IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

FILED IN OPEN COURT

AUG 18 2020

CLERK, U.S. DISTRICT COURT
DISTRICT OF COLUMBIA

Holding a Criminal Term
Grand Jury Sworn in on May 7, 2019

UNITED STATES OF AMERICA	:	CRIMINAL NO.
	:	
v.	:	GRAND JURY ORIGINAL
	:	
WONG ONG HUA,	:	VIOLATIONS:
	:	18 U.S.C. § 1962(c)
and	:	(Racketeering)
	:	
LING YANG CHING,	:	18 U.S.C. § 1962(d)
	:	(Racketeering Conspiracy)
Defendants.	:	
	:	18 U.S.C. § 1028(a)(7)
	:	(Identity Theft)
	:	
	:	18 U.S.C. § 1028A
	:	(Aggravated Identity Theft)
	:	
	:	18 U.S.C. § 1029(a)(2)
	:	(Access Device Fraud)
	:	
	:	18 U.S.C. § 1030(a)(2), (c)(2)(B)
	:	(Obtaining Information By Unauthorized
	:	Access To Protected Computers)
	:	
	:	18 U.S.C. § 1030(a)(4), (c)(3)(A)
	:	(Furthering Fraud By Unauthorized
	:	Access To Protected Computers)
	:	
	:	18 U.S.C. § 1030(a)(5)(A), (c)(4)(B)
	:	(Intentionally Causing Damage To
	:	Protected Computers)
	:	
	:	18 U.S.C. § 1956(a)(2)(A)
	:	(Money Laundering)
	:	
	:	18 U.S.C. § 2
	:	Aiding and Abetting
	:	
	:	18 U.S.C. § 3559(g)(1)
	:	False Registration Of A Domain Name

Case: 1:20-cr-00166
Assigned To : Mehta, Amit P.
Assign. Date : 8/18/2020
Description: INDICTMENT (B)
Case related to 19-cr-274 and 20-cr-158 (APM)

: **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).**

INDICTMENT

The Grand Jury charges:

At all times relevant to this Indictment:

INTRODUCTION

1. Defendant WONG ONG HUA ("WONG") was a resident and citizen of Malaysia, who had no residence or last known residence in the United States.

2. Defendant LING YANG CHING ("LING") was a resident and citizen of Malaysia, who had no residence or last known residence in the United States.

3. WONG was the founder and Chief Executive Officer of SEA Gamer Mall SDN BHD ("SEA GAMER"), a privately-owned company registered and located in Malaysia.

4. LING was the Chief Product Officer and a shareholder of SEA GAMER.

5. SEA GAMER operated an internet-based platform for the sale of digital goods and services related to video games, including in-game currency and other video game-related digital goods. SEA GAMER sold digital goods through its website located at seagm.com. In addition to those direct sales, seagm.com also included a link to kaleoz.com, a platform known as Kaleoz, which ostensibly allowed "peer to peer" sales among third party customers.

6. SEA GAMER had customers in the United States and elsewhere, sold digital goods related to video games played and operated in the United States and elsewhere, and conducted business with commercial payment providers, commercial electronic communications providers, and commercial remote computing providers in the United States and elsewhere.

7. Tan Dailin ("Tan"), also known as 谭戴林, was a resident of the People's Republic of China ("PRC") with no known residence or past residence in the United States. Tan was a sophisticated and advanced computer hacker.

8. Zhang Haoran ("Zhang"), also known as 张浩然, was a resident of the PRC with no known residence or past residence in the United States. Zhang was a sophisticated and advanced computer hacker.

9. Between at least June 2014 and December 2018, WONG and LING, together with others known and unknown to the Grand Jury, including Tan and Zhang, participated in a criminal scheme to profit from the sale of illegally obtained digital goods related to video games; to illegally obtain those digital goods by means of fraud, computer hacking, identity theft, and promotional money laundering; and to sell those illegally-obtained digital goods through SEA GAMER, its website, its employees, and other agents working under its direction.

10. As part of and in furtherance of the scheme, WONG and LING worked with computer hackers who were not SEA GAMER employees ("computer hackers"), including but not limited to Tan and Zhang, to illegally obtain digital goods related to video games. In exchange for payments from WONG and SEA GAMER, the computer hackers obtained unauthorized access to video game company networks, including through identity theft, fraud, and money laundering, and used their unauthorized access to help SEA GAMER obtain digital goods. WONG and LING, together with other SEA GAMER agents and employees, generated profit for the scheme by selling the illegally obtained digital goods through SEA GAMER agents and employees.

11. WONG and LING executed the scheme, in part, through SEA GAMER employees and agents, using SEA GAMER accounts and resources, and by conducting SEA GAMER affairs

through a pattern of illegal activity, including by illegally obtaining digital goods for sale through SEA GAMER employees and agents and using SEA GAMER resources.

12. WONG and LING, together with others known and unknown to the Grand Jury, including the computer hackers, worked to obtain "illegal goods," as one computer hacker called them, by targeting video game companies in the United States and around the world, including the companies referred to here as VICTIM ONE through VICTIM NINE.

13. VICTIM ONE was a United States-based video game company which operated protected computers in California and elsewhere. VICTIM ONE operated a video game referred to here as ALPHA. VICTIM C-1 was an employee of VICTIM ONE.

14. VICTIM TWO was a United States-based video game company which operated protected computers in California and elsewhere.

15. VICTIM THREE was a video game company based in France, which operated protected computers in France and elsewhere. VICTIM THREE operated a video game referred to here as BETA.

16. VICTIM FOUR was a South Korea-based video game company with protected computers affiliates in South Korea, the United States and elsewhere. VICTIM FOUR was the parent company of VICTIM FOUR-A and VICTIM FOUR-B. VICTIM FOUR-A was a United States-based video game company which operated protected computers in Washington, Illinois, and elsewhere. VICTIM FOUR-B was a South Korea-based company with operations and protected computers in South Korea, the United States, and elsewhere. VICTIM FOUR, together with affiliated companies, including VICTIM FOUR-A and VICTIM FOUR-B, operated video games referred to here as GAMMA and DELTA. VICTIM C-2 and VICTIM C-3 were employees of VICTIM FOUR.

17. VICTIM FIVE was a video game company based in the South Korea, which operated protected computers in South Korea, the United States, and elsewhere. VICTIM FIVE operated a video game referred to here as ZETA.

18. VICTIM SIX was a video game company which was headquartered in Japan, and which operated protected computers in Japan, the United States, and elsewhere.

19. VICTIM SEVEN was a United States-based video game company, which operated protected computers in New York and elsewhere.

20. VICTIM EIGHT was a United States-based video game company, which operated protected computers in California and elsewhere.

21. VICTIM NINE was a video game company based in Singapore. VICTIM NINE distributed software which was used by other companies and individuals, including VICTIM EIGHT.

COUNT ONE
(Racketeer Influenced and Corrupt Organization ("RICO") Conspiracy)

22. Paragraphs 1 to 21 are re-alleged here.

The Enterprise

23. SEA GAMER (the "Enterprise") constituted an enterprise as defined in 18 U.S.C. § 1961(4), that is, a legal entity, which was engaged in, and the activities of which affected, interstate and foreign commerce.

24. The purposes of the Enterprise included generating money for its owners, shareholders, officers, employees, agents, and associates. This purpose was implemented by officers, employees, agents, and associates of the Enterprise through commercial activity, which

included the commission of various criminal acts, including identity theft, wire fraud, money laundering, computer fraud and abuse, and various forms of computer intrusions.

The Racketeering Conspiracy

25. Beginning no later than about June 2014 and continuing at least until December 2018, and beginning outside of the jurisdiction of any particular State or district and, pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, WONG ONG HUA and LING YANG CHING, being persons employed by and associated with SEA GAMER, an Enterprise which engaged in, and the activities of which affected, interstate and foreign commerce, knowingly and intentionally conspired, together and with others known and unknown to the Grand Jury, to violate 18 U.S.C. § 1962(c), that is, to conduct, and participate, directly and indirectly, in the conduct of, the affairs of said Enterprise through a pattern of racketeering activity, as defined in 18 U.S.C. §§ 1961(1) and (5), consisting of multiple acts indictable under the following provisions of federal law:

a. 18 U.S.C. § 1028 (relating to fraud and related activity in connection with identification documents);

b. 18 U.S.C. § 1029 (relating to fraud and related activity in connection with access devices);

c. 18 U.S.C. § 1030(a)(5)(A) (relating to protection of computers);

d. 18 U.S.C. § 1343 (relating to wire fraud); and

e. 18 U.S.C. § 1956 (relating to the laundering of monetary instruments).

