IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

SEALED

Holding a Criminal Term
Grand Jury Sworn in on July 6, 2017

UNITED STATES OF AMERICA	:	CRIMINAL NO.
	:	
v.	:	GRAND JURY ORIGINAL
	:	
YIN KECHENG,	:	VIOLATIONS:
	:	
a/k/a "YKCAI,"	:	18 U.S.C. § 1343
	:	(Wire Fraud)
Defendant.	:	
	:	18 U.S.C. § 1030(a)(5)
	:	(Computer Fraud)
	:	
	:	18 U.S.C. § 1030(a)(2)
	:	(Computer Fraud)
	:	
	:	18 U.S.C. § 1028A(a)(1)
	:	(Aggravated Identity Theft)
	:	
	:	Criminal Forfeiture:
	:	18 U.S.C. § 981(a)(1)(C); 18 U.S.C.
	:	§ 982(a)(2); 18 U.S.C. §§ 1030(i) and (j);
	:	28 U.S.C. § 2461(c); and 21 U.S.C. §
	:	853(p).

Case: 1:18-cr-00126
Assigned To : Judge Amit P. Mehta
Assign. Date : 5/2/2018
Description: INDICTMENT(B)

INDICTMENT

The Grand Jury charges that:

INTRODUCTION

At times material to this indictment:

1. YIN KECHENG was a Chinese national and a resident of Shanghai, in the People's Republic of China ("PRC"). YIN KECHENG used the online alias "YKCAI."

2. YIN KECHENG had no known residence or past residence in the United States.

3. Victim A was a technology and engineering firm located in the United States. Victim A was a defense contractor, which provided technical, engineering, and information technology services to the United States government.

4. Victim B was a technology firm located in the United States. Victim B was a defense contractor, which provided technology services to the United States government.

5. Victim C was a supplier of aerospace components and systems located in the United States. Victim C designed, tested, and manufactured components for different types of aircraft, including military aircraft.

6. Victim D was a research and policy think-tank located in the District of Columbia.

7. Victim E was a research and policy think-tank located in the District of Columbia.

The Scheme

8. Beginning no later than August 2013, and continuing until at least December 2015, and beginning outside of the jurisdiction of any particular State or district, including inside the PRC, YIN KECHENG devised, intended to devise, executed, and participated in a computer intrusion scheme that constituted a scheme to defraud organizations in the United States, including Victims A, B, C, D, and E, and to obtain money and property from said organizations by means of materially false and fraudulent pretenses and representations, and by concealment of material facts.

9. During September 2013, in communications with an associate, YIN KECHENG described his intent to carry out the scheme, his intent to profit from the scheme, and certain computer intrusion strategies that could be used to carry out the scheme. For example:

a. YIN KECHENG explained that he wanted to "mess with the American military" and "break into a big target" so that he could earn enough money to buy a car.

b. YIN KECHENG discussed his preference for American targets. YIN KECHENG emphasized that "anything within the top 100" of defense contractors would suffice, but that he was targeting "American ones." YIN KECHENG's associate criticized him for "only [knowing] how to work on America," even though "[o]ther countries have good stuff, too." YIN KECHENG's associate noted, for example, that the "Ministry of Railways . . . had a very high demand for high speed rail, especially rail design, smelting technology, etc." YIN KECHENG replied, "I just like the Americans, nothing else is as good."

c. YIN KECHENG and his associate discussed technical aspects and various strategy concerns. On one occasion, YIN KECHENG's associate explained that he preferred to "go after the subsidiary companies of the big companies, focus on copying the production of the big companies' equipment," and suggested that they should "go after the subsidiaries of some of those big American companies or their partner companies, they are the same and easier to attack." YIN KECHENG's associate emphasized, "we're always able to get to the big company through their partners." YIN KECHENG agreed that this strategy was "correct."

10. It was part of the scheme that YIN KECHENG used materially false representations to obtain and maintain access and use the computer networks owned and controlled by Victims A, B, C, D, and E for the purpose of stealing proprietary and confidential computer files and data. YIN KECHENG fraudulently obtained unauthorized access and use of the victims' networks by:

a. falsely representing the nature of malicious computer files, or "malware," sent to the victims' networks;

b. using intermediary computer servers known as "hop points" in order to misrepresent and conceal his true identity and location;

c. using fraudulent domains (or web addresses) to falsely represent and conceal the true nature of internet traffic between the hop points and the victims' networks, as YIN KECHENG remotely browsed, copied, and exfiltrated the victims' computer data; and

d. using stolen network credentials (usernames and passwords belonging to authorized users) in order to falsely represent his identity in order to gain access to victims' computer networks (and to different parts of those networks) under false pretenses.

