COPY

FILED

18 OCT 25 PM 3:09

CLERK, U.S. DISTRICT COURT
SOUTHERN DISTRICT OF CALIFORNIA

BY: DEPUTY

SEALED

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

June 2017 Grand Jury

UNITED STATES OF AMERICA,
Plaintiff,

v.

ZHANG ZHANG-GUI (1),
aka "leanov,"
aka "leaon,"
ZHA RONG (2),
CHAI MENG (3),
aka "Cobain,"
LIU CHUNLIANG (4),
aka "sxpdlcl,"
aka "Fangshou,"
GAO HONG KUN (5),
aka "mer4en7y,"
ZHUANG XIAOWEI (6),
aka "jpxxav,"
MA ZHIQI (7),
aka "Le Ma,"
LI XIAO (8),
aka "zhuan86,"
GU GEN (9),
aka "Sam Gu,"
TIAN XI (10),

Defendants.

Case No. 13CR3132-H

INDICTMENT
(Superseding)

Title 18, U.S.C., Secs. 371
1030(a)(5)(A) and 1030(c)(4)(B)(i)-
Conspiracy to Damage Protected
Computers; Title 18, U.S.C.,
Secs. 371, 1030(a)(2)(C),
1030(c)(2)(B)(i) and (iii) -
Conspiracy to Obtain Information;
Title 18, U.S.C., Secs.
1030(a)(5)(A), 1030(c)(4)(B)(i) -
Damaging Protected Computers;
Title 18, U.S.C.,
Sec. 982(a)(1) and (b)(1) -
Criminal Forfeiture

The grand jury charges:

//

cc: Pretrial / AUSA Alexandra Foster

JNP:nlv:(1)San Diego:10/25/18

6

At various times relevant to this indictment:

INTRODUCTION

1. The Jiangsu Province Ministry of State Security ("JSSD") was a provincial foreign intelligence arm of the People's Republic of China's Ministry of State Security ("MSS"), headquartered in Nanjing, China. The MSS, and by extension the JSSD, was primarily responsible for domestic counter-intelligence, non-military foreign intelligence, and aspects of political and domestic security. From January 2010 to May 2015, JSSD employees, along with individuals working at the direction of the JSSD, conspired to steal sensitive commercial technological, aviation, and aerospace data by hacking into computers in the United States and abroad.

2. Supervising and managing officers at JSSD, including defendants ZHA RONG, CHAI MENG, aka "Cobain," and others, directed hackers, including ZHANG ZHANG-GUI, aka "leanov," aka "leaon," LIU CHUNLIANG, aka "sxpdlcl," "Fangshou," GAO HONG KUN, aka "mer4en7y," ZHUANG XIAOWEI, aka "jpxxav," and MA ZHIQI, aka "Le Ma," as well as victim company insiders, including GU GEN, aka "Sam Gu," and TIAN XI, to hack into or facilitate intrusions into computers of companies based in the United States and abroad for the purpose of gaining and maintaining unauthorized access to those computers, stealing information, and using the computers to facilitate additional computer intrusions.

3. Members of the conspiracy targeted, among other things, companies in the aerospace and other high-technology industries, and attempted to steal intellectual property and confidential business information, including information that was commercial in nature.

//

//

4. Members of the conspiracy included, but were not limited to:

a. ZHA RONG (查荣 STC[1] 2686/2837), a Division Director in the JSSD who supervised and directed human intelligence and other activities directed towards the theft of intellectual property and confidential business information conducted by one or more members of the conspiracy. Among other things, ZHA RONG oversaw the intrusion into Company I and received updates from one or more members of the conspiracy on the day of the intrusion.

b. CHAI MENG, aka "Cobain," (**柴萌** STC 2693/5492), a JSSD Section Chief who supervised and directed human intelligence and other activities directed towards the theft of intellectual property and confidential business information conducted by one or more members of the conspiracy. Among other things, CHAI MENG served as a point of contact to coordinate the activities of hacker LIU CHUNLIANG, as well as the activities of victim company insiders, during the intrusion into Company I.

c. ZHANG ZHANG-GUI, aka "leanov," aka "leaon," (张长贵 STC 1728/7022/6311), a computer hacker who operated at the direction of the JSSD. Among other things, ZHANG ZHANG-GUI tested spear phishing messages and established and maintained infrastructure used in multiple intrusions. In addition, as described in detail herein, *infra*, ZHANG

