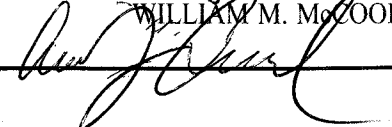


Presented to the Court by the foreman of the Grand Jury in open Court, in the presence of the Grand Jury and FILED in the U.S. DISTRICT COURT at Seattle, Washington.

January 10 20 19
WILLIAM M. McCOOL, Clerk
By  Deputy

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

UNITED STATES OF AMERICA,
Plaintiff,

v.

HO JUN JIA,
a/k/a Matthew Ho,
a/k/a "Prefinity,"
a/k/a "Ethereum Vendor,"
Defendant.

NO. **CR19-007** JLR

INDICTMENT

The Grand Jury charges that:

1. For purposes of this Indictment:

- a. The defendant, HO JUN JIA, also known as Matthew HO (hereinafter, "HO"), is a resident and citizen of the Republic of Singapore.
- b. Amazon.com, Inc. (hereinafter, "Amazon") is an electronic commerce, cloud computing, and consumer electronic device company headquartered in Seattle, Washington, within the Western District of Washington.
- c. Amazon Web Services (hereinafter, "AWS") is a subsidiary of Amazon that provides on-demand cloud computing platforms to individuals, companies

1 and governments, on a paid subscription basis. AWS provides subscribers with access to
2 a variety of computing services and differing levels of storage and computing power
3 through the Internet. AWS operates out of Seattle, Washington, within the Western
4 District of Washington.

5 d. "Victim-1" is a resident of the state of California and is the co-
6 founder of a video game developer and eSports tournament organizer based in Los
7 Angeles, California (hereinafter, "Company-1").

8 e. "Victim-2" is a resident of the state of Texas.

9 f. "Victim-3" is a resident and citizen of a foreign country and believed
10 to be the co-founder and an executive of a technology company in the Republic of India.

11 g. Cloud Computing is the practice of using a network of remote
12 servers hosted on the Internet, commonly referred to as "the cloud," to store, manage, and
13 process data, rather than a local server or a personal computer.

14 h. Cryptocurrency is a digital currency or asset that employs encryption
15 or cryptography techniques to secure and verify the transfer of funds and to regulate the
16 generation of additional units of currency. Cryptocurrencies operate independently of a
17 central bank system and typically work through distributed ledger technology, a public
18 and decentralized ledger commonly referred to as a "blockchain," that serves as a public
19 financial transaction database. Examples of decentralized cryptocurrencies include
20 Bitcoin (BTC), Ethereum (ETH), Litecoin (LTC), Zcash (ZEC), Dash (DASH), Ripple
21 (XRP), and Monero (XMR), among many others.

22 i. Cryptocurrency mining is the process by which cryptocurrency
23 transactions are verified and added to the public ledger, i.e., the blockchain, and also the
24 means through which new cryptocurrency units are generated and released. Generally
25 speaking, transactions are verified and assembled into "blocks" through the creation of
26 hashes that fulfill certain requirements, which are then appended to the blockchain.
27 Those that carry out the task of verifying "blocks" of legitimate transactions, often
28 referred to as "miners," are rewarded with an amount of that cryptocurrency. With the

1 growth and increased prevalence and valuation of cryptocurrencies, successful mining
2 operations have required and consumed increasingly large amounts of computing power
3 and hardware.

4 **COUNTS 1 - 8**

5 **(Wire Fraud)**

6 **A. Overview**

7 2. The defendant, HO JUN JIA, a/k/a Matthew HO, operated a large-scale
8 cryptocurrency mining operation, propelled predominantly, if not exclusively, through
9 fraud and identity theft. HO, a resident and citizen of Singapore, engaged in a
10 sophisticated fraud scheme that involved the use of stolen personal and financial
11 information of individual victims, including U.S. citizens, and a web of fraudulently
12 registered accounts at various online service providers, such as Amazon and AWS, to
13 gain access to immense amounts of computer processing power and storage, which he
14 used to mine various cryptocurrencies. Through such mining activity, HO acquired
15 cryptocurrency, such as Bitcoin and Ethereum, which he in turn sold and exchanged for
16 traditional funds through online cryptocurrency vendor websites.