26. It was a part of the conspiracy that each defendant agreed that a conspirator would commit at least two acts of racketeering activity in the conduct of the affairs of the Enterprise.

Manner and Means of the Racketeering Conspiracy

Overview

27. WONG and LING worked with one another and with others known and unknown to the Grand Jury, such as Tan and Zhang, to conduct the affairs of SEA GAMER by illegally obtaining and generating digital goods related to video games, so that WONG and LING, working with other SEA GAMER agents and employees, could sell those illegally obtained goods for a profit.

28. The scheme depended on illegal and fraudulent conduct by each participant. WONG, LING, and SEA GAMER agents and employees fraudulently registered game playing accounts for the purpose of receiving the illegally obtained digital goods. Computer hackers gained unauthorized access into video game company computer networks, including through sophisticated malware, fraudulent spear-phishing e-mails, identity theft, and fraudulently modified software. WONG and LING worked with the computer hackers to fraudulently obtain and generate digital goods in game playing accounts controlled by WONG, LING, and other SEA GAMER agents and employees. WONG, LING, and other SEA GAMER agents and employees then worked together, in coordination with the computer hackers, to sell those illegally obtained digital goods through SEA GAMER platforms.

Game Player Accounts

29. WONG, LING, and other SEA GAMER agents and employees fraudulently obtained and controlled game player accounts for the targeted video games. Those game player accounts were used to receive or generate illegal digital goods. WONG, LING, and other SEA GAMER agents and employees obtained those game player accounts for commercial use, that is, for the purpose of illegally obtaining and selling digital goods for profit. WONG, LING, and other

SEA GAMER agents and employees obtained those game player accounts by creating hundreds and thousands of separate e-mail accounts, by using proxy services which provided access to numerous IP addresses, and by fraudulently providing false identification information to video game companies in order to register game player accounts.

Computer Hacking

30. The computer hackers gained unauthorized access to victim company computer networks through sophisticated and evolving hacking techniques, malware, and computer infrastructure. The computer hackers used tradecraft such as spear-phishing e-mails with attached malware that communicated with the malicious domain names, servers, and other hacking infrastructure, including malicious web pages. Their tradecraft also included more sophisticated methods, including stolen software signing certificates which fraudulently asserted that malware was legitimate software authored by legitimate companies, as well as "supply chain attacks," through which the hackers victimized software development companies and then fraudulently modified those companies' software to include malicious code, thereby enabling the computer hackers to compromise the companies' customers.

31. The computer hackers' tradecraft typically included obtaining means of identification and access devices, including login credentials, belonging to individuals with administrative access to victim computer networks, and then using those login credentials to expand their unauthorized access to those networks.

32. The computer hackers used their unauthorized access to victim company networks in order to access video game databases and to fraudulently modify database entries (that is, to modify records concerning game player accounts controlled by SEA GAMER participants, for example, by fraudulently increasing the in-game currency or other digital goods in the accounts),

and to otherwise fraudulently generate, and to allow WONG, LING and SEA GAMER agents and employees to fraudulently generate, digital goods related to video games.

33. In some cases, the computer hackers also used their unauthorized network access to take action against other unrelated groups that were similarly engaged in the illegal generation of digital goods, thereby attempting to eliminate the criminal competition.

Successfully Selling Illegally Obtained Goods

34. WONG, LING, and other participants, including the computer hackers, profited from the sale, by SEA GAMER and its agents and employees, of the illegally obtained goods to third-party customers.

35. SEA GAMER had no legitimate means of selling the illegally obtained digital goods. Many victim video game companies explicitly prohibited the sale of digital goods associated with their platforms (except through specified platforms operated by the companies themselves), and many companies employed corporate fraud detection personnel tasked with identifying and terminating accounts involved in the sale of digital goods. Thus, in order to successfully sell their illegally obtained goods, the participants in the scheme worked to avoid detection, developing specific procedures for the purchase and sale of their illegally obtained goods.

36. The computer hackers supported those efforts by using their unauthorized network access to monitor the victim companies' fraud detection personnel. For example, the computer hackers identified the methods or formulas used by the corporate fraud detection authorities, and, working with WONG and LING, used that information to develop specific sales procedures. In a further attempt to avoid detection, the computer hackers also used their access to fraudulently

modify records concerning game player accounts used by SEA GAMER, for example, by fraudulently changing records of the IP addresses associated with particular game player accounts.

37. The participants in the scheme also hoped to avoid detection by working internationally, targeting video game companies and computer servers in countries outside Malaysia and the PRC, based on an apparent belief that law enforcement would be unable to investigate "across national borders." As WONG explained on one occasion, "It is definitely illegal. So we do it overseas."

Infrastructure for the Computer Hacking

38. The computer hacking operations supporting the scheme required the type of internet infrastructure that is typically required for such operations: e-mail accounts to send spear-phishing e-mails, communicate with other participants, and obtain additional resources; command-and-control computer servers (or "C2 Servers") to control malware installed on victim computers; and command-and-control domain names (or "C2 Domains") and web pages which covertly facilitated communication between C2 servers and malware ("C2 Dead Drops").

39. In addition to infrastructure obtained in Malaysia, the PRC, and elsewhere, the participants in the scheme used a number of C2 Servers located in the United States, registered domain names (to be used as C2 Domains) through providers in the United States, and obtained e-mail and social media accounts from providers in the United States, including accounts to host C2 Dead Drops.

40. The participants in the scheme typically obtained e-mail and social media accounts without any payment. They also typically obtained servers and domain names from commercial providers, and typically paid for such servers and domains using funds which originated outside the United States, which were then paid to providers in the United States. Those payments were

necessary to the scheme because they provided access to infrastructure that was necessary to execute the computer hacking.

41. For example, HOP POINT ONE was a server located in California, which was leased from a provider located in California. The participants in the scheme used HOP POINT ONE as a C2 Server to carry out computer intrusion activity. In order to maintain their use of HOP POINT ONE, the participants in the scheme caused monthly payments to be sent to the California-based provider. Those payments originated outside the United States and were paid to the provider in the United States.

42. Similarly, HOP POINT TWO was a server located in New York, which was leased from a provider located in New York. HOP POINT TWO was used as a C2 Server to carry out computer intrusion activity. In order to obtain their use of HOP POINT TWO, the participants in the scheme paid the New York-based provider. That payment originated outside the United States and was paid to the provider in the United States.

43. As a final example, operatingbox.com, which the conspirators used as a C2 Domain, was registered through an Arizona-based provider. In order to maintain their use of operatingbox.com, the participants in the scheme caused payment to the Arizona-based provider. That payment originated outside the United States and was paid to the provider in the United States.

Overt Acts

44. In furtherance of the conspiracy, and to achieve the object and purposes thereof, beginning outside of the jurisdiction of any particular State or district and, pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, the defendants WONG and LING, together with others known and

unknown to the Grand Jury, performed and caused to be performed the following overt acts, among others:

a. On or about May 8, 2014, an account used by the conspirators was used to register a player account with VICTIM ONE, for an ALPHA game.

b. On or about June 16, 2014, fraudulent spear-phishing e-mails were sent to about fourteen employees of VICTIM ONE. The spear-phishing e-mails were fraudulently written as if they had been sent by a former employee of VICTIM TWO who had attached his resume as part of a job search. In fact, the "resume" contained malware. The spear-phishing e-mails led to the installation of malware on a protected computer owned by VICTIM ONE. The installation of that malware provided unauthorized access to numerous computers owned by VICTIM ONE.

c. Between about June 2014 and about April 2015, that unauthorized access was used to obtain information from protected computers owned by VICTIM ONE. That information included login credentials belonging to numerous employees of VICTIM ONE. Those credentials were used to obtain additional unauthorized access to protected computers owned by VICTIM ONE.

d. Between about January 2015 and about March 2015, in connection with the VICTIM ONE game ALPHA, SEA GAMER paid "3,779,440" in unlisted currency to bank accounts in the names of Zhang and his wife.

e. On or about February 24, 2015, in connection with the VICTIM ONE game ALPHA, money was transferred into a bank account held at a bank in the PRC in the name of Zhang.

