

UNITED STATES DISTRICT COURT

for the

Northern District of California

FILED

May 14 2021

SUSAN Y. SOONG
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO

United States of America
v.

Joseph James O'Connor

Case No.3:21-mj-70812 MAG

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of July - August, 2020 in the county of San Francisco in the Northern District of California, the defendant(s) violated:

Table with 2 columns: Code Section, Offense Description. Rows include 18 U.S.C. § 371 (Conspiracy), 18 U.S.C. § 1030(a)(2)(C) (Computer Intrusion), 18 U.S.C. § 875(d) (Extortive Communications), 18 U.S.C. § 2261A(2) (Stalking), 18 U.S.C. § 875(c) (Threatening communications).

(See attached sheet for counts and maximum penalties)

This criminal complaint is based on these facts:

See attached affidavit of FBI Special Agent R. Montgomery

Continued on the attached sheet.

Approved as to form /s/ AUSA Andrew F. Dawson

/s/ Complainant's signature R. Montgomery, Special Agent, FBI Printed name and title

Sworn to before me by telephone.

Date: 05/14/2021

Judge's signature

City and state: San Francisco, CA

Hon. Thomas S. Hixson, U.S. Magistrate Judge Printed name and title

Counts and Maximum Penalties:

Counts One, Three, and Five: Conspiracy to commit any offense against the United States, i.e., intentionally accessing a computer without authorization and thereby obtaining information from a protected computer, in violation of 18 U.S.C. § 1030(a)(2)(C), all in violation of 18 U.S.C. § 371.

Penalties: 5 years' prison; 3 years' supervised release; \$250,000 fine; \$100 special assessment per count; restitution; forfeiture.

Counts Two and Four: Computer Intrusion, i.e., intentionally accessing a computer without authorization and thereby obtaining information from a protected computer, in violation of 18 U.S.C. § 1030(a)(2)(C), and aiding and abetting, in violation of 18 U.S.C. § 2

Penalties: 5 years' prison; 3 years' supervised release; \$250,000 fine; \$100 special assessment per count; restitution; forfeiture.

Count Six: Conspiracy to commit any offense against the United States, i.e., intentionally accessing a computer without authorization and with the intent to extort from a person a thing of value, transmitting a communication containing a threat to reveal confidential information or transmitting a communication containing a demand or request for a thing of value in relation to damage to a protected computer where such damage was caused to facilitate the extortion, in violation of 18 U.S.C. § 1030(a)(7), all in violation of 18 U.S.C. § 371

Penalties: 5 years' prison; 3 years' supervised release; \$250,000 fine; \$100 special assessment per count; restitution; forfeiture

Count Seven: Extortive communications, i.e., knowingly transmitting in interstate and foreign commerce, with intent to extort from a person a thing of value, a communication containing a threat to injure the reputation of another person, in violation of 18 U.S.C. § 875(d)

Penalties: 2 years' prison; 3 years' supervised release; \$250,000 fine; \$100 special assessment per count; restitution; forfeiture

Counts Eight and Ten: Stalking, i.e., with the intent to injure, harass, and cause substantial emotional distress to a person in another state, using facilities of interstate and foreign commerce, including an interactive computer service and electronic communication service, to engage in a course of conduct that causes substantial emotional distress to the victim and placed the victim in reasonable fear of death or serious bodily injury, in violation of 18 U.S.C. § 2261A(2)

Penalties: 5 years' prison; 3 years' supervised release; \$250,000 fine; \$100 special assessment per count; restitution; forfeiture

Count Nine: Threatening communications, i.e., knowingly sending a message in interstate and foreign commerce containing a true threat to injure the person of another, in violation of 18 U.S.C. § 875(c)

Penalties: 5 years' prison; 3 years' supervised release; \$250,000 fine; \$100 special assessment per count; restitution; forfeiture

UNITED STATES DISTRICT COURT)

)

NORTHERN DISTRICT OF CALIFORNIA)

**AFFIDAVIT IN SUPPORT OF APPLICATION FOR
ARREST WARRANT AND CRIMINAL COMPLAINT**

I. INTRODUCTION AND AGENT BACKGROUND

I, R. Montgomery¹, being duly sworn, state as follows:

1. I am employed as a Special Agent with the Federal Bureau of Investigation (“FBI”) in San Francisco, California and have been so employed since 2015. I am sworn and empowered to investigate criminal activity involving violations of federal law. I am currently assigned to FBI’s San Francisco Division Criminal Cyber-Crime Squad, which investigates crimes carried out using computers or computer networks. I have participated in numerous interviews of witnesses and have been the affiant of federal search warrants involving suspected criminal violations where records, of the type involved in this investigation, were seized. My investigative experience includes, but is not limited to interviewing subjects, targets and witnesses; executing search and arrest warrants; handling and supervising confidential human sources; conducting surveillance; and analyzing phone records and financial records.

2. This affidavit is made in support of an issuance of an arrest warrant and ten-count criminal complaint alleging that **Joseph James O’Connor** committed:

- Conspiracy to commit any offense against the United States, i.e., intentionally accessing a computer without authorization and thereby obtaining information from a protected

¹ Your affiant seeks to use a first initial throughout the affidavit and complaint due to O’Connor’s involvement in online threats. O’Connor has potentially been linked to additional prior swatting incidents and possibly (although not confirmed and currently still under investigation) the swatting of a U.S. law enforcement officer.

computer, in violation of 18 U.S.C. § 1030(a)(2)(C), all in violation of 18 U.S.C. § 371 (Counts One, Three, and Five);

- Computer Intrusion, i.e., intentionally accessing a computer without authorization and thereby obtaining information from a protected computer, in violation of 18 U.S.C. § 1030(a)(2)(C), and aiding and abetting, in violation of 18 U.S.C. § 2 (Counts Two and Four);
- Conspiracy to commit any offense against the United States, i.e., intentionally accessing a computer without authorization and with the intent to extort from a person a thing of value, transmitting a communication containing a threat to reveal confidential information or transmitting a communication containing a demand or request for a thing of value in relation to damage to a protected computer where such damage was caused to facilitate the extortion, in violation of 18 U.S.C. § 1030(a)(7), all in violation of 18 U.S.C. § 371 (Count Six);
- Extortive communications, i.e., knowingly transmitting in interstate and foreign commerce, with intent to extort from a person a thing of value, a communication containing a threat to injure the reputation of another person, in violation of 18 U.S.C. § 875(d) (Count Seven);
- Stalking, i.e., with the intent to injure, harass, and cause substantial emotional distress to a person in another state, using facilities of interstate and foreign commerce, including an interactive computer service and electronic communication service, to engage in a course of conduct that causes substantial emotional distress to the victim and placed the victim in reasonable fear of death or serious bodily injury, in violation of 18 U.S.C. § 2261A(2) (Counts Eight and Ten); and
- Threatening communications, i.e., knowingly sending a message in interstate and foreign commerce containing a true threat to injure the person of another, in violation of 18 U.S.C. § 875(c) (Count Nine).

| | | |
|-------------|---|--|
| Count One | Conspiracy to intentionally access a computer without authorization and thereby obtain information from a protected computer, in connection with Twitter and Twitter accountholders | 18 U.S.C. § 1030(a)(2)(C), 18 U.S.C. § 371 |
| Count Two | Intentionally accessing a computer without authorization and thereby obtaining information from a protected computer; Aiding and abetting, in connection with TikTok and Victim 1 | 18 U.S.C. § 1030(a)(2)(C), 18 U.S.C. § 2 |
| Count Three | Conspiracy to intentionally access a computer without authorization and thereby obtain information from a protected computer, in connection with TikTok and Victim 1 | 18 U.S.C. § 1030(a)(2)(C), 18 U.S.C. § 371 |
| Count Four | Intentionally accessing a computer without authorization and thereby obtaining information from a protected computer; Aiding and abetting, in connection with Snap and Victim 2 | 18 U.S.C. § 1030(a)(2)(C), 18 U.S.C. § 2 |
| Count Five | Conspiracy to intentionally access a computer without authorization and thereby obtain information from a protected computer, in connection with Snap and Victim 2 | 18 U.S.C. § 1030(a)(2)(C), 18 U.S.C. § 371 |
| Count Six | Conspiracy to intentionally access a computer without authorization and with the intent to extort from a person a thing of value, transmitting a communication containing a threat to reveal confidential information; or transmitting a communication containing a demand or request for a thing of value in relation to damage to a protected computer where such damage was caused to facilitate the extortion, in connection with Snap and Victim 2 | 18 U.S.C. § 1030(a)(7)(B) and (C), 18 U.S.C. § 371 |
| Count Seven | Extortive communications, in connection with Victim 2 | 18 U.S.C. § 875(d) |
| Count Eight | Stalking, in connection with Victim 2 | 18 U.S.C. § 2261A(2) |
| Count Nine | Threatening communications, in connection with Victim 3 | 18 U.S.C. § 875(c) |
| Count Ten | Stalking, in connection with Victim 3 | 18 U.S.C. § 2261A(2) |

3. For the reasons set forth below, there is probable cause to believe that **Joseph James O'Connor** has committed the foregoing violations of federal law.

4. The facts set forth in this affidavit are based on information that I have obtained from my personal involvement in the investigation and from other law enforcement officers who

have been involved in this investigation (including special agents of the Internal Revenue Service and United States Secret Service). This affidavit does not set forth all of my knowledge about this matter; it is intended to only show that there is sufficient probable cause for the requested warrant and criminal complaint.

II. APPLICABLE STATUTES

5. Title 18, United States Code, Section 1030(a)(2)(C), in relevant part, makes it a crime for an individual to intentionally access a computer without authorization or exceed authorized access, and thereby obtain information from a protected computer. Under Section 1030(c)(2)(B), the offense is a felony if “committed for purposes of commercial advantage or private financial gain,” “committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State,” or if “the value of the information obtained exceeds \$5,000.” A “protected computer” means a computer that is used in or affecting interstate or foreign commerce or communication (as defined by 18 U.S.C. § 1030(e)(2)(B)).

6. Title 18, United States Code, Section 1030(a)(7)(B) and (C), in relevant part, makes it a crime for an individual to, with the intent to extort from a person any money or other thing of value, transmit in interstate or foreign commerce any communication containing any threat to impair the confidentiality of information obtained from a protected computer without authorization; or a demand or request for a thing of value in relation to damage to a protected computer where such damage was caused to facilitate the extortion.

7. Title 18, Section 371, makes it a crime for two or more persons to conspire either to commit any offense against the United States or to defraud the United States. Any person who does any act to effect the object of the conspiracy is punishable.

8. Title 18, United States Code, Section 2, in relevant part, provides that whoever aids, abets, counsels, commands, induces, or procures the commission of a federal offense is punishable as a principal.

9. Title 18, United States Code, Section 875(d), in relevant part, criminalizes whoever, with the intent to extort from a person any thing of value, transmits in interstate or foreign commerce any communication containing any threat to injure the property or reputation of a person.

10. Title 18, United States Code, Section 875(c), in relevant part, criminalizes whoever transmits in interstate or foreign commerce any communication containing any threat to injure the person of another.

11. Title 18, United States Code, Section 2261A(2), in relevant part, criminalizes whoever with the intent to kill, injure, harass, intimidate, or place under surveillance with intent to kill, injure, harass, or intimidate another person, uses the mail, any interactive computer service or electronic communication service or electronic communication system of interstate commerce, or any other facility of interstate or foreign commerce to engage in a course of conduct that causes, attempts to cause, or would be reasonably expected to cause substantial emotional distress to a person.

III. DEFINITIONS

12. I know from my training and experience as a Special Agent with the FBI that the following definitions apply to the activity discussed in this affidavit:

13. **Server**: A server is a computer that provides services to other computers. Examples include web servers which provide content to web browsers and email servers which act as a post office to send and receive email messages.

14. **Domain**: “Domain” is short for “domain name.” Under 18 U.S.C. § 3559(g)(2)(B), the definition of “domain name” is based on the Trademark Act, under 15 U.S.C. § 1127. Under the Trademark Act, “domain name” means “any alphanumeric designation which is registered with or assigned by any domain name registrar, domain name registry, or other domain name registration authority as part of an electronic address on the Internet.” A “subdomain” is a subdivision of a domain.

15. **Domain Name System**: The Domain Name System (“DNS”) is a hierarchical and decentralized Internet service that translated domain names into Internet Protocol (“IP”) addresses. A “top-level domain” is the last segment (i.e., suffix) in a domain (e.g., “.com” or “.net”) associated with the highest level of the DNS.

16. **Registrar & Registrant**: “Registration” is the act of reserving a domain on the Internet for a specific time period. In order to do so, the “domain registrant” would usually apply online to a company that managed the reservation of Internet domain names, known as a registrar. A “registrar” operates in accordance with the guidelines of the designated organizations that managed top-level domains, known as registries. The domain name registrant is bound by the terms and conditions of the registrar with which it registered its domain name, for instance adhering to a certain code of conduct or indemnifying the registrar and registry against any legal or civil action taken as a result of use of the domain name.

17. **Bitcoin**: Bitcoin is a type of virtual currency, circulated over the Internet as a form of value. Bitcoin is not issued by any government, bank, or company, but rather is generated and controlled through computer software operating via a decentralized, peer-to-peer network. Bitcoin is just one of many varieties of virtual currency.

18. **Bitcoin exchangers**: Exchangers are persons or entities in the business of exchanging fiat currency (currency that derives its value from government regulation or law, such as the U.S. dollar) for bitcoin, and exchanging bitcoin for fiat currency. When a user wishes to purchase bitcoin from an exchanger, the user will typically send payment in the form of fiat or other convertible virtual currency to an exchanger, usually via wire or ACH, for the corresponding number of bitcoin based on a fluctuating exchange rate. The exchanger, often for a commission, will then typically attempt to broker the purchase with another user of the exchange that is trying to sell bitcoin, or, in some instances, will act as the seller itself. If the exchanger can place a buyer with a seller, then the transaction can be completed. Based on my training and experience, bitcoin exchanges send confirmation emails to the email account used to register the member exchange

account for each deposit, trade, and/or withdraw bitcoin and fiat transactions conducted by the user on the exchange.