17 3. More specifically, as discussed in more detail below, beginning in late
18 2017, which followed the surge in popularity of cryptocurrencies, HO used victims'
19 personal and stolen credit card information, along with phony email addresses, which he
20 created, designed to spoof the authentic email account of identity-theft victims, to open
21 accounts and to obtain access to cloud computing services. HO employed social
22 engineering techniques to trick providers into approving heightened privileges and
23 benefits, including elevated levels of cloud computing services and deferred billing
24 accommodations, and to deflect inquiries from service providers regarding questionable
25 data usage and mounting unpaid subscription balances.

26 4. For instance, in October and November 2017, HO opened numerous
27 accounts at Amazon (retail), AWS and Google Cloud Services in the name of Victim-1, a
28 resident of California, using Victim-1's personal information, including his name,

1 address, and credit card information, along with a seemingly authentic email account and
2 California state driver's license. By associating with Victim-1's company, Company-1, a
3 legitimate and sizeable AWS customer, and through social engineered communications
4 and additional deceptive tactics, HO gained access to a premium suite of cloud
5 computing services and, for a brief period, was one of AWS's largest consumer of data
6 usage by volume.

7 5. HO also created a fictitious individual to communicate with AWS
8 ostensibly on Victim-1's behalf, designed to legitimize the abnormal cloud computing
9 usage. For instance, HO registered an online domain designed to spoof the name of
10 another video game developer based in Los Altos, California (hereinafter, "Company-2")
11 recently acquired by Company-1 (Victim-1's company). Using that spoofed domain, HO
12 then created an email account for a non-existent person, "Daniel Piers," which he used to
13 communicate with AWS regarding billing issues and account maintenance ostensibly on
14 Victim-1's behalf. The exploitation of Company-1 and Company-2 illustrates HO's
15 sophistication and use of social engineering to perpetuate the fraud scheme.

16 6. HO used the fraudulently-created cloud services accounts and computing
17 power and data storage primarily, if not exclusively, as part of a large-scale
18 cryptocurrency mining operation, which he supported through additional third-party
19 services similarly acquired through fraud and the use of victim information. Through
20 such mining activity, HO acquired cryptocurrency to enrich himself.

21 7. HO registered and managed various accounts on cryptocurrency
22 marketplace websites, such as localbitcoins.com and localethereum.com. Through these
23 sites, and using monikers, to include "Prefinity" and "Ethereum Vendor," HO sold and
24 exchanged cryptocurrency, including Bitcoin and Ethereum obtained through the
25 aforementioned mining activity, for traditional funds. HO also used social media, such as
26 Facebook, to solicit interest in cryptocurrency and to advertise the fluctuations in price
27 and exploit the growing attention to and popularity of cryptocurrency and virtual
28 currency markets.

1 8. In furtherance of the scheme, HO consumed more than \$5 million in unpaid
2 cloud computing services. Portions (i.e., hundreds of thousands of dollars) of past due
3 balances were charged to victim credit cards, some of which the accountholder paid
4 before the fraud and compromise of the credit card account were discovered.

5 **B. Scheme and Artifice to Defraud**

6 9. The allegations set forth in Paragraphs 1 through 8 of this Indictment are
7 re-alleged and incorporated as if fully set forth herein.

8 10. Beginning at a time unknown, but no later than October 2017, and
9 continuing until at least February 2018, at Seattle, within the Western District of
10 Washington, and elsewhere, the defendant, HO JUN JIA, a/k/a Matthew HO, and others
11 known and unknown to the Grand Jury, devised and intended to devise a scheme and
12 artifice to defraud and to obtain money and property by means of materially false and
13 fraudulent pretenses, representations and promises.

14 11. The essence of the scheme and artifice to defraud was to use stolen personal
15 and financial information to open accounts in the names of others, without authorization,
16 in order to obtain things of value, including computing and data storage services. The
17 scheme and artifice to defraud also involved the use of computing services to engage in a
18 coordinated cryptocurrency mining operation to generate cryptocurrency units, a thing of
19 value, which were then sold and exchanged for traditional government-issued currency.
20 The object of the scheme and artifice to defraud, at bottom, was to achieve financial
21 enrichment through fraud and deception.

22 **C. Manner and Means**

23 12. The manner and means of the scheme and artifice to defraud included the
24 conduct described herein and the following:

25 a. HO, either personally or through an accomplice, obtained personally
26 identifiable information and financial information belonging to others, including, but not
27 limited to, Victim-1, Victim-2, and Victim-3, without their knowledge or permission.
28

1 b. HO created phony email accounts, typically at Google (i.e.,
2 @gmail.com) or at unique domains that he registered and managed, designed to spoof
3 authentic email accounts, including those of identity-theft victims. The fake email
4 accounts were intended and used, in conjunction with additional information, to deceive
5 and to obtain services and items of value. By way of example,

6 i. On about October 19, 2017, HO created an email account in
7 the name of Victim-1, namely, ██████████@gmail.com, that incorporated Victim-1's
8 first initial and full last name (hereinafter, the "V1 Email Account").

