THE UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF MISSOURI
WESTERN DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. MICHAEL D. MIHALO, a/k/a DALE MICHAEL MIHALO, JR., [DOB: 2/12/1983] SIMON KAURA, [DOB: 10/25/1988] TAYLOR ROSS STAATS, [DOB: 3/21/1983] Defendants.	No. _____ **COUNT ONE:** ***Conspiracy to Commit Access Device Fraud*** 18 U.S.C. § 1029(b)(2) NMT 5 Years Imprisonment NMT 3 Years Supervised Release NMT $250,000 Fine **COUNT TWO:** ***Access Device Fraud*** 18 U.S.C. §§ 1029(a)(2) & 2 NMT 10 Years Imprisonment NMT 3 Years Supervised Release NMT $250,000 Fine **COUNT THREE:** ***Money Laundering Conspiracy*** 18 U.S.C. § 1956(h) NMT 20 Years Imprisonment NMT $500,000 Fine NMT 3 Years Supervised Release **COUNTS FOUR through NINE:** ***Money Laundering*** 18 U.S.C. §§ 1957 & 2 NMT 10 Years Imprisonment NMT $250,000 Fine NMT 3 Years Supervised Release **FORFEITURE ALLEGATIONS:** 18 U.S.C. § 982, 18 U.S.C. § 1029, 21 U.S.C. § 853

I N D I C T M E N T

THE GRAND JURY CHARGES THAT:

COMMON ALLEGATIONS

At all times relevant to this Indictment:

1. Defendant MICHAEL MIHALO resided in or around Naperville, Illinois.

2. Defendant SIMON KAURA resided in or around Kent, United Kingdom.

3. Defendant TAYLOR ROSS STAATS resided in or around Dallas, Texas.

4. UMB Bank, NA was a financial institution headquartered in Kansas City, Missouri.

Darknet Markets

5. Markets A, B, C, and D (collectively, the "Markets") were darknet markets that allowed users in the United States and elsewhere to buy and sell some or all of the following illegal goods: stolen and fraudulent financial information and payment cards, computer hacking tools, access device-making equipment, and other illegal contraband using Bitcoin and other digital currencies. While operational, these sites enabled thousands of users to distribute illegal contraband over the Internet to buyers throughout the world, and to launder millions of dollars derived from the illegal transactions conducted on the Markets.

6. Each Market existed on the Dark Web (or "darknet"), meaning that the Markets were accessible through the "Tor" network, an online network designed specifically to facilitate anonymous communication over the Internet. The use of the Tor network was intended to, and successfully made it difficult to, identify the true physical locations of the Markets' underlying computer servers, as well as to identify and locate their administrators, moderators, and users. Market A (and its associated discussion forum) also operated "mirror" sites, or replica websites, on the Clearnet (i.e., the ordinary Internet).

7. Each Market operated much like a conventional e-commerce website, except that the goods sold on the Market were primarily, if not exclusively, criminal in nature. Users could

register a free account and choose a username and password. Once an account was created, users were able to browse and search for illegal contraband for sale on the Market, and ultimately purchase illegal contraband for delivery either over the Internet or via the mails.

8. Each Market required users to transact in digital currencies, including Bitcoin, and did not permit transactions in official, government-backed currencies. Digital currencies are electronically sourced units of value that exist on the Internet and are not stored in a physical form. They are not issued by any government, but instead are generated and controlled through computer software operating on decentralized peer-to-peer networks. Users of digital currencies send units of value to and from "addresses," which are unique strings of numbers and letters functioning like a public account number. Digital currency transactions are recorded on a publicly available, distributed ledger, often referred to as a "blockchain." Because digital currencies are transferred peer-to-peer, users can avoid traditional, regulated financial institutions, which collect information about their customers and maintain anti-money laundering and fraud programs. The Markets and their users were able to bypass the traditional financial systems by only accepting digital currencies.

