IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

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

Case: 1:20-cr-00158
Assigned To : Mehta, Amit P.
Assign. Date : 8/11/2020
Description: INDICTMENT (B)
Case Related to 19-cr-274 (APM)

UNITED STATES OF AMERICA	:	**CRIMINAL NO.**
	:	
v.	:	**GRAND JURY ORIGINAL**
	:	
JIANG LIZHI,	:	**VIOLATIONS:**
	:	**18 U.S.C. § 1962(d)**
A/K/A 蒋立志,	:	**(Racketeering Conspiracy)**
	:	
QIAN CHUAN,	:	**18 U.S.C. § 371**
	:	**(Conspiracy)**
A/K/A 钱川,	:	
	:	**18 U.S.C. § 1028(a)(7)**
FU QIANG,	:	**(Identity Theft)**
	:	
A/K/A 付强,	:	**18 U.S.C. § 1028A**
	:	**(Aggravated Identity Theft)**
Defendants.	:	
	:	**18 U.S.C. § 1029(a)(2)**
	:	**(Access Device Fraud)**
	:	
	:	**18 U.S.C. § 1030(a)(2)(C), (b), (c)(2)(B)**
	:	**(Obtaining Information By Unauthorized**
	:	**Access To Protected Computers)**
	:	
	:	**18 U.S.C. § 1030(a)(5)(A), (b), (c)(4)(B)**
	:	**(Intentionally Causing Damage To**
	:	**Protected Computers)**
	:	
	:	**18 U.S.C. § 1030(a)(7)(C), (b), (c)(3)(A)**
	:	**(Threatening to Damage a Protected**
	:	**Computer)**
	:	
	:	**18 U.S.C. § 1956(a)(2)(A)**
	:	**(Money Laundering)**
	:	
	:	**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); 18**
	:	**U.S.C. § 1963; 28 U.S.C. § 2461(c); 21**
	:	**U.S.C § 853(p).**

INDICTMENT

The Grand Jury charges:

At all times relevant to this Indictment:

INTRODUCTION

1. Defendant JIANG LIZHI ("JIANG"), also known as "蒋立志" and "Blackfox," was a resident and citizen of the People's Republic of China ("the PRC"), who had no residence or last known residence in the United States.

2. Defendant QIAN CHUAN ("QIAN"), also known as "钱川" and "Squall," was a resident and citizen of the PRC, who had no residence or last known residence in the United States.

3. Defendant FU QIANG ("FU"), also known as "付强" and "StandNY," was a resident and citizen of the PRC, who had no residence or last known residence in the United States.

4. Since about May 2014, JIANG, QIAN, and FU have worked for, and been officers of, Chengdu 404 Network Technology Co., Ltd. ("CHENGDU 404"), a company registered in the PRC and based in Chengdu, Sichuan Province. QIAN has been President of CHENGDU 404; JIANG has been Vice President for the Technical Department; and FU has been Manager for Big Data Development.

5. CHENGDU 404 has publicly described itself as a network security company, composed of elite "white hat" hackers, which provided defensive and counter-offensive network security services and data analytics services, including penetration testing, password recovery services, "mobile device forensics," and other services. The company's website boasted about its "patriotic spirit" and claimed that its customers include "public security, military, and military enterprises." The CHENGDU 404 front desk is pictured below.

6. However, in addition to any purported "white hat" or defensive network security services which it provided, CHENGDU 404 was also responsible for "offensive" network security operations. That is to say, CHENGDU 404 employees and officers including JIANG, QIAN, and FU committed, and conspired to commit, criminal computer intrusion offenses targeting computer networks around the world, including, and as described further herein, over 100 victim companies, organizations, and individuals in the United States and around the world, including in South Korea, Japan, India, Taiwan, Hong Kong, Malaysia, Vietnam, India, Pakistan, Australia, the United Kingdom, Chile, Indonesia, Singapore, and Thailand. CHENGDU 404 employees and officers including JIANG, QIAN, and FU conspired to commit those computer intrusions, and committed those computer intrusions, by various fraudulent means, installing malware on protected computers, and obtaining, using, maintaining, and communicating with computer and internet infrastructure located in the United States or obtained from commercial providers in the United States. The CHENGDU 404 infrastructure included electronic communications accounts (*e.g.*, e-mail accounts), social media accounts, computer servers, domain names, computer software, and other items.

7. JIANG, QIAN, and FU conducted, supported, and conspired to conduct computer intrusions using CHENGDU 404 resources, and by conducting CHENGDU 404 affairs through a pattern of illegal activity, including identity theft, access device fraud, computer fraud, wire fraud, and money laundering, and related criminal activity. QIAN led these efforts as the President of CHENGDU 404, JIANG was a hacker and manager in the Technical Department, and FU was a business manager and a manager for "big data" analytics, which could be used, among other things, to analyze and exploit data obtained through hacking – and thus serve as a means of identifying additional targets, providing actionable information, and maximizing the value of stolen data.