9 ii. On about November 18, 2017, HO created an email account
10 in the name of Victim-2, namely, ██████████@gmail.com, that incorporated Victim-
11 2's first and last name (hereinafter, the "V2 Email Account").

12 iii. On about November 24, 2017, HO created an email account
13 in the name of Victim-3, namely, ██████████@gmail.com, that incorporated
14 Victim-3's first and last name (hereinafter, the "V3 Email Account").

15 c. HO used personal and financial information of others to open
16 multiple retail accounts at Amazon. HO then attempted to purchase things of value,
17 including instrumentalities of the scheme, using victim credit cards and accumulated
18 membership rewards points. By way of example,

19 i. On about October 19, 2017, HO opened an Amazon retail
20 account in the name of Victim-1, using another email address incorporating Victim-1's
21 first and last name at a domain HO registered and managed, namely,
22 ██████████@corestratos.com, and Victim-1's American Express credit card information.
23 On the same date, HO attempted to purchase computer-related items through this
24 account, using Victim-1's credit card.

25 ii. On about October 20, 2017, HO opened another Amazon
26 retail account in the name of Victim-1, using the V1 Email Account, Victim-1's credit
27 card information, and the address of a property located in Santa Monica, California,
28

1 | owned by Victim-1. On the same date, HO attempted to purchase a computer-related
2 | item through this account, using Victim-1's credit card.

3 | iii. On about November 4, 2017, HO opened yet another Amazon
4 | retail account in the name of Victim-1, again using the V1 Email Account and Victim-1's
5 | credit card information and Santa Monica, California address. On about November 6,
6 | 2017, HO attempted to purchase a Bitcoin mining contract through this account, using
7 | Victim-1's credit card.

8 | d. HO used personal and financial information of others to open
9 | multiple accounts for cloud computing services at providers such as AWS and Google.
10 | HO, through use of social engineering and other deceptive tactics, sought elevated access
11 | and privileges related to data storage and usage. By way of example,

12 | i. On about November 1, 2017, HO opened a cloud services
13 | account with Google Cloud Services in the name of Victim-1, using the V1 Email
14 | Account and Victim-1's credit card information and Santa Monica, California address.

15 | ii. On about November 2, 2017, HO opened a cloud services
16 | account with AWS in the name of Victim-1, using the V1 Email Account, Victim-1's
17 | credit card information and Santa Monica, California address.

18 | iii. On about November 4, 2017, as verification for the AWS
19 | account opened in Victim-1's name, HO submitted to AWS copies of an account
20 | statement for Victim-1's credit card and a fake California driver's license bearing Victim-
21 | 1's name and photograph.

22 | iv. On November 20, 2017, HO, through use of the V1 Email
23 | Account, requested and obtained access for elevated privileges for the AWS account in
24 | Victim-1's name.

25 | v. On about November 18, 2017, HO opened a cloud services
26 | account with AWS in the name of Victim-2, using the V2 Email Account and Victim-2's
27 | Visa credit card information and address in Haltom City, Texas.

1 vi. On about November 24, 2017, HO opened a cloud services
2 account with AWS in the name of Victim-3, using the V3 Email Account, Victim-3's
3 Visa credit card information, and an address in Singapore.

4 vii. On about November 29, 2017, as verification for the AWS
5 account opened in Victim-3's name, HO submitted to AWS a copy of a bank statement of
6 another person.

7 e. HO also secured services and contracts from third-party vendors in
8 relation to cryptocurrency mining activity. For instance, on about October 20, 2017, HO
9 registered an account with CCG Mining, a company that provides cryptocurrency and
10 blockchain consulting services, in Victim-1's name and using the V1 Email Account.
11 HO then used the account to acquire information and services related to the mining,
12 marketing, and sale of cryptocurrency, all using Victim-1's identity, in furtherance of his
13 fraudulent scheme.

14 f. HO used the fraudulently obtained computing power and data
15 storage and related services obtained through the cloud service providers primarily, if not
16 exclusively, to mine cryptocurrency. As a result, HO earned and acquired units of
17 cryptocurrency, such as Bitcoin and Ethereum, which he transferred into cryptocurrency
18 wallets he maintained.