Darknet Sales

9. MIHALO operated widely on the darknet under aliases known to the grand jury, including [ALIAS-1].[1] MIHALO was a prominent "carding" (stolen financial information) vendor on multiple darknet markets, including Markets B, C, and D. In addition to conducting his own sales under the username "ALIAS-1," MIHALO assembled a team to help him sell stolen financial

[1] This alias is known to the grand jury but anonymized here to protect ongoing investigations.

information on the darknet using the ALIAS-1 brand name. Members of the conspiracy benefitted from this arrangement by gaining access to stolen payment cards obtained by MIHALO, taking advantage of MIHALO's reputation as a "trusted" source for stolen payment card information, and being able to sell more stolen financial information than each would have been able to sell individually—all in exchange for a share in the profits. Between on or about February 22, 2016, until on or about October 1, 2019, MIHALO and his co-conspirators conducted tens of thousands of illegal transactions (valued at over $1 million) on Markets A, B, C, and D.

Market A

10. In or about early 2016, MIHALO, KAURA (operating under three aliases known to the grand jury), and others agreed to establish a new carding market on the darknet, initially called ALIAS-1 and subsequently branded as Market A. Setting up their own market allowed the co-conspirators to sell directly to consumers without paying commissions and/or fees to other darknet markets' operators. Instead, the profits from each sale accrued directly to the co-conspirators, who played various roles in the site's operation and the illegal activities conducted upon it.

11. In or about April 2016, the co-conspirators launched the new darknet market, which offered the "BEST CVV's CVV2, Fresh cards updated daily." Soon thereafter, they launched a "mirror" site accessible on the Clearnet domain [ALIAS-1].com.

12. Market A's product offerings focused almost entirely on stolen financial information. Once an account was created, users were able to browse or search for stolen financial information, which was organized by card Type (e.g., Visa, MasterCard), bank identification

number (BIN), City/State/Country, Level (e.g., Gold, Business, Signature), Class (e.g., Credit/Debit), and Price. Market A also sold "SOCKS proxies," or a technology that allowed users to hide their true IP addresses in order to appear as if they are located in the general location of the credit card they are attempting to use.

13. Finally, the co-conspirators launched a forum associated with Market A in early 2016, which provided a place for members to discuss fraud-related activities. The forum was also used to promote ALIAS-1's sales on the darknet, and to direct potential buyers to specific listings associated with the ALIAS-1 brand name.

14. Market A's staff was comprised of several individuals, each of whom operated under online aliases and had various roles within the organization. Some of these individuals included:

a. MICHAEL MIHALO, who was the site's founder and the group's organizational leader. MIHALO was primarily responsible for obtaining the stolen payment card information that was sold on the site and directing the other co-conspirators' activities.

b. SIMON KAURA, who operated under several aliases known to the grand jury. KAURA performed web development (with others) for the Market A Clearnet and darknet sites, approved Market A's users to become vendors, and helped maintain and operate the sites.

c. TAYLOR ROSS STAATS, who operated under an alias known to the grand jury and was a "card-checker." STAATS's primary responsibility was to use online tools

to verify whether the tens of thousands of stolen payment card numbers obtained by MIHALO and others remained active or had been closed by the issuing financial institutions. STAATS then organized this financial information into an easily distributable format.

15. From at least on or about February 22, 2016, until on or about October 1, 2019, the co-conspirators possessed, trafficked in, and sold tens of thousands of stolen payment card numbers belonging to U.S. victims and issued by U.S. financial institutions, all in violation of U.S. law.