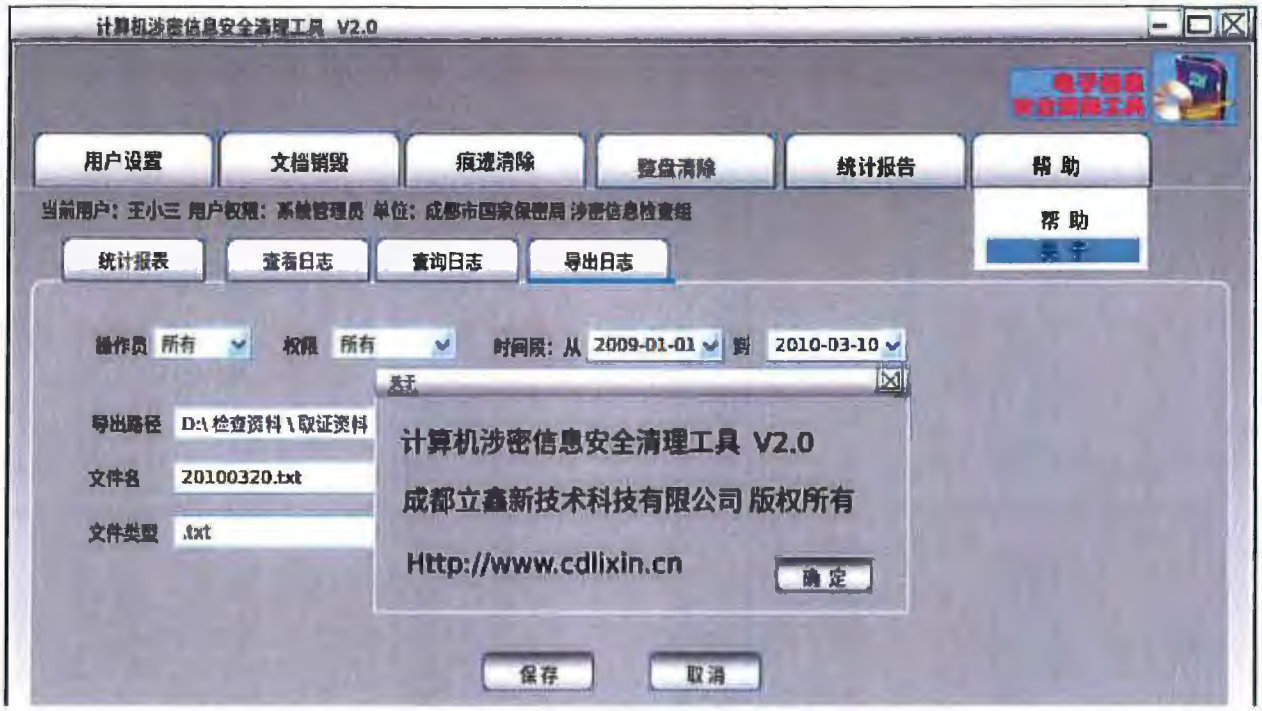
Defendants' Backgrounds

8. JIANG has been involved with professional computer hacking since at least 2007, when he worked for another PRC-based company that, between 2008 and 2010, advertised on its website that it had established an "offensive hacking group," and described some of its clients as "government agencies." JIANG worked at the company between at least 2007 and 2011. The same company employed other computer hackers who collaborated with JIANG, including Zhang Haoran, also known as 张浩然, who worked at the company between 2008 and 2014, and Tan Dailin, also known as 谭戴林, who worked at the company in at least 2011.

9. JIANG's professional history includes criminal computer hacking and collaborating with professional computer hackers such as Zhang Haoran and Tan Dailin, but including others as well. For example, in November 2012, in a discussion with another hacker, JIANG referred to criminal computer hacking as "his old business." JIANG told his associate that he had been using phishing websites and spear-phishing e-mails, and was looking to improve his computer hacking skills related to the Linux operating system. The criminal nature of JIANG's activities is likewise reflected in June 2012 communications with an associate who was also a

computer hacker, and who was concerned about "公a" ("Gong A"), which is short for 公安 ("Gong An"), the PRC Ministry of Public Security. JIANG advised his associate not to "touch domestic stuff anymore." JIANG's associate agreed, explaining that, if he were to commit such "a crime, [he] couldn't even get out of Sichuan [Province in the PRC]." JIANG boasted that he was "the classic example of maintaining low key," and claimed that he was "very close" with the "GA", meaning the PRC Ministry of State Security. JIANG and his associate agreed that JIANG's working relationship with the Ministry of State Security provided JIANG protection, because that type of association with the Ministry of State Security provided such protection, including from the Ministry of Public Security, "unless something very big happens."

10. QIAN's professional history also includes projects supporting the Chinese government. For example, in 2010, in connection with a software development project developed for the "Chengdu National Secrecy Bureau," QIAN provided an associate with a mock-up of the user-interface for software which was designed as a "Confidential Information Security Cleaning Tool" to wipe confidential information from digital media. The mock-up is pictured below:



11. Since at least 2012, JIANG and QIAN have been collaborating together. Since that time, QIAN and JIANG have conducted criminal computer hacking activity, together and with others known and unknown to the Grand Jury, which has in some instances been tracked by cybersecurity professionals under the threat group labels "APT41," "Barium," "Winnti," "Wicked Panda," and "Wicked Spider." QIAN and JIANG have also collaborated with, and used overlapping tactics, techniques, procedures, and malware with, other computer hackers, including Zhang Haoran and Tan Dailin, whose activities have been tracked under those same threat group labels. QIAN, JIANG, and those other computer hackers carried out their hacking using specialized malware, such as malware that cybersecurity experts named "PlugX/Fast," "Winnti/Pasteboy," "Shadowpad," "Barlaiy/Poison Plug," and "Crosswalk/ProxIP."

12. During 2012 and 2013, when Winnti malware was relatively new and largely unknown to cyber security researchers, QIAN communicated with and worked with other criminal computer hackers on various malicious tools, including malware controller software named

"treadstone." The "treadstone" malware controller software was designed to work with Winnti malware which, at the time, was used only by a small group of hackers – hackers such as QIAN and JIANG, and others they associated with.

13. FU has been working closely with JIANG since at least 2008, and worked with JIANG at multiple internet and video game related companies. FU has been working with QIAN and JIANG together since at least 2013. Before joining CHENGDU 404, FU described himself as a skilled programmer and developer, with expertise in developing search applications, including search applications which helped monitor and report about "internet sentiment."

OVERVIEW OF THE CONDUCT

14. Between about May 2014 and about August 2020, JIANG, QIAN, and FU, together and with others known and unknown to the Grand Jury (collectively referred to here as "the conspirators"), conspired to commit a sprawling array of computer intrusions targeting protected computers belonging to hospitality, video game, technology and telecommunications companies, research universities, non-governmental organizations, and other organizations around the world, including in the United States and the District of Columbia.

15. The conspirators used those intrusions to facilitate the theft of source code, software code signing certificates, customer account data, and personally identifiable information (or "PII"), and to carry out sophisticated "supply chain" attacks, in which a computer intrusion at one company was used to as a means of compromising protected computers belonging to its customers.

16. The conspirators also used those intrusions to facilitate other criminal schemes, including ransomware schemes and "crypto-jacking" schemes.