19. **Bitcoin address**: Bitcoin addresses are the particular virtual locations to which bitcoin are sent and received. A Bitcoin address is analogous to a bank account number and is represented as a 26-to-35-character-long case-sensitive string of letters and numbers.

20. **Private key**: Each bitcoin address is controlled through the use of a unique corresponding private key, a cryptographic equivalent of a password needed to access the address. Only the holder of an address's private key can authorize a transfer of Bitcoin from that address to another Bitcoin address.

21. **Bitcoin wallet**: A bitcoin wallet is an application that holds a user's bitcoin addresses and private keys. A bitcoin wallet also allows users to send, receive, and store bitcoins. It is usually associated with a bitcoin address.

22. **Blockchain**: All bitcoin transactions are recorded on what is known as the blockchain. The blockchain is essentially a distributed public ledger that keeps track of all bitcoin transactions, incoming and outgoing, and updates approximately six times per hour. The blockchain records every bitcoin address that has ever received bitcoin and maintains records of every transaction and all the known balances for each bitcoin address. As a result, forensic analytical tools are able to review the blockchain, identify which bitcoin addresses are related and owned by the same individual or entity (called a cluster), and calculate the total number of bitcoins in all of these related bitcoin addresses.

23. **SIM Swapping**: SIM swapping is a type of account takeover fraud that generally targets weaknesses in authentication mechanisms targeting mobile telephones, allowing criminals to take over a victim's telephone and its communications. Criminals will generally change the SIM card associated with a victim's account and/or telephone number with a SIM card the criminal controls. Once the SIM card is changed, the criminal controls the victim's telephone number.

24. **Swatting**: Swatting is the act of illegally calling law enforcement to report a false emergency at a target location with the intent to create a tactical response by law enforcement.

Individuals will often “swat” others to seek revenge for a grievance or to instill fear in others, which has resulted in multiple deaths across the United States where law enforcement mistakenly shot and killed innocent people after false information was reported.

IV. FACTS ESTABLISHING PROBABLE CAUSE IN SUPPORT OF THE ARREST WARRANT AND CRIMINAL COMPLAINT

A. TWITTER HACK

1. Background – Twitter Hack and Transfer of Funds to and from Scam Address

25. Twitter, Inc. (“Twitter”) operates a microblogging and social networking service used by hundreds of millions of users, including politicians, celebrities, and musicians. Many such high-profile individuals have “verified” their accounts by proving to Twitter they are indeed the real person named on the account.

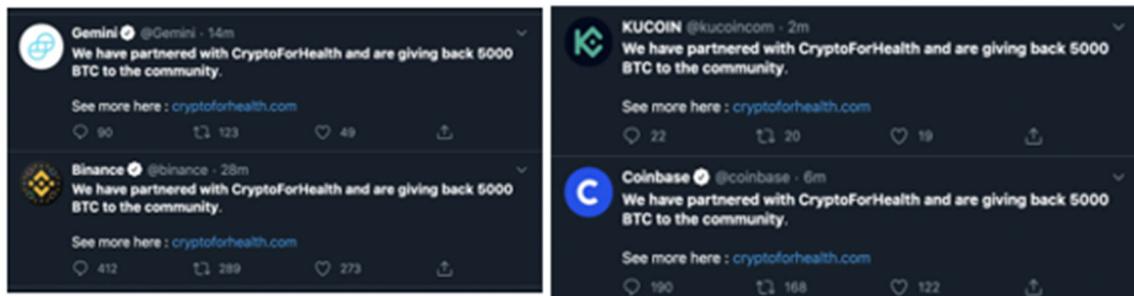
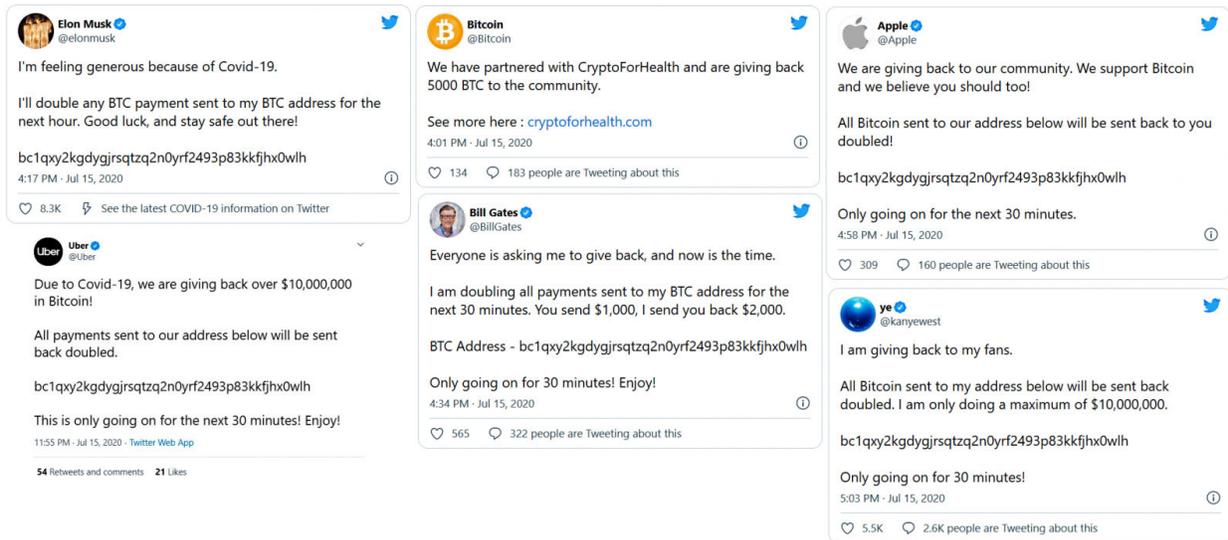
26. On July 15, 2020, approximately 130 Twitter accounts were compromised. This includes multiple high-profile verified accounts, including those of Bill Gates, Elon Musk, Kanye West, Joe Biden, Barack Obama, Jeff Bezos, Mike Bloomberg, Warren Buffett, Benjamin Netanyahu, and Kim Kardashian. Accounts belonging to cryptocurrency exchanges, such as Binance, Gemini, Coinbase, Bitfinex, and AngeloBTC were also compromised, as were prominent companies like Apple Inc. and Uber Technologies Inc. For a subset of those accounts, the attackers were able to gain control of the accounts and send tweets from those accounts. The servers hosting the data for at least some of the affected accounts are located in the Northern District of California.

27. Many of the compromised accounts posted messages directing victims to send cryptocurrency to various accounts, including the bitcoin address “bc1qxy2kgdygjrstzq2n0yrf2493p83kkfjhx0wlh” (hereinafter, the “Scam Address”), which received approximately \$117,000 in 415 transfers. Two other bitcoin addresses were also posted on some Twitter accounts: “bc1q0kznuxzk6d82e27p7gplwl68zkv40swyy4d24x” and “bc1qwr30ddc04zqp878c0evdrqfx564mmf0dy2w39l”, which both received approximately

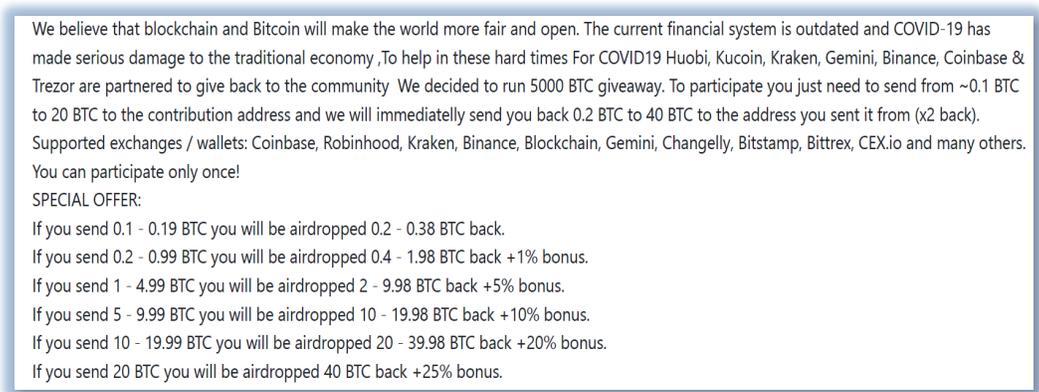
\$6,700 in 100 transactions. However, the primary bitcoin address known to be directly associated with the Twitter hack is the Scam Address.

28. In some of the Twitter posts, the actor(s) provided the actual bitcoin address, while in others the posts guided victims to a website hosted at the domain cryptoforhealth.com, which also provided the same bitcoin address. In all of these cases, the Twitter postings said that individuals who sent any bitcoin to the aforementioned address would receive double the bitcoin in return. Multiple individuals and companies confirmed publicly and/or to the FBI that their accounts had been hacked and they did not post messages directing individuals to send them bitcoin.

29. Below are screen captures of some of the Twitter posts from the compromised accounts related to sending cryptocurrency to the bitcoin address and directing users to a link to a website hosted at the domain cryptoforhealth.com.



30. The website hosted at cryptoforhealth.com led to a webpage that, like the other Twitter posts, directed individuals to send bitcoin to the Scam Address, in exchange for twice the amount of bitcoin deposited in return. Though the cryptoforhealth.com website was taken down as of July 16, 2020, the below image from the website was taken from an archive of the site on the “Wayback Machine”²:



31. Blockchain analysis reveals that between July 15, 2020, when the hack of the verified Twitter accounts occurred, and July 16, 2020, the bitcoin wallet associated with the Scam Address had conducted approximately 426 transfers.

32. Approximately 415 of those transfers consisted of transfers from other bitcoin addresses into the Scam Address account, totaling approximately 12.86 bitcoin, worth approximately \$117,457.58 as of July 16, 2020 (at a rate of \$9,133.56 per bitcoin). Eleven (11) of those transfers were from the wallet associated with the Scam Address to other bitcoin addresses, siphoning off approximately 99.74% of the bitcoin deposited, or 12.83 bitcoin, worth \$117,183.57, leaving a remaining balance of \$274.01 in the account. No bitcoin was returned to the victims.

33. In my training and experience, individuals will shuffle bitcoin from one wallet to another in order to obfuscate its origin. Based on my training and experience, I believe the above-described transfers out of the origin bitcoin wallet to other addresses were intended to conceal the origin of the funds.

² Archive of cryptoforhealth.com on July 15, 2020, WAYBACK MACHINE, https://web.archive.org/web/*/cryptoforhealth.com (last visited Jul. 16, 2020).

34. I believe that the actor(s) who controlled the cryptoforhealth.com domain and the Scam Address hacked popular, and trusted, verified Twitter accounts for high-profile individuals and companies—including those belonging to cryptocurrency exchanges. I further believe that the same actor(s) used those trusted, now hacked, accounts to post messages, reaching those Twitter accounts' followers, with an offer to double their bitcoin—both directly, and via a message posted on the website hosted at the domain cryptoforhealth.com—in order to entice individuals into sending bitcoin to the Scam Address. The individual(s) then stole the bitcoin, and transferred it out of the account.

2. Juvenile 1 Sold Access to Hacked Twitter Accounts

35. From the investigation, I believe that Juvenile 1³ played a central role in the compromise of Twitter on July 15, 2020. I further believe that Juvenile 1 used the moniker “Kirk#5270” in the course of the commission of the compromise. On July 31, 2020, Juvenile 1 was arrested in connection with his/her role in this offense. Pursuant to the Juvenile Delinquency Act, Juvenile 1 was referred to the State Attorney for the 13th Judicial District in Tampa, Florida for further proceedings.

36. Pursuant to search warrants signed by U.S. Magistrate Judge Sallie Kim in the Northern District of California on July 17, 2020, and July 19, 2020, Discord, Inc.⁴ provided the content of Discord messaging accounts, which included Discord chats between Juvenile 1 utilizing the username “Kirk#5270” and others.

³ The identity of Juvenile 1 is known to your affiant. On or about July 30, 2020, Juvenile 1 was charged by criminal complaint in the Northern District of California in relation to this investigation. Pursuant to the Juvenile Delinquency Act, juvenile proceedings in federal court are sealed to protect the identity of the juvenile. That complaint was subsequently dismissed in favor of prosecution by state authorities in Florida. Juvenile 1 was charged in the State of Florida for violating the following Florida criminal offenses: Unauthorized Access to a Computer System (F.S. 815.06(2)(a) and (3)(b) 2.), “Scheme to Defraud” Florida Communications Fraud Act (F.S. 817.034(4)(a)1), “Communications Fraud”).

⁴ Discord is a free voice over internet protocol (“VoIP”) application and digital distribution platform. It was initially designed for the video gaming community but has since expanded to a wider audience. Discord offers chat channels where users can communicate via text messages, voice, and video.

37. Among the content provided by Discord were communications sent by Juvenile 1 (as “Kirk#5270”) to multiple individuals in which Juvenile 1 represented that he/she could reset, swap, and control any Twitter account at will, and would do so in exchange for bitcoin transfers. For example, in one Discord chat on July 15, 2020, Juvenile 1 stated, “I work for Twitter” and “I can claim any name, let me know if you’re trying to work.” Juvenile 1 also sent images of an internal administrative tool used by Twitter to make changes to user accounts.