Money Laundering

16. As part of their scheme for financial enrichment through fraud, the co-conspirators agreed to disguise the nature, location, source, ownership, and control of their illicit funds, and to use their illicit funds to further promote their scheme. To disguise the illicit nature of their funds, the co-conspirators conducted sales using and receiving digital currencies, including Bitcoin. The co-conspirators also paid themselves and others for goods and services using the illegally obtained Bitcoin. Operating Market A and selling stolen financial information on other Markets required significant expenditures, which the co-conspirators paid using the proceeds of their illicit activities. To further the scheme, the co-conspirators used illicit funds to pay for stolen payment card information and identity information, internet hosting, website design, card checking (checking validity of stolen card information), card cleaning (organizing/cataloguing stolen credit card information), digital currency mixing services, and digital currency transaction fees, and customer service costs on the Markets.

17. All co-conspirators agreed and understood that the profits from the scheme needed to be disguised, or laundered, in order to avoid detection by law enforcement. To achieve their goal of turning illicit funds into seemingly legitimate assets, the co-conspirators oftentimes sent their illicit profits, in the form of digital currencies, through multiple Bitcoin wallets. The co-conspirators also employed the use of "mixers" or "tumblers," which are services designed to conceal the transaction history of digital currencies and make them more difficult to trace. Mixers charge a transaction fee for their services, which is typically paid with a portion of the digital currency sent to be mixed. The co-conspirators also advised others on how to launder digital currency and methods to "cashout" or to convert digital currency to government-backed currency.

18. The co-conspirators used various methods to convert the digital currencies into legitimate, government-backed currencies, including schemes that employed the use of legitimate businesses and financial institutions. MIHALO and his co-conspirators successfully converted illegally obtained Bitcoin into over one million U.S. dollars.

19. During the course of the conspiracy, undercover law enforcement agents purchased stolen credit card information using Market A, which was transferred by the co-conspirators to the agents located in the Western District of Missouri.

COUNT ONE
Conspiracy to Commit Access Device Fraud

20. Paragraphs 1 through 19 of this Indictment are incorporated by reference as fully set forth herein.

21. From at least February 22, 2016, through on or about October 1, 2019, in the Western District of Missouri, and elsewhere, the defendants,

MICHAEL MIHALO,

SIMON KAURA, and

TAYLOR ROSS STAATS

did knowingly and intentionally conspire together and with other persons, known and unknown to the Grand Jury, to violate Title 18, United States Code, Sections 1029(a)(1), (2), and (3).

22. It was a part and object of the conspiracy that MIHALO, KAURA, STAATS, and other persons, known and unknown to the Grand Jury, would and did knowingly and with the intent to defraud, traffic in one and more counterfeit access devices, as defined in Title 18, United States Code, Section 1029(e)(2), affecting interstate and foreign commerce, in violation of Title 18, United States Code, Section 1029(a)(1).

23. It was a part and object of the conspiracy that MIHALO, KAURA, STAATS, and other persons, known and unknown to the Grand Jury, would and did knowingly and with the intent to defraud, traffic in one and more unauthorized access devices, as defined in Title 18, United States Code, Section 1029(e)(3), during any one-year period, and by such conduct obtained anything of value aggregating to $1,000 or more during that period, affecting interstate and foreign commerce, in violation of Title 18, United States Code, Section 1029(a)(2).

24. It was a part and object of the conspiracy that MIHALO, KAURA, STAATS, and other persons, known and unknown to the Grand Jury, would and did knowingly and with the intent to defraud, possess fifteen and more devices which were counterfeit and unauthorized access

devices, affecting interstate and foreign commerce, in violation of Title 18, United States Code, Section 1029(a)(3).

OVERT ACTS

25. In furtherance of the conspiracy and to effectuate the objects and purposes of the conspiracy, the following overt acts, in addition to others, were committed in the Western District of Missouri and elsewhere:

a. Between February 22, 2016, and October 1, 2019, MIHALO, KAURA, STAATS, and other persons, known and unknown to the Grand Jury, possessed and sold thousands of stolen credit card numbers and associated information across various darknet markets.

b. On or about February 22, 2016, KAURA created and sent MIHALO a Bitcoin wallet address beginning with "1G6ah…" to facilitate payments from buyers of stolen credit card information on Market B.