11. As a result of the scheme, YIN KECHENG fraudulently gained access to the victims' networks and exfiltrated hundreds of gigabytes of information, including proprietary business information and technical data.

The Malware

12. In furtherance of the scheme, YIN KECHENG caused computer programs, including programs known as "fierce" and "nmap," to scan the networks of Victims B, C, D, and E, in order to identify each victims' network architecture, operating systems, and access points from the internet – for the purpose of infecting their computers and networks with malware.

13. It was further part of the scheme that YIN KECHENG used multiple variations of a type of malware known as "PlugX." Once PlugX malware was installed on a victim's computers, YIN KECHENG could remotely perform data theft and other unauthorized computer activity on a victim's computers and networks, such as opening, copying, modifying, and creating files.

14. It was further part of the scheme that YIN KECHENG falsely represented and caused to be falsely represented the origin, authenticity, and nature of PlugX files that were installed on victims' computers. YIN KECHENG used PlugX malware concealed within computer files that falsely appeared to be authored and cryptographically signed by legitimate software manufacturers.

15. For example, on or about March 30, 2015, YIN KECHENG falsely represented and caused to be falsely represented the origin, authenticity, and nature of the following computer file package sent to Victim D: "RavXP.exe," "ProcCom.dll," and "ProcCom.dyload," which purported to be anti-virus software that was authored and certified as "secure" by a known software manufacturer. In fact, YIN KECHENG knew that this package of files contained PlugX malware, which was not authored by, nor certified as "secure" by, any legitimate software manufacturer.

The Hop Points

16. It was further part of the scheme that YIN KECHENG caused a Chinese-based intermediary to lease various computer servers, or "hop points," that YIN KECHENG controlled from the PRC.

17. YIN KECHENG used these hop points to conceal his true Internet Protocol ("IP") addresses, location, and identity, while using PlugX malware to remotely access and use the victims' networks. YIN KECHENG also used the hop points to host various fraudulent domains, as further described below.

18. It was further part of the scheme that YIN KECHENG set up multiple "virtual machines" or operating systems on the hop points, in order to control the PlugX malware that YIN KECHENG had caused to be installed on victims' computers.

19. It was further part of the scheme that YIN KECHENG configured the PlugX malware so that it would cause infected computers to send automated, electronic signals or "beacons" from the victims' networks to the various hop points associated with fraudulent domains, which allowed YIN KECHENG to monitor the status of the malware on victims' networks.

The Fraudulent Domains

20. It was further part of the scheme that YIN KECHENG's PlugX malware would cause infected computers to contact the fraudulent domains that were specified in the malware code. These fraudulent domains, in turn, directed infected computers to communicate with IP addresses that corresponded to one of YIN KECHENG's hop points.

21. It was further part of the scheme that beginning no later than March 29, 2011, YIN KECHENG caused the registration and use of multiple fraudulent domains, which gave the false appearance that they were affiliated and controlled by legitimate companies and network security organizations. These fraudulent domains include "darkhero.org," "blackcmd.com," "hotmail-onlines.com," "lnip.org," "update-onlines.com," "[Victim A]-na.com," "[Victim B]-na.com" and "windows-updateonlines.com."

22. YIN KECHENG further used misleading and fraudulent subdomains, such as "services.darkhero.org," "helpdesk.[Victim A]-na.com," and "news.hotmail-onlines.com" to control the PlugX malware on the victims' networks and conceal the existence of the scheme.

The Stolen Credentials

23. It was further part of the scheme that YIN KECHENG used stolen network credentials to gain access to different parts of the victims' networks and steal data.

24. It was further part of the scheme that YIN KECHENG did misrepresent, conceal, and hide, and cause to be misrepresented, concealed, and hidden, acts done in furtherance of the scheme and the purpose of those acts.