38. The individuals with whom Juvenile 1 communicated included an individual identified as Nima Fazeli⁵ who used the Discord moniker “Rolex#0373” and an individual identified as Mason Sheppard⁶ (using the moniker “ever so anxious#001”). Upon receiving the image of the Twitter internal tool, Fazeli responded, “I’m in,” and Juvenile 1 responded with a bitcoin address: “1Ai52Uw6usjhpcDrwSmkUvjuqLpcznUuyF” (hereinafter, the “Kirk#5270 Address”). Based on my training and experience, I understand this to be a bitcoin address used to send and receive bitcoin payments and that Juvenile 1 (using the “Kirk#5270” moniker) was requesting payment via bitcoin for access to Twitter accounts. Juvenile 1 provided Sheppard (using the moniker “ever so anxious#001”) with images of administrator-level access to Twitter accounts “@bumblebee,” “@sc,” “@vague,” and “@R9,” among many others.

39. Based on the chats as a whole, it appears that Juvenile 1 used Fazeli, Sheppard, and others as proxies, or middle-men, to help Juvenile 1 find buyers for Twitter usernames in exchange for a fee. For instance, Sheppard (using the moniker “ever so anxious#001”) wrote to Juvenile 1 (using the moniker “Kirk#5270”), “I have a buyer rn”, “someone’s interested”, and “i have a buyer for 50 for 3k u down?” I believe these messages were meant to communicate to Juvenile 1 that Sheppard had a buyer ready (i.e. “right now” or “rn”) to purchase Twitter usernames—50 usernames for \$3,000 (“50 for 3k”). Among the discussions, Sheppard wrote, “send your bitcoin addy too,” to which Juvenile 1 provided the Kirk#5270 Address. Juvenile 1 mentioned the

⁵ On or about July 30, 2020, Nima Fazeli was charged by criminal complaint in the Northern District of California in connection with this investigation and was arrested on July 31, 2020.

⁶ On or about July 30, 2020, Mason Sheppard, a U.K national, was charged by criminal complaint in the Northern District of California in connection with this investigation.

Kirk#5270 Address approximately sixteen times throughout the chat in discussions about payment for accounts. Sheppard asked Juvenile 1 about the accounts “@vampire,” “@xx,” and “@dark”. Per information provided to the FBI by Twitter, the accounts of “@vampire,” “@xx,” and “@dark” were compromised on July 15, 2020. As discussed in paragraph 78, an individual I believe to be **O’Connor** asked Sheppard if “@vampire” was available for purchase.

3. Juvenile 2’s Statements on the Role of the Individual using the Shinji and PlugwalkJoe Monikers in the Twitter Hack

40. On July 21, 2020, federal agents executed a search warrant authorized by U.S. Magistrate Judge Alex G. Tse at a residence in the Northern District of California. Among the occupants of the home was a juvenile (hereinafter “Juvenile 2”). Juvenile 2 was believed to be a Discord user who assisted Juvenile 1 and Sheppard in selling access to Twitter accounts related to the July 15, 2020 Twitter hack. Upon execution of the search warrant, Juvenile 2 agreed to be interviewed. Juvenile 2 admitted to law enforcement agents that he/she was the Discord user who was identified in chats as assisting the user of Discord moniker “Kirk#5270” in the sale of illegal Twitter access. Juvenile 2 admitted that he/she worked with Sheppard, whom Juvenile 2 knew by the name “Mason,” to sell Twitter account access through Juvenile 1.

41. When asked whether Juvenile 2 was familiar with the name “**Joseph O’Connor**,” Juvenile 2 stated that he/she knew that individual to be a hacker and thought that he/she may have messaged that individual once. When asked about the Twitter handle “@shinji,” Juvenile 2 stated that it was common knowledge that the “@shinji” handle was an online moniker used by the individual he/she had referred to as the hacker. Juvenile 2 stated that during the time period of the Twitter hack, that individual had communicated with Juvenile 2 over Discord for access to a particular Twitter account.

42. On July 24, 2020, Juvenile 2 was interviewed again by the FBI. When Juvenile 2 was asked how he/she knew **O’Connor**’s full name, Juvenile 2 stated that he/she learned it from reading a news article online. When asked about the individual who used the “@shinji” Twitter account, Juvenile 2 conveyed that the individual also utilized the online moniker of “plugwalkjoe.”

Juvenile 2 stated that that the individual identified as “plugwalkjoe” was known amongst the OGUUsers⁷ community to have previously perpetrated the hacking of a Twitter account and put the text “plugwalkjoe” in a Twitter message that was associated with the hack. Juvenile 2 stated that during the course of the July 2020 Twitter hack, that individual had discussed purchasing Twitter accounts with Juvenile 2 and had stated that he had purchased the “@6” account earlier that day. The individual that Juvenile 2 was chatting with inquired about a few different Twitter accounts including Donald Trump’s account. Juvenile 2 added Juvenile 1 into a group chat with that individual in order for the individual to communicate directly with Juvenile 1. Juvenile 1 refused to engage in the chat and told Juvenile 2 not to add him/her to that chat. Juvenile 2 stated that he/she recalled the individual to be using a Discord username that contained the word “insane.” As noted below, a Discord account that was believed to be used by **O’Connor** contained the word “insane” at one point.

43. On August 26, 2020, Juvenile 2 was interviewed by the FBI pursuant to a federal proffer agreement, with Juvenile 2’s defense attorney present. Juvenile 2 provided more detail about his/her chat with the individual discussed above. On the morning of July 15, 2020, that individual made contact with Juvenile 2 via the Discord account with the “insane” username, introducing himself as “Joe.” Included in the chat were two other parties, though Juvenile 2 could not recall their names. Part of the conversation was via text, but Juvenile 2 also spent approximately 20 minutes in a voice call with the individual via Discord. Juvenile 2 described the individual’s voice as having a distinct and recognizable British or Australian accent. Juvenile 2 previously viewed a video posted online by the “@shinji” Twitter account of the “@shinji” user speaking, and Juvenile 2 believed the voice from the “@shinji” account matched the voice of the individual he/she spoke with via Discord. Throughout the text and voice conversations, the individual inquired about purchasing multiple single-letter Twitter accounts, which I am aware are status symbols among individual seeking short single letter, digit or word account names. The

⁷ OGUUsers is an online forum that has been abused by criminal networks who trade in stolen social media credentials.

individual also asked Juvenile 2 about an account associated with “BTS,” a Korean musical group. The individual stated that he wanted to obtain this account to post a “shout-out” to one of the individual’s Instagram accounts identified as “@kpop.”⁸ At the conclusion of the interview after discussing a number of topics not related to **O’Connor**, FBI agents played Juvenile 2 a portion of the recorded call more fully described below in paragraph 113 and asked Juvenile 2 to indicate whether any of the voices in the recording sounded familiar. Within seconds of the recording being played, Juvenile 2 indicated the voice sounded like the individual he/she had the 20-minute call with over Discord.

44. I have reviewed records provided to the FBI by Facebook regarding the Instagram account of “@kpop.” The account was registered on November 5, 2019, using the email address of reactjoe1337r@protonmail.com. The account was logged into via IP addresses 185.230.124.52 and 195.206.107.147, among others, which have been utilized by **O’Connor** to login to his other accounts, as demonstrated below in paragraph 123. I believe the term “react” used within the email address is likely a reference to **O’Connor**’s relationship to the REACT Task Force, as explained below.

4. Juvenile 1’s Statements about the Twitter Hack and the Involvement of the Individual using the Online Moniker PlugwalkJoe

45. As mentioned above, on or about July 30, 2020, Juvenile 1 was charged related to the Twitter hack. On August 25, 2020, and August 28, 2020, Juvenile 1 was interviewed by a law enforcement officer from the Florida Department of Law Enforcement and federal agents while in custody, pursuant to State and Federal proffer agreements. Juvenile 1’s defense attorney was also present.

46. Juvenile 1 admitted to his/her involvement in the Twitter hack, admitted that he/she was the only individual in control of the Kirk#5270 account, and that he/she had received cryptocurrency into bitcoin addresses controlled by Juvenile 1.

⁸ I believe “kpop” to be a reference to “K-Pop,” a term used to describe Korean popular music.

47. Juvenile 1 also stated that in conducting the attack, he/she had worked directly with other individuals to sell access to Twitter accounts. Juvenile 1 contacted individuals on the OGUUsers online forum and communicated with them via Discord to serve as middlemen in finding buyers for Juvenile 1. It was the intention that these buyers would pay bitcoin in exchange for access to compromised Twitter accounts. Juvenile 1 stated that individuals that he/she worked with as proxies included “LOL” (known now to law enforcement as Juvenile 2, as discussed above), “Rolex” (known now to law enforcement as Nima Fazeli, as discussed above), “Chaewon,” also known as “ever so anxious,” (known now to law enforcement as Mason Sheppard, as discussed above), and “Verdict.” Juvenile 1 took screenshots of images of the Twitter administrative tools, which Juvenile 1 then shared with middlemen and/or buyers. Juvenile 1 stated that among other services he/she offered, Juvenile 1 offered to update the actual Twitter account with a new e-mail address provided by the buyer, allowing the buyer to directly access the Twitter account. Juvenile 1 said he/she and co-conspirators earned approximately \$40,000 by providing this service, paid in bitcoin.

48. Per Juvenile 1, Juvenile 1 was connected through either “LOL” or “ever so anxious” to an individual he/she referred to as “plugwalkjoe” and **Joseph O’Connor**, though Juvenile 1 did not clarify how he/she came to learn the full name for the individual. Juvenile 1 was asked by either “LOL” or “ever so anxious” to make changes to the “@6” Twitter account. Those changes included changing the display name to “pwj” and changing the profile picture to an anime picture. Juvenile 1 understood “pwj” to stand for “plugwalkjoe.” Juvenile 1 stated that he/she did not sell the “@6” account and that **O’Connor** was not involved in the hacking of Twitter, but Juvenile 1 confirmed that the requested changes to the display name and profile picture were made at the request of “LOL” or “ever so anxious.”

B. IDENTIFICATION OF JOSEPH JAMES O’CONNOR’S ROLE IN THE TWITTER HACK

1. Identification of Joseph James O’Connor and his Statements Related to his Role in the Twitter Hack

49. There is probable cause to believe that **Joseph James O’Connor** conspired with Juvenile 1 and others to benefit from the compromise of Twitter accounts from the July 15, 2020 hack.

50. Per information provided by D.B.,⁹ Criminal Investigator for the Santa Clara District Attorney, and C.T.,¹⁰ Criminal Investigator for the Santa Clara District Attorney, and members of the REACT Task Force,¹¹ REACT began receiving tips in late 2018 regarding the illegal activity of an individual using the online moniker “PlugwalkJoe,” purportedly identified as **O’Connor** from the United Kingdom. In or about January 2019, an individual claiming to be **O’Connor** reached out to C.T. C.T. was aware of an individual he believed to be **O’Connor** who had contacted a person who had been arrested and charged by REACT in unrelated criminal activity. That individual contacted the arrestee in jail, and C.T. reviewed those recorded calls, matching the voice to the individual who contacted him in or about January 2019. The individual who contacted C.T. initially identified himself to C.T. as “PlugwalkJoe.” That individual continued to periodically contact C.T. via text and over the phone using multiple different Google Voice¹² telephone numbers. C.T. eventually asked the individual what the individual’s true-life identity was, which the individual provided as **Joseph O’Connor**. Based on C.T.’s prior interactions with this individual since January 2019, C.T. believed that he knew that individual’s voice and believed it to be a distinctive voice and accent. Based on conversations with that individual, who as noted,

⁹ The full name of D.B. is known to your affiant but is redacted from this affidavit for the protection of the individual.

¹⁰ The full name of C.T. is known to your affiant but is redacted from this affidavit for the protection of the individual.

¹¹ The REACT Task Force is the Regional Enforcement Allied Computer Team located in Santa Clara, California. The REACT Task Force is a partnership of local, state, and federal agencies formed to combat the escalating problem of high technology crime.

¹² Google Voice is a VoIP (voice over internet protocol) phone service offered by Google LLC.

identified himself as **Joseph O'Connor**, C.T. learned from the individual that he used the moniker “pwj,” and that he had moved to Spain due to death threats he received related to other illegal activity in which he was involved.

51. After the July 15, 2020 Twitter hack became public, C.T. received a series of text messages from the individual he believed to be **O'Connor** who was using the telephone number 304-745-0329. In the initial text message, the sender said, in part, “Hey, its joe,” and later stated, “Kirk#5270 this is the twitter hacker.” The individual who C.T. believed to be **O'Connor** subsequently called the REACT Task Force general number from 678-685-9876 at 1:54 PM PDT on July 22, 2020, and left a voicemail. C.T. informed me he listened to the voicemail and believed the voice on the voicemail to be the same as the individual who had previously identified himself as **O'Connor**. The caller identified himself as “Joe” and “pwj” and requested to be contacted at 678-685-9876. The caller stated it was regarding the Twitter hack and that he had nothing to do with it. Additionally, on July 22, 2020, a message was submitted via REACT’s online tip line. The submission form listed the name as “pwj,” the email address as daisymorrowphamsc53@gmail.com, the associated IP address as 195.206.107.147, a message that provided the telephone number 678-685-9876, and requested someone to “text me on my new GV [Google Voice] please.” I believe “pwj” to be shorthand for “plugwalkjoe.” Furthermore, I am aware that the IP address 195.206.107.147 is associated with other accounts that I believe have been used by **O'Connor**, as discussed below.