c. On or about February 26, 2016, MIHALO directed KAURA to develop what became Market A, stating: "ok, new job…you are on autoshop duty as of right now…. Give me the details of what it will take for an autoshop on tor that can be similar to hat [sic] you see on cardz.cc, but we it better lol."

d. Between on or about February 22, 2016, and July 12, 2018, MIHALO, KAURA, and other persons, known and unknown to the Grand Jury, designed and programmed Market A.

e. By at least April 19, 2016, MIHALO, KAURA, and a co-conspirator publicly launched Market A under the brand name "ALIAS-1."

f. On or about April 20, 2016, KAURA sent MIHALO a Bitcoin wallet address beginning with "13V9h…" to receive payment for programming Market A.

g. On or about May 11, 2016, STAATS offered to help MIHALO run Market A, stating:

> Let's take a step back and evaluate your operation and let's try and structure it to help you.
>
> Job:
> CEO: [Alias associated with MIHALO]
> Web developer: [Alias associated with KAURA]
> Customer service on site: [a co-conspirator]
> Marketing/advertisements: No one
> Customer service on forums no one ([KAURA] + [a co-conspirator] when they can)
>
> What I think you need is another person to help with extra slack. There should be no reason why YOU, the CEO, should be answering noobs pm's. That's not your job. Your job is to make sure that the people running your shit are doing it properly….

h. Between May 1, 2016, and May 31, 2017, STAATS cleaned tens of thousands of cards for sale on darknet markets, including Markets A and B, by other co-conspirators.

i. On or about May 26, 2016, STAATS sent MIHALO a Bitcoin wallet address beginning with "1NMtF…" to receive payment for card cleaning services.

j. On or about May 27, 2016, a co-conspirator registered a domain similar to [ALIAS-1].com with U.S.-based domain name registrar Namecheap.com.

k. On or about June 7, 2016, MIHALO, KAURA, and another co-conspirator launched the Market A Clearnet page site, stating:

> Welcome to the best online market
> Here you will find the "BEST" CVV's CVV2, Fresh cards updated daily, we have been in the business for a really long time our name is very well known over the darknet, we just moved to Clearnet for people who doesnt like to use tor you can still find us @[Market A's web address]
> …
> If you are looking for fresh WORKING and high balance cards, you came to the right place, our prices are reasonable considering the quality of cards we offer, a whole selection of card type including: WORLD CARDS, GOLD, BUSINESS, STRIPE, and many more. Any country you wish, USA, CANADA, UK, Europe.

l. On or about May 27, 2016, a co-conspirator registered an account with a United States-based internet service provider of "proxy" (or Internet relay) services which the co-conspirators used to hide the true IP address of numerous of Market A's mirror sites.

m. Between on or about May 11, 2016, and October 11, 2016, MIHALO transferred digital currency to a U.S.-based digital currency exchange (hereinafter, "Exchange 1").

n. Between on or about May 11, 2016, and October 19, 2016, MIHALO used Exchange 1's services to convert digital currency obtained from access device fraud into U.S. dollars.

o. Between in or about February 2018 and in or about September 2021, MIHALO used another U.S.-based digital currency exchange (hereinafter, "Exchange 2") to convert digital currency into U.S. dollars, and transferred over $1,500,000 from this account to bank accounts in his name.

p. On or about October 24, 2016, MIHALO told Exchange 1, "Bitcoin coming in was a gift from a friend and it grew last year. Stated this several times when asked the last 8 months. If this does not conclude these questions, I will be using another service since I can no longer relay [sic] on [Exchange 1]. I have done nothing wrong, yet now my account is limited with no specifics or reasoning why."

q. On or about March 19, 2021, MIHALO told Exchange 2, "I purchased my Bitcoin in late 2015 via cash from Local Bitcoins on my lunch break. I don't have any purchase information."