[1] STC is the Standard Telegraphic Code for Chinese, Japanese, and Korean characters.

coordinated hacking activities and shared infrastructure with fellow hacker LIU.

d. LIU CHUNLIANG, aka "sxpdlcl," "Fangshou," (**刘春亮** STC 0491/2504/0081), a computer hacker who operated at the direction of the JSSD, and coordinated the activities of other computer hackers and malware developers, including GAO HONG KUN, aka "mer4en7y," ZHUANG XIAOWEI, aka "jpxxav," MA ZHIQI, aka "Le Ma," and an identified unindicted co-conspirator ("UCC-1"). Among other things, LIU established, maintained and paid for infrastructure used in multiple intrusions, deployed malware, and engaged in domain hijacking in connection with the intrusion of Company H.

e. GAO HONG KUN, aka "mer4en7y," (**高洪坤** STC 7559/3163/0981), a computer hacker who operated at the direction of LIU and was an associate of ZHANG. Among other things, GAO was involved in the computer intrusions into Capstone Turbine and Company F.

f. ZHUANG XIAOWEI, aka "jpxxav," (**庄**枭伟 STC 8369/2743/0251), a computer hacker and malware developer, who operated at the direction of LIU. Among other things, ZHUANG managed malware on Company G's systems and stole Company G's data from no earlier than September 26, 2014, through May 7, 2015.

g. MA ZHIQI, aka "Le Ma," (马志琪 STC 7456/1807/3825), a computer hacker who operated at the direction of LIU and was a personal acquaintance of LIU and UCC-1. Among other things, on February 19, 2013, one or more members of the conspiracy hacked into a Company F server affiliated with LIU, using credentials LIU had provided to MA on December 14, 2012.

h. GU GEN, aka "Sam Gu," (顾根 STC 7357/2704), a Chinese employee of Company I, a French aerospace manufacturer with an office in Suzhou, Jiangsu province, China. GU was Company I's Information Technology ("IT") Infrastructure and Security Manager in Suzhou. Among other things, while under the direction of an identified JSSD intelligence officer ("JSSD Intelligence Officer A"), GU provided information to JSSD concerning Company I's internal investigation into the computer intrusions carried out by members of the conspiracy.

i. TIAN XI (田曦 STC 3944/2569), a Chinese employee at Company I, who worked in its Suzhou office as a Product Manager. Among other things, TIAN unlawfully installed Sakula malware on a Company I computer at the behest of JSSD Intelligence Officer A.

5. Members of the conspiracy hacked into protected computers— that is, computers used in and affecting interstate and foreign commerce and communications- operated by the following companies, among others, to steal information, including intellectual property and confidential business data, and to use these companies' computers to facilitate further computer intrusions into other companies:

a. Company A, a Massachusetts-based aerospace company,

b. Company B, an aerospace company based in the United Kingdom, with offices in Pennsylvania,

c. Company C, an aerospace company based in the United Kingdom, with offices in New York,

d. Company D, a multinational conglomerate that produces commercial and consumer products and aerospace systems,

e. Company E, a French aerospace company,

f. Company F, an Arizona-based aerospace company,

g. Company G, an Oregon-based aerospace supplier,

h. Company H, a San Diego-based technology company,

i. Company I, a French aerospace manufacturer with an office in Suzhou, Jiangsu province, China,

j. Company J, a critical infrastructure company operating in San Diego and elsewhere,

k. Company K, a Wisconsin-based aerospace company,

l. Company L, an Australian domain registrar, and

m. Capstone Turbines, a Los Angeles-based gas turbine manufacturer.

6. Members of the conspiracy targeted, among other things, data and information related to a turbofan engine used in commercial jetliners. At the time of the intrusions, a Chinese state-owned aerospace company was working to develop a comparable engine for use in commercial aircraft manufactured in China and elsewhere. The turbofan engine targeted by members of the conspiracy was being developed through a partnership between Company I and an aerospace company based in the U.S. As described herein, members of the conspiracy hacked Company I and other companies that manufactured parts for the turbofan engine, including Companies A, F, and G, to steal sensitive data from these companies that could be used by Chinese entities to build the same or

similar engine without incurring substantial research and development expenses.