52. On July 23, 2020, C.T. and FBI agents called the individual who had previously identified himself as **O'Connor** at phone number 678-685-9876. C.T. informed the individual that the FBI was on the telephone and wished to speak with him. The individual agreed to speak with the FBI along with C.T. and the interview was audio recorded. Throughout the interview, the individual was referred to by investigators as “Mr. O'Connor” and “Joe,” though at no point did agents ask the individual to identify his full name. The individual, however, did refer to his online moniker “PlugwalkJoe.” The individual provided the following information regarding the July 15, 2020 Twitter hack. The individual stated that he had been in a chat with two people, the user who

I know to be Juvenile 2,¹³ and the user who I know to be Mason Sheppard—who the individual identified as “Mason” and “ever so anxious.” The individual inquired with Sheppard about purchasing some Twitter accounts, and Sheppard agreed to get the individual accounts to resell for a profit. Either Juvenile 2 or Sheppard sent the individual a picture of the Twitter administrative tools, which the individual subsequently posted on Twitter. The individual denied purchasing the Twitter account “@6” but confirmed the account name was changed to “pwj” and the account avatar was also changed, all at his request. The individual admitted to speaking with an individual he referred to as “Kirk” (Juvenile 1) once in a group chat. During the interview, the individual referred to his online moniker, “PlugwalkJoe,” being used in “shout-outs” he received from various accounts. For example, the individual denied being involved in the hack of Twitter CEO Jack Dorsey’s Twitter account but stated he received a “shout-out” tweet during the hack saying “unsuspend plugwalkjoe.” Furthermore, the individual stated he communicated with individuals who hacked the Twitter account of Internet personality Logan Paul in September 2018 who said they would give the individual a “shout-out” on Paul’s Twitter account, which included the name “PlugwalkJoe”, as referenced in paragraph 61. After the interview, C.T. informed me the voice of the individual interviewed matched the voice of the individual he had spoken with since early 2019 who had identified himself as **O’Connor**.

53. I have reviewed records provided to the FBI by Google regarding the Google Voice telephone number of 304-745-0329. The number is registered to “Sueann Bergnaum” using the email address of bergnaumsueann@gmail.com. The current subscriber started utilizing the telephone number on May 18, 2020. Subscriber information for bergnaumsueann@gmail.com shows the account was created on May 6, 2020. The email account was logged into via the IP addresses of 45.152.183.29, 141.98.252.169, and 195.206.107.147, which have been utilized by **O’Connor** to login to his other accounts, as demonstrated below in paragraph 123.

¹³ As discussed, Juvenile 2 is an individual who assisted Juvenile 1 and Sheppard in selling access to Twitter accounts related to the July 15, 2020 Twitter hack. Following a search warrant on the residence of Juvenile 2, Juvenile 2 agreed to be interviewed and has continued providing information with the FBI.

54. I have reviewed records provided to the FBI by Google regarding the Google Voice telephone number of 678-685-9876. The number is registered to “Daisey Morrow” using the email address of daisemorrowphamsc53@gmail.com. The current subscriber started utilizing the telephone number on June 20, 2020. Subscriber information for daisemorrowphamsc53@gmail.com shows the account was created on June 12, 2020. On July 17, 2020, the email account was logged into via the IP address 91.207.175.216. As demonstrated below in paragraph 59, this IP address is linked to “@PlugwalkJoe” Twitter account, which is one of **O’Connor**’s online accounts.

55. Based on my training and experience, I know cyber criminals register numerous email accounts with fake registration information in order to obfuscate the true identity of the individual utilizing the account. As such, I believe the above email accounts were registered with fake information to obfuscate the identity of the user.

2. Use of Virtual Private Networks by O’Connor in Accessing Various Accounts

56. As explained more fully below, the accounts utilized by **O’Connor** to commit the criminal activity described herein were logged into via multiple IP addresses associated with M247 and other Virtual Private Network (VPN) providers. A VPN is a means for an individual to connect to the Internet. The user’s device connects to the VPN, and then the VPN connects to Internet via its own IP addresses.¹⁴ By using a VPN, a user can mask his/her own IP address when accessing Internet sites, because the Internet sites can only see the IP address associated with the VPN. I believe, based on my training and experience, that **O’Connor**’s use of VPNs was for the purpose of obfuscating his physical location. It should be noted that online accounts discussed in this affidavit are password-protected and typically only one individual has access to a given account. While these IP addresses were hosted by VPNs that could potentially be used by hundreds or thousands of different users at the same time, the timestamps for the accounts accessed by

¹⁴ An “IP address” is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication.

O'Connor reveal that he accessed several of these accounts on the same day, frequently within minutes or seconds of each other. Given how close in time these accounts were accessed from the same IP address, I believe that **O'Connor** was the individual accessing each of these accounts. While the specific IP addresses used to login to each account will be stated, the timestamps associated with those logins will be provided later through a visual representation.

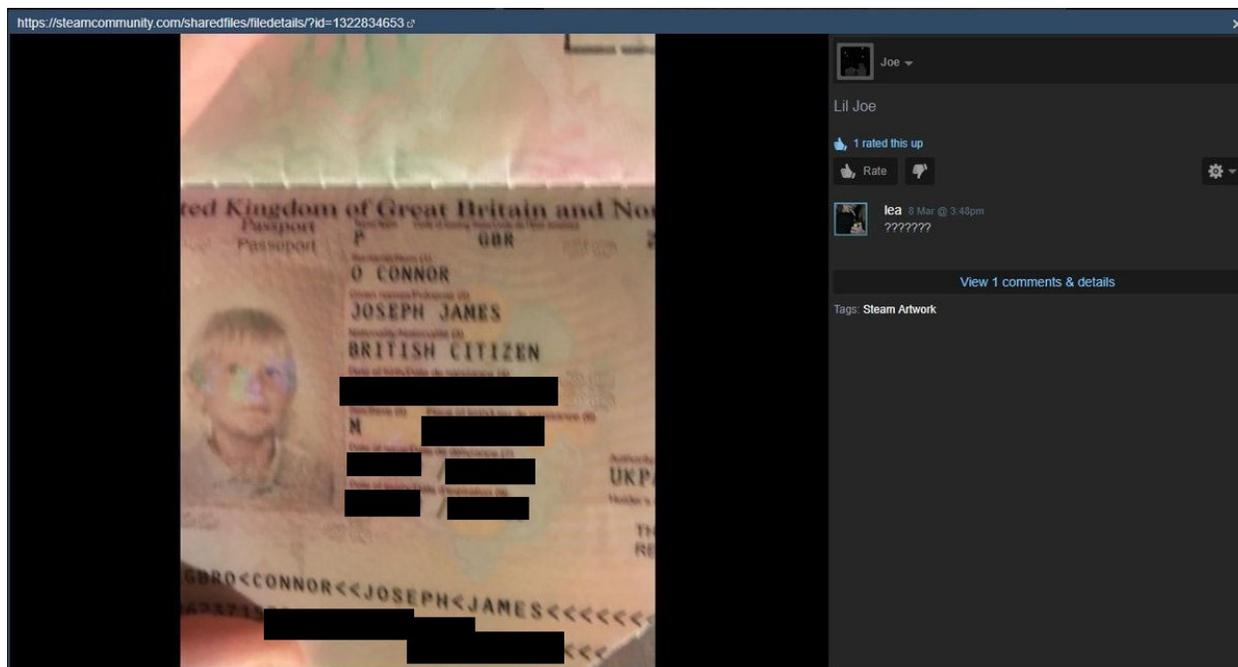
57. It should also be noted that users of VPN services are given the ability to select a location from which to generate their IP address. Users will often select a location close to their actual location to improve the speed of the Internet connection and reduce latency. For example, a user physically located in Spain is likely to choose an IP address originating near Spain. VPN providers have a specific number of IP addresses for each location, and choosing the same location over and over again over a long period of time will likely result in the same IP address being assigned to the same user multiple times.

3. PlugwalkJoe Twitter Account and J.OConnor99 Snapchat Account are Connected to United Kingdom Citizen Joseph James O'Connor

58. I have reviewed records provided by Investigator D.B. of the REACT Task Force. The records were obtained pursuant to a search warrant signed by Judge Charles E. Wilson, Superior Court of Santa Clara County, compelling Twitter to provide records pertaining to, among several other accounts, the Twitter account of “@PlugwalkJoe” from the time period of January 1, 2017, to January 11, 2019. The account was registered on April 12, 2018, to the email address smurferino13378@gmail.com.

59. The “@PlugwalkJoe” Twitter records included IP address login activity, which showed the account was accessed via 91.207.175.216 on November 28, 2018 and via 81.92.206.45 on January 8, 2019 . There is IP overlap between these IP addresses and other accounts with the offenses in this case. For example, the IP address of 91.207.175.216 was also used on July 17, 2020 to access the email account that is associated with the 678-685-9876 Google Voice number. That Google Voice number was used in a phone conversation with me and the individual who referred to himself as “PlugwalkJoe.” Additionally, the IP address of 81.92.206.45 was used to

access the j.oconnor99 Snapchat account on the same day as the “@PlugwalkJoe” Twitter account. The Twitter records also included a tweet created by “@PlugwalkJoe” on May 4, 2018, stating “Here is my real childhood pics @piugwalkjoe.”¹⁵ The tweet included an image, as pictured below, of a United Kingdom passport for **Joseph James O’Connor**, listing a date of birth and place of birth. The passport number, however, was outside the picture frame. I am aware, based on my conversations with the National Crime Agency of the United Kingdom, that **O’Connor** has a date of birth and place of birth that match the information in the passport image tweeted on May 4, 2018, by “@PlugwalkJoe.”



60. On August 2, 2018, “@PlugwalkJoe” published a tweet that included a video approximately 54 seconds long. C.T. informed me he believed the voice in the video matched the voice he knew to be the individual he has spoken with who has identified himself as **O’Connor**.

61. On September 22, 2018, “@PlugwalkJoe” sent a direct message to another Twitter user. The message included an image of Logan Paul’s Twitter account with a tweet from September 11, 2018, stating, in part, “Follow @plugwalkjoe.” “@PlugwalkJoe” sent more direct

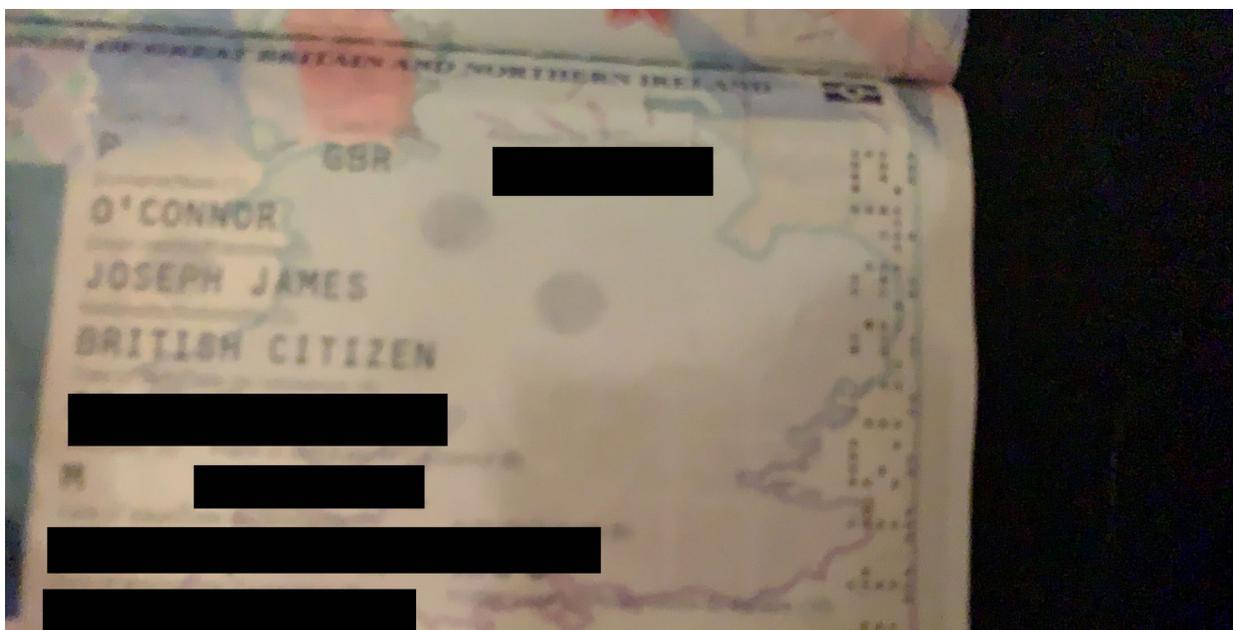
¹⁵ I believe that the reference to “@piugwalkjoe” was a typographical error that was intended as “@plugwalkjoe.”

messages referencing the hack of Logan Paul's Twitter account, one on September 30, 2018, stating, "oh that's when I hacked logan paul," and another on December 11, 2018, stating, "she had no followers until I hacked @loganpaul and shouted her out." As discussed earlier in paragraph 52, when I spoke with the individual who referred to himself as "PlugwalkJoe" and who had previously identified himself as "**Joseph O'Connor**" to C.T., that individual stated that he had communicated with the individuals who hacked Logan Paul's account in September 2018 and that they would give him a "shout-out."

62. Additionally, I have reviewed records provided to the FBI by the Portland Police Bureau in Portland, Oregon. The records were obtained pursuant to a search warrant signed in December 2019 by a Judge in the Circuit Court of the State of Oregon for Multnomah County, compelling Snap, Inc. to provide any and all records pertaining to the Snapchat account of "j.oconnor99" ("J.OConnor99 Snapchat account"). The J.OConnor99 Snapchat was registered on October 14, 2015, had a registered email address of radarg1@hotmail.com, and a display name of "joseph." The Snapchat records included IP address login and logout activity, which showed the account was logged out of via 185.230.124.52 on November 26, 2019, via 194.99.104.27 on November 25, 2019, and via 37.120.148.86 and 194.99.104.29 on November 23, 2019. On January 8, 2019, the account was logged into via 81.92.206.45. This IP address activity, as noted below in paragraph 123, matches activity associated with **O'Connor**'s other online accounts.

63. The Snapchat records also included a photograph from the account's "memories"¹⁶ section. The "memory," which was from August 30, 2019, was a photograph of a United Kingdom passport for **Joseph James O'Connor**, listing a date of birth, place of birth, and passport number. I am aware, based on my conversations with the National Crime Agency of the United Kingdom, that **O'Connor** has a date of birth, place of birth, and United Kingdom passport number that match the information in the passport image from the Snapchat account.