r. On or about March 31, 2017, STAATS sent MIHALO approximately 459 cleaned credit card numbers and associated account information, and stated,

> ANY CHANCE I CAN GET PAID TODAY? NEED TO PLACE A RATHER LARGE ORDER AND WOULD LIKE TO DO IT TODAY IF ALL POSSIBLE.
> WOULD $750 BE OK FOR A PAYMENT? IF SO, CAN YOU PLEASE SEND IT TO:
> BTC ADDRESS - 1Nrgz[…]

s. On or about August 9, 2017, MIHALO posted a message on Market A promoting the launch of Market A's "SHOP 2.0":

> SHOP 2.0 GOING LIVE IN 3, 2, 1
> [New web address of Market A]
> PREP YOUR BTC AND BE READY
> BE HERE FOR LINKS IN 2 HOURS AND PASS WORD AROUND

t. On or about April 5, 2018, the co-conspirators transferred the stolen credit card information of T.W. to Market A user "Yomommaknows," an undercover law enforcement agent, located in Kansas City, Missouri.

u. On or about April 16, 2018, the co-conspirators transferred the stolen credit card information of S.F. to Market A user "Yomommaknows," an undercover law enforcement agent, located in Kansas City, Missouri.

v. On or about April 16, 2018, the co-conspirators transferred the stolen credit card information of D.C. to Market A user "Yomommaknows," an undercover law enforcement agent, located in Kansas City, Missouri.

w. On or about April 16, 2018, the co-conspirators transferred the stolen credit card information of R.R., a resident of the Western District of Missouri, to Market A user "Yomommaknows," an undercover law enforcement agent, located in Kansas City, Missouri.

x. On or about May 17, 2018, the co-conspirators transferred the stolen credit card information of M.P. to Market A user "Yomommaknows," an undercover law enforcement agent, located in Kansas City, Missouri.

y. On or about May 17, 2018, the co-conspirators transferred the stolen credit card information of T.W. to Market A user "Yomommaknows," an undercover law enforcement agent, located in Kansas City, Missouri.

z. On or about May 17, 2018, the co-conspirators transferred the stolen credit card information of S.R.T., a resident of the Western District of Missouri, to Market A user "Yomommaknows," an undercover law enforcement agent, located in Kansas City, Missouri.

All in violation of Title 18, United States Code, Section 1029(b)(2).

COUNT TWO
Access Device Fraud

26. Paragraphs 1 through 19 of this Indictment are re-alleged and incorporated by reference as fully set forth herein.

27. From on or about May 18, 2017, to on or about May 17, 2018, the defendants,

MICHAEL MIHALO,

SIMON KAURA, and

TAYLOR ROSS STAATS

with other persons, known and unknown to the Grand Jury, in Jackson County, within the Western District of Missouri and elsewhere, knowingly and with intent to defraud, did and attempted to traffic in and use one and more unauthorized access devices, to wit, payment card account numbers and card verification values during a one-year period, and by such conduct did obtain things of value aggregating $1,000 and more during that period, to wit, Bitcoin and lines of credit associated with payment card account numbers, such conduct affecting interstate and foreign commerce.

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

COUNT THREE
Money Laundering Conspiracy

28. Paragraphs 1 through 19 of this Indictment are re-alleged and incorporated by reference as if fully set forth herein.

29. From on or about February 22, 2016, through at least on or about February 1, 2022, in the Western District of Missouri, and elsewhere, the defendants,

MICHAEL MIHALO,

SIMON KAURA, and

TAYLOR ROSS STAATS

did knowingly combine, conspire, agree, and have a tacit understanding with others known and unknown to the Grand Jury to commit certain offenses against the United States, that is, to knowingly conduct and attempt to conduct financial transactions affecting interstate and foreign commerce, knowing which transactions involved the proceeds of some form of unlawful activity, (1) with the intent to promote the carrying on of specified unlawful activity, in violation of Title 18, United States Code, Section 1956(a)(1)(A)(i), and (2) knowing that the transactions were designed in whole and in part to conceal and disguise the nature, the location, the source, the ownership, and the control of the proceeds of specified unlawful activity, in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i).