Count 1

7. Paragraphs 1 to 6 are re-alleged and incorporated as if set forth in full herein.

8. From a date unknown, but no later than January 8, 2010, up to and including May 7, 2015, within the Southern District of California, and elsewhere, defendants ZHANG ZHANG-GUI, aka "leanov," aka "leaon," ZHA RONG, CHAI MENG, aka "Cobain," LIU CHUNLIANG, aka "sxpdlcl," "Fangshou," GAO HONG KUN, aka "mer4en7y," ZHUANG XIAOWEI, aka "jpxxav," MA ZHIQI, aka "Le Ma," GU GEN, aka "Sam Gu," and TIAN XI did knowingly and intentionally conspire with each other and other persons known and unknown to the grand jury to commit an offense against the United States, that is, to:

a. cause the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally cause damage without authorization to a protected computer, including loss to at least one person during a one-year period aggregating at least $5,000 in value, in violation of Title 18, United States Code, Sections 371, 1030(a)(5)(A) and 1030(c)(4)(B)(i); and

b. intentionally access computers without authorization, and thereby obtain information from at least one protected computer, such conduct having involved an interstate and foreign communication, and the offense was committed for purposes of commercial advantage and private financial gain and information valued at greater than $5,000, in violation of 18, United States Code, Sections 371, 1030(a)(2)(C) and 1030(c)(2)(B)(i) and (iii).

MANNER AND MEANS

9. Members of the conspiracy used the following manner and means, among others, to accomplish the objects of the conspiracy:

a. Certain defendants used email accounts hosted by webmail providers worldwide, including in the United States and China. The accounts often used false subscriber information. Defendants communicated using these email accounts and often encrypted their communications.

b. Certain defendants, directly and through intermediaries, attempted to hide the nature and origin of their Internet traffic and reduce the likelihood of detection by leasing servers or server space worldwide, including in the United States. Members of the conspiracy forwarded Internet traffic through multiple such servers using software to hide the true source and destination of the traffic.

c. Members of the conspiracy used a variety of computer intrusion tactics, alone or in combination, including but not limited to:

i. Spear phishing, the use of fictitious emails embedded with malicious code (malware) that facilitated access to the email recipient's computer and connected network,

ii. Malware, including but not limited to certain malware, such as Sakula and IsSpace, that was uniquely used by members of the conspiracy during the period of the conspiracy,

iii. Doppelganger Domain Names, the creation and use of domain names that closely resemble legitimate domain names to trick unwitting recipients of spear phishing emails,

iv. Dynamic Domain Name Service (DNS) Accounts, a service of DNS providers that allows users, including members of the conspiracy, to register one or more domain names under a single account and frequently change the Internet Protocol (IP) address assigned to a registered domain name.

v. Domain Hijacking, the compromise of domain registrars in which one or more members of the conspiracy redirected a victim company's domain name at a domain registrar to a malicious IP address in order to facilitate computer intrusions,

vi. Watering Hole Attacks, the installation of malware on legitimate web pages of victim companies to facilitate intrusions of computers that visited those pages, and

vii. Co-Opting Victim Company Employees, the use of insiders at victim companies to facilitate computer intrusions or monitor investigations of computer intrusion activity.

//

//

OVERT ACTS

10. In furtherance of the conspiracy and to effect the objects thereof, the following overt acts, among others, were committed within the Southern District of California and elsewhere, on or about the dates below:

Establishment of DNS Accounts and Malicious Domain Names

a. On April 26, 2011, LIU registered DNS ACCOUNT-3 and DNS ACCOUNT-4 at a DNS provider to facilitate computer intrusions. LIU paid for DNS ACCOUNT-3 and DNS ACCOUNT-4.

b. On April 26, 2011, LIU registered domain names, some of which were doppelganger domain names of hacked or targeted companies, to be used to facilitate computer intrusions.

c. On May 25, 2012, LIU registered DNS ACCOUNT-2 at a DNS provider to facilitate computer intrusions. LIU paid for DNS ACCOUNT-2.

d. On June 20, 2012, ZHANG registered DNS ACCOUNT-1 at a DNS provider to facilitate computer intrusions. LIU paid for DNS ACCOUNT-1.

e. On June 25, 2012, LIU registered domain names, some of which were doppelganger domain names of hacked or targeted companies, to be used to facilitate computer intrusions.

f. On November 20, 2014, ZHANG modified domain name records to facilitate computer intrusions.

g. On February 27, 2015, LIU modified domain name records to facilitate computer intrusions.

h. Each of the intrusions of the victim companies described herein, *infra*, at Paragraph 10, involved malware that was configured to beacon or otherwise linked to one or more of these DNS ACCOUNTS between January 2010 and May 2015.