¹⁶ I understand Snapchat "memories" to be a searchable and shareable archive of a user's photos to which the Snapchat user has access.



64. The J.OConnor99 Snapchat account contained an audio file from September 12, 2019. The audio consists of an individual saying the words “plug walk joe.” The account also contained a video file from December 1, 2019. The video shows an individual walking and talking about taking the “rubbish” out “featuring plug walk.” C.T. informed me he believed the voice in the audio file and video file matched the voice he knew to be the individual he has spoken with who has identified himself as **O’Connor**.

4. **PlugwalkJoe Twitter Account Replaced by Shinji Twitter Account, Which is Used during the Twitter Hack**

65. Pursuant to a search warrant signed by U.S. Magistrate Judge Sallie Kim in the Northern District of California on July 19, 2020, Twitter, Inc. provided the content of the Twitter account “@shinji” to agents. The account’s display name was “joseph.”

66. In multiple messages sent from the “@shinji” account, the user referred to himself as “PlugwalkJoe.” For example, in a direct message sent by the account on January 1, 2020, “@shinji” stated “follow plugwalkjoe new twit @shinji he will follow back old followers.” I believe that “@shinji” was communicating with his “followers” from his “@PlugwalkJoe” account to let them know that he had replaced his “@PlugwalkJoe” account and was now using the “@shinji” account on Twitter. Similarly, in another direct message sent on January 30, 2020,

“@shinji” stated, “tell her you know plugwalkjoe.” Based on this communication, I understand that the user of the “@shinji” account was referring to himself as “plugwalkjoe.”

67. On July 4, 2020, “@shinji” sent a direct message with a link to a video. The video is approximately 29 seconds long and contains audio of an individual speaking. C.T. informed me that he listened to the audio of the video and he believed the voice in the video from the “@shinji” account matched the voice he knew to be the individual he has spoken with who has identified himself as **O’Connor**.

68. On July 15, 2020, “@shinji” received a direct message from the Twitter user ID of 1247923305149054977¹⁷ which included an image of what I know to be the internal Twitter administrative tool. The administrative tool was accessing the Twitter account of “@arceus,” which was compromised as noted below in paragraph 69. Further, on July 15, 2020, the user of “@shinji” posted a public message, which included the aforementioned image of the internal Twitter administrative tool accessing the “@arceus” account, along with an image of the tool accessing the account of “@b.” The text of the tweet stated, “twitter admin tools be like.”

69. Based on information provided to the FBI by Twitter, Twitter indicated the evidence pointed to the account of “@shinji” as having been utilized by an accomplice or an actual individual who compromised Twitter’s internal systems. Twitter made this determination based on the timeline of the attack on Twitter, records from Twitter indicating that the “@shinji” account viewed a number of Twitter accounts, and that only the active accounts viewed by “@shinji” were subsequently compromised in the attack. Additionally, if “@shinji” viewed an account that was suspended, the account was not accessed via the internal Twitter tools. Twitter had no evidence that “@shinji” was compromised in any way and “@shinji” was active throughout the entire compromise of Twitter. I believe this activity, in light of the evidence discussed above, indicates that the user of “@shinji” would view an account in order to determine if the account was suspended or active, and then inquire with middlemen about purchasing those accounts. The

¹⁷ Based on publicly available tools that convert Twitter user IDs to Twitter screen names, on August 19, 2020 at 5:32 PM, the user ID of 1247923305149054977 was associated with the Twitter screen name @nakitama.

following is a non-exhaustive example of Twitter accounts viewed by “@shinji,” when those accounts were subsequently taken over by the attacker, or if the account was merely accessed by the attacker with no account take over initiated:

| Date and Time (UTC) | Twitter Profile Viewed by @shinji | Timestamp of Password Reset During Incident (UTC) |
|---------------------|-----------------------------------|---|
| 7/15/2020 13:37:30 | lost | Accessed by attacker during incident, but no account takeover |
| 7/15/2020 13:38:08 | w | 7/15/2020 17:08:00 |
| 7/15/2020 13:44:16 | dark | 7/15/2020 16:13:00 |
| 7/15/2020 13:45:59 | alone | Accessed by attacker during incident, but no account takeover |
| 7/15/2020 13:51:03 | vampire | Accessed by attacker during incident, but no account takeover |
| 7/15/2020 14:11:08 | y | 7/15/2020 12:49:00 |
| 7/15/2020 19:17:29 | binance | 7/15/2020 18:41:00 |
| 7/15/2020 20:10:28 | 6 | 7/15/2020 17:23:00 |
| 7/15/2020 22:52:50 | mrbeastyt | 7/15/2020 21:37:00 |
| 7/15/2020 22:54:46 | arceus | 7/15/2020 22:13:00 |

70. As referenced in paragraph 78, the following records from Discord show the timing of when the Discord account username “Deleted User 93949#7739,” which I believe to be used by **O’Connor**, inquired with Sheppard about Twitter accounts:

| Date and Time (UTC) | Message Sender | Message |
|---------------------|-------------------------|--------------------|
| 7/15/2020 13:38:59 | Deleted User 93949#7739 | i want @6 |
| 7/15/2020 13:41:26 | Deleted User 93949#7739 | how much for @lost |
| 7/15/2020 13:42:44 | Deleted User 93949#7739 | was y in active |
| 7/15/2020 13:46:13 | Deleted User 93949#7739 | @alone |
| 7/15/2020 13:51:11 | Deleted User 93949#7739 | @vampire is lovked |

71. Following these communication between O’Connor and Sheppard, as discussed in paragraph 77, Sheppard then relayed O’Connor’s interest in purchasing “@6” to Juvenile 1 (using the moniker “Kirk#5270”) and requested that the display name be changed to “pwj”.

72. The “@shinji” account’s most recent login IP addresses were 194.99.104.27, 194.99.104.29, 194.99.104.28, 89.26.241.130, 185.230.124.52, 37.120.148.86, 185.230.124.51, 89.26.241.86, and 185.230.124.50, which all match those used to login to the Discord account of “Deleted User93949#7739.” As discussed previously, these IP addresses are assigned to VPN servers operated by M247 and may be used by more than one individual at any given time. As

noted, other individuals involved in the Twitter hack also used Internet Service Providers commonly associated with VPNs like M247.

5. Use of Discord Accounts “Deleted User 93949#7739” and “beyond insane#7739” During the Twitter Hack

73. As discussed in paragraph 36, pursuant to legal process, Discord provided records to agents including subscriber information and chat communications between multiple individuals involved in the lead up to the Twitter compromise. In chats produced by Discord, an individual believed to be **O’Connor**, using the username “Deleted User 93949#7739,” communicated with Juvenile 1 (“Kirk#5270”). Prior to the account name being changed to “Deleted User 93949#7739,” this account went through several name changes. Specifically, the account was named “beyond insane#7739” from July 10, 2020, to July 15, 2020 at 19:43 UTC. The account was renamed again twice before finally being renamed “Deleted User 93949#7739” on July 15, 2020, at 22:13 UTC. The account now identified as “Deleted User 93949#7739” was registered to the email address of jcodiscord++@protonmail.com. Login IP address history shows “Deleted User 93949#7739” was accessed via the IP address of 194.99.104.27, which resolves to Spain, and is assigned to a VPN server operated by M247.

74. On July 15, 2020, Discord user “TEDx#2252” sent a message to “Deleted User 93949#7739” and asked “plugwalkjoe?” “Deleted User 93949#7739” responded, “sure. What you need.” I believe Discord user “TEDx#2252” was confirming that “Deleted User 93949#7739” was “PlugwalkJoe.” “Deleted User 93949#7739” responded positively, confirming he was indeed “PlugwalkJoe.”

75. “Deleted User 93949#7739” also participated in a group chat with Discord user “New acc (haha)#1234” and Juvenile 1 on July 15, 2020, the day of the Twitter hack. Based on my review of the conversation provided by Discord, “Deleted User 93949#7739” appears to have deleted almost all of his communications. However, during the course of the chat, Juvenile 1 provided “Deleted User 93949#7739” with the Kirk#5270 Address and stated, “send money and @s...send the money and ill get ur shit done.” Discord user “New acc (haha)#1234” later stated,

“WE NEED TO SNITCH BRO WE NEED TO SNITCH ON KIRK.” In one undeleted message, “Deleted User 93949#7739” asked, “why you scam” to Juvenile 1. Metadata of this specific conversation showed “Deleted User 93949#7739” contributed approximately 160 lines of the 700 lines of communication in the conversation, however, nearly all of the conversation was deleted. I believe the individual using the “Deleted User 93949#7739” account deleted other chats with Juvenile 1 that were incriminating but did not delete the message “why you scam” to appear as an innocent bystander who was upset by Juvenile 1’s crimes, when in fact “Deleted User 93949#7739” was actually involved in the conversation and in the scheme.

76. On July 15, 2020, Sheppard, using the Discord moniker “ever so anxious#0001,” said to “Deleted User 93949#7739,” “hi joe its mas u need twits.” Sheppard later indicated he sold “@38 @drug and a few others so far.” “Deleted User 93949#7739” responded, “il pay more.” “Deleted User 93949#7739” asked, “can he do susd accts or nah” and Sheppard responded, “nah not suspended.” “Deleted User 93949#7739” said, “I want @6.” Sheppard replied, “I tried it, itnwas axtive 6hr ago.”

77. In separate Discord communications between Sheppard (using the moniker “ever so anxious#0001”) and Juvenile 1 (using the moniker “Kirk#5270”), Sheppard relayed the interest of “pwj” in acquiring the “@6” Twitter account. Sheppard asked Juvenile 1 to change the account avatar (referred to as “avi”) and the display name to “pwj”. Portions of the chat are excerpted below:

| Date and Time | Message Sender | Message |
|----------------------------|----------------------|--|
| 2020-07-15 13:06:15.429000 | ever so anxious#0001 | would u do @6 10k |
| 2020-07-15 17:27:17.264000 | Kirk#5270 | i have @6 ready with password |
| 2020-07-15 17:32:12.392000 | ever so anxious#0001 | he asked if u can put this the avi on 6 with pwj on the display nmae LOL |
| 2020-07-15 17:32:25.121000 | Kirk#5270 | not on the avi |
| 2020-07-15 17:32:33.845000 | Kirk#5270 | that's weird |
| 2020-07-15 17:32:48.400000 | Kirk#5270 | updated pwj |
| 2020-07-15 17:32:49.080000 | Kirk#5270 | though |
| 2020-07-15 17:34:25.988000 | ever so anxious#0001 | he said can u make this avi |

| | | |
|----------------------------|----------------------|------------------------------------|
| 2020-07-15 17:34:57.343000 | Kirk#5270 | Done |
| 2020-07-15 18:07:18.877000 | Kirk#5270 | can you list @6 for me |
| 2020-07-15 18:07:31.943000 | ever so anxious#0001 | the guy i was telling u abt before |
| 2020-07-15 18:07:33.806000 | ever so anxious#0001 | will buy it |
| 2020-07-15 18:07:36.435000 | Kirk#5270 | ok |

78. In continued chats between “Deleted User 93949#7739” and Sheppard, “Deleted User 93949#7739” asked “how much for @lost. Like 3k?” Sheppard responded, “6k bin¹⁸ he wants.” Additionally, “Deleted User 93949#7739” also inquired about “@alone,” “@0,” and “@vampire” before the chat ended. I believe this conversation between “Deleted User 93949#7739” and Sheppard shows “Deleted User 93949#7739” engaging and negotiating with Sheppard for Twitter accounts hacked by Juvenile 1 utilizing Sheppard as an intermediary. As discussed in paragraph 39, Sheppard relayed the request of “Deleted User 93949#7739” for the account “@vampire” to Juvenile 1, and Twitter confirmed to FBI that this account was accessed. Also as discussed in paragraph 69, the “@shinji” Twitter account viewed the accounts “@lost,” “@vampire,” and “@alone.” I know from my training and experience that these short Twitter handles because short “original” (or “OG”) Twitter handles are seen as status symbols and are desirable. During this conversation, Sheppard identifies “Deleted User 93949#7739” as “Joe.”

79. Further, in a chat that occurred on July 12, 2020, between “Deleted User 93949#7739” and Discord user “leana#9873,” “Deleted User 93949#7739” stated, “I live in spain im@from England tho.” I am aware from information learned during the course of this investigation that **O’Connor** is a U.K. citizen from England, who was believed to have been living in Spain.

80. The user of the “Deleted User 93949#7739” account also demonstrated inside knowledge about the hack of Twitter. On July 15, 2020 at 22:02:30 UTC, in a conversation with an unknown user who deleted his/her side of the chat, “Deleted User 93949#7739” stated, “twit tools uses slak,” “idk what hes saying honestly,” and “slak as leverage for company vpn.” I believe the term “slak” to be a reference to Slack, a business communication platform developed by Slack

¹⁸ I believe the term “bin” to be a common shorthand for “Buy It Now.”

Technologies, Inc. and utilized by Twitter and other companies. Twitter provided information to the FBI indicating that as part of the hack of Twitter, Twitter employees were socially engineered via Slack and a follow-up telephone call which directed employees to a fraudulent VPN website that was used to steal login credentials. These statements evidencing “Deleted User 93949#7739”’s knowledge of this method of compromise preceded the first time it was publicly reported in the media.

6. Overlapping IP Addresses Indicating O’Connor’s Use of Other Relevant Discord Accounts

81. I have reviewed chats produced to the FBI by Discord related to the accounts “richest discord user#4558,” “Deleted User 6y56yh#1943,” “you disgust me#8223,” and “sick in the head#1461,” among others. All four of these accounts are registered to email addresses with similar naming conventions as the email address registered to “Deleted User 93949#7739.”¹⁹ Additionally, all four of these accounts have substantial IP overlap with each other and/or with other accounts discussed above, specifically, “Deleted User 93949#7739” and “@shinji.”