f. On or about March 4, 2015, in connection with the VICTIM ONE game ALPHA, money was transferred into a bank account held at a bank in the PRC in the name of Zhang's wife.

g. In or about March 2015, in connection with the VICTIM ONE game ALPHA, VICTIM ONE databases were fraudulently modified, to increase account balances on accounts related to ALPHA.

h. On or about November 26, 2014, malware was installed on protected computers at VICTIM TWO, including malware that provided unauthorized access to, and information from, protected computers belonging to VICTIM TWO.

i. On or about November 26, 2014, LING joined a Facebook Group titled, "[VICTIM TWO GAME] Black Market," a Facebook Group which members used to illicitly market digital goods related to a VICTIM TWO game.

j. On or about December 9, 2014, malware installed on protected computers at VICTIM TWO caused said computers to communicate, by means of interstate wire communications between Texas and California.

k. On or about May 14, 2015, the domain name operatingbox.com was registered with DOMAIN REGISTRAR ONE, a domain registrar located in Arizona.

l. On or about May 14, 2015, as payment for the registration of operatingbox.com, ¥192.39, then worth approximately $1.61, was transmitted, transported, and transferred from outside of the United States to DOMAIN REGISTRAR ONE in the United States.

m. On or about May 19, 2015, spear-phishing e-mails were sent to employees of more than ten video game-related companies, including employees of VICTIM TWO.

n. On or about October 11, 2015, ELECTRONIC ACCOUNT ONE was registered with a provider in the United States.

o. On or about October 11, 2015, ELECTRONIC ACCOUNT ONE was used to register an account with VICTIM ONE. Thereafter, the account was used in connection with ALPHA.

p. On or about March 17, 2016, HOP POINT ONE and a computer belonging to VICTIM ONE engaged in electronic and wire communications with one another, which caused a protected computer owned by VICTIM ONE to transmit information to HOP POINT ONE.

q. On or about March 24, 2016, a computer hacker sent a file containing IP addresses and other information concerning VICTIM THREE computer servers to WONG.

r. On or about March 30, 2016, and continuing until about August 9, 2016, the conspirators caused HOP POINT ONE, in California, to engage in communication with IP addresses owned by VICTIM THREE, in France, which caused a protected computer owned by VICTIM THREE to transmit information to HOP POINT ONE.

s. On or about May 23, 2016, ELECTRONIC ACCOUNT ONE received an e-mail from VICTIM ONE. The e-mail contained a security code which could

be used to access the VICTIM ONE account associated with ELECTRONIC ACCOUNT ONE.

t. On or about June 22, 2016, $362.85 was transmitted, transported, and transferred from outside of the United States into the United States, as payment for the continued lease of HOP POINT ONE.

u. On or about July 25, 2016, HOP POINT ONE, in California, engaged in electronic and wire communications with a computer belonging to VICTIM ONE, which was also located in California, which caused a protected computer belonging to VICTIM ONE to transmit information to HOP POINT ONE.

v. On or about August 14, 2016, HOP POINT ONE, in California, engaged in electronic and wire communications with a computer belonging to VICTIM ONE, which was also located in California, which caused a protected computer belonging to VICTIM ONE to transmit information to HOP POINT ONE.

w. On or about August 20, 2016, WONG sent Visa gift card information to a computer hacker. The Visa gift cards were issued in the United States.

x. On or about February 27, 2017, and beginning prior to that date, a software signing certificate belonging to VICTIM FOUR-A was stolen and fraudulently appended to malware which was installed on VICTIM FOUR-A computers, and which was used for purposes of a computer intrusion, or attempted computer intrusions, at VICTIM FOUR, VICTIM FOUR-A, and at VICTIM SIX between February 27, 2017, and July 20, 2017.

y. On or about February 27, 2017, WONG sent a file containing IP addresses and other information concerning VICTIM FOUR and VICTIM FOUR-A game servers to a computer hacker.

z. On or about February 27, 2017, malware was installed on a protected computer belonging to VICTIM FOUR-A. The malware was configured to, and did, communicate with a subdomain of operatingbox.com as its C2 Domain, thereby sending the C2 Server information from protected computers belonging to VICTIM FOUR-A.

aa. On or about March 9, 2017, an access device, that is, a means of access belonging to VICTIM FOUR, was used to gain unauthorized access to a protected computer used by VICTIM SIX.

bb. In or about April 2017, means of identification, that is, usernames that provided computer access, belonging to VICTIMS C-2 and C-3, were used to attempt communications between a C2 Server in Texas and protected computers belonging to VICTIM FOUR.

cc. On July 29, 2017, a computer hacker advised WONG that he was finished with his work on the ZETA game in South Asia, noted that "Southeast Asia projects don't seem to have very encouraging revenue," and asked WONG to recommend "some better quality ones." WONG suggested targeting "US/Europe," as well as the game referred to here as BETA.

dd. On July 29, 2017, a computer hacker advised WONG, "[ALPHA] is okay too, we have privileges." WONG recommended waiting to exploit ALPHA until

after VICTIM ONE released the following year's version of ALPHA, because "currency value is high early on."

ee. On or about August 10, 2017, ELECTRONIC ACCOUNT FOUR was used to register a game player account with VICTIM SIX.

ff. On or about August 17, 2017, ELECTRONIC ACCOUNT TWO and ELECTRONIC ACCOUNT THREE were registered with a U.S. provider.

gg. On or about August 18, 2017, LING registered ELECTRONIC ACCOUNT FIVE with a U.S. provider.

hh. On or about August 18, 2017, LING began using ELECTRONIC ACCOUNT FIVE to communicate with a computer hacker about the operation of the scheme.

ii. On or about October 19, 2017, WONG discussed with a computer hacker a refund request from a customer whose accounts were "shut down" by a video game company after the customer purchased illegally obtained digital goods from SEA GAMER, through its agents or employees.

jj. On or about November 22, 2017, a computer hacker asked WONG to help him re-register operatingbox.com, which had recently expired. WONG responded that he would be unable to re-register the domain because it had been registered by somebody else, as of November 15, 2017.

kk. On or about February 18, 2018, WONG discussed with a computer hacker possible international travel for the purpose of obtaining a private bank account in which to deposit the proceeds of the conspiracy. The computer hacker

expressed fear that "the Americans are after me" and that the Americans "have stuff on us."

ll. On or about February 22, 2018, WONG urged a computer hacker to work on "[GAMMA] in Thailand."

mm. On or about February 23, 2018, WONG and LING discussed with a computer hacker the procedures that should be used to facilitate the sale of digital goods, while avoiding detection by the relevant victim video game company.

nn. On or about February 24, 2018, LING discussed those same procedures with a SEA GAMER employee and instructed the SEA GAMER employee to follow those procedures to avoid detection by the video game company.

oo. On or about March 11, 2018, WONG and a computer hacker discussed whether they were the only group with "illegal goods" in one particular part of ZETA.

pp. Beginning on or about August 4, 2018, HOP POINT TWO was leased from a cloud computing provider located in New York. HOP POINT TWO was used as a C2 server.

qq. On or about August 4, 2018, in order to obtain HOP POINT TWO, $5.00 was paid to the cloud computing provider located in New York. The payment was transmitted, transported, and transferred from outside of the United States into the United States.

rr. On or about August 14, 2018, the domain name gxxservice.com was registered using DOMAIN REGISTRAR TWO, which is based in California.

ss. On or about November 16, 2018, VICTIM EIGHT installed what appeared to be legitimate software on one of its internet-connected computers in California. VICTIM EIGHT obtained the software from VICTIM NINE. Unbeknownst to VICTIM EIGHT, as a means of a supply chain attack, computer hackers had earlier fraudulently modified the software installed by VICTIM EIGHT, such that it included malicious code within the otherwise-legitimate software package.

tt. Shortly after installation, the malicious code caused VICTIM EIGHT's computer to engage in wire communications with a subdomain of gxxservice.com, which then directed VICTIM EIGHT's computer to contact HOP POINT TWO, and which caused a protected computer belonging to VICTIM EIGHT to transmit information to HOP POINT TWO.