The Computer Intrusions

25. On or about August 20, 2013, YIN KECHENG used PlugX malware to access and use Victim A's computer networks and steal the network credentials of one of Victim A's employees. YIN KECHENG caused the stolen credentials to be transferred to one of the hop points.

26. On or about September 27, 2013, YIN KECHENG used PlugX malware to access and use Victim B's networks, steal network credentials for one of Victim B's employees, and steal company data. YIN KECHENG configured the PlugX malware so that it would cause infected computers to contact subdomains of the fraudulent domains "update-onlines.com" and "windows-updateonlines.com." YIN KECHENG caused stolen company data to be transferred to two different hop points.

27. Beginning in February 2014, and continuing through May 2014, YIN KECHENG used PlugX malware to access and use Victim B's networks for the purpose of stealing additional company data. YIN KECHENG configured the PlugX malware so that it would cause infected computers to contact a subdomain of the fraudulent domain "[Victim A]-na.com."

28. Beginning no later than July 2014, and continuing through April 2015, YIN KECHENG used PlugX malware to access and use Victim C's networks and steal approximately 526 gigabytes of company data. YIN KECHENG caused computers on Victim C's networks to communicate with subdomains of the fraudulent domains "hotmail-onlines.com," "lnip.org," and

"[Victim A]-na.com," all of which were hosted on hop points that he controlled. YIN KECHENG used PlugX malware, including PlugX malware that was configured to cause infected computers to contact a subdomain of the fraudulent domain "[Victim A]-na.com." YIN KECHENG used his access to Victim C's computers to cause stolen company data to be transferred to hop points that he controlled.

29. Beginning no later than in or about February 2015, and continuing until at least July 2015, YIN KECHENG used PlugX malware to access and use Victim D's networks and remove data. YIN KECHENG used PlugX malware that was configured to cause infected computers to contact subdomains of the fraudulent domains "[Victim A]-na.com," "[Victim B]-na.com," and "lnip.org," all of which were hosted on hop points that he controlled. YIN KECHENG thereby caused computers on Victim D's networks to communicate with hop points that he controlled.

30. Beginning no later than in or about April 2015, and continuing until August 2015, YIN KECHENG used PlugX malware to access and use Victim E's networks and remove data. YIN KECHENG's PlugX malware was configured to beacon to a subdomain of the fraudulent domain "[Victim A]-na.com." YIN KECHENG caused computers on Victim E's networks to communicate with hop points that he controlled.

31. In or about July 2015, YIN KECHENG used a hop point to scan Victim D's networks and to obtain unauthorized access to Victim D's networks using stolen login credentials.

32. In or about August 2015, YIN KECHENG used a hop point to scan Victim C's networks and to obtain unauthorized access to Victim C's networks using stolen login credentials.

33. In or about September 2015, YIN KECHENG used PlugX malware to access and use Victim B's networks. YIN KECHENG configured the PlugX malware to beacon directly to an IP address that corresponded to one of the hop points.

COUNT ONE

34. Paragraphs 1 through 33 are re-alleged here.

35. On or about August 20, 2013, beginning outside of the jurisdiction of any particular State or district, YIN KECHENG, for the purpose of executing the scheme to defraud and to obtain money and property by means of materially false and fraudulent pretenses and representations, and by concealment of material facts, knowingly caused to be transmitted by means of wire communication in interstate commerce between Texas and Virginia, certain writings, signs, and signals, namely, an electronic transmission of stolen network credentials from a computer in Victim A's network to a hop point.

(**Wire Fraud,** in violation of Title 18, United States Code, Section 1343)

COUNT TWO

36. Paragraphs 1 through 33 are re-alleged here.

37. On or about September 29, 2013, beginning outside of the jurisdiction of any particular State or district, and later within the District of Columbia and elsewhere, YIN KECHENG, for the purpose of executing the scheme to defraud and to obtain money and property by means of materially false and fraudulent pretenses and representations, and by concealment of material facts, knowingly caused to be transmitted by means of wire communication in interstate commerce between the District of Columbia and California, certain writings, signs, and signals, namely, an electronic connection between a hop point and a computer in Victim B's network.