82. On July 5, 2020, the individual using the Discord account “richest discord user#4558” provided the Twitter account “@shinji” in response to a question from another Discord user who asked for his Twitter account. On July 15, 2020 the individual using “sick in the head#1461” stated, “follow me on Twitter @6.” As discussed previously, on July 15, 2020, in a Discord chat between “Deleted User 93949#7739” and Sheppard, “Deleted User 93949#7739” requested the Twitter account “@6,” and Sheppard relayed this request to Juvenile 1 and asked Juvenile 1 to change the display name to “pwj.” On June 30, 2020, “you disgust me#8223” responded, “joe,” to a question from another user who asked who it was. Additionally, on June 30,

¹⁹ “richest discord user#4558” is registered to the email address of jocodiscord+@protonmail.com; “you disgust me#8223” is registered to the email address of joco2019+++++++@protonmail.com; “Deleted User 6y56yh#1943” is registered to the email address of jocodiscord@protonmail.com; and “sick in the head#1461” is registered to the email address of joco2019+++++++@protonmail.com. As discussed in paragraph 73, “Deleted User 93949#7739” is registered to the email address of jocodiscord++@protonmail.com.

2020, the individual using the account “you disgust me#8223” was told “see u around joe” by another user.

7. Summary

83. Based on the above information, I believe O’Connor conspired with others to access the computers of Twitter to gain access to certain Twitter accounts and obtain information. As discussed earlier, **Joseph O’Connor** admitted to FBI that the account name for Twitter account “@6” was changed to “pwj” at his request. Juvenile 1 and Juvenile 2 both discussed the role of **O’Connor** in requesting access to certain Twitter accounts, including the “@6” Twitter account and that the “@6” account was changed to “pwj” at **O’Connor**’s request. Among other overt acts, **O’Connor** using Twitter account “@shinji” viewed multiple Twitter profiles, and then using Discord account “Deleted User 93949#7739,” inquired with Sheppard about purchasing those accounts. Sheppard, in turn, relayed **O’Connor**’s interest in those accounts to Juvenile 1, including the account “@6.”

C. O’CONNOR’S INVOLVEMENT IN HACKING VICTIM 1’S TIKTOK ACCOUNT

84. As background, I know from public sources that a U.S.-based victim (hereinafter “Victim 1”) is known to operate a specific TikTok²⁰ account (hereinafter “Victim 1’s TikTok”). “Victim 1’s TikTok” account is one of the most viewed and followed accounts on TikTok. Per publicly available media reporting, Victim 1’s TikTok was accessed without authorization and taken over on or about August 15, 2020. Per those media reports, the TikTok username was changed to “joeandzak1” and the biography section of the account was changed to include the message of “plugwalkjoe zak n crippin.” In addition, multiple videos were posted to the account

²⁰ TikTok is a video-sharing social networking service owned by ByteDance. It is used to create short music, lip-sync, dance, comedy, and talent videos of 3 to 15 seconds, and short looping videos of 3 to 60 seconds. Videos can be shared or stored publicly or privately. The TikTok app allows users to interact with each other through comments to videos, direct messages, and live chats.

during the time it was compromised. Pursuant to records lawfully obtained from TikTok, the account was taken over on or about August 14, 2020, from 23:55:11 UTC to on or about August 15, 2020, 00:47:43 UTC.

85. On or about January 27, 2021, I spoke with a representative of TikTok regarding the compromise of Victim 1's TikTok. Additionally, pursuant to a search warrant signed by U.S. Magistrate Judge Laurel Beeler in the Northern District of California on February 4, 2021, TikTok provided the content of Victim 1's TikTok from during the time period around its compromise. Information from TikTok revealed that the account was compromised and subsequently accessed via a web browser using the IP address 212.102.49.185. The first mobile device to access the account during the compromise was also used to access the TikTok account identified with the username of "JoeComplex" ("JoeComplex TikTok account"). The JoeComplex TikTok account was created using a process that links the TikTok account with a Twitter social media account and was accessed via the IIP address of 212.102.49.251 on or about August 16, 2020. The Twitter account used to create the JoeComplex TikTok account had the Twitter account ID of 1182402251920478213.

86. A TikTok representative further clarified that users of TikTok are able to use valid Twitter accounts to create and log into a TikTok account. In order to create a TikTok account using a Twitter account, the user must log into their Twitter account to create the TikTok account. This creates a validated link between the Twitter account and newly created TikTok account, establishing valid ownership of each account. The user is then able to access the newly created TikTok account when logged into their Twitter account.

87. I have reviewed subscriber records lawfully provided to the FBI by Twitter regarding the Twitter account ID of 1182402251920478213. The account was created on or about October 10, 2019, had a username of "yoongi," and a registered email address of yoongicontact@protonmail.com ("Yoongi Twitter account"). Additionally, the Yoongi Twitter account was accessed approximately 11 times via the IP address of 212.102.49.251, the same IP address used to access the JoeComplex TikTok account. The Yoongi Twitter account was also

accessed via 212.102.49.185, the same IP address used to access Victim 1's TikTok and the Instagram account "@j0e" discussed in paragraphs 85 and 100.

88. Pursuant to the search warrant referenced above for the Twitter account "@shinji", I have located evidence attributing the "@yoongi" Twitter username to **O'Connor**. For example, in direct messages sent by the "@shinji" account on or about May 18, 2020, and June 12, 2020, "@shinji" stated, in part, "I own @yoongi." This information confirms **O'Connor** was the user of the Yoongi Twitter account that was used to register the JoeComplex TikTok account.

89. Further evidence demonstrates **O'Connor**'s access to Victim 1's TikTok. Pursuant to search warrants signed by U.S. Magistrate Judge Jacqueline Scott Corley in the Northern District of California on September 29, 2020 and U.S. Magistrate Judge Laurel Beeler in the Northern District of California on February 24, 2021, the FBI reviewed material that had been produced to law enforcement by Snap, Inc.²¹ for the content of the Snapchat account "dog" ("Dog Snapchat account"). The account was created on February 27, 2012, and had a registered email address of joeisadog@protonmail.com.

90. Images and communications from the Dog Snapchat account contained multiple screenshots of the "@shinji" Twitter account, references to "PlugwalkJoe," and screenshots of chats involving the Discord usernames of "sick in the head" and "beyond insane." Further, the Dog Snapchat account contained hundreds of images, audio files, and video files of the user of the account, which I know to be consistent with the voice and appearance of **O'Connor**.

91. The Dog Snapchat account also contained chat messages and images related to the compromise of Victim 1's TikTok. On or about July 29, 2020, the Snapchat user "yupcal" sent the Dog Snapchat account several chat messages. These chats contained the names of several well-known individuals, along with telephone numbers. On or about August 6, 2020, the "yupcal" account sent a message to the Dog Snapchat account and stated, "I got [Victim 1] number too

²¹ Snapchat, provided by Snap, Inc., is a messaging application for mobile phones with Apple's iOS operating system and Google's Android operating system. Snapchat offers various ways for users to communicate with each other.

now...she's sprint." The user of the Dog Snapchat account then provided the names of individuals whom I believe to be Victim 1's parents. The user of "yupcal" then stated, "if you do her and get her tiktok s/o my twit gonna charge phone for a bit @speaker is twit." I believe that the user of "yupcal's" request for a "s/o" refers to "shout-out," that his or her Twitter account "@speaker" be published by Victim 1's TikTok account while it was compromised. As discussed below, during the compromise of Victim 1's TikTok, a video was posted during which there was an individual who stated follow "@speaker" on Twitter.

92. On or about August 14, 2020, the user of the Dog Snapchat account sent a screenshot to "yupcal" containing an image of Victim 1's TikTok account profile page. The screenshot contained an "Edit profile" button in the center of the image, which indicates the individual had the ability to make changes to the profile. Having the ability to make changes to a profile requires an individual to have logged into the TikTok account. Possession of this image by the user of the Dog Snapchat account indicates the accountholder, believed to be **O'Connor**, was involved in the compromise of Victim 1's TikTok.

93. Evidence obtained from Victim 1's TikTok further implicates **O'Connor** as being responsible for hacking Victim 1's TikTok. As discussed previously, pursuant to a search warrant, TikTok provided agents with the content of Victim 1's TikTok during the time period around its compromise. Subscriber records for the account show it was logged into via the IP address of 212.102.49.185 on August 14, 2020, at 23:55 UTC and August 15, 2020, at 00:01 UTC. As shown below, the Instagram account of "@j0e" was accessed via the same IP address around the same time.

94. In one video posted to Victim 1's TikTok on August 15, 2020, the video showed the notepad application on a computer screen with links to two Discord chats. The text stated, "Join these discords for [Victim 1] nudes #plugwalkwashere." The audio of the video was of a male voice with a British accent saying, "yo, join these servers man. Plug walk." I believe the voice in the video is the same voice known to me to belong to **O'Connor**.

95. In multiple other videos, a male voice with a British accent can be heard speaking. The voice in each video is the same voice known to me to belong to **O'Connor**. One such video, posted on August 15, 2020, was of the Twitter page for “@speaker.” The same voice can be heard saying, “yo. Shout out to my boy Cal on Park Lane, for real. Follow @speaker on Twitter. I’ll give you [Victim 1’s] number or nudes. Whatever you want, bro.” I believe this video was posted based on the request the Snapchat user “yupcal” made to the Snapchat user “dog” mentioned above. Another video was posted with the caption “#fyp plug walk joe.” The video was of a diamond encrusted watch with the same individual saying, in part, “Zak and Joe up in this bitch, man.”

96. Based on the above information, I believe **O'Connor** was involved in discussions of specific high-profile social media accounts, including Victim 1’s TikTok account, to compromise and take over. I know individuals who perform account takeovers will typically utilize SIM swapping to perform that takeover. The reference to Victim 1’s telephone number on Sprint by “yupcal” suggests a plan to conduct a SIM swap. Further, I believe that the request by “yupcal” for a “s/o” refers to a “shout-out,” and was therefore a request by the user of “yupcal” that his/her Twitter account be published by Victim 1’s TikTok while it was compromised. That request was fulfilled by the individual who took over the account, an individual whose voice I know to be **O'Connor**’s. Also, the reference to “Joe,” “Plug Walk Joe,” and “Plug Walk” are references to **O'Connor**’s first name and his moniker. Further, as stated by TikTok, the first access to Victim 1’s TikTok was completed by the same device that accessed the JoeComplex TikTok account, which was created using the Yoongi Twitter account, which I know **O'Connor** controlled. Based on these facts, there is probable cause to believe that **O'Connor** was involved of the hacking of Victim 1’s TikTok. Among other overt acts, **O'Connor** accessed Victim 1’s TikTok using a device and IP address that associated with other **O'Connor** accounts, posted videos on Victim 1’s TikTok that referred to **O'Connor**’s moniker “Plugwalk Joe,” and communicated with others before and during the compromise of Victim 1’s TikTok about the plan to access Victim 1’s account.

D. O’CONNOR’S INVOLVEMENT IN HACKING VICTIM 2’S SNAPCHAT ACCOUNT AND SUBSEQUENT EXTORTION ATTEMPTS

97. As background, I know that a U.S.-based victim (hereinafter “Victim 2”) who is a public figure operates a Snapchat account (hereinafter “Victim 2’s Snapchat”). In June 2019, Victim 2 was the victim of an account compromise in which his/her Snapchat account was hacked, nude photographs were taken from the account, and attempts were made by the hackers to extort Victim 2 in exchange for a post by Victim 2 thanking the hackers using their monikers.

98. During the review of the search warrant returns of the J.OConnor99 Snapchat account referenced above in paragraph 62, the Portland Police Bureau (“PPB”) identified nude photographs of Victim 2 within the account. I have reviewed these records and found the following evidence.

99. On June 13, 2019, at 21:11 UTC, the user of the J.OConnor99 Snapchat account sent a video of a screen recording from an iPhone on the Vodafone UK network with the clock set to 22:06 (indicating it was in a UTC + 1 time zone, which covers the United Kingdom and a portion of Spain), using a VPN, of an iPhone receiving a stream of notifications from the Snapchat app.



Seconds later, the J.OConnor99 Snapchat account sent a screenshot to another individual of Victim 2's Snapchat profile page, which showed that the user was logged in. A screenshot of this Snapchat profile page would only be obtainable by someone with access to the account. In the following minutes, the J.OConnor99 Snapchat account sent nude photographs of Victim 2 to multiple people. An hour and a half later, on June 14, 2019 at 1:31 UTC, the J.OConnor99 Snapchat account received a screenshot of a post from Victim 2's account stating that viewers should "Add j.oconnor99 on Snapchat for [Victim 2] nudes he's dropping them on story at 20 k adds." In another screenshot of a newspaper article in DailyMail.com, which was sent to the J.OConnor99 Snapchat account, Victim 2's Snapchat account posted "Will drop nudes if 5000 of you follow @PlugwalkJoe."



She shared a set of screenshots of the explicit images she said the hacker was threatening her with.

'Here's the photos he's been threatening me with, in other words here's my bobbies. So here f*** u, and the last 24 hours I have been crying instead of celebrating my book while doing my book press,' she wrote.