(**Racketeering Conspiracy**, in violation of Title 18, United States Code, Sections 1962(d))

COUNT TWO
(Racketeering in Violation of 18 U.S.C. § 1962(c))

45. Paragraphs 1 to 21 are re-alleged here.

The Enterprise

46. Paragraphs 23 to 24 are re-alleged here.

Manner and Means of the Racketeering

47. Paragraphs 27 to 43 are re-alleged here.

The Racketeering Violation

48. Between at least June 2014 and December 2018, and beginning outside of the jurisdiction of any particular State or district, and, pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, WONG

ONG HUA and LING YANG CHING, together with others known and unknown to the Grand Jury, being persons employed by and associated with the SEA GAMER Enterprise described above, which Enterprise was engaged in and the activities of which affected interstate and foreign commerce, did knowingly and unlawfully conduct and participate, directly and indirectly, in the conduct of the affairs of said Enterprise, through a pattern of racketeering activity, as that term is defined in Title 18, United States Code, Sections 1961(1) and 1961(5), through the commission of the racketeering acts set forth below.

The Pattern of Racketeering Activity

49. The pattern of racketeering activity as defined in Title 18, United States Code, Sections 1961(1) and 1961(5), consisted of:

Racketeering Act One
Intrusion Related to Victim One

50. WONG ONG HUA and LING YANG CHING, together with others known and unknown to the Grand Jury, committed the following acts, any one of which alone constitutes the commission of Racketeering Act One:

a. On or about June 16, 2014, and beginning outside of the jurisdiction of any particular State or district and, pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, WONG ONG HUA and LING YANG CHING, together with others known and unknown to the Grand Jury, knowingly attempted to cause, and did cause, the transmission of a program, information, code, and command, and, as a result of such conduct, attempted to cause, and did intentionally cause, damage without authorization to protected computers belonging to VICTIM

ONE, and the offense caused or, if completed would have caused, damage affecting 10 or more protected computers during a one-year period.

(**Intentional Damage to a Protected Computer**, in violation of Title 18, United States Code, Sections 1030(a)(5)(A), (b), and 2)

b. Between about June 2014 and April 2015, and beginning outside of the jurisdiction of any particular State or district and, pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, WONG ONG HUA and LING YANG CHING, together with others known and unknown to the Grand Jury, did knowingly and with intent to defraud, and in a manner affecting interstate and foreign commerce by the use of interstate and foreign wire transmissions use one or more unauthorized access devices, that is, login credentials, including a username, for access to protected computers operated by VICTIM ONE, and by such conduct, between June 14, 2014, and June 13, 2015, in a period of less than one year, attempted to obtain and did obtain anything of value aggregating $1,000 or more.

(**Access Device Fraud**, in violation of Title 18, United States Code, Sections 1029(a)(2), (b), and 2)

c. Between about June 2014 and April 2015, and beginning outside of the jurisdiction of any particular State or district and, pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, WONG ONG HUA and LING YANG CHING, together with others known and unknown to the Grand Jury, did knowingly possess and use, and attempt to possess and use, in a manner affecting interstate commerce, without lawful authority, a means of identification of another

person, that is, login credentials, including a username, which provided VICTIM C-1 access to protected computers, knowing that the means of identification belonged to another actual person, with the intent to commit, and to aid and abet, and in connection with, unlawful activity that constitutes a violation of Federal law, that is, wire fraud, in violation of Title 18, United States Code, Section 1343, and access device fraud, in violation of Title 18, United States Code, Section 1029(a)(2).

(**Identity Theft**, in violation of Title 18, United States Code, Sections 1028(a)(7), (f), and 2)

Racketeering Act Two
Intrusion Related to Victim Two

51. WONG ONG HUA and LING YANG CHING, together with others known and unknown to the Grand Jury, committed the following acts, any one of which alone constitutes the commission of Racketeering Act Two:

a. On or about November 26, 2014, and beginning outside of the jurisdiction of any particular State or district and, pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, WONG ONG HUA and LING YANG CHING, together with others known and unknown to the Grand Jury, knowingly attempted to cause, and did cause, the transmission of a program, information, code, and command, and, as a result of such conduct, attempted to cause, and did intentionally cause, damage without authorization to protected computers belonging to VICTIM TWO, and the offense caused or, if completed would

have caused, damage affecting 10 or more protected computers during a one-year period.

(**Intentional Damage to a Protected Computer**, in violation of Title 18, United States Code, Sections 1030(a)(5)(A), (b), and 2)

b. On or about December 9, 2014, and beginning outside of the jurisdiction of any particular State or district and, pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, and with intent to defraud, having knowingly devised and intended to devise a scheme and artifice to defraud, and in order to obtain money and property, to wit, information and digital goods, by means of materially false and fraudulent pretenses, representations, and promises, as set forth in Paragraphs 1 to 21 and 27 to 43, WONG ONG HUA and LING YANG CHING, together with others known and unknown to the Grand Jury, for the purpose of executing the scheme and artifice to defraud, did transmit and cause to be transmitted, by means of wire communications in interstate and foreign commerce between the Texas and California, writings, signs, and signals, that is, communications exchanging electronic information between a server in California and a protected computer owned by VICTIM TWO.

(**Wire Fraud**, in violation of Title 18, United States Code, Sections 1343 and 2)

c. On or about May 19, 2015, and beginning outside of the jurisdiction of any particular State or district and, pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, WONG ONG HUA and LING YANG CHING, together with others known and unknown to the Grand Jury, knowingly attempted to cause, and did

cause, the transmission of a program, information, code, and command, and, as a result of such conduct, attempted to cause damage without authorization to protected computers belonging to VICTIM TWO, and, if completed, the offense would have caused damage affecting 10 or more protected computers during a one-year period.

(**Attempted Intentional Damage to a Protected Computer**, in violation of Title 18, United States Code, Sections 1030(a)(5)(A), (b), and 2)

Racketeering Act Three
Intrusion Related to Victim Three

52. WONG ONG HUA and LING YANG CHING, together with others known and unknown to the Grand Jury, committed the following acts, any one of which alone constitutes the commission of Racketeering Act Three:

a. On or about March 30, 2016, and beginning outside of the jurisdiction of any particular State or district and, pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, and with intent to defraud, having knowingly devised and intended to devise a scheme and artifice to defraud, and in order to obtain money and property, to wit, information and digital goods, by means of materially false and fraudulent pretenses, representations, and promises, as set forth in Paragraphs 1 to 21 and 27 to 43, WONG ONG HUA and LING YANG CHING, together with others known and unknown to the Grand Jury, for the purpose of executing the scheme and artifice to defraud, did transmit and cause to be transmitted, by means of wire communications in interstate and foreign commerce between the State of California and France, writings, signs, and signals, that is,

communications exchanging electronic information between HOP POINT ONE and a protected computer owned by VICTIM THREE.

(**Wire Fraud**, in violation of Title 18, United States Code, Sections 1343 and 2)

b. On or about August 9, 2016, and beginning outside of the jurisdiction of any particular State or district and, pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, and with intent to defraud, having knowingly devised and intended to devise a scheme and artifice to defraud, and in order to obtain money and property, to wit, information and digital goods, by means of materially false and fraudulent pretenses, representations, and promises, as set forth in Paragraphs 1 to 21 and 27 to 43, WONG ONG HUA and LING YANG CHING, together with others known and unknown to the Grand Jury, for the purpose of executing the scheme and artifice to defraud, did transmit and cause to be transmitted, by means of wire communications in interstate and foreign commerce between the State of California and France, writings, signs, and signals, that is, communications exchanging electronic information between HOP POINT ONE and a protected computer owned by VICTIM THREE.

(**Wire Fraud**, in violation of Title 18, United States Code, Sections 1343 and 2)

Racketeering Act Four
Intrusion Related to Gamma

53. WONG ONG HUA and LING YANG CHING, together with others known and unknown to the Grand Jury, committed the following acts, any one of which alone constitutes the commission of Racketeering Act Four:

a. On or about February 27, 2017, and beginning outside of the jurisdiction of any particular State or district and, pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, WONG ONG HUA and LING YANG CHING, together with others known and unknown to the Grand Jury, knowingly attempted to cause, and did cause, the transmission of a program, information, code, and command, and, as a result of such conduct, attempted to cause, and did intentionally cause, damage without authorization to protected computers belonging to VICTIM FOUR-A, and the offense caused or, if completed would have caused, damage affecting 10 or more protected computers during a one-year period.