17. The ransomware schemes were extortion schemes, in which the conspirators gained access to protected computers, encrypted data stored on those computers, and thereby rendered that data inaccessible to those computers' owners. The conspirators would then send a ransom

demand claiming that if the victim sent a ransom payment to a designated account, the data would be decrypted.

18. The "crypto-jacking" schemes were schemes to gain unauthorized access to thousands of protected computers at a time, and then to use those compromised machines by hijacking their computing power to generate crypto-currency through a process known as "crypto-mining."

19. The underlying common goal of the conspiracy was to obtain commercial success for CHENGDU 404 – and personal financial gain for members of the conspiracy – through computer intrusions targeting protected computers.

20. The conspirators obtained initial unauthorized access to protected computers using a variety of means, including spear phishing e-mail messages, network compromises using exploit code to compromise vulnerable software, and supply chain attacks. The conspirators typically sought to convert their initial access into long-term, persistent access using several methods, including by installing, on compromised computers, sophisticated Remote Access Trojan ("RAT") malware, "webshells" which provided unauthorized access to victim networks through compromised web servers, and unauthorized Virtual Private Network ("VPN") software.

21. The conspirators used command-and-control servers ("C2 Servers") to control their malware and communicate with compromised protected computers. In some cases, they used malware that communicated with those C2 Servers by seeking contact with pre-selected domain names, which cybersecurity professionals refer to as command-and-control domains ("C2 Domains"). The conspirators also used more advanced tradecraft, including command-and-control web pages which the conspirators created using legitimate websites, and which cybersecurity professionals refer to as "C2 Dead Drops." These web pages, including "profile" pages on

legitimate websites, were surreptitiously encoded with the internet protocol ("IP") addresses of C2 Servers.

22. The conspirators' tradecraft also included other sophisticated methods, including stolen code signing certificates used to cryptographically "sign" malware, which fraudulently represented malware to be legitimate software authored by legitimate software providers. Their tradecraft also included supply chain attacks carried out using a variety of advanced techniques, including the use of encrypted malicious payloads that would only be decrypted if they were installed on computers operated by high-priority, specifically designated victims.

23. The conspirators' tradecraft typically included efforts to obtain and expand their unauthorized access by stealing means of identification and access devices, including login credentials, belonging to individuals who had administrative access to victim computer networks. The conspirators were then able to use their expanded access to accomplish the goals of the intrusion, such as the theft of data, additional supply chain attacks, ransomware attacks, or crypto-jacking schemes.

24. In or about 2019 and 2020, the conspirators also conducted a massive campaign to rapidly exploit publicly identified security vulnerabilities. This technique allowed the conspirators to hack into protected computers using publicly available exploit code – without using their own distinctive or identifying malware – so long as the conspirators acted before victim companies updated their systems. This campaign included the use of security vulnerabilities such as CVE-2019-19781, CVE-2019-11510, CVE-2019-16920, CVE-2019-16278, CVE-2019-1652/CVE-2019-1653, and CVE-2020-10189. These compromises typically resulted in the installation of widely-available RAT malware which was not uniquely used by the conspirators.

25. The conspirators executed the conspiracy using infrastructure of the type described in Paragraphs 6 and 21 in the United States, Europe, the PRC, and elsewhere in Asia and the world.

The conspirators obtained that infrastructure for purposes of their computer hacking offenses, and they obtained it using, among other things, payments from outside of the United States, which were made to providers inside the United States.

COMPUTER INTRUSION ACTIVITY

ECS #1 Supply Chain Attack

26. ECS #1 was an electronic communications services provider, which was based in Europe and which operated protected computers in Europe, the United States, and elsewhere around the world. ECS #1 developed and distributed software that was popular among individuals, businesses, and a variety of other organizations.

27. Beginning no later than June 2015, the conspirators installed malware on protected computers belonging to ECS #1 and thereby caused ECS #1 computers to communicate with HOP POINT ONE, a C2 Server in California. The conspirators maintained access to ECS #1 protected computers through at least February 2017, including through the installation and use of Winnti/Pasteboy malware.

28. Between about June 2015 and about February 2017, the conspirators compromised dozens of protected computers belonging to ECS #1. The conspirators used their unauthorized access to ECS #1 computers to view source code and code-signing certificates belonging to ECS #1, and obtained other valuable business and personal information from protected computers belonging to ECS #1, including login credentials for customer accounts provided by ECS #1.

29. The conspirators subsequently used that information to gain unauthorized access to accounts, and then the networks, of ECS #1 customers, which consisted of a broad range of organizations, including, as examples, MANUFACTURER #2 and MEDICAL PROVIDER #3.

30. MANUFACTURER #2 was a hardware manufacturer based in the United States, which operated protected computers in California and elsewhere. MANUFACTURER #2

specialized in high-end hardware for organizations in the United States and elsewhere around the world.

31. On or about January 12, 2017, the conspirators gained unauthorized access to an ECS #1 account assigned to MANUFACTURER #2. The conspirators exploited that access to compromise MANUFACTURER #2's protected computers. The conspirators installed Winnti/Pasteboy and Barlaiy/PoisonPlug malware on MANUFACTURER #2's protected computers. The conspirators carried out the intrusion, in part, through HOP POINT ONE.

32. By using this malware, the conspirators obtained information through unauthorized access to MANUFACTURER #2's protected computers. In addition, the intrusion caused damages to MANUFACTURER #2, including remediation costs, which exceeded $1,000,000.

33. MEDICAL PROVIDER #3 was a medical provider and research organization based in the United States, which maintained protected computers in the United States.

34. On or about May 3, 2018, the conspirators gained unauthorized access to an ECS #1 account assigned to MEDICAL PROVIDER #3. The conspirators exploited that access to compromise MEDICAL PROVIDER #3's protected computers, including a protected computer which MEDICAL PROVIDER #3 used for medical research. The conspirators installed Crosswalk/ProxIP malware on MEDICAL PROVIDER #3's protected computers. The conspirators carried out the intrusion, in part, through HOP POINT TWO, a C2 Server in California.