Intrusion Into Capstone Turbine Computers

i. On January 8, 2010, members of the conspiracy infiltrated the Capstone Turbine computer network, created an email account in the Capstone Turbine email server, and tested a potential spear phishing email by sending an email from the newly-created Capstone Turbine email account to ZHANG's personal email account.

j. On May 24, 2012, a member of the conspiracy installed malware on Capstone Turbine's web server to facilitate a watering hole attack.

k. On or before May 24, 2012, a member of the conspiracy installed Winnti malware in Capstone Turbine's computer systems, and the malware, as programmed, sent "beacons" to domain names hosted by DNS ACCOUNT-1, as well as to a blog controlled by "mer4en7y," which is an alias used by GAO. Malware is designed to "beacon" in order to, among other things, notify members of the conspiracy that the malware has been successfully installed.

l. On or about May 30, 2012, a server associated with ZHANG, which was located in Nanjing, China, was used to gain unauthorized access to Capstone Turbine's web server.

m. On May 31, 2012, a member of the conspiracy used the IP address of a server associated with ZHANG to connect to the Capstone Turbine web server using a Capstone Turbine administrative account with system administrator privileges (which meant the account user had access to most areas of the Capstone Turbine network).

n. On June 1, 2012, a member of the conspiracy used the same administrative account to upload malware to Capstone Turbine’s web server for use in a watering hole attack.

o. On August 23, 2012, ZHANG tested a potential spear phishing email that used the doppelganger domain name capstonetrubine.com (emphasis added). At that time, the doppelganger domain name capstonetrubine.com was registered to DNS ACCOUNT-2.

p. On or before December 29, 2012, members of the conspiracy caused Sakula malware on Capstone Turbine’s server to send a beacon to an account under the control of one or more members of the conspiracy.

Intrusion Into Company F’s Computers

q. On May 30, 2012, a member of the conspiracy caused malware to be installed on Company F’s computer network through a spear phishing attack, which contained a link to a domain on DNS ACCOUNT-2. Company F manufactured parts for the turbofan engine developed by Company I and an aerospace company based in the U.S.

r. On June 8, 2012, a member of the conspiracy first accessed a specific Company F server (the “Compromised Company F Server”).

s. On December 14, 2012, LIU gave MA directions on how to hack into the Compromised Company F Server. LIU provided MA with LIU’s credentials to access the server and provided guidance as to how MA could package and steal data from the server to minimize detection.

t. On February 19, 2013, a member of the conspiracy accessed the Compromised Company F Server, created a compressed file of Company F's confidential data, and saved it on Company F's server, using the IP address, username, password and methodology, which LIU had provided to MA on December 14, 2012.

u. On March 18, 2013, LIU gave GAO the IP address assigned to a domain name under the control of one or more members of the conspiracy, so GAO could access the malware installed within Company F's computer network.

v. Between June 8, 2012 and May 9, 2013, LIU, GAO, MA, and other members of the conspiracy accessed Company F's server for the purpose of stealing data related to Company F's products.

Intrusion Into Company H's Computers

w. No later than August 7, 2012, a member of the conspiracy caused malware to be installed on Company H's computer network.

x. On or before August 23, 2012, a member of the conspiracy caused PlugX malware named "capstone.exe" to be installed in Company H's computer systems to send beacons to four domain names registered to DNS ACCOUNT-1, including doppelganger domain name "capstoneturbine.cechire.com."

y. On August 28, 2013, LIU sent MA a link to a news article that explained how the Syrian Electronic Army (SEA) had hacked into the computer systems of Company L, a domain registrar, in order to facilitate intrusions.

z. On December 3, 2013, members of the conspiracy used the same method as the SEA to hack into the computer systems of Company L and hijack domain names of Company H, which were hosted by Company L.

aa. On December 3, 2013, a member of the conspiracy installed Sakula malware on Company H's computer network and caused the malware to send a beacon to a doppelganger domain name under the control of one or more members of the conspiracy. Notably, the doppelganger domain name was designed to resemble the real domain of Company A, which had previously been hacked by members of the conspiracy.

bb. Between December 3, 2013, and January 15, 2014, members of the conspiracy accessed approximately 40 computer systems operated by Company H and installed a variety of malware, including Sakula, Winnti, and PlugX, to steal Company H's data.