(**Intentional Damage to a Protected Computer**, in violation of Title 18, United States Code, Sections 1030(a)(5)(A), (b), and 2)

b. In about March 2017, and beginning outside of the jurisdiction of any particular State or district and, pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, WONG ONG HUA and LING YANG CHING, together with others known and unknown to the Grand Jury, did knowingly and with intent to defraud, and in a manner affecting interstate and foreign commerce by the use of interstate and foreign wire transmissions, use one or more unauthorized access devices, that is, login credentials, including a username, for access to protected computers operated by VICTIM FOUR, and by such conduct, between January 1, 2017, and December 31, 2017, in a period of less than one year, attempted to obtain and did obtain anything of value aggregating $1,000 or more.

(**Access Device Fraud**, in violation of Title 18, United States Code, Sections 1029(a)(2), (b), and 2)

c. In or about March 2017, and beginning outside of the jurisdiction of any particular State or district and, pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, WONG ONG HUA and LING YANG CHING, together with others known and unknown to the Grand Jury, did knowingly possess and use, and attempt to possess and use, in a manner affecting interstate commerce, without lawful authority, a means of identification of another person, that is, login credentials, including a username, which provided VICTIM C-2 access to protected computers, knowing that the means of identification belonged to another actual person, with the intent to commit, and to aid and abet, and in connection with, unlawful activity that constitutes a violation of Federal law, that is, wire fraud, in violation of Title 18, United States Code, Section 1343, and access device fraud, in violation of Title 18, United States Code, Section 1029(a)(2).

(**Identity Theft**, in violation of Title 18, United States Code, Sections 1028(a)(7), (b), and 2)

Racketeering Act Five
Intrusion Related to Delta

54. WONG ONG HUA and LING YANG CHING, together with others known and unknown to the Grand Jury, committed the following acts, any one of which alone constitutes the commission of Racketeering Act Five:

a. On or about September 29, 2017, and beginning outside of the jurisdiction of any particular State or district and, pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the

District of Columbia, WONG ONG HUA and LING YANG CHING, together with others known and unknown to the Grand Jury, knowingly attempted to cause, and did cause, the transmission of a program, information, code, and command, and, as a result of such conduct, attempted to intentionally cause damage without authorization to protected computers operated by VICTIM FOUR-B and used in connection with DELTA, and the offense, if completed, would have caused loss to one or more persons during one-year period from a related course of conduct affecting protected computers aggregating at least $5,000 in value, and, if completed, the offense would have caused damage affecting 10 or more protected computers during a one-year period.

(**Intentional Damage to a Protected Computer**, in violation of Title 18, United States Code, Sections 1030(a)(5)(A), (b), and 2)

b. On or about October 4, 2017, and beginning outside of the jurisdiction of any particular State or district and, pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, WONG ONG HUA and LING YANG CHING, together with others known and unknown to the Grand Jury, knowingly attempted to cause, and did cause, the transmission of a program, information, code, and command, and, as a result of such conduct, attempted to intentionally cause damage without authorization to protected computers used in connection with VICTIM FOUR-B and DELTA, and the offense, if completed, would have caused loss to one or more persons during one-year period from a related course of conduct affecting protected computers aggregating at least $5,000 in value, and, if completed, the

offense would have caused damage affecting 10 or more protected computers during a one-year period.

(**Attempted Intentional Damage to a Protected Computer**, in violation of Title 18, United States Code, Sections 1030(a)(5)(A), (b), and 2)

c. On or about December 25, 2017, and beginning outside of the jurisdiction of any particular State or district and, pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, WONG ONG HUA and LING YANG CHING, together with others known and unknown to the Grand Jury, knowingly attempted to cause, and did cause, the transmission of a program, information, code, and command, and, as a result of such conduct, attempted to intentionally cause damage without authorization to protected computers used in connection with VICTIM FOUR-B and DELTA, and the offense, if completed, would have caused loss to one or more persons during one-year period from a related course of conduct affecting protected computers aggregating at least $5,000 in value, and, if completed, the offense would have caused damage affecting 10 or more protected computers during a one-year period.

(**Attempted Intentional Damage to a Protected Computer**, in violation of Title 18, United States Code, Sections 1030(a)(5)(A), (b), and 2)

Racketeering Act Six
Intrusion Related to Victim Eight

55. WONG ONG HUA and LING YANG CHING, together with others known and unknown to the Grand Jury, committed the following acts, any one of which alone constitutes the commission of Racketeering Act Six:

a. On or about November 16, 2018, and beginning outside of the jurisdiction of any particular State or district and, pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, WONG ONG HUA and LING YANG CHING, together with others known and unknown to the Grand Jury, knowingly attempted to cause, and did cause, the transmission of a program, information, code, and command, and, as a result of such conduct, attempted to cause, and intentionally did cause, damage without authorization to protected computers belonging to VICTIM EIGHT, and the offense caused or, if completed would have caused, damage affecting 10 or more protected computers during a one-year period.

(**Intentional Damage to a Protected Computer**, in violation of Title 18, United States Code, Sections 1030(a)(5)(A), (b), and 2)

b. On or about November 16, 2018, and beginning outside of the jurisdiction of any particular State or district and, pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, and with intent to defraud, having knowingly devised and intended to devise a scheme and artifice to defraud, and in order to obtain money and property, to wit, information and digital goods, by means of materially false and fraudulent pretenses, representations, and promises, as set forth in Paragraphs 1 to 21 and 27 to 43, WONG ONG HUA and LING YANG CHING, together with others known and unknown to the Grand Jury, for the purpose of executing the scheme and artifice to defraud, did transmit and cause to be transmitted, by means of wire communications in interstate and foreign commerce between the State of California and the State of New York, writings,

signs, and signals, that is, communications exchanging electronic information between a protected computer belonging to VICTIM EIGHT and HOP POINT TWO.

(**Wire Fraud**, in violation of Title 18, United States Code, Sections 1343 and 2)

Racketeering Act Seven
Acquisition and Use of Property to Promote Computer Hacking

56. WONG ONG HUA and LING YANG CHING, together with others known and unknown to the Grand Jury, committed the following acts, any one of which alone constitutes the commission of Racketeering Act Seven:

a. On or about May 14, 2015, and beginning outside of the jurisdiction of any particular State or district and, pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, WONG ONG HUA and LING YANG CHING, together with others known and unknown to the Grand Jury, knowingly transported, transmitted, and transferred funds, and aided, abetted, and willfully caused, the transport, transmitting, and transfer of funds, that is, a ¥192.39 payment (then worth approximately $1.61) for the registration of operatingbox.com, to a place in the United States from and through a place outside the United States, with the intent to promote the carrying on of specified unlawful activity, that is, intentionally damaging, and obtaining information by unauthorized access to, protected computers, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and 1030(a)(2), identity theft, in violation of United States Code, Section

1028(a)(7), and wire fraud, in violation of Title 18, United States Code, Section 1343.

(**Money Laundering**, in violation of Title 18, United States Code, Sections 1956(a)(2)(A) and 2)

b. On or about March 23, 2016, and beginning outside of the jurisdiction of any particular State or district and, pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, WONG ONG HUA and LING YANG CHING, together with others known and unknown to the Grand Jury, knowingly transported, transmitted, and transferred funds, and aided, abetted, and willfully caused, the transport, transmitting, and transfer of funds, that is, a $362.85 payment for the lease of HOP POINT ONE, to a place in the United States from and through a place outside the United States, with the intent to promote the carrying on of specified unlawful activity, that is, intentionally damaging, and obtaining information by unauthorized access to, protected computers, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and 1030(a)(2), identity theft, in violation of United States Code, Section 1028(a)(7), and wire fraud, in violation of Title 18, United States Code, Section 1343.

(**Money Laundering**, in violation of Title 18, United States Code, Sections 1956(a)(2)(A) and 2)

c. On or about June 22, 2016, and beginning outside of the jurisdiction of any particular State or district and, pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, WONG ONG HUA and LING YANG CHING, together with others known and unknown to the Grand Jury, knowingly transported, transmitted, and

transferred funds, and aided, abetted, and willfully caused, the transport, transmitting, and transfer of funds, that is, a $362.85 payment for the lease of HOP POINT ONE, to a place in the United States from and through a place outside the United States, with the intent to promote the carrying on of specified unlawful activity, that is, intentionally damaging, and obtaining information by unauthorized access to, protected computers, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and 1030(a)(2), identity theft, in violation of United States Code, Section 1028(a)(7), and wire fraud, in violation of Title 18, United States Code, Section 1343.