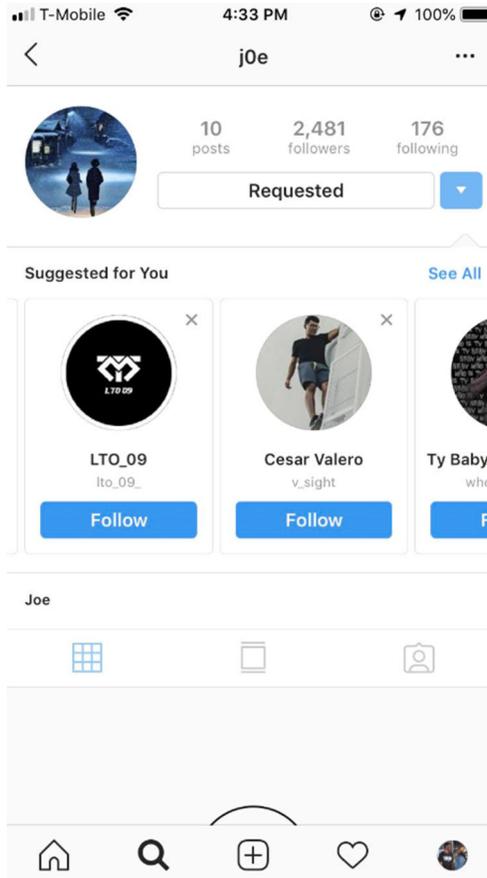
Daily Thomas Fisher
In the state of California it is illegal to distribute intimate photos without the subject's consent and can result in up to six months' jail time and a fine of up to \$1,000

DailyMail.com

DailyMail [Subscribe](#)

100. Victim 2's Snapchat account also posted the below screenshot of the Instagram account "@j0e" ("j0e Instagram account"). Pursuant to records from Instagram, the j0e Instagram account was logged into, among others, via the IP addresses of 185.230.124.52, 194.99.104.29, 37.120.148.86, 212.102.49.251, 185.210.219.154, and 212.102.49.185.²² Victim 2's Snapchat account was accessed on June 13, 2019, via the IP address of 185.210.219.154 two times. The j0e Instagram account was accessed minutes later via this same IP address.

²² Records additional indicated that j0e Instagram was registered on January 9, 2018, and had registered email addresses of ssssmufmanlndfjgijhjh33711+++@protonmail.com and ssssmufmanlndfjgijhjh33711@protonmail.com.



101. On June 14, 2019, the J.OConnor99 Snapchat account sent nine nude photographs and four nude videos of Victim 2 to Snapchat user “cute”. On June 15, 2019, at 8:35 UTC (9:35 in the time zone of the screenshot creator), “cute” sent a screenshot to the J.OConnor99 Snapchat account of a text conversation between a telephone number and an individual who stated he/she had hacked Victim 2’s account. I am aware that the telephone number belongs to Victim 2. In the message, Victim 2 stated, “Feels so weird someone I don’t know looking at my personal shit.” The hacker responded, “listen Do the tweet n we good? It’ll be the entire internet looking at your personal shit.. just do my tweet.”

102. PPB referred the matter to the Los Angeles Police Department (“LAPD”) based on Victim 2’s location. LAPD interviewed Victim 2 on March 4, 2020, and on March 17, 2021, I conducted a follow-up interview with Victim 2. Victim 2 reported the following information. On June 14, 2019, Victim 2 received a text message that stated, “yo [Victim 2] this is the hacker from

yday I got your nudes from yday but I won't show anyone or leak them if you just tweet out like 'I was hacked yesterday, thanks to the hackers @MyUsername for giving me my accounts back.'" The individual later stated, "the tweet would be this 'I was hacked yesterday, thanks to @NuBLoM, Debug and PlugwalkJoe for giving me my accounts back.'" Victim 2 also asked for proof the individual possessed photographs of him/her, and the individual sent Victim 2 a nude photograph of him/her. The individual also sent nine additional pictures, containing nude images of Victim 2 that matched the images sent by the J.OConnor99 Snapchat account to "cute".

103. On June 15, 2019, Victim 2 posted on Twitter that he/she had been "threatened with my own nudes," and Victim 2 posted screenshots of the text message with the individual who had extorted him/her. Victim 2 stated that he/she would release the photographs so that the individual would not be able to "take yet another thing from me." The screenshots of the text messages showed a phone number. On June 15, 2019, at 15:07 UTC, "cute" told the user of the J.OConnor99 Snapchat account, "[He/She] leaked my GVoice [Google Voice]."

104. Victim 2 reported to law enforcement that he/she lost service on his/her phone for about six hours the day before he/she was contacted by the hacker. He/she contacted the phone carrier and recovered access to his/her phone. Victim 2 provided me with screenshots of his/her entire text message conversation with the attacker. A portion of these text message communications matched the screenshot shared with the J.OConnor99 Snapchat account by "cute" referenced above.

105. In addition to the references to accounts and monikers known to be used by O'Connor, including the J.OConnor99 Snapchat account, @PlugwalkJoe, and the j0e Instagram account, there was also overlapping IP records for Victim 2's Snapchat account and an account associated with O'Connor. Specifically, IP records from Snapchat reveal that Victim 2's Snapchat account was accessed on June 13, 2019, via the IP address of 185.210.219.154 two times. The j0e Instagram account was accessed minutes later via this same IP address.

106. Pursuant to a search warrant signed by Magistrate Judge David Herriford in the Superior Court of California County of Los Angeles on April 16, 2020, Snap, Inc. provided LAPD

with records for Victim 2's Snapchat account. On June 13, 2019, the account was accessed via the IP address of 185.210.219.154 two times. As shown below, the Instagram account of "@j0e" was accessed minutes later via this same IP address. Also provided pursuant to the search warrant were records from AT&T pertaining to Victim 2's telephone number. The records indicated that on June 13, 2019 a SIM card change was made on Victim 2's account. Approximately 5 hours later, another SIM card change was made to Victim 2's account with the reason being, "Per customer request." I am aware that when an individual conducts a SIM swap, the cell phone provider will switch the SIM number associated with the cell phone account.

107. Based on the above information, I believe **O'Connor** was involved in the compromise of Victim 2's Snapchat account, obtained information from the account include nude images of Victim 2, and was involved in extorting Victim 2 using those nude images. I believe that **O'Connor** conducted a SIM swap to take over Victim 2's Snapchat account and obtain information. **O'Connor** then posted references to his moniker "PlugwalkJoe" and to various other **O'Connor** accounts. **O'Connor** also sent this information to co-conspirators who communicated with Victim 2 in an attempt to extort Victim 2 so that Victim 2 would post a message about **O'Connor** and his co-conspirators. Based on these facts, there is probable cause to believe that **O'Connor** was involved of the hacking of Victim 2's Snapchat and conducted numerous overt acts in furtherance of the computer intrusion.

E. SWATTING AND CYBERSTALKING OF VICTIM 3

108. I have reviewed several reports filed by the Garden Grove Police Department ("GGPD") in Garden Grove, California. One report details an incident occurring on June 25, 2020, in which the GGPD was dispatched to Residence 1²³ in Garden Grove in reference to an armed and dangerous individual threatening to kill his wife and children.

²³ Residence 1 is at an address known to your affiant but not included in this affidavit for the privacy of the occupants.

109. On June 25, 2020, an individual called law enforcement from 405-358-7214, a Google Voice telephone number. The caller did not identify himself but was described in the police report as speaking in an “English or Australian” accent and indicated he caught his wife cheating and planned to kill her and his six children unless he received \$50,000. The caller also claimed he would kill any law enforcement officer responding to the scene. Furthermore, the caller said his children were black and he wanted to kill them because “black lives don’t matter.” The caller stated that he had a Molotov cocktail.

110. Based on the nature of the call, GGPD dispatched every on-duty officer and two sergeants to respond. While officers responded, the caller reported to the Orange County Fire Authority that Residence 1 was on fire and also reported to the Orange County Sheriff’s Department that he was in Residence 1 and was going to kill his wife and children. GGPD officers made contact with the occupants of Residence 1, who indicated they knew nothing about any calls to law enforcement. GGPD was given consent to search the home for victims or suspects, but no evidence of the reported crime was found.

111. A second report filed by GGPD detailed a similar incident occurring at a high school in Garden Grove, California on June 25, 2020. The high school principal reported the school received an email from markwoodjhonson02@gmail.com originating from IP address of 45.152.183.29. I have reviewed a copy of the email from GGDP, which stated in part, “Hello, my name is [Jane Doe].²⁴ I will be shooting up schools in Garn Grove, California at random times on Tuesday. . . I will be aiming at minority students (Black, Mexican, Asian, Etc) As they need to get the fuck off American soil and give us our freedom back!! All those niggers do is rob and steal! . . . I also snuck in over the weekend and put pipe bombs and duffel bags with bombs in them.” Based on the email address markwoodjhonson02@gmail.com being associated with the threats

²⁴ The individual identified in this affidavit as “Victim 3” was listed in the relevant emails and social media posts by a name similar to his/her true name. However, there were variations of the name that included last name of a relative. The true name and the names included in the threats are known to your affiant but not included in this affidavit for the privacy of the juvenile victim.

described here and in paragraph 112, I believe these threats to be perpetrated by the same individual.

112. On the same day, June 25, 2020, there were posts on the social communication platform Reddit threatening Joe's Crab Shack and Coco's Bakery Restaurant in Garden Grove, California. The language was similar as the email send to the high school. The post stated in part, "Hello, my name is [Jane Doe]. I will be shooting at people in Garn Drove, California at random times on Tuesday . . . I will be aiming at minorities (Black, Mexican, Asian, Etc) As they need to get the fuck off American soil and give us our freedom back!! Also those niggzzz do is rob and steal! . . . I've planted pipe bombs in the Joes Crab Shack . . . and at Coco's Bakery Restaurant." The post was made by the Reddit user "u/Strange_Departure355." Based on the similarity in the language used in this post and the language used in the email referenced in paragraph 111, along with this activity occurring on June 25, 2020, I believe these threats to be perpetrated by the same individual.

113. Also on the same day, June 25, 2020, the Orange County Sheriff's Department ("OCSD") received a call from a male identifying himself as [Jane Doe] who stated he was "a transgender going to blow up the airport in 24 hours." The caller requested \$60,000 or else he would kill everyone at the airport. The caller directed the money be sent to Residence 1. The call originated from 405-358-7214, the number associated with the swatting offense on Residence 1 referenced in paragraphs 108-09. Shortly after the initial call, an individual believed to be the same caller called back and stated, "I have an AR-15 with a silencer and I just killed my wife. I told you guys to come." In the call, the caller provided his address as Residence 1 and telephone number as 714-520-0282. I have reviewed portions of the call that were recorded. I have provided portions of this recorded call to C.T. of the REACT Task Force. C.T. informed me he believed the voice in the recorded call matched the voice he knew to be the individual he has spoken with who has identified himself as **O'Connor**.

114. GGPD believed detectives made contact with a juvenile (referred to herein as "Victim 3") who resided near Residence 1 and had a similar name to the "Jane Doe" name being

utilized in the threats. Victim 3 reported that four days prior to the incidents, he/she met an individual online who he/she believed was calling in these false emergencies. Victim 3 met a 21-year-old male named “Joseph” who said that he was from Spain in a Discord chat. Victim 3 stated that “Joseph’s” Instagram account was j0e Instagram. “Joseph” began sending Victim 3 inappropriate messages, which included saying he would kill him/her and “fuck” his/her dead body. Victim 3 also showed GGPd a picture from “Joseph” that depicted his penis. The picture included comments such as “. . . fuck your mouth and cum down into your stomach.” Victim 3 received this picture after informing “Joseph” he/she was 16. Victim 3 also stated that Joseph had live-streamed a call to police on Discord. Victim 3 was not aware of how “Joseph” was able to figure out the area in which Victim 3 lived.

115. I interviewed Victim 3 on August 17, 2020, at which time he/she confirmed the information previously provided to GGPd was accurate. In addition, Victim 3 stated the individual he/she knew as “Joseph” began calling several of Victim 3’s relatives on July 16, 2020, from the telephone number of 304-745-0329, a Google Voice number that was used to communicate with C.T. following the Twitter hack, as referenced in paragraph 51. In each call with Victim 3’s relatives, the individual identified as “Joseph” threatened to kill the individual he was speaking with. On July 25, 2020, “Joseph” called Victim 3 via FaceTime, a video chat application, from the email address of yuckkk828@yopmail.com, and “Joseph” apologized for his actions but thought Victim 3 deserved it. “Joseph” asked Victim 3’s age and was informed his/her age was 16. Victim 3 stated “Joseph” responded by saying, “wow you’re actually really young.” Despite knowing Victim 3’s age, “Joseph” continued to make comments of a sexual nature toward Victim 3. Victim 3 provided a screenshot of the call record, showing the conversation lasted one hour and eight minutes.

116. From multiple conversations with “Joseph,” Victim 3 was aware that the individual identified as “Joseph” was born in the United Kingdom and attended school in Spain. Victim 3

was also aware from his/her conversations with another individual that “Joseph” had been doxed,²⁵ through which he/she learned his name to be **Joseph James O’Connor**. Victim 3 asked “Joseph” if this was his name, to which he responded it was **Joseph O’Connor**. Victim 3 also communicated with “Joseph” via the Instagram account of “j0e.” Based on my interactions with Victim 3 and his/her recounting of the experience with “Joseph,” I understood Victim 3 to have endured substantial emotional distress over the events perpetrated by the individual who I believe to be **O’Connor**.

117. As discussed previously, pursuant to search warrants, Snap Inc. provided the content of the Dog Snapchat account to the FBI. The account contained an image from June 19, 2020, of a login screen for the PlayStation Network, an online gaming platform. The sign-in field was filled in with the email address of joco2019++@protonmail.com, which matches the naming convention **O’Connor** is known to use across various email accounts he used to register accounts, further attributing the Dog Snapchat account to **O’Connor**.

118. Records from the Dog Snapchat account included multiple audio files which I believe are recordings between **O’Connor** and Victim 3. In one recording, **O’Connor** stated, “I doxed you and called your mom...I doxed you. Is that fucked up?” In another recording, **O’Connor** claimed he did not call the police. The recordings appear to have been sent or received on July 25, 2020, the same day Victim 3 said he/she spoke with **O’Connor** via FaceTime. In addition, the Dog Snapchat account included text messages between Victim 3 and **O’Connor** between June 20, 2020 and August 22, 2020. On June 23, 2020, **O’Connor** sent the email address of joseph@thug.org. The following day, on June 24, 2020, **O’Connor** stated “keep my name our ur mouth.”