Intrusion Into Company I's Computers

cc. In mid-November 2013, JSSD Intelligence Officer A met TIAN, an employee of Company I, at a restaurant in Suzhou, Jiangsu province, China. The turbofan engine targeted by members of the conspiracy was being developed through a partnership between Company I and an aerospace company based in the U.S.

dd. On November 27, 2013, JSSD Intelligence Officer A communicated to TIAN, in substance and in part, "I'll bring the horse [i.e., Trojan horse malware] to you tonight. Can you take the Frenchmen out to dinner tonight? I'll pretend I bump into you at the restaurant to say hello. This way we don't need to meet in Shanghai."

ee. On November 27, 2013, TIAN met JSSD Intelligence Officer A at a restaurant.

ff. In December 2013, JSSD Intelligence Officer A contacted TIAN three times and asked, in substance and in part, if TIAN had "plant[ed] the horse."

gg. On January 17, 2014, JSSD Intelligence Officer A met GU, the IT Infrastructure and Security Manager for Company I, at the same restaurant where he had previously met TIAN.

hh. JSSD Intelligence Officer A and CHAI coordinated with each other and provided same-day updates to their colleagues and superiors, including ZHA, on the targeting of and intrusion into Company I.

ii. On January 17, 2014, JSSD Intelligence Officer A informed CHAI, in substance and in part, "I just met with Xiao GU. GU said that [Company I] was warning people about a fake email from company top management. Did you guys write the email?" CHAI responded, in substance and in part, "We sent a fake email pretending to be from network management."

jj. On January 17, 2014, JSSD Intelligence Officer A informed CHAI that he told GU that CHAI's group had sent the email.

kk. On January 25, 2014, a Company I laptop computer was infected with Sakula malware through a USB drive installed by TIAN, which beaconed to a doppelganger domain name under the control of one or more members of the conspiracy during that period. Notably, this was the same doppelganger domain designed to resemble the real domain of Company A, which members of the conspiracy had used when hacking into Company H.

ll. On January 25, 2014, TIAN texted JSSD Intelligence Officer A, "The horse was planted this morning." Shortly thereafter, JSSD Intelligence Officer A texted CHAI with a message that read, in part: "I briefed ZHA about the incident in Suzhou."

mm. On February 19, 2014, a Company I computer beaconed to domain ns24.dnsdojo.com, which was then managed by DNS ACCOUNT-3. Shortly thereafter, U.S. law enforcement authorities notified French officials of the beacon activity.

nn. On February 26, 2014, JSSD Intelligence Officer A texted CHAI, "The French are asking Little GU [Company I's IT manager] to inspect the record: ns24.dnsdojo.com. Does it concern you guys?" CHAI responded, "I'll ask."

oo. Several hours after that text exchange, a member of the conspiracy logged into DNS ACCOUNT-3, an account controlled by LIU, and deleted the domain name ns24.dnsdojo.com.

Intrusion Into Company G's Computers

pp. On September 25, 2014, ZHUANG created a Google AppEngine account named "apple-qts."

qq. On September 26, 2014, members of the conspiracy caused malware to be installed on at least one Company G computer through a watering hole attack hosted on a Company I domain. Company G manufactured parts for the turbofan engine developed by Company I and an aerospace company based in the U.S.

rr. On March 28, 2015, members of the conspiracy caused a computer belonging to Company G to beacon to a domain registered to DNS ACCOUNT-4.

ss. ZHUANG used his apple-qts Google AppEngine account to manage malware, including IsSpace, on Company G's systems and steal commercial data from Company G from no earlier than September 26, 2014, through May 7, 2015.

All in violation of Title 18, United States Code, Sections 371, 1030(a)(5)(A), 1030(c)(4)(B)(i), 1030(a)(2)(C) and 1030(c)(2)(B)(i) and (iii).