(**Money Laundering**, in violation of Title 18, United States Code, Sections 1956(a)(2)(A) and 2)

d. On or about August 4, 2018, and beginning outside of the jurisdiction of any particular State or district and, pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, WONG ONG HUA and LING YANG CHING, together with others known and unknown to the Grand Jury, knowingly transported, transmitted, and transferred funds, and aided, abetted and willfully caused, the transport, transmitting, and transfer of funds, that is, a $5.00 payment for the lease of HOP POINT TWO, to a place in the United States from and through a place outside the United States, with the intent to promote the carrying on of specified unlawful activity, that is, intentionally damaging, and obtaining information by unauthorized access to, protected computers, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and 1030(a)(2), identity theft, in violation

of United States Code, Section 1028(a)(7), and wire fraud, in violation of Title 18, United States Code, Section 1343.

(**Money Laundering**, in violation of Title 18, United States Code, Sections 1956(a)(2)(A) and 2)

(**Racketeering**, in violation of Title 18, United States Code, Sections 1962(c) and 2)

COUNT THREE
(Money Laundering)

57. Paragraphs 1 to 21 are re-alleged here.

58. On or about May 14, 2015, and beginning outside of the jurisdiction of any particular State or district and, pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, WONG ONG HUA and LING YANG CHING, together with others known and unknown to the Grand Jury, knowingly transported, transmitted, and transferred funds, and aided, abetted and willfully caused, the transport, transmitting, and transfer of funds, that is, a ¥192.39 payment (then worth approximately $1.61) for the registration of operatingbox.com, to a place in the United States from and through a place outside the United States, with the intent to promote the carrying on of specified unlawful activity, that is, intentionally damaging, and obtaining information by unauthorized access to, protected computers, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and 1030(a)(2), and identity theft, in violation of United States Code, Section 1028(a)(7).

(**Money Laundering**, in violation of Title 18, United States Code, Sections 1956(a)(2)(A) and 2)

COUNT FOUR
(Furthering Fraud by Unauthorized Access to a Protected Computer)

59. Paragraphs 1 to 21 are re-alleged here.

60. In about March 2015, and beginning outside of the jurisdiction of any particular State or district and, pursuant to Title 18, United States Code, Section 3238, within the venue of

the United States District Court for the District of Columbia, WONG ONG HUA and LING YANG CHING, together with others known and unknown to the Grand Jury, knowingly and with intent to defraud, accessed a protected computer without authorization, that is, a protected computer belonging to VICTIM ONE, and aided and abetted the same, and by means of such conduct, furthered the intended fraud and obtained something of value, specifically, digital goods.

(Furthering Fraud by Unauthorized Access to a Protected Computer, in violation of Title 18, United States Code, Sections 1030(a)(4), (b), (c)(3)(A), and 2)

COUNT FIVE
(Access Device Fraud)

61. Paragraphs 1 to 21 are re-alleged here.

62. In about March 2015, and beginning outside of the jurisdiction of any particular State or district and, pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, WONG ONG HUA and LING YANG CHING, together with others known and unknown to the Grand Jury, did knowingly and with intent to defraud, and in a manner affecting interstate and foreign commerce by the use of interstate and foreign wire transmissions, use one or more unauthorized access devices, that is, login credentials, including a username, for access to protected computers operated by VICTIM ONE, and aided and abetted the same, and by such conduct, between June 14, 2014, and June 13, 2015, in a period of less than one year, attempted to obtain and did obtain anything of value aggregating $1,000 or more.

(Access Device Fraud, in violation of Title 18, United States Code, Sections 1029(a)(2), (b), and (c)(1)(A)(i) and (2))

COUNT SIX
(Identity Theft)

63. Paragraphs 1 to 21 are re-alleged here.

64. In about March 2015, and beginning outside of the jurisdiction of any particular State or district and, pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, WONG ONG HUA and LING YANG CHING, together with others known and unknown to the Grand Jury, did knowingly possess and use, and attempt to possess and use, in a manner affecting interstate commerce, without lawful authority, a means of identification of another person, that is, login credentials, which provided VICTIM C-1 access to protected computers, and aided and abetted the same, knowing that the means of identification belonged to another actual person, with the intent to commit, and to aid and abet, and in connection with, unlawful activity that constitutes a violation of Federal law, that is, wire fraud, in violation of Title 18, United States Code, Section 1343, and access device fraud, in violation of Title 18, United States Code, Section 1029(a)(2).

(**Identity Theft,** in violation of Title 18, United States Code, Sections 1028(a)(7) and (b)(2)(B))

COUNT SEVEN
(Obtaining Information by Unauthorized Access to a Protected Computer)

65. Paragraphs 1 to 21 are re-alleged here.

66. On or about March 30, 2016, and beginning outside of the jurisdiction of any particular State or district and, pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, and 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, that is, wire fraud, in violation of Title 18, United States Code, Section 1343, WONG ONG HUA and LING YANG CHING, together with others known and unknown to the Grand Jury, attempted to intentionally access, and did intentionally access, a protected computer without authorization, and aided and abetted the

same, and thereby obtained, and attempted to obtain, information from a protected computer belonging to VICTIM THREE.

(**Obtaining Information by Unauthorized Access to a Protected Computer,** in violation of Title 18, United States Code, Sections 1030(a)(2)(C), (b), and (c)(2)(B)(i) and (ii) and 2)

COUNT EIGHT
(Furthering Fraud by Unauthorized Access to a Protected Computer)

67. Paragraphs 1 to 21 are re-alleged here.

68. On or about March 30, 2016, and beginning outside of the jurisdiction of any particular State or district and, pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, WONG ONG HUA and LING YANG CHING, together with others known and unknown to the Grand Jury, knowingly and with intent to defraud, accessed a protected computer without authorization, that is, a protected computer belonging to VICTIM THREE, and aided and abetted the same, and by means of such conduct, attempted to further the intended fraud and obtain something of value, specifically, digital goods, in violation of 18 U.S.C. §§ 1030(a)(4), (b), and (c)(3)(A).

(**Furthering Fraud by Unauthorized Access to a Protected Computer**, in violation of Title 18, United States Code, Sections 1030(a)(4), (b), (c)(3)(A), and 2)

COUNT NINE
(Money Laundering)

69. Paragraphs 1 to 21 are re-alleged here.

70. On or about June 22, 2016, and beginning outside of the jurisdiction of any particular State or district and, pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, WONG ONG HUA and LING YANG CHING, together with others known and unknown to the Grand Jury, knowingly transported, transmitted, and transferred funds, and aided, abetted and willfully caused, the

transport, transmitting, and transfer of funds, that is, a $362.85 payment for the lease of HOP POINT ONE, to a place in the United States from and through a place outside the United States, with the intent to promote the carrying on of specified unlawful activity, that is, intentionally damaging, and obtaining information by unauthorized access to, protected computers, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and 1030(a)(2), and identity theft, in violation of United States Code, Section 1028(a)(7).

(**Money Laundering**, in violation of Title 18, United States Code, Sections 1956(a)(2)(A) and 2)

COUNT TEN
(Obtaining Information by Unauthorized Access to a Protected Computer)

71. Paragraphs 1 to 21 are re-alleged here.

72. On or about July 25, 2016, and beginning outside of the jurisdiction of any particular State or district and, pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, and 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, that is, wire fraud, in violation of Title 18, United States Code, Section 1343, WONG ONG HUA and LING YANG CHING, together with others known and unknown to the Grand Jury, attempted to intentionally access, and did intentionally access, a protected computer without authorization, and aided and abetted the same, and thereby obtained, and attempted to obtain, information from a protected computer belonging to VICTIM ONE.

(**Obtaining Information by Unauthorized Access to a Protected Computer,** in violation of Title 18, United States Code, Sections 1030(a)(2)(C), (b), and (c)(2)(B)(i) and (ii) and 2)

COUNT ELEVEN
(Obtaining Information by Unauthorized Access to a Protected Computer)

73. Paragraphs 1 to 21 are re-alleged here.

74. On or about August 14, 2016, and beginning outside of the jurisdiction of any particular State or district and, pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, and 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, that is, wire fraud, in violation of Title 18, United States Code, Section 1343, WONG ONG HUA and LING YANG CHING, together with others known and unknown to the Grand Jury, attempted to intentionally access, and did intentionally access, a protected computer without authorization, and aided and abetted the same, and thereby obtained, and attempted to obtain, information from a protected computer belonging to VICTIM ONE.