35. The conspirators used unauthorized access to accounts provided by ECS #1 in connection with other criminal schemes. The operations of those schemes were reflected in electronic communications among the conspirators, including November 13, 2017, communications between JIANG and another conspirator associated with CHENGDU 404, referred to here as "HACKER FOUR." During this conversation, JIANG and HACKER FOUR

discussed searching for computers to compromise using unauthorized access to accounts provided by ECS #1. JIANG told HACKER FOUR that it was "easy" to find companies to target by searching lists of publicly-traded companies through "stock websites." JIANG told HACKER FOUR to identify such publicly-traded companies, find their website addresses, and then "search directly" for ECS #1 accounts associated with those addresses. In one case, HACKER FOUR followed JIANG's recommendations and targeted a hotel chain headquartered in Hong Kong, as shown in Table 1.

Table 1

Sender	Recipient	Translated Content
HACKER FOUR	JIANG	You're getting addicted to playing with [ECS #1]. When I first started playing with [ECS #1] I was like that too, hahahaha.
HACKER FOUR	JIANG	Feels kind of like playing lottery.
JIANG	HACKER FOUR	Plan to gather twenty or thirty thousand machines, so there would be some income.
HACKER FOUR	JIANG	What is the other company?
HACKER FOUR	JIANG	See if other people have ones to pay.
JIANG	HACKER FOUR	A company in Malaysia, related to cars, don't know the details yet...
HACKER FOUR	JIANG	OK, I'm going to get ready and shower first.
JIANG	HACKER FOUR	I see [HOTEL COMPANY]
HACKER FOUR	JIANG	Hotel?
JIANG	HACKER FOUR	Yes...
JIANG	HACKER FOUR	Looks like there are plenty of machines...
HACKER FOUR	JIANG	That'll work.
JIANG	HACKER FOUR	I think the libraries will also be valuable...

Table 1		
Sender	**Recipient**	**Translated Content**
HACKER FOUR	JIANG	Look up check-in records.
JIANG	HACKER FOUR	Right...
HACKER FOUR	JIANG	Right.
HACKER FOUR	JIANG	Hahaha, all rich people.
JIANG	HACKER FOUR	Imagine that, sending mass blackmail emails, hahahahaha.
HACKER FOUR	JIANG	There should be quite a lot to take advantage of from this, just have to figure out how to use it.

36. In some cases, JIANG and HACKER FOUR leveraged their unauthorized access to ECS #1 accounts to compromise corporate networks containing thousands of protected computers, and then used protected computers on those networks to carry out a crypto-jacking scheme. For example, on December 6, 2017, JIANG advised HACKER FOUR that the "mining is starting to run here, a Singapore domain with over 7000 machines. The last peak number of online machines was about 1000. I think the computing power will be lowered significantly. I suppose a lot are off work now. We should get more domains to increase the computing power. Let's see how the profit is if we get a total of around 10,000 machines." In order to identify additional targets, JIANG advised HACKER FOUR that "France and Italy are pretty good, lots of well-known corporations, and mostly not in IT . . . Just search for well-known French and Italian corporations and do those. . . . The only thing is that the time difference is a bit troublesome. Going on [ECS #1] at night happens to be their work hours."

37. The conspirators sometimes worked to gain control over "domain controllers," servers, which many corporate networks used to control security authentication requests and other

privileges for all users within a particular network segment. This access could then be used to facilitate widespread access to computers that are members of the corporate domain. For example, as shown in Table 2, on November 29, 2017, JIANG and HACKER FOUR discussed efforts to compromise domain controllers at a multinational retailer, based in Sweden, including by stealing passwords.

Table 2

Sender	Recipient	Message Content
JIANG	HACKER FOUR	The [MULTINATIONAL RETAILER] one, did you get the domain controller password?
HACKER FOUR	JIANG	No, don't you have the domain controller machine on your side already?
HACKER FOUR	JIANG	I didn't grab the password.
HACKER FOUR	JIANG	I've been having trouble getting the domain controller of this domain for the past couple of days. It's fucking hard to get.
JIANG	HACKER FOUR	Oh, yeah, but I didn't get the domain password...
HACKER FOUR	JIANG	Want the plain text password, right?
HACKER FOUR	JIANG	I'll take a look in a while.
JIANG	HACKER FOUR	Yeah, because they need the domain controller account to deploy mining programs...

Targeting Universities

38. The conspirators also conducted computer intrusion activity at more than a dozen prominent universities in the United States, Hong Kong, and Taiwan, including, as examples, UNIVERSITY #4, UNIVERSITY #5, HONG KONG UNIVERSITY #6, HONG KONG UNIVERSITY #7, and TAIWAN UNIVERSITY #8.

39. UNIVERSITY #4 was a research university in the United States, which maintained operations and protected computers in Indiana and elsewhere.

40. In about May 2018, the conspirators installed Crosswalk/ProxIP malware on multiple UNIVERSITY #4 protected computers, including computers used by individuals associated with the Departments of Computer Science, Veterinary Science, Pharmacy, and Athletics, as well as a network administrator. The conspirators carried out the intrusion, in part, using HOP POINT TWO.

41. On or about May 8, 2019, the conspirators installed a webshell on a protected computer belonging to UNIVERSITY #4. The conspirators carried out this intrusion, in part, using one of several C2 Servers leased from VPS PROVIDER.

42. UNIVERSITY #5 was a research university in the United States, which maintained operations and protected computers in Texas and elsewhere.

43. Between about 2018 and about 2020, the conspirators compromised protected computers belonging to UNIVERSITY #5. The conspirators carried out the intrusion, in part, using HOP POINT TWO, as well as C2 Servers leased from VPS PROVIDER.

44. During the intrusion at UNIVERSITY #5, the conspirators used VPS PROVIDER servers to browse file servers on the UNIVERSITY #5's computer network. The conspirators browsed files related to network security at UNIVERSITY #5, as well as data related to Geographic Information Systems, and accessed files containing password data. In all, the conspirators browsed at least 4,200 files and directories on over 75 servers.

45. The conspirators also obtained a UNIVERSITY #5 network security application designed to hunt for malware. The conspirators installed and executed this application on a VPS PROVIDER C2 Server on or about January 10, 2019.