(**Wire Fraud,** in violation of Title 18, United States Code, Section 1343)

COUNT THREE

38. Paragraphs 1 through 33 are re-alleged here.

39. On or about July 10, 2014, beginning outside of the jurisdiction of any particular State or district, YIN KECHENG, for the purpose of executing the scheme to defraud and to obtain money and property by means of materially false and fraudulent pretenses and representations, and by concealment of material facts, knowingly caused to be transmitted by means of wire communication in interstate commerce between Pennsylvania and California, certain writings, signs, and signals, namely, an electronic connection between a hop point and a computer in Victim C's network.

(**Wire Fraud,** in violation of Title 18, United States Code, Section 1343)

COUNT FOUR

40. Paragraphs 1 through 33 are re-alleged here.

41. On or about March 12, 2015, beginning outside of the jurisdiction of any particular State or district, YIN KECHENG, for the purpose of executing the scheme to defraud and to obtain money and property by means of materially false and fraudulent pretenses and representations, and by concealment of material facts, knowingly caused to be transmitted by means of wire communication in interstate commerce between Pennsylvania and California, certain writings, signs, and signals, namely, electronic connections between a computer in Victim C's network and a hop point that hosted fraudulent domains.

(**Wire Fraud,** in violation of Title 18, United States Code, Section 1343)

COUNT FIVE

42. Paragraphs 1 through 33 are re-alleged here.

43. On or about April 1, 2015, beginning outside of the jurisdiction of any particular State or district, and later within the District of Columbia and elsewhere, YIN KECHENG, for the purpose of executing the scheme to defraud and to obtain money and property by means of materially false and fraudulent pretenses and representations, and by concealment of material facts, knowingly caused to be transmitted by means of wire communication in interstate commerce between the District of Columbia and California, certain writings, signs, and signals, namely, an electronic connection between a hop point and a computer in Victim D's network.

(**Wire Fraud,** in violation of Title 18, United States Code, Section 1343)

COUNT SIX

44. Paragraphs 1 through 33 are re-alleged here.

45. Between on or about April 12, 2015, and April 23, 2015, beginning outside of the jurisdiction of any particular State or district, YIN KECHENG, for the purpose of executing the scheme to defraud and to obtain money and property by means of materially false and fraudulent pretenses and representations, and by concealment of material facts, knowingly caused to be transmitted by means of wire communication in interstate commerce between New York and California, certain writings, signs, and signals, namely, electronic transmissions that caused a computer in Victim C's network to transfer stolen data to a hop point.

(**Wire Fraud,** in violation of Title 18, United States Code, Section 1343)

COUNT SEVEN

46. Paragraphs 1 through 33 are re-alleged here.

47. On or about July 22, 2015, beginning outside of the jurisdiction of any particular State or district, and later within the District of Columbia and elsewhere, YIN KECHENG, for the purpose of executing the scheme to defraud and to obtain money and property by means of materially false and fraudulent pretenses and representations, and by concealment of material facts, knowingly caused to be transmitted by means of wire communication in interstate commerce between the District of Columbia and Texas, certain writings, signs, and signals, namely, an electronic connection between a computer in Victim D's network and a hop point.

(**Wire Fraud,** in violation of Title 18, United States Code, Section 1343)

COUNT EIGHT

48. Paragraphs 1 through 33 are re-alleged here.

49. On or about August 10, 2015, beginning outside of the jurisdiction of any particular State or district, and later within the District of Columbia and elsewhere, YIN KECHENG, for the purpose of executing the scheme to defraud and to obtain money and property by means of materially false and fraudulent pretenses and representations, and by concealment of material facts, knowingly caused to be transmitted by means of wire communication in interstate commerce between California and the District of Columbia certain writings, signs, and signals, namely, electronic connections between a hop point and a computer in Victim E's network.

(**Wire Fraud,** in violation of Title 18, United States Code, Section 1343)

COUNT NINE

50. Paragraphs 1 through 33 are re-alleged here.

51. On or about September 27, 2013, beginning outside of the jurisdiction of any particular State or district, and later within the District of Columbia and elsewhere, YIN KECHENG knowingly caused the transmission of a program, information, code, and command, and as a result of such conduct, would and did intentionally cause damage without authorization to a protected computer and caused more than $5,000 in loss in one year to Victim B.

(**Computer Fraud,** in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and (c)(4)(B)(i))

COUNT TEN

52. Paragraphs 1 through 33 are re-alleged here.

53. On or about March 25, 2015, beginning outside of the jurisdiction of any particular State or district, YIN KECHENG knowingly caused the transmission of a program, information, code, and command, and as a result of such conduct, would and did intentionally cause damage without authorization to a protected computer and caused more than $5,000 in loss in one year to Victim C.