(**Obtaining Information by Unauthorized Access to a Protected Computer,** in violation of Title 18, United States Code, Sections 1030(a)(2)(C), (b), and (c)(2)(B)(i) and (ii) and 2)

COUNT TWELVE
(Furthering Fraud by Unauthorized Access to a Protected Computer)

75. Paragraphs 1 to 21 are re-alleged here.

76. On or about August 14, 2016, and beginning outside of the jurisdiction of any particular State or district and, pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, WONG ONG HUA and LING YANG CHING, together with others known and unknown to the Grand Jury, knowingly and with intent to defraud, accessed a protected computer without authorization, that is, a protected computer belonging to VICTIM ONE, and aided and abetted the same, and by means of such

conduct, attempted to further the intended fraud and obtain something of value, specifically, digital goods, in violation of 18 U.S.C. §§ 1030(a)(4), (b), and (c)(3)(A).

(Furthering Fraud by Unauthorized Access to a Protected Computer, in violation of Title 18, United States Code, Sections 1030(a)(4), (b), (c)(3)(A), and 2)

COUNT THIRTEEN
(Attempted Intentional Damage to a Protected Computer)

77. Paragraphs 1 to 21 are re-alleged here.

78. On or about October 17, 2016, and beginning outside of the jurisdiction of any particular State or district and, pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, WONG ONG HUA and LING YANG CHING, together with others known and unknown to the Grand Jury, knowingly attempted to cause, and did cause, the transmission of a program, information, code, and command, and, as a result of such conduct, attempted to intentionally cause damage without authorization to protected computers belonging to VICTIM SEVEN, and aided and abetted the same, and the offense, if completed, would have caused loss to one or more persons during one-year period from a related course of conduct affecting protected computers aggregating at least $5,000 in value, and, if completed, the offense would have caused damage affecting 10 or more protected computers during a one-year period.

(Attempted Intentional Damage to a Protected Computer, in violation of Title 18, United States Code, Sections 1030(a)(5)(A), (b), and (c)(4)(B) and 2)

COUNT FOURTEEN
(Intentional Damage to a Protected Computer)

79. Paragraphs 1 to 21 are re-alleged here.

80. On or about February 27, 2017, and beginning outside of the jurisdiction of any particular State or district and, pursuant to Title 18, United States Code, Section 3238, within the

venue of the United States District Court for the District of Columbia, WONG ONG HUA and LING YANG CHING, together with others known and unknown to the Grand Jury, knowingly attempted to cause, and did cause, the transmission of a program, information, code, and command, and, as a result of such conduct, attempted to cause, and intentionally did cause, damage without authorization to protected computers operated by VICTIM FOUR-A, and aided and abetted the same, and the offense caused, or if completed would have caused, loss to one or more persons during one-year period from a related course of conduct affecting protected computers aggregating at least $5,000 in value, and the offense caused, or if completed would have caused, damage affecting 10 or more protected computers during a one-year period.

(Intentional Damage to a Protected Computer, in violation of Title 18, United States Code, Sections 1030(a)(5)(A), (b), and (c)(4)(B) and 2)

COUNT FIFTEEN
(Obtaining Information by Unauthorized Access to a Protected Computer)

81. Paragraphs 1 to 21 are re-alleged here.

82. On or about February 27, 2017, and beginning outside of the jurisdiction of any particular State or district and, pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, and 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, that is, wire fraud, in violation of Title 18, United States Code, Section 1343, WONG ONG HUA and LING YANG CHING, together with others known and unknown to the Grand Jury, attempted to intentionally access, and did intentionally access, a protected computer without authorization, and aided and abetted the

same, and thereby obtained information, and attempted to obtain information, from a protected computer belonging to VICTIM FOUR-A.

(**Obtaining Information by Unauthorized Access to a Protected Computer,** in violation of Title 18, United States Code, Sections 1030(a)(2)(C), (b), and (c)(2)(B)(i) and (ii) and 2)

COUNT SIXTEEN
(Furthering Fraud by Unauthorized Access to a Protected Computer)

83. Paragraphs 1 to 21 are re-alleged here.

84. On or about February 27, 2017, and beginning outside of the jurisdiction of any particular State or district and, pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, WONG ONG HUA and LING YANG CHING, together with others known and unknown to the Grand Jury, knowingly and with intent to defraud, accessed a protected computer without authorization, that is, a protected computer belonging to VICTIM FOUR-A, and aided and abetted the same, and by means of such conduct, attempted to further the intended fraud and obtain something of value, specifically, digital goods, in violation of 18 U.S.C. §§ 1030(a)(4), (b), and (c)(3)(A).

(**Furthering Fraud by Unauthorized Access to a Protected Computer**, in violation of Title 18, United States Code, Sections 1030(a)(4), (b), (c)(3)(A), and 2)

COUNT SEVENTEEN
(Access Device Fraud)

85. Paragraphs 1 to 21 are re-alleged here.

86. In about March 2017, and beginning outside of the jurisdiction of any particular State or district and, pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, WONG ONG HUA and LING YANG CHING, together with others known and unknown to the Grand Jury, did knowingly and with intent to defraud, and in a manner affecting interstate and foreign commerce by the use of

interstate and foreign wire transmissions, use one or more unauthorized access devices, that is, login credentials, including a username, for access to protected computers operated by VICTIM FOUR and VICTIM FOUR-A, and aided and abetted the same, and by such conduct, between January 1, 2017, and December 31, 2017, in a period of less than one year, attempted to obtain and did obtain anything of value aggregating $1,000 or more.

(**Access Device Fraud**, in violation of Title 18, United States Code, Sections 1029(a)(2) and (c)(1)(A)(i) and (2))

COUNT EIGHTEEN
(Identity Theft)

87. Paragraphs 1 to 21 are re-alleged here.

88. In or about March 2017, and beginning outside of the jurisdiction of any particular State or district and, pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, WONG ONG HUA and LING YANG CHING, together with others known and unknown to the Grand Jury, did knowingly possess and use, and attempt to possess and use, in a manner affecting interstate commerce, without lawful authority, a means of identification of another person, that is, login credentials, including a username, which provided VICTIM C-2 access to protected computers, and aided and abetted the same, knowing that the means of identification belonged to another actual person, with the intent to commit, and to aid and abet, and in connection with, unlawful activity that constitutes a violation of Federal law, that is, wire fraud, in violation of Title 18, United States Code, Section 1343, and access device fraud, in violation of Title 18, United States Code, Section 1029(a)(2).

(Identity Theft, in violation of Title 18, United States Code, Sections 1028(a)(7) and (b)(2)(B))

COUNT NINETEEN
(Aggravated Identity Theft)

89. Paragraphs 1 to 21 are re-alleged here.

90. In or about March 2017, and beginning outside of the jurisdiction of any particular State or district and, pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, WONG ONG HUA and LING YANG CHING, together with others known and unknown to the Grand Jury, during and in relation to the crime of wire fraud, in violation of Title 18, United States Code, Section 1343, and the crime of obtaining information by unauthorized access to a protected computer, in violation of Title 18, United States Code, Section 1030(a)(2), did knowingly transfer, possess, and use, without lawful authority, a means of identification of another person, that is, VICTIM C-3, an employee of VICTIM FOUR, and aided and abetted the same.

(Aggravated Identity Theft, in violation of Title 18, United States Code, Sections 1028A(a)(1), 1028A(b), 1028A(c)(4), (5) and 2)

COUNT TWENTY
(Money Laundering)

91. Paragraphs 1 to 21 are re-alleged here.

92. On or about August 4, 2018, and beginning outside of the jurisdiction of any particular State or district and, pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, WONG ONG HUA and LING YANG CHING, together with others known and unknown to the Grand Jury, knowingly transported, transmitted, and transferred funds, and aided, abetted and willfully caused, the transport, transmitting, and transfer of funds, that is, a $5.00 payment for the lease of HOP POINT TWO, to a place in the United States from and through a place outside the United States, with the intent to promote the carrying on of specified unlawful activity, that is, intentionally damaging,

and obtaining information by unauthorized access to, protected computers, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and 1030(a)(2), and identity theft, in violation of United States Code, Section 1028(a)(7).