119. I have reviewed records provided to the FBI by Google regarding the telephone number of 405-358-7214. The number was registered to Jhonson Markwood using the email address of markwoodjhonson02@gmail.com. The current subscriber started utilizing the telephone

²⁵ Doxing, or to be doxed, is the publication of an individual’s private information on the Internet, which can include the individual’s name, date of birth, and other identifying information.

number on April 16, 2020. Subscriber information for markwoodjhonson02@gmail.com shows the account was created on April 13, 2020. The account had been logged into on June 25, 2020, via the IP address of 45.152.183.29.

120. I have reviewed records provided to the FBI by Reddit regarding the account of “u/Strange_Departure355.” The account was registered on June 25, 2020, using the email address of markwoodjhonson02@gmail.com. The account was logged into, among others, via the IP addresses of 45.152.183.29 and 195.206.107.147.

121. I believe the above threats were made in an attempt to seek revenge against Victim 3 for a perceived slight. The calls to police were made in an attempt to elicit a law enforcement response at Victim 3’s residence, though I believe the incorrect address and last name for Victim 3 was provided. These threats were perceived to be legitimate enough that the entirety of a town’s on-duty police force were required to respond. The threats to Victim 3’s family members were intended to intimidate and harass Victim 3 and his/her family. Both sets of conduct caused Victim 3 substantial emotional distress. Based on the phone calls, emails, and social media postings of threats involving conduct at Residence 1 and referencing a name similar to Victim 3, the subsequent phone calls to Victim 3’s family members threatening to kill each individual, messages sent through **O’Connor’s** Dog Snapchat account and other accounts known to be used by **O’Connor**, there is probable cause to believe that **O’Connor** was responsible for swatting and cyberstalking Victim 3.

F. OVERLAPPING IP ADDRESSES REVEAL THAT THE SAME INDIVIDUAL INVOLVED WITH THE TWITTER HACK COMMITTED THE HACKING OF VICTIM 1’S TIKTOK ACCOUNT, THE HACKING OF VICTIM 2’S SNAPCHAT ACCOUNT, AND THE CYBERTHREATS AGAINST VICTIM 3

122. As stated above, the same IP addresses hosted by VPNs were used to access different online accounts discussed in this affidavit. The user of the Twitter account “@plugwalkjoe” and the J.OConnor99 Snapchat account previously posted images of his passport, revealing the name and identity of the person named **Joseph James O’Connor** charged in the accompanying complaint. The user of the Twitter account “@shinji” stated that the account

replaced his “plugwalkjoe” account. The individual using the Google Voice phone numbers 678-685-9876 and 304-745-0329, which were associated with daiseymorrowphamsc53@gmail.com and bergnaumsueann@gmail.com, respectively, had spoken with C.T. since January 2019 and had previously identified himself as **Joseph O’Connor**. The same individual who used the Google Voice phone numbers 678-685-9876 and 304-745-0329 and was interviewed by FBI agents and C.T. spoke about the individuals who hacked Logan Paul’s account giving him a shout-out, and the “@PlugwalkJoe” Twitter account sent direct messages related to the hacking. The individual who spoke with Victim 3 used the Instagram account “j0e”, confirmed that his name was **Joseph O’Connor**, and communicated Victim 3 via the Dog Snapchat account. Furthermore, the user of the J.OConnor99 Snapchat account was involved in the hacking of Victim 2’s Snapchat and attempted extortion of Victim 2.

123. Each of these accounts had substantial IP overlap with other accounts believed to be used by **O’Connor** that are associated with the Twitter hack, the hacking of Victim 1’s TikTok, the hacking of Victim 2’s Snapchat, and the cyberthreat and swatting of Victim 3. The following table is a visual representation showing the commonalities of the IP addresses associated with use of the relevant accounts believed to have been involved in the illegal activity mentioned above, along with other related accounts, sorted chronologically based on timing of first IP address access and bolding accounts from which **O’Connor** posted his passport:

| No. | Username | IP Address | Timestamp | IP Location |
|-----|-------------------------|----------------|------------------|---------------|
| 1 | j.oconnor99 | 194.99.104.29 | 11/23/2019 15:29 | Madrid, Spain |
| 1 | @j0e | 194.99.104.29 | 3/11/2020 17:21 | Madrid, Spain |
| 1 | Deleted User 93949#7739 | 194.99.104.29 | 7/15/2020 8:02 | Madrid, Spain |
| 1 | @shinji | 194.99.104.29 | 7/15/2020 11:16 | Madrid, Spain |
| 2 | j.oconnor99 | 37.120.148.86 | 11/23/2019 20:16 | Madrid, Spain |
| 2 | @j0e | 37.120.148.86 | 1/15/2020 18:57 | Madrid, Spain |
| 2 | Deleted User 93949#7739 | 37.120.148.86 | 7/14/2020 23:29 | Madrid, Spain |
| 2 | @shinji | 37.120.148.86 | 7/14/2020 23:38 | Madrid, Spain |
| 3 | j.oconnor99 | 194.99.104.27 | 11/25/2019 7:03 | Madrid, Spain |
| 3 | @shinji | 194.99.104.27 | 7/15/2020 19:10 | Madrid, Spain |
| 3 | Deleted User 93949#7739 | 194.99.104.27 | 7/15/2020 19:10 | Madrid, Spain |
| 4 | j.oconnor99 | 185.230.124.52 | 11/26/2019 22:34 | Madrid, Spain |
| 4 | Deleted user 93949#7739 | 185.230.124.52 | 7/15/2020 21:09 | Madrid, Spain |

| | | | | |
|----|-------------------------|-----------------|------------------|-------------------------|
| 4 | @shinji | 185.230.124.52 | 7/15/2020 21:10 | Madrid, Spain |
| 4 | @j0e | 185.230.124.52 | 7/21/2020 2:14 | Madrid, Spain |
| 5 | j.oconnor99 | 81.92.206.45 | 1/08/2019 20:32 | Manchester, England |
| 5 | @PlugwalkJoe | 81.92.206.45 | 1/08/2019 22:24 | Manchester, England |
| 6 | @PlugwalkJoe | 91.207.175.216 | 11/28/2018 13:23 | Los Angeles, California |
| 6 | daiseymorrowphamsc53 | 91.207.175.216 | 7/17/2020 21:55 | Los Angeles, California |
| 7 | Deleted User 93949#7739 | 185.230.124.50 | 7/13/2020 12:02 | Madrid, Spain |
| 7 | @shinji | 185.230.124.50 | 7/13/2020 14:24 | Madrid, Spain |
| 8 | u/Strange_Departure355 | 195.206.107.147 | 6/25/2020 18:11 | Madrid, Spain |
| 8 | bergnaumsueann | 195.206.107.147 | 6/30/2020 8:50 | Madrid, Spain |
| 8 | sick in the head#1461 | 195.206.107.147 | 6/30/2020 9:46 | Madrid, Spain |
| 8 | Deleted User 93949#7739 | 195.206.107.147 | 7/15/2020 22:14 | Madrid, Spain |
| 8 | daiseymorrowphamsc53 | 195.206.107.147 | 7/22/2020 | Madrid, Spain |
| 8 | @kpop | 195.206.107.147 | 11/5/2019 | Madrid, Spain |
| 8 | @yoongi | 195.206.107.147 | 10/01/2020 21:53 | Madrid, Spain |
| 9 | sick in the head#1461 | 45.152.183.29 | 6/25/2020 10:50 | Madrid, Spain |
| 9 | u/Strange_Departure355 | 45.152.183.29 | 6/25/2020 11:29 | Madrid, Spain |
| 9 | markwoodjhonson02 | 45.152.183.29 | 6/25/2020 11:34 | Madrid, Spain |
| 9 | bergnaumsueann | 45.152.183.29 | 6/30/2020 12:21 | Madrid, Spain |
| 10 | @shinji | 185.230.124.51 | 7/15/2020 14:25 | Madrid, Spain |
| 10 | Deleted User 93949#7739 | 185.230.124.51 | 7/15/2020 15:04 | Madrid, Spain |
| 10 | @shinji | 194.99.104.28 | 7/14/2020 8:51 | Madrid, Spain |
| 10 | Deleted User 93949#7739 | 194.99.104.28 | 7/14/2020 8:55 | Madrid, Spain |
| 11 | JoeComplex | 212.102.49.251 | 8/16/2020 | Madrid, Spain |
| 11 | @j0e | 212.102.49.251 | 8/16/2020 06:57 | Madrid, Spain |
| 11 | @yoongi | 212.102.49.251 | 10/01/2020 23:03 | Madrid, Spain |
| 12 | Deleted User 93949#7739 | 45.152.183.28 | 7/14/2020 00:17 | Madrid, Spain |
| 12 | @yoongi | 45.152.183.28 | 10/01/2020 23:57 | Madrid, Spain |
| 13 | Victim 1's TikTok | 212.102.49.185 | 8/15/2020 00:01 | Madrid, Spain |
| 13 | @j0e | 212.102.49.185 | 8/15/2020 01:28 | Madrid, Spain |
| 13 | @yoongi | 212.102.49.185 | 10/08/2020 23:30 | Madrid, Spain |
| 14 | @shinji | 89.26.241.86 | 7/9/2020 20:19 | Lisbon, Portugal |
| 14 | Deleted User 93949#7739 | 89.26.241.86 | 7/9/2020 20:19 | Lisbon, Portugal |
| 15 | @shinji | 89.26.241.130 | 7/10/2020 10:16 | Lisbon, Portugal |
| 15 | Deleted User 93949#7739 | 89.26.241.130 | 7/10/2020 10:18 | Lisbon, Portugal |
| 16 | bergnaumsueann | 141.98.252.169 | 7/1/2020 2:13 | London, England |
| 16 | Deleted User 93949#7739 | 141.98.252.169 | 7/5/2020 22:36 | London, England |
| 17 | Victim 2's Snapchat | 185.210.219.154 | 6/13/2020 20:57 | Vienna, Austria |
| 17 | @j0e | 185.210.219.154 | 6/13/2020 21:01 | Vienna, Austria |

124. Each of the accounts in this table have substantial IP address overlap with other accounts that are associated with **O'Connor** and his various illegal activities. Many of these logins above are particularly notable for their proximity in time to logins into other accounts. Based on my training and experience, and the evidence set forth in this affidavit, including the account logins

set forth in the table immediately above, I believe all of these accounts were controlled by the same user. Further, two of these accounts are directly linked to posted pictures of what is believed to be authentic passports of British citizen **Joseph James O'Connor** – the J.OConnor99 Snapchat account (which posted a passport picture) and the @shinji Twitter account (directly linked to the @plugwalkjoe Twitter account, which posted a passport picture). Additionally, the daiseymorrowphamsc53@gmail.com and bergnaumsueann@gmail.com accounts are linked to the identity of **Joseph O'Connor** through the Google Voice calls to C.T. Therefore, I believe, based on my training and experience, that all of the accounts set forth in the table immediately above were controlled by **Joseph James O'Connor**, the individual charged in the instant complaint.

V. CONCLUSION

125. Based on the above information, I respectfully submit that there is probable cause to believe that **Joseph James O'Connor** conspired to commit a crime against the United States, namely, intentionally accessing the computers of Twitter, TikTok, and Snapchat, and thereby obtained information from a protected computer, without the authorization of Twitter, TikTok, and Snapchat, and applicable Twitter accountholders, Victim 1, and Victim 2, in violation of 18 U.S.C. § 1030(a)(2)(C), all in violation of 18 U.S.C. § 371.

126. I also submit that there is probable cause to believe that **Joseph James O'Connor** intentionally accessed the computer(s) of TikTok and thereby obtained information from a protected computer, without the authorization of TikTok and Victim 1; accessed the computer(s) of Snapchat and thereby obtained information from a protected computer, without the authorization of Snapchat and Victim 2; and aided and abetted others in doing so, in violation of 18 U.S.C. §§ 1030(a)(2)(C) and 2.

127. I also submit that there is probable cause to believe that **Joseph James O'Connor** conspired to commit a crime against the United States, namely, with the intent to extort from a person a thing of value, transmitting a communication containing a threat to reveal confidential information, and transmitting a communication containing a demand and request for a thing of

value in relation to damage to a protected computer where such damage was caused to facilitate the extortion, in violation of 18 U.S.C. § 1030(a)(7), all in violation of 18 U.S.C. § 371.

128. I also submit there is probable cause to believe that **Joseph James O'Connor** perpetrated an act of extortive communications against Victim 2, and aided and abetted others in doing so, in violation of 18 U.S.C. §§ 875(d) and 2.

129. I further submit there is probable cause to believe that **Joseph James O'Connor** with the intent to injure, harass, and intimidate another person, namely, Victim 2, used any interactive computer service and electronic communication service and electronic communication system of interstate commerce, and any other facility of interstate and foreign commerce to engage in a course of conduct that causes, attempts to cause, and would be reasonably expected to cause substantial emotional distress to Victim 2, and aided and abetted others in doing so, in violation of 18 U.S.C. §§ 2261A(2) and 2.

130. I also submit there is probable cause to believe that **Joseph James O'Connor** transmitted in interstate and foreign commerce any communication containing any threat to injure the person of another, namely, Victim 3, and aided and abetted others in doing so, in violation of 18 U.S.C. §§ 875(c) and 2.

131. I further submit there is probable cause to believe that **Joseph James O'Connor** with the intent to injure, harass, and intimidate another person, namely, Victim 3, used any interactive computer service and electronic communication service and electronic communication system of interstate commerce, and any other facility of interstate and foreign commerce to engage in a course of conduct that causes, attempts to cause, and would be reasonably expected to cause substantial emotional distress to Victim 3 and an immediate family member of Victim 3, and aided

//

//

//

//

//

and abetted others in doing so, in violation of 18 U