(**Computer Fraud,** in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and (c)(4)(B)(i))

COUNT ELEVEN

54. Paragraphs 1 through 33 are re-alleged here.

55. On or about March 30, 2015, beginning outside of the jurisdiction of any particular State or district, and later within the District of Columbia and elsewhere, YIN KECHENG

knowingly caused the transmission of a program, information, code, and command, and as a result of such conduct, would and did intentionally cause damage without authorization to a protected computer and caused more than $5,000 in loss in one year to Victim D.

(**Computer Fraud,** in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and (c)(4)(B)(i))

COUNT TWELVE

56. Paragraphs 1 through 33 are re-alleged here.

57. In or about May 2015, beginning outside of the jurisdiction of any particular State or district, and later within the District of Columbia and elsewhere, YIN KECHENG knowingly caused the transmission of a program, information, code, and command, and as a result of such conduct, would and did intentionally cause damage without authorization to a protected computer and caused more than $5,000 in loss in one year to Victim E.

(**Computer Fraud,** in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and (c)(4)(B)(i))

COUNT THIRTEEN

58. Paragraphs 1 through 33 are re-alleged here.

59. Between on or about April 12, 2015, and April 23, 2015, beginning outside of the jurisdiction of any particular State or district, YIN KECHENG, for purposes of commercial advantage and private financial gain, and in furtherance of a criminal and tortious act in violation of the Constitution and the laws of the United States, specifically, wire fraud, in violation of Title 18, United States Code, Section 1343, intentionally accessed a computer without authorization,

and thereby obtained information from a protected computer, such conduct having involved an interstate and foreign communication, said protected computer belonging to Victim C.

(**Computer Fraud,** in violation of Title 18, United States Code, Sections 1030(a)(2) and (c)(2)(B)(i) and (ii))

COUNT FOURTEEN

60. Paragraphs 1 through 33 are re-alleged here.

61. On or about August 10, 2015, beginning outside of the jurisdiction of any particular State or district, YIN KECHENG, for purposes of commercial advantage and private financial gain, and in furtherance of a criminal and tortious act in violation of the Constitution and the laws of the United States, specifically, wire fraud, in violation of Title 18, United States Code, Section 1343, intentionally accessed a computer without authorization, and thereby obtained information from a protected computer, such conduct having involved an interstate and foreign communication, said protected computer belonging to Victim E.

(**Computer Fraud,** in violation of Title 18, United States Code, Sections 1030(a)(2) and (c)(2)(B)(i) and (ii))

COUNT FIFTEEN

62. Paragraphs 1 through 33 are re-alleged here.

63. On or about August 20, 2013, beginning outside of the jurisdiction of any particular State or district, YIN KECHENG, during and in relation to the crime of wire fraud, in violation of Title 18, United States Code, Section 1343, as more fully set forth in Count One above, did knowingly transfer, possess, and use, without lawful authority, a means of identification of another person, namely, B.B., an employee of Victim A.

(**Aggravated Identity Theft,** in violation of Title 18, United States Code, Sections 1028A(a)(1), 1028A(b), 1028A(c)(4), (5))

COUNT SIXTEEN

64. Paragraphs 1 through 33 are re-alleged here.

65. On or about September 27, 2013, beginning outside of the jurisdiction of any particular State or district, and later within the District of Columbia and elsewhere, YIN KECHENG, during and in relation to the crime of wire fraud, in violation of Title 18, United States Code, Section 1343, and causing damage to a protected computer, in violation of Title 18, United States Code, Section 1030(a)(5)(A), as more fully set forth in Counts Two and Nine above, did knowingly transfer, possess, and use, without lawful authority, a means of identification of another person, namely, L.V., an employee of Victim B.