(**Money Laundering**, in violation of Title 18, United States Code, Sections 1956(a)(2)(A) and 2)

COUNT TWENTY-ONE
(Intentional Damage to a Protected Computer)

93. Paragraphs 1 to 21 are re-alleged here.

94. On or about November 16, 2018, and beginning outside of the jurisdiction of any particular State or district and, pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, WONG ONG HUA and LING YANG CHING, together with others known and unknown to the Grand Jury, knowingly attempted to cause, and did cause, the transmission of a program, information, code, and command, and, as a result of such conduct, attempted to cause, and intentionally did cause, damage without authorization to protected computers belonging to VICTIM EIGHT, and aided and abetted the same, and the offense caused, or if completed would have caused, loss to one or more persons during one-year period from a related course of conduct affecting protected computers aggregating at least $5,000 in value, and the offense caused, or if completed would have caused, damage affecting 10 or more protected computers during a one-year period.

(**Intentional Damage to a Protected Computer**, in violation of Title 18, United States Code, Sections 1030(a)(5)(A), (b), and (c)(4)(B) and 2)

COUNT TWENTY-TWO
(Obtaining Information by Unauthorized Access to a Protected Computer)

95. Paragraphs 1 to 21 are re-alleged here.

96. On or about November 16, 2018, and beginning outside of the jurisdiction of any particular State or district and, pursuant to Title 18, United States Code, Section 3238, within the

venue of the United States District Court for the District of Columbia, and 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, that is, wire fraud, in violation of Title 18, United States Code, Section 1343, WONG ONG HUA and LING YANG CHING, together with others known and unknown to the Grand Jury, attempted to intentionally access, and did intentionally access, a protected computer without authorization, and aided and abetted the same, and thereby attempted to obtain, and did obtain, information from a protected computer belonging to VICTIM EIGHT.

(**Obtaining Information by Unauthorized Access to a Protected Computer,** in violation of Title 18, United States Code, Sections 1030(a)(2)(C), (b), and (c)(2)(B)(i) and (ii) and 2)

COUNT TWENTY-THREE
(Furthering Fraud by Unauthorized Access to a Protected Computer)

97. Paragraphs 1 to 21 are re-alleged here.

98. On or about November 16, 2018, and beginning outside of the jurisdiction of any particular State or district and, pursuant to Title 18, United States Code, Section 3238, within the venue of the United States District Court for the District of Columbia, WONG ONG HUA and LING YANG CHING, together with others known and unknown to the Grand Jury, knowingly and with intent to defraud, accessed a protected computer without authorization, that is, a protected computer belonging to VICTIM EIGHT, and aided and abetted the same, and by means of such conduct, attempted to further the intended fraud and obtain something of value, specifically, digital goods, in violation of 18 U.S.C. §§ 1030(a)(4), (b), and (c)(3)(A).

(**Furthering Fraud by Unauthorized Access to a Protected Computer**, in violation of Title 18, United States Code, Sections 1030(a)(4), (b), (c)(3)(A), and 2)

FALSE REGISTRATION OF DOMAIN NAMES

99. In furtherance of the offenses alleged in Counts 1 to 3, 14 to 19, and 21 to 23, WONG ONG HUA and LING YANG CHING, together with others known and unknown to the Grand Jury, knowingly falsely registered, and willfully caused to be knowingly falsely registered, domain names, and knowingly used, or knowingly caused to be used, said domain names in the course of committing the offenses alleged in Counts 1 to 3, 14 to 19, and 21 to 23, namely, WONG ONG HUA and LING YANG CHING, together with others known and unknown to the Grand Jury, registered domains, including operatingbox.com and gxxservice.com, with false names and addresses, and used those domains in the course of committing the felony offenses charged in Counts 1 to 3, 14 to 19, and 21 to 23.

(**False Registration of a Domain Name**, in Violation of Title 18, Section 3559(g)(1))

FORFEITURE ALLEGATION

1. Upon conviction of either of the offenses alleged in Counts 1 and/or 2 of this Indictment, the defendants shall forfeit to the United States:

a) any interests the defendants acquired or maintained in violation 18 U.S.C. § 1962, which interests are subject to forfeiture to the United States pursuant to 18 U.S.C. § 1963(a)(1);

b) any interest in, security of, claim against, and/or property or contractual rights of any kind which afford a source of influence over, any enterprise which the defendants established, operated, controlled, conducted, and/or participated in the conduct of, in violation of 18 U.S.C. § 1962, which interests, securities, claims, and rights are subject to forfeiture to the United States pursuant to 18 U.S.C. § 1963(a)(2);

c) any property constituting, or derived from, any proceeds obtained, directly or indirectly, from racketeering activity, in violation of 18 U.S.C. § 1962, which property is subject to

forfeiture to the United States pursuant to 18 U.S.C. § 1963(a)(3).

The United States will also seek a forfeiture money judgment against the defendants equal to the value of this property.

2. Upon conviction of any of the offenses alleged in Counts 4, 5, 6, 7, 8, 10, 11, 12, 13, 14, 15, 16, 17, 18, 21, 22, and/or 23 of this Indictment, the defendants shall forfeit to the United States any property constituting, or derived from, proceeds that the defendants obtained directly or indirectly, as the result of these violations, pursuant to 18 U.S.C. § 982(a)(2)(B). The United States will also seek a forfeiture money judgment against the defendants equal to the value of any property constituting, or derived from, proceeds that the defendants obtained directly or indirectly, as the result of these violations.

3. Upon conviction of any of the offenses alleged in Counts 4, 5, 6, 7, 8, 10, 11, 12, 13, 14, 15, 16, 17, 18, 21, 22, and/or 23 of this Indictment, the defendants 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 violations; (b) any property, real or personal, constituting or derived from, any proceeds the defendants obtained, directly or indirectly, as a result of these violations; (c) any personal property used or intended to be used to commit or to facilitate the commission of these violations; and (d) any property, real or personal, which constitutes or is derived from proceeds traceable to these violations, pursuant to 18 U.S.C. §§ 1030(i) and (j). The United States will also seek a forfeiture money judgment against the defendants equal to the value of this property.

4. Upon conviction of any of the offenses alleged in Counts 1, 2, 4, 5, 6, 7, 8, 10, 11, 12, 13, 14, 15, 16, 17, 18, 21, 22, and/or 23 of this Indictment, the defendants 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 defendants equal to the value of any property, real or personal, which constitutes or is derived from proceeds traceable to these offenses.

5. Upon conviction of the offense alleged in Count 17 of this Indictment, the defendants shall forfeit to the United States any personal property used or intended to be used to commit this offense, pursuant to 18 U.S.C. §§ 1029(c)(1)(C). The United States will also seek a forfeiture money judgment against the defendants equal to the value of any personal property used or intended to be used to commit this offense.

6. Upon conviction of the offense alleged in Count 18 of this Indictment, the defendants shall forfeit to the United States any personal property used or intended to be used to commit this offense, pursuant to 18 U.S.C. §§ 1028(b)(5). The United States will also seek a forfeiture money judgment against the defendants equal to the value of any personal property used or intended to be used to commit this offense.

7. Upon conviction of any of the offenses alleged in Counts 3, 9 and or 20 of this Indictment, the defendants shall forfeit to the United States any property, real or personal, involved in these offenses or any property traceable to such property, pursuant to 18 U.S.C. § 982(a)(1). The United States will also seek a forfeiture money judgment against the defendants equal to the value of any property, real or personal, involved in this offense, or any property traceable to such property.

8. 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 defendants shall forfeit to the United States any other property of the defendants, up to the value of the property described above, pursuant to 21 U.S.C. § 853(p) and 18 U.S.C. § 1963(m).

(**Criminal Forfeiture**, pursuant to Title 18, United States Code, Sections 981(a)(1)(C), 982(a)(1), 982(a)(2), 1030(i) and (j), and Section 1963, Title 28, United Sates Code, Section 2461(c), and Title 21, United States Code, Section 853(p)).

A TRUE BILL

_____

Michael Sherwin /by

MICHAEL SHERWIN
ACTING UNITED STATES ATTORNEY IN AND FOR
THE DISTRICT OF COLUMBIA

U.S. District and Bankruptcy Courts
for the District of Columbia
A TRUE COPY
ANGELA D. CAESAR, Clerk
By _____
Deputy Clerk