19 g. HO registered domains and emails and created fictitious individuals
20 to communicate with service providers ostensibly on the accountholder's behalf. For
21 instance, on about January 18, 2018, HO created a web domain designed to spoof
22 Company-2 and an email account for "Daniel Piers," which he used to communicate with
23 AWS representatives about a billing arrangement for the AWS account opened in the
24 name of Victim-1.

25 h. HO, without authorization, authorized and caused payments for
26 goods and services on the victim credit cards. By way of example,

27 i. Beginning on about November 4, 2017, and on numerous
28 dates thereafter, at least 16 payments in varying amounts, totaling roughly \$240,000,

1 were charged to Victim-1's credit card toward the balance owed on the Google Cloud
2 Services account opened in the name of Victim-1. Such payments to Google include, but
3 are not limited to, two payments totaling \$40,000 on about February 20, 2018; two
4 payments totaling \$40,000 on about February 21, 2018; and three attempted charges
5 totaling \$105,000 on about February 22, 2018.

6 ii. On about December 3, 2017, a payment in the amount of
7 \$135,861.12 was charged to Victim-1's credit card toward the balance owed on the AWS
8 account opened in the name of Victim-1.

9 i. HO advertised, sold, and exchanged such cryptocurrency on various
10 cryptocurrency marketplace websites, such as localbitcoins.com and localethereum.com,
11 in order to obtain traditional funds. To conceal his true identity, HO used online
12 monikers, such as "Prefinity" and "Ethereum Vendor," respectively.

13 j. HO also used social media and online services to solicit interest in
14 cryptocurrency and to advertise the fluctuations in price and exploit the growing attention
15 to and popularity of cryptocurrency and virtual currency markets. For instance, on about
16 December 8, 2017, HO posted on Facebook the message: "ETH/BTC levels are at all
17 time low since march when ETH cost around \$36. ...whats your move?"

18 **D. Execution of Scheme and Artifice to Defraud**

19 13. On or about the dates set forth below, at Seattle, within the Western District
20 of Washington, and elsewhere, the defendant, HO JUN JIA, a/k/a Matthew HO, and
21 others known and unknown to the Grand Jury, having devised a scheme and artifice to
22 defraud, and to obtain money and property by means of materially false and fraudulent
23 pretenses, representations, and promises, did knowingly transmit and cause to be
24 transmitted writings, signs, signals, pictures, and sounds, for the purpose of executing
25 such scheme, by means of wire communication in interstate and foreign commerce,
26 including the following transmissions, each of which caused the transmission of an
27 electronic signal between the state of Washington and a location outside of the state of
28 Washington, and each of which constitutes a separate count of this Indictment:

Count	Date(s)	Wire Transmission
1	11/2/2017	Registration of AWS account in name of Victim-1
2	11/4/2017	Submission of American Express credit card statement and driver's license in the name of Victim-1
3	11/18/2017	Registration of AWS account in name of Victim-2
4	11/20/2017	Communication with AWS regarding cloud services privileges for account in the name of Victim-1
5	11/24/2017	Registration of AWS account in name of Victim-3
6	11/30/2017	Communication with AWS regarding account service for account in the name of Victim-1
7	12/3/2017	Payment to AWS account in the name of Victim-1 charged to Victim-1's credit card
8	1/18/2018	Generation and communication of payment instructions for AWS account in the name of Victim-1

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

COUNTS 9 - 12

(Access Device Fraud)

14. The allegations set forth in Paragraphs 1 through 12 of this Indictment are re-alleged and incorporated as if fully set forth herein.

15. On or about the dates set forth below, at Seattle, within the Western District of Washington, and elsewhere, the defendant, HO JUN JIA, a/k/a Matthew HO, and others known and unknown to the Grand Jury, knowingly and with intent to defraud, used and trafficked in an unauthorized access device, as described below, and other means of account access that can be used, alone and in conjunction with another access device, to obtain a thing of value, and by such conduct, obtained things of value worth \$1,000 or more during a one-year period; said activity affecting interstate and foreign commerce.

Count	Date(s)	Access Device
9	10/19/2017	Victim-1's credit card information (transmission to Amazon)
10	11/2/2017	Victim-1's credit card information (transmission to AWS)
11	11/18/2017	Victim-2's credit card information (transmission to AWS)
12	11/24/2017	Victim-3's credit card information (transmission to AWS)

All in violation of Title 18, United States Code, Sections 1029(a)(2) and 1029(c)(1)(A)(i), and 2.