Count 2

11. Paragraphs 1 to 10 are re-alleged and incorporated as if set forth in full herein.

12. From a date unknown, but no later than September 3, 2012, up to and including February 11, 2014, within the Southern District of California, and elsewhere, defendants ZHANG ZHANG-GUI, aka "leanov," aka "leaon," and LI XIAO, aka "zhuan86," did knowingly and intentionally conspire with each other and other persons known and unknown to the grand jury to commit an offense against the United States, that is, to:

a. cause the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally cause damage without authorization to a protected computer, including loss to at least one person during a one-year period aggregating at least $5,000 in value, in violation of Title 18, United States Code, Sections 371, 1030(a)(5)(A) and 1030(c)(4)(B)(i); and

b. intentionally access one and more computers without authorization, and thereby obtain information from at least one protected computer, such conduct having involved an interstate and foreign communication, and the offense was committed for purposes of commercial advantage and private financial gain and information valued greater than $5,000, in violation of 18, United States Code, Sections 371, 1030(a)(2)(C) and 1030(c)(2)(B)(i) and (iii).

13. LI XIAO, aka "zhuan86," (李潇 STC 2621/3469), is a computer hacker and a personal friend of ZHANG ZHANG-GUI, aka "leanov," aka "leaon". ZHANG supplied LI with variants of the malware that had been developed and deployed by members of the separate JSSD-related conspiracy charged in Count 1, as described herein, *supra*, at Paragraphs 7 through 10. LI subsequently used malware that had been supplied by ZHANG, as well as other malware, in his attempts to hack into Company H's computers, which ZHANG and others had also targeted in the separate conspiracy charged in Count 1.

OVERT ACTS

Intrusion Into Company H's Computers

14. In furtherance of the conspiracy and to effect the objects thereof, the following overt acts, among others, were committed within the Southern District of California and elsewhere, on or about the dates below:

//

//

a. On September 3, 2012, ZHANG emailed LI a set of malicious files, that was a subset of the malware installed on Capstone Turbine's web server on June 1, 2012, as described herein, *supra*, at Paragraph 10(n).

b. On or about October 27, 2012, LI created a Google AppEngine application to facilitate computer intrusions.

c. On September 11, 2013, a web shell or script was installed on a web server operated by Company H, which allowed a user to gain remote administrative control of Company H's server.

d. On or before September 29, 2013, a second web shell was installed on the same web server to facilitate computer intrusion activities on Company H's server.

e. On or about September 29, 2013, LI used the Google AppEngine application to access the second shell on Company H's server. LI did so in order to leverage the hack of Company H's server into intrusions of other victims.

f. On or about October 10, 2013, LI attempted to use one of the shells to gain access to a third-party website.

g. On or about February 11, 2014, LI installed malicious code on a Company H server to exploit an Internet Explorer vulnerability, which had previously been used by ZHANG and other members of the conspiracy described herein, *supra*, at Paragraphs 7 through 10.

All in violation of Title 18, United States Code, Sections 371, 1030(a)(5)(A), 1030(c)(4)(B)(i), 1030(a)(2)(C) and 1030(c)(2)(B)(i) and (iii).

Count 3

15. From no later than August 7, 2012, up to and including January 14, 2014, within the Southern District of California and elsewhere, defendant ZHANG ZHANG-GUI, aka "leanov," aka "leaon," knowingly caused the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally caused damage without authorization to a protected computer, and the loss caused by such behavior was at least $5,000, to wit, ZHANG accessed without authorization computer servers in the Southern District of California belonging to Company H and thereby caused loss of at least $5,000; in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and (c)(4)(B)(i).

Criminal Forfeiture

16. Upon conviction of the offenses alleged in this indictment, defendants shall forfeit to the United States of America, pursuant to Title 18, United States Code, Section 982(a)(1), any property, real and personal, involved in such offenses, and any property traceable to such property.

17. In the event that any of the property described above, 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, the United States of America shall be entitled to forfeit substitute property pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 982(b)(1).

All in violation of Title 18, United States Code, Sections 982(a)(1) and (b)(1).

DATED: October 25, 2018.

A TRUE BILL:

Foreperson

ADAM L. BRAVERMAN
United States Attorney

By:
TIMOTHY F. SAXEL
Assistant U.S. Attorney