30. It is further alleged that the specified unlawful activity included fraud and related activity in connection with access devices in violation of Title 18, United States Code, Section 1029.

All in violation of Title 18, United States Code, Section 1956(h).

COUNTS FOUR through NINE
Money Laundering

31. Paragraphs 1 through 19 of this Indictment are re-alleged and incorporated by reference as if fully set forth herein.

32. On or about the dates set forth below, in the Western District of Missouri and elsewhere, defendant MICHAEL MIHALO, knowingly engaged in, attempted to engage in and

caused to be engaged in, a monetary transaction affecting interstate or foreign commerce, that is, the withdrawal, deposit and transfer of funds via Electronic Funds Transfer from and to the financial institutions identified below, in criminally derived property of a value greater than $10,000 derived from specified unlawful activity, that is, access device fraud, to wit:

Count	Date	From	To	Amount
4	January 28, 2021	Michael Mihalo Wells Fargo Account x-5368 (San Francisco, California)	Michael Mihalo Fidelity NA Account x-2836 (UMB Bank, NA, Kansas City, Missouri)	$25,000
5	January 28, 2021	Michael Mihalo Wells Fargo Account x-5368 (San Francisco, California)	Michael Mihalo Fidelity NA Account x-2836 (UMB Bank, NA, Kansas City, Missouri)	$25,000
6	May 12, 2021	Michael Mihalo Fidelity NA Account x-2836 (UMB Bank, NA, Kansas City, Missouri)	Michael Mihalo Wells Fargo Account x-5368 (San Francisco, California)	$100,000
7	May 13, 2021	Michael Mihalo Fidelity NA Account x-2836 (UMB Bank, NA, Kansas City, Missouri)	Michael Mihalo Wells Fargo Account x-5368 (San Francisco, California)	$100,000
8	May 14, 2021	Michael Mihalo Fidelity NA Account x-2836 (UMB Bank, NA, Kansas City, Missouri)	Michael Mihalo Wells Fargo Account x-5368 (San Francisco, California)	$100,000

9	May 17, 2021	Michael Mihalo Fidelity NA Account x-2836 (UMB Bank, NA, Kansas City, Missouri)	Michael Mihalo Wells Fargo Account x-5368 (San Francisco, California)	$100,000

All in violation of Title 18, United States Code, Sections 1957 & 2.

FORFEITURE ALLEGATION 1

The allegations of this Indictment are re-alleged and incorporated by reference for the purpose of alleging forfeitures pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1029(c)(1)(C).

Upon conviction of the offense in violation of Title 18, United States Code, Section 1029 set forth in Counts One and Two of this Indictment, the defendants shall forfeit to the United States (a) all property, real and personal, used and intended to be used to commit the offense and (b) any property constituting or derived from, proceeds obtained, directly or indirectly, as a result of such violation. The property to be forfeited includes, but is not limited to: a money judgment and the following:

1. The contents of USAA Federal Savings Bank, Account Number: x-5841, held in the name of Michael Mihalo.

2. The contents of Wells Fargo Bank, N.A., Account Numbers: x-5368 and x-6985, held in the name of Michael Mihalo.

3. The contents of Gemini Trust Company, LLC, User ID: x-18, held in the name of Michael Mihalo.

4. The contents of Social Finance Inc., Account Number: x-48-10, held in the name of Michael Mihalo.

5. The contents of Coinbase, Inc., User ID: x-7a15, held in the name of Michael Mihalo.

6. The contents of Fidelity Investments, Account Number: x-2836, held in the name of Michael Mihalo.

7. The Real Property known and numbered as 335 Colonial Circle, Geneva, Kane County, Illinois, with all improvements, appurtenances, and attachments thereon, described as: LOT 91 OF UNIT NO. 4, WILLIAMSBURG, GENEVA, KANE COUNTY, ILLINOIS, IN THE CITY OF GENEVA, KANE COUNTY, ILLINOIS.

