insider (CC-3)
12	November 13, 2014	MUHAMMAD FAHD GHULAM JIWANI	Payment of \$4,052 by Western Union, from outside the State of Washington, to an AT&T insider (CC-2) in Lynnwood, Washington, to pay a bribe to that insider
13	November 13, 2014	MUHAMMAD FAHD GHULAM JIWANI	Payment of \$948 by Western Union, from outside the State of Washington, to an AT&T insider (CC-5), in Everett, Washington, to pay a bribe to that insider
14	August 10, 2015	MUHAMMAD FAHD GHULAM JIWANI	Purchase of ticket for flight by an AT&T insider (CC-2), and subsequent flight by that insider, by commercial airline from SeaTac, Washington, to Dubai, United Arab Emirates, to meet MUHAMMAD FAHD and GHULAM JIWANI

23
24 All in violation of Title 18, United States Code, Sections 1952(a)(1) and (3),
25 and 2.
26
27
28

FORFEITURE ALLEGATIONS

61. The allegations contained in Counts 1 through 14 of this Superseding Indictment are hereby re-alleged and incorporated by reference for the purpose of alleging forfeitures pursuant to Title 18, United States Code, Section 981(a)(1)(C), Title 28, United States Code, Section 2461(c), Title 18, United States Code, Section 982(a)(2)(B), and Title 18, United States Code, Section 1030(i).

62. Pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c), upon conviction of a conspiracy to violate Title 18, United States Code, Section 1349, as set forth in Count 1, of a violation of Title 18 United States Code, Section 1343, as set forth in Counts 3 through 6, the defendants shall forfeit to the United States of America, any property, real or personal, which constitutes or is derived from proceeds traceable to the charged offense. The property to be forfeited includes, but is not limited to, a sum of money representing the amount of proceeds the defendant obtained as a result of the charged offense.

63. Pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c), upon conviction of a conspiracy to violate Title 18, United States Code, Sections 1030(a)(4) and (c)(3)(A) and Title 18, United States Code, Sections 1030(a)(5)(A) and (c)(4)(B)(i), in violation of Title 18, United States Code, Section 371, as set forth in Count 2, the defendants shall forfeit to the United States of America any property, real or personal, which constitutes or is derived from proceeds traceable to the charged offense. The property to be forfeited includes, but is not limited to, the following: a sum of money representing the amount of proceeds the defendant obtained as a result of the charged offense.

64. Pursuant to Title 18, United States Code, Section 982(a)(2)(B), and Title 18, United States Code, Section 1030(i), upon conviction of a violation of Title 18, United States Code, Sections 1030(a)(4) and (c)(3)(A), as set forth in Counts 7 and 9, the defendant shall forfeit to the United States of America any property, real or personal, which constitutes or is derived from proceeds traceable to the charged offense. The

1 property to be forfeited includes, but is not limited to, the following: a sum of money
2 representing the amount of proceeds the defendant obtained as a result of the charged
3 offense.

4 65. Pursuant to Title 18, United States Code, Section 982(a)(2)(B), and Title
5 18, United States Code, Section 1030(i) , upon conviction of a violation of Title 18,
6 United States Code, Sections 1030(a)(5)(A) and (c)(4)(B)(i), as set forth in Counts 8 and
7 10, the defendant shall forfeit to the United States of America any property, real or
8 personal, which constitutes or is derived from proceeds traceable to the charged offense.
9 The property to be forfeited includes, but is not limited to, the following: a sum of money
10 representing the amount of proceeds the defendant obtained as a result of the charged
11 offense.

12 66. Pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28,
13 United States Code, Section 2461(c), upon conviction of a Travel Act violation, in
14 violation of Title 18, United States Code, Section 1952(a)(1) and (3), as set forth in
15 Counts 11 through 14, the defendants shall forfeit to the United States of America any
16 property, real or personal, which constitutes or is derived from proceeds traceable to the
17 charged offense. The property to be forfeited includes, but is not limited to, the
18 following: a sum of money representing the amount of proceeds the defendant obtained
19 as a result of the charged offense.

20 67. If any of the property described above, as a result of any act or omission
21 of the defendants:

- 22 a. cannot be located upon the exercise of due diligence;
- 23 b. has been transferred or sold to, or deposited with, a third party;
- 24 c. has been placed beyond the jurisdiction of the court;
- 25 d. has been substantially diminished in value; or
- 26 e. has been commingled with other property which cannot be divided
27 without difficulty, the United States of America shall be entitled to
28

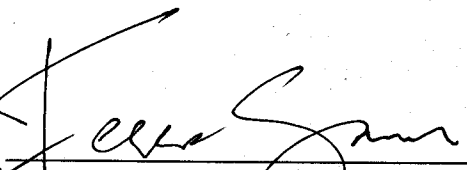
1 forfeiture of substitute property pursuant to Title 21, United States
2 Code, Section 853(p), as incorporated by Title 28, United States
3 Code, Section 2461(c).
4


5 A TRUE BILL:
6

7 DATED: / - 31 - 2018
8

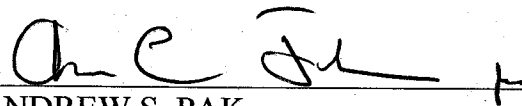
9 (Signature of Foreperson redacted pursuant
10 to the policy of the Judicial Conference)

11 _____
12 FOREPERSON
13

14 
15 _____
16 ANNETTE L. HAYES
17 United States Attorney

18 
19 _____
20 ANDREW C. FRIEDMAN
21 Assistant United States Attorney

22 
23 _____
24 FRANCIS FRANZE-NAKAMURA
25 Assistant United States Attorney

26 
27 _____
28 ANDREW S. PAK
Trial Attorney
Computer Crimes and Intellectual Property Section