46. HONG KONG UNIVERSITY #6 was a university located in Hong Kong. On or about November 1, 2019, using the open source phishing tool "GOPHISH," and a C2 Server leased

from VPS PROVIDER, the conspirators sent spear-phishing e-mails to multiple recipients at three universities in Hong Kong, including HONG KONG UNIVERSITY #6.

47. HONG KONG UNIVERSITY #7 was a university located in Hong Kong. In about January 2020, the conspirators installed PlugX malware on four of HONG KONG UNIVERSITY #7's protected computers. The conspirators carried out the intrusion, in part, using a C2 Server leased from VPS PROVIDER.

48. During the intrusion, the conspirators caused HONG KONG UNIVERSITY #7's protected computers to transmit information, including system details and registry information, to a C2 Server leased from VPS PROVIDER. For example, between about January 16, 2020, and January 18, 2020, a C2 Server leased from VPS PROVIDER sent electronic communications to, and received electronic communications from, four of HONG KONG UNIVERSITY #7's protected computers.

49. TAIWAN UNIVERSITY #8 was a research university in Taiwan, which maintained operations and protected computers in Taiwan. In or about 2019, the conspirators compromised protected computers at TAIWAN UNIVERSITY #8. The conspirators carried out the intrusion, in part, through a C2 Server leased from VPS PROVIDER.

50. During the intrusion, in about October 2019, the conspirators caused TAIWAN UNIVERSITY #8's protected computers to transmit information to a C2 Server leased from VPS PROVIDER. The conspirators obtained extensive information from TAIWAN UNIVERSITY #8 protected computers, including over 67,000 photographs with filenames bearing peoples' names. The image depicted below captures a redacted portion of the directory, which included those 67,000 images.

Targeting Telecommunications Providers

51. The conspirators also targeted and compromised prominent electronic communications services and telecommunications providers in the United States and around the world, including in Australia, China (Tibet), Chile, India, Indonesia, Malaysia, Pakistan, Singapore, South Korea, Taiwan, and Thailand. These providers included, as examples, ECS #9, ECS #10, ECS #11, and ECS #12.

52. ECS #9 was an electronic communications services provider, which was based in the United States and operated protected computers in California and elsewhere. ECS #9 developed and distributed a popular communications platform.

53. On or about April 15, 2015, the conspirators sent a spear-phishing email to ECS #9 employees. The header of the e-mail showed that it had been sent from HOP POINT ONE. The e-mail fraudulently purported to contain a job-seeker's resume. In fact, the e-mail contained a malicious attachment designed to install malware on the recipient's protected computer, and that initial malware was designed to facilitate the installation of a second stage of malware. The second stage malware was designed to cause ECS #9 computers to contact a C2 Dead Drop page. The conspirators created that C2 Dead Drop page using a website that was popular with information technology professionals.

54. ECS #10 was an electronic communications services and social media provider based in the United States, with protected computers in California and elsewhere. During 2015, the conspirators targeted protected computers belonging to ECS #10. For example, on or about May 5, 2015, the conspirators sent over 140 spear-phishing e-mails to ECS #10 employees. Those spear-phishing e-mails contained the same malicious attachments which were contained in the spear-phishing e-mails directed against ECS #9.

55. The conspirators also used ECS #10 to register fraudulent communications and social media accounts. The conspirators used those accounts to conduct target research and to engage in other activities in support of their hacking. For example, between about July 2017 and December 2017, the conspirators registered four social media accounts with ECS #10. The conspirators obtained their ECS #10 accounts using fake names and other fake personal information, and then used those accounts to seek contact with individuals employed by universities, manufacturers, hospitality, travel and ride sharing companies, and ECS #10 itself.

56. ECS #11 was an electronic communications services provider, which operated protected computers in the United States, Europe, Asia, and elsewhere. ECS #11 developed and distributed a popular encrypted communications platform.

57. The conspirators compromised protected computers belonging to ECS #11 beginning no later than March 2015, and continuing through 2020. During the intrusion, the conspirators installed Winnti/Pasteboy and other malware on protected computers belonging to ECS #11. The conspirators carried out the intrusion, in part, using HOP POINT ONE, HOP POINT TWO, and C2 Servers leased from VPS PROVIDER.

58. The conspirators used their unauthorized access to ECS #11's protected computers to obtain corporate data, including source code for ECS #11 software, in 2015. The conspirators continued their ECS# 11 intrusion campaign through at least January 2020.

59. In about January 2020, on a C2 Server leased from VPS PROVIDER, the conspirators possessed software which was designed to extract user contact data from protected computers that were ECS #11 servers. The conspirators used C2 Servers leased from VPS PROVIDER to conduct over 4,000,000 queries for ECS #11 user accounts that were linked to telephone numbers in over 200 countries. These queries revealed ECS #11 accounts linked to over 700,000 phone numbers with country codes for Russia; ECS #11 accounts linked to over 268,000 phone numbers with country codes for Myanmar; ECS #11 accounts linked to over 262,000 phone numbers with country codes for Iraq; and ECS #11 accounts linked to over 100,000 phone numbers with country codes for Vietnam, Egypt, Algeria, Ukraine, and the Philippines.

60. ECS #12 was an electronic communications and telecommunications provider based in Pakistan. In about April 2019 and May 2019, the conspirators compromised protected computers at ECS #12. The conspirators carried out the intrusion, in part, using C2 Servers leased from VPS PROVIDER. During the intrusion, the conspirators caused ECS #12 servers to communicate with C2 Servers leased from VPS PROVIDER. In about May 2019, on a C2 Server leased from VPS PROVIDER, the conspirators possessed keylogger data which captured the e-mail addresses and login credentials of at least three ECS #12 employees.

Targeting Non-Profit Organizations

61. The conspirators also targeted think-tank, non-profit, and non-governmental organizations in the United States and around the world, including, for example, NGO #13.

62. NGO #13 was a non-profit organization based in the United States, with protected computers in the District of Columbia.

63. In about 2018, the conspirators compromised at least twelve NGO #13 protected computers that were located in the District of Columbia. During the course of the intrusion, the conspirators installed Winnti/Pasteboy and Crosswalk/ProxIP malware on twelve of NGO #13's

protected computers in the District of Columbia, including an e-mail server. The conspirators carried out the intrusion, in part, using HOP POINT TWO.

64. In about May 2018, as part of the computer intrusion at NGO #13, the conspirators caused NGO #13's protected computers in the District of Columbia to communicate with HOP POINT TWO.

Targeting Video Game Companies

65. The conspirators also targeted video game companies in the United States and elsewhere, including, as examples, VIDEO GAME COMPANY #14 and VIDEO GAME COMPANY #15.

66. VIDEO GAME COMPANY #14 was a video game company which maintained protected computers in Brazil and elsewhere. VIDEO GAME COMPANY #14 was partly owned by a PRC-based multinational conglomerate holding company which owned or invested in subsidiary companies which specialized in various Internet-related services and products, entertainment, artificial intelligence and technology. In about April 2015, through unauthorized access to VIDEO GAME COMPANY #14 computers, the conspirators obtained a copy of a database containing approximately 25 million records reflecting customer names, addresses, password hashes, e-mail addresses, and other personal identifying information. The conspirators carried out the intrusion, in part, using HOP POINT ONE.

67. VIDEO GAME COMPANY #15 was a video game company based in the United States, which maintained protected computers in Washington and elsewhere. On or about June 15, 2016, malware was installed on a protected VIDEO GAME COMPANY #15 computer which was located in Washington. The conspirators carried out the intrusion, in part, using HOP POINT ONE.

68. During the course of the intrusion, the conspirators caused compromised VIDEO GAME COMPANY #15 computers to seek contact with a C2 Dead Drop page and to communicate with HOP POINT ONE. The intrusion led to the compromise of dozens of VIDEO GAME COMPANY #15 protected computers, as well as the theft of login credentials for multiple VIDEO GAME COMPANY #15 employees.

Ransomware Attacks

69. In about 2020, in addition to the other types of computer intrusions described above, the conspirators also deployed ransomware and demanded ransom payments from victims, including NGO #16, DEVELOPER #17, and ENERGY COMPANY #18.

70. NGO #16 was a global non-profit organization dedicated to combatting poverty around the world, which maintained protected computers in the United States and elsewhere. On or about March 8, 2020, using a C2 Server leased from VPS PROVIDER, the conspirators used the vulnerability designated CVE-2020-10189 to obtain unauthorized access to an NGO #16 protected computer located in the United States. On or about March 23, 2020, the conspirators encrypted a compromised NGO #16 computer with ransomware software that displayed a ransom note. The ransom note demanded payment in exchange for decryption. The note also directed NGO #16 to communicate with RANSOMWARE E-MAIL ACCOUNT #1 to arrange payment.

71. DEVELOPER #17 was a real estate company based in the United States, which maintained protected computers in Ohio and elsewhere. On or about March 8, 2020, using a C2 Server leased from VPS PROVIDER, the conspirators used the vulnerability designated CVE-2020-10189 to obtain unauthorized access to a DEVELOPER #17 protected computer located in Ohio. On or about March 19, 2020, the conspirators encrypted four DEVELOPER #17 protected computers with ransomware software that displayed a ransom note. The ransom note demanded

payment in exchange for decryption. The note also directed DEVELOPER #17 to communicate with RANSOMWARE E-MAIL ACCOUNT #1 to arrange payment.

72. ENERGY COMPANY #18 was an energy company, which was based in Taiwan and maintained protected computers in Taiwan. On or about May 4, 2020, using a C2 Server in California, the conspirators caused ransomware to be installed on ENERGY COMPANY #18 protected computers, which caused compromised computers to be encrypted. The intrusion disrupted ENERGY COMPANY #18 systems, including payment systems used in connection with ENERGY COMPANY #18 retail operations.

Targeting Foreign Governments

73. The conspirators have also targeted and compromised computer networks belonging to foreign government entities in Vietnam, India, and the United Kingdom. In connection with these activities, the conspirators used several commercial penetration testing tools, including Acunetix, a popular web vulnerability scanning tool, SQLMap, a database vulnerability scanning tool, and the Cobalt Strike penetration testing framework. The conspirators carried out these activities, in part, using C2 Servers leased from VPS PROVIDER.

74. In about September 2018, using malware that was configured to work with the C2 Domain remoteset.zyns[.]com, the conspirators compromised protected computers belonging to the government of Vietnam.

75. In about 2019, the conspirators compromised government of India websites, as well as virtual private networks and database servers supporting the government of India. The conspirators used VPS PROVIDER servers to connect to an OpenVPN network owned by the government of India. During the attacks, the conspirators installed Cobalt Strike malware on Indian government protected computers.

76. In about December 2019, the conspirators used Acunetix tools to target websites belonging to the government of United Kingdom's websites.

Sonar-X

77. CHENGDU 404, including FU, developed a "big data" product named "SonarX," which was described in QIAN's records as an "Information Risk Assessment System." SonarX served as an easily searchable repository for social media data that previously had been obtained by CHENGDU 404, including data concerning ECS #11 users.

78. On or about March 19, 2018, FU registered domain name "sonarx[.]net."

79. On or about November 12, 2018, QIAN saved records reflecting a SonarX query for individuals linked to various Hong Kong democracy and independence movements. This query result displayed a link chart with several dozen entities depicted by name as blue circles, including entities highlighted as red circles. The chart depicted links among the various entities, some with solid lines and some with dotted lines. The individuals represented by red circles included HONG KONG CITIZEN #1, a member of the Hong Kong Legislative Council; HONG KONG CITIZEN #2, a founding member of the Hong Kong Civic Party, a pro-democracy political party in Hong Kong; HONG KONG CITIZEN #3, a former member of the Legislative Council of Hong Kong; HONG KONG CITIZEN #4, an individual associated with the Hong Kong independence movement; and HONG KONG CITIZEN #5, a Hong Kong pro-democracy activist who is currently wanted by the Hong Kong police under the new PRC security law recently enacted in Hong Kong in 2020.

80. On or about December 19, 2018, QIAN saved records reflecting a SonarX query for a U.S. telephone number. The query results linked the telephone number to MEDIA ORGANIZATION #19, a United States government–funded, nonprofit international broadcasting

corporation which has documented a selection of news from and about Uyghur people living in China's Xinjiang region.

81. On or about February 21, 2019, QIAN saved records reflecting a SonarX query for the name of a Tibetan Buddhist monk. The query results revealed that the monk used ECS #11 for communication, and listed the monk's region as "India." The query results contain entries concerning "chat content," "contacts," and "platforms" used by the monk.

COUNT ONE

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

82. Paragraphs 1 to 19 are re-alleged here.

The Enterprise

83. CHENGDU 404 (the "Enterprise") was an enterprise within the meaning of 18 U.S.C. § 1961(4), that is, a legal entity, which was engaged in interstate and foreign commerce, and which was engaged in activities which affected the interstate and foreign commerce of the United States.

84. The purposes of the Enterprise included generating money for its owners, officers, employees, and associates, including through "offensive" criminal computer hacking. This purpose was implemented by officers, employees, associates, and conspirators of the Enterprise through commercial activity, which included the commission of various criminal acts, including identity theft, wire and access device fraud, money laundering, and various forms of computer intrusions. The commercial activity of the Enterprise included the purchase, lease, and other use of services, computer infrastructure, and other goods in the United States and from providers in the United States.

The Racketeering Conspiracy

85. Between about May 2014 and about August 2020, and beginning outside of the jurisdiction of any particular State or district and, pursuant to 18 U.S.C. §§ 3237 and 3238, within the venue of the United States District Court for the District of Columbia, JIANG LIZHI, QIAN CHUAN, and FU QIANG, together with others known and unknown to the Grand Jury, being persons employed by and associated with CHENGDU 404, 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 identity theft);

b. 18 U.S.C. § 1029 (relating to access device fraud)

c. 18 U.S.C. § 1030(a)(5)(A) and (c)(4)(A)(i)(VI) (relating to computer fraud)

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

e. 18 U.S.C. § 1956 (relating to money laundering).

86. 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

87. The manner and means of the conspiracy include the manner and means described in Paragraphs 20 to 81, which are re-alleged here.

88. 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, Sections 3237 and 3238, within the venue of the United States District Court

for the District of Columbia, JIANG LIZHI, QIAN CHUAN, and FU QIANG, together with other conspirators known and unknown to the Grand Jury, performed or caused to be performed the acts described in Paragraphs 20 to 81, which are re-alleged here. In addition,

a. Between about May 2014 and about August 2020, in order to promote the carrying on of computer hacking activity, the conspirators used and shared computer infrastructure in the PRC, including a corporate VPN service. For example, on November 6, 2017, in connection with an ongoing hacking operation, JIANG advised HACKER FOUR, "you'll have to dial the VPN to the company," and then specified "vpn2.umisen[.]com," as well as a username and the password "wahaha@20170";

b. Between about 2014 and about 2017, in order to promote the carrying on of computer hacking activity, and through payments which originated outside of the United States, and which were paid to a provider in California, the conspirators leased HOP POINT ONE;

c. Beginning in 2014, in order to promote the carrying on of computer hacking activity, using domain registrars in the United States and elsewhere, the conspirators registered domain names which were used for C2 Domains;

d. In about April and May 2015, using e-mail accounts which were accessed from HOP POINT ONE, the conspirators sent hundreds of fraudulent spear-phishing e-mails to technology and video game companies, including VIDEO GAME COMPANY #15. For example, in one three-day period, between June 1, 2015, and June 3, 2015, one account sent 362 spear-phishing e-mails containing one of three attachments, all of which appeared to contain a legitimate resume, but which in fact contained malware.

e. In or about 2015, the conspirators also used some e-mail accounts both to send spear-phishing e-mails and to register C2 Domains. For example, one e-mail account was used (1) to register domains using DOMAIN REGISTRAR, and also (2) to send fraudulent spear-phishing e-mails. Between about April 30, 2015, and May 14, 2015, the conspirators used this e-mail account to send several hundred fraudulent spear-phishing e-mails to e-mail accounts for employees of ECS #20, an online file storage provider, and VIDEO GAME COMPANY #21, a company which was based in the United States.

f. On or about June 28, 2016, through the computer intrusion at VIDEO GAME COMPANY #15, and to obtain additional access to protected computers at VIDEO GAME COMPANY #15, the conspirators obtained login credentials belonging to K.C., an employee of VIDEO GAME COMPANY #15, and used those login credentials in furtherance of the conspiracy.

g. Between about 2017 and 2019, in order to promote the carrying on of computer hacking activity, and through payments which originated outside of the United States, and which were paid to a provider in California, the conspirators leased HOP POINT TWO;

h. Beginning in about 2017, in order to promote the carrying on of computer hacking activity, and through payments which originated outside of the United States, and which were paid to a provider in Florida, the conspirators leased servers from VPS PROVIDER, and used those servers as C2 Servers.

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

COUNT TWO

(Conspiracy to Commit Computer Hacking Offenses in Violation of 18 U.S.C. § 1030)

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

Overview of the Conspiracy

90. Between at least May 2014 and August 2020, and beginning outside of the jurisdiction of any particular State or district and, pursuant to 18 U.S.C. §§ 3237 and 3238, within the venue of the United States District Court for the District of Columbia, JIANG LIZHI, QIAN CHUAN, and FU QIANG, together with other conspirators known and unknown to the Grand Jury, did knowingly and willfully combine, conspire, confederate, and agree with each other to commit the following offenses against the United States:

a. 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, intentionally accessed, and attempted to access, computers without authorization, and thereby obtained, and attempted to obtain, information from protected computers, such conduct having involved an interstate and foreign communication, in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and (c)(2)(B)(i) and (ii); and

b. Knowingly caused the transmission of a program, information, code, and command, and as a result of such conduct, intentionally caused, or attempted to cause, damage without authorization to protected computers, and caused, or attempted to cause, more than $5,000 in loss in one year, and caused, or attempted to cause, damage affecting 10 or more protected

computers during a one-year period, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and (c)(4)(B);

c. With intent to extort from any person any money or other thing of value, transmitted in interstate or foreign commerce, communications containing any demand or request for money or other thing of value, in relation to damage to a protected computer, where such damage was caused to facilitate the extortion, in violation of Title 18, United States Code, Sections 1030(a)(7)(c) and (c)(3)(A);

in violation of Title 18, United States Code, Sections 371, 1030(a)(2)(C) and (c)(2)(B)(i) and (ii), and Sections 1030(a)(2)(C), (a)(5)(A), (a)(7)(C), and (c).