COUNT 13

(Aggravated Identity Theft)

16. The allegations set forth in Paragraphs 1 through 15 of this Indictment are re-alleged and incorporated as if fully set forth herein.

17. On multiple dates, beginning on or about October 19, 2017, and including November 2, 2017, and continuing until January 2018, at Seattle, within the Western District of Washington, and elsewhere, the defendant, HO JUN JIA, a/k/a Matthew HO, did knowingly transfer, possess, and use, without lawful authority, a means of identification of another person, to wit: the name, address, and credit card information of Victim-1, a real person, during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c), that is, wire fraud, in violation of 18 U.S.C. § 1343, as charged in Counts 1, 2, 4, 6, 7, and 8, and access device fraud, in violation of 18 U.S.C. § 1029, as charged in Counts 9 and 10, knowing that the means of identification belonged to another actual person.

All in violation of Title 18, United States Code, Sections 1028A(a) and 2.

1 **COUNT 14**

2 **(Aggravated Identity Theft)**

3 18. The allegations set forth in Paragraphs 1 through 15 of this Indictment are
4 re-alleged and incorporated as if fully set forth herein.

5 19. On or about November 18, 2017, at Seattle, within the Western District of
6 Washington, and elsewhere, the defendant, HO JUN JIA, a/k/a Matthew HO, did
7 knowingly transfer, possess, and use, without lawful authority, a means of identification
8 of another person, to wit: the name, address, and credit card information of Victim-2, a
9 real person, during and in relation to a felony violation enumerated in 18 U.S.C.
10 § 1028A(c), that is, wire fraud, in violation of 18 U.S.C. § 1343, as charged in Count 3,
11 and access device fraud, in violation of 18 U.S.C. § 1029, as charged in Count 11,
12 knowing that the means of identification belonged to another actual person.

13 All in violation of Title 18, United States Code, Sections 1028A(a) and 2.

14 **FORFEITURE ALLEGATION**

15 20. The allegations contained in Counts 1 through 8 of this Indictment are
16 hereby realleged and incorporated by reference for the purpose of alleging forfeitures
17 pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States
18 Code, Section 2461(c). Upon conviction of any of the offenses charged in Counts 1
19 through 8, the defendant shall forfeit to the United States any property, real or personal,
20 which constitutes or is derived from proceeds traceable to such offenses, including but
21 not limited to a judgment for a sum of money representing the property described in this
22 paragraph.

23 21. The allegations contained in Counts 9 through 12 of this Indictment are
24 hereby realleged and incorporated by reference for the purpose of alleging forfeitures
25 pursuant to Title 18, United States Code, Sections 981(a)(1)(C) and 1029(c)(1)(C), and
26 Title 28, United States Code, Section 2461(c). Upon conviction of any of the offenses
27 charged in Counts 9 through 12, the defendant shall forfeit to the United States any
28 property, real or personal, which constitutes or is derived from proceeds traceable to such

1 offense, and shall also forfeit any personal property used or intended to be used to
2 commit such offense, including but not limited to a judgment for a sum of money
3 representing the property described in this paragraph.

4 ***(Substitute Assets)***

5 22. If any of the property described above, as a result of any act or omission of
6 the defendant:

- 7 a. cannot be located upon the exercise of due diligence;
- 8 b. has been transferred or sold to, or deposited with, a third party;
- 9 c. has been placed beyond the jurisdiction of the court;
- 10 d. has been substantially diminished in value; or
- 11 e. has been commingled with other property which cannot be divided
12 without difficulty,

13 //

14 //

15 //

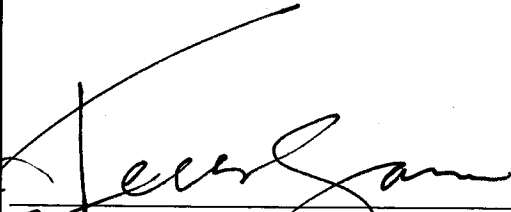
1 the United States of America shall be entitled to forfeiture of substitute property pursuant
2 to Title 21, United States Code, Section 853(p), as incorporated by Title 28, United States
3 Code, Section 2461(c).


4 A TRUE BILL:


5 DATED: 1-10-2019

6 *(Signature of Foreperson redacted pursuant to*
7 *policy of the Judicial Conference)*

8 FOREPERSON

9
10 
11 ANNETTE L. HAYES
12 United States Attorney

13 
14 ANDREW C. FRIEDMAN
15 Assistant United States Attorney

16 
17 STEVEN MASADA
18 Assistant United States Attorney