If any of the property described above as being subject to forfeiture, as a result of any act or omission of the defendants –

(1) cannot be located upon the exercise of due diligence

(2) has been transferred or sold to or deposited with, a third person;

(3) has been placed beyond the jurisdiction of the Court;

(4) has been substantially diminished in value; or

(5) has been commingled with other property, which cannot be subdivided without difficulty;

the United States of America shall be entitled to forfeiture of substitute property pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18 United States Code,

Section 982(b)(1) and 1029(c)(2) and Title 28, United States Code, Section 2461(c), to seek forfeiture of any other property of defendants up to the value of the above-described forfeitable property.

All pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1029(c).

FORFEITURE ALLEGATION 2

The allegations of this Indictment are re-alleged and fully incorporated herein for the purpose of alleging forfeiture to the United States of America of certain property in which the defendants have an interest, pursuant to the provisions of Title 18, United States Code, Section 982(a)(1), and the procedures outlined in Title 21, United States Code, Section 853.

Upon conviction of any violation of Title 18, United States Code, Section 1956 or Section 1957, defendants shall forfeit to the United States any property, real or personal, involved in such offense, or traceable to such property, pursuant to Title 18, United States Code, Section 982(a)(1).

The property subject to forfeiture includes, but is not limited to, a forfeiture money judgment representing the proceeds obtained by the defendants, in that such sum in aggregate, is involved in, or is derived from, proceeds traceable to the offense set forth in Counts Three through Nine and the following property:

1. The contents of USAA Federal Savings Bank, Account Number: x5841, held in the name of Michael Mihalo.

2. The contents of Wells Fargo Bank, N.A., Account Numbers: x-5368 and x-6985, held in the name of Michael Mihalo.

3. The contents of Gemini Trust Company, LLC, User ID: x-18, held in the name of Michael Mihalo.

4. The contents of Social Finance Inc., Account Number: x-48-10, held in the name of Michael Mihalo.

5. The contents of Coinbase, Inc., User ID: x-7a15, held in the name of Michael Mihalo.

6. The contents of Fidelity Investments, Account Number: x-2836, held in the name of Michael Mihalo.

7. The Real Property known and numbered as 335 Colonial Circle, Geneva, Kane County, Illinois with all improvements, appurtenances, and attachments thereon, described as: LOT 91 OF UNIT NO. 4, WILLIAMSBURG, GENEVA, KANE COUNTY, ILLINOIS, IN THE CITY OF GENEVA, KANE COUNTY, ILLINOIS.

If the property described above as being subject to forfeiture as a result of any act or omission of the defendants,

(1) cannot be located upon the exercise of due diligence;

(2) has been transferred or sold to, or deposited with a third person;

(3) has been placed beyond the jurisdiction of the Court;

(4) has been substantially diminished in value; or

(5) has been commingled with other property which cannot be subdivided without difficulty;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 982(b), to seek forfeiture of any other property of the defendants up to the value of the above-forfeitable property or to seek return of the property to the jurisdiction of the Court so that the property may be seized and forfeited.

All pursuant to the provisions of Title 18, United States Code, Section 982(a)(2) and the procedures outlined in Title 21, United States Code, Section 853(p).

A TRUE BILL.

/s/ Kathleen Shaw
FOREPERSON OF THE GRAND JURY

/s/ Matthew Blackwood
Matthew Blackwood
Assistant United States Attorney

Leigh Farmakidis
Assistant United States Attorney

/s/ Louisa K. Marion
Louisa K. Marion
Senior Counsel
U.S. Department of Justice, Criminal Division
Computer Crime & Intellectual Property Section

Dated: 2/9/2022
Kansas City, Missouri