(**Aggravated Identity Theft,** in violation of Title 18, United States Code, Sections 1028A(a)(1), 1028A(b), 1028A(c)(4), (5))

COUNT SEVENTEEN

66. Paragraphs 1 through 33 are re-alleged here.

67. On or about July 10, 2014, beginning outside of the jurisdiction of any particular State or district, YIN KECHENG, during and in relation to the crime of wire fraud, in violation of Title 18, United States Code, Section 1343, causing damage to a protected computer, in violation of Title 18, United States Code, Section 1030(a)(5)(A), and unauthorized access to a protected computer, in violation of Title 18, United States Code, Section 1030(a)(2), as more fully set forth in Counts Three, Four, Six, Ten, and Thirteen above, did knowingly transfer, possess, and use,

without lawful authority, a means of identification of another person, namely, S.D., an employee of Victim C.

(**Aggravated Identity Theft,** in violation of Title 18, United States Code, Sections 1028A(a)(1), 1028A(b), 1028A(c)(4), (5))

COUNT EIGHTEEN

68. Paragraphs 1 through 33 are re-alleged here.

69. On or about March 18, 2015, beginning outside of the jurisdiction of any particular State or district, YIN KECHENG, during and in relation to the crime of wire fraud, in violation of Title 18, United States Code, Section 1343, causing damage to a protected computer, in violation of Title 18, United States Code, Section 1030(a)(5)(A), and unauthorized access to a protected computer, in violation of Title 18, United States Code, Section 1030(a)(2), as more fully set forth in Counts Six, Ten, and Thirteen above, did knowingly transfer, possess, and use, without lawful authority, a means of identification of another person, namely, T.F., an employee of Victim C.

(**Aggravated Identity Theft,** in violation of Title 18, United States Code, Sections 1028A(a)(1), 1028A(b), 1028A(c)(4), (5))

COUNT NINETEEN

70. Paragraphs 1 through 33 are re-alleged here.

71. On or about April 21, 2015, beginning outside of the jurisdiction of any particular State or district, and later within the District of Columbia and elsewhere, YIN KECHENG, during and in relation to the crime of wire fraud, in violation of Title 18, United States Code, Section 1343, as more fully set forth in Count Seven above, did knowingly transfer, possess, and use,

without lawful authority, a means of identification of another person, namely, A.C., an employee of Victim D.

(**Aggravated Identity Theft,** in violation of Title 18, United States Code, Sections 1028A(a)(1), 1028A(b), 1028A(c)(4), (5))

FORFEITURE ALLEGATION

1. Upon conviction of any of the offenses alleged in Count One through Count Eight, the defendant shall forfeit to the United States any property, real or personal, which constitutes or is derived from proceeds traceable to these offenses, pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c). The United States will also seek a forfeiture money judgment against the defendant equal to the value of any property, real or personal, which constitutes or is derived from proceeds traceable to these offenses.

2. Upon conviction of any of the offenses alleged in Count Nine through Count Fourteen, the defendant shall forfeit to the United States any property constituting, or derived from, proceeds that the defendant obtained directly or indirectly, as the result of these offenses, pursuant to 18 U.S.C. § 982(a)(2)(B). The United States will also seek a forfeiture money judgment against the defendant equal to the value of any property constituting, or derived from, proceeds that the defendant obtained directly or indirectly, as the result of these offenses.

3. Upon conviction of any of the offenses alleged in Count Nine through Count Fourteen, the defendant shall forfeit to the United States: (a) the defendant's interest in any personal property that was used or intended to be used to commit or to facilitate the commission of these offenses; (b) any property, real or personal, constituting or derived from, any proceeds the defendant obtained, directly or indirectly, as a result of these offenses; (c) any personal property

used or intended to be used to commit or to facilitate the commission of these offenses; and (d) any property, real or personal, which constitutes or is derived from proceeds traceable to any violation of these offenses pursuant to 18 U.S.C. §§ 1030(i) and (j).

4. If any of the property described above as being subject to forfeiture, as a result of any act or omission of the defendant:

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 that cannot be divided without difficulty;

the defendant shall forfeit to the United States any other property of the defendant, up to the value of the property described above, pursuant to 21 U.S.C. § 853(p).

(**Criminal Forfeiture**, pursuant to Title 18, United States Code, Section 981(a)(1)(C), Title 28, United Sates Code, Section 2461(c), Title 18, United States Code, Section 982(a)(2), Title 18, United States Code, Sections 1030(i) and (j), and Title 21, United States Code, Section 853(p)).

A TRUE BILL

_____
Foreperson

Jessie K. Liu /JPH
JESSIE LIU
UNITED STATES ATTORNEY