Objects, Manners, and Means of the Conspiracy

91. The objects of the conspiracy were to obtain and install malware on protected computers, to damage such computers, to gain unauthorized access to those and other protected computers, to obtain information of value that belonged to the owners and users of the targeted protected computers, and to do so by means of materially false and fraudulent representations and pretenses, and to otherwise defraud and obtain information and digital items of value, including software signing certificates, data, personal information, and means to conduct further intrusions.

92. As part of the conspiracy to commit computer hacking offenses, the conspirators used the same manners and means which are described in Paragraphs 20 to 25. The manners and means described in Paragraphs 20 to 25 are re-alleged here.

Overt Acts

93. In furtherance of the conspiracy to commit computer hacking offenses, the overt acts described in Paragraphs 26 to 81, and in Paragraph 88, were committed beginning outside of the jurisdiction of any particular State or district and, pursuant to Title 18, United States Code,

Sections 3237 and 3238, within the venue of the United States District Court for the District of Columbia. The overt acts described in Paragraphs 26 to 81, and in Paragraph 88 are thus re-alleged here.

94. The malware installed on computers which were successfully compromised by the conspirators typically, and including for MANUFACTURER #2, caused losses exceeding $5,000.

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

COUNT THREE
(Intentional Damage to a Protected Computer)

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

96. On or about May 1, 2018, and beginning outside of the jurisdiction of any particular State or district and, pursuant to 18 U.S.C. §§ 3237 and 3238, within the venue of the United States District Court for the District of Columbia, JIANG LIZHI, QIAN CHUAN, and FU QIANG, together with other conspirators known and unknown to the Grand Jury, knowingly attempted to cause, and did cause, the transmission of a program, information, code, and command, and aided and abetted the same, and, as a result of such conduct, intentionally caused damage without authorization to protected computers in the District of Columbia, said computers belonging to NGO #13. The offense caused loss resulting from a related course of conduct affecting one or more other protected computers aggregating at least $5,000 in value, and the offense 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) and (c)(4)(B) and 2)

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

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

98. On or about May 1, 2018, and beginning outside of the jurisdiction of any particular State or district and, pursuant to 18 U.S.C. §§ 3237 and 3238, within the venue of the United States District Court for the District of Columbia, JIANG LIZHI, QIAN CHUAN, and FU QIANG, together with other conspirators known and unknown to the Grand Jury, 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, attempted to intentionally access, and did intentionally access, a protected computer belonging to NGO #13 without authorization, and aided and abetted the same, and thereby obtained, and attempted to obtain, information from a protected computer belonging to NGO #13.

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

COUNT FIVE
(Threatening to Damage a Protected Computer)

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

100. On or about March 19, 2020, and beginning outside of the jurisdiction of any particular State or district and, pursuant to 18 U.S.C. § 3238, within the venue of the United States District Court for the District of Columbia, JIANG LIZHI, QIAN CHUAN, and FU QIANG, together with other conspirators known and unknown to the Grand Jury, with intent to extort from DEVELOPER #17 money and other things of value, transmitted in interstate and foreign commerce a communication containing a demand and request for money and other thing of value in relation to damage to a protected computer, and aided and abetted the same, where such damage was caused to facilitate the extortion.

(**Threatening to Damage a Protected Computer,** in violation of Title 18, United States Code, Sections 1030(a)(7)(C), (b), (c)(3)(A), and 2)

COUNT SIX
(Access Device Fraud)

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

102. On or about June 28, 2016, and beginning outside of the jurisdiction of any particular State or district and, pursuant to 18 U.S.C. § 3238, within the venue of the United States District Court for the District of Columbia, JIANG LIZHI, QIAN CHUAN, and FU QIANG, together with other conspirators 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, possess and use one or more unauthorized access devices, that is, login credentials belonging to K.C., an employee of VIDEO GAME COMPANY #15, for access to protected computers of VIDEO GAME COMPANY #15, and aided and abetted the same, and by such conduct, between June 15, 2016, and June 15, 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 SEVEN
(Identity Theft)

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

104. On or about June 29, 2016, and beginning outside of the jurisdiction of any particular State or district and, pursuant to 18 U.S.C. § 3238, within the venue of the United States District Court for the District of Columbia, JIANG LIZHI, QIAN CHUAN, and FU QIANG, together with other conspirators 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 belonging to M.B., an employee of VIDEO GAME COMPANY #15, 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 and that constitutes a felony under any applicable State and local 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), and 2)

COUNT EIGHT
(Aggravated Identity Theft)

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

106. On or about June 28, 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, JIANG LIZHI, QIAN CHUAN, and FU QIANG, together with other conspirators 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)(C), did knowingly transfer, possess, and use, without lawful authority, a means of identification of another person, K.C., an employee of VIDEO GAME COMPANY #15, 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 NINE
(Money Laundering)

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

108. On or about April 14, 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, JIANG LIZHI, QIAN CHUAN, and FU QIANG, together with other conspirators 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 $143.67 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)(C), 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)

FORFEITURE ALLEGATION

1. Upon conviction of the offense alleged in Count 1 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).

2. Upon conviction of any of the offenses alleged in Counts 2, 3, 4, 5, 6, and/or 7 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 2, 3, 4, and/or 5 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 2, 3, 4, 5, 6, and/or 7 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 6 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 7 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 the offense alleged in Count 9 of this Indictment, the defendants shall forfeit to the United States any property, real or personal, involved in this offense 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 defendant shall forfeit to the United States any other property of the defendant, up to the value of the property described above, pursuant to 18 U.S.C. § 1963(m) and 21 U.S.C. § 853(p).

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

A TRUE BILL

_____
Foreperson

_____ /by DSA
MICHAEL SHERWIN
ACTING UNITED STATES ATTORNEY IN AND FOR
THE DISTRICT OF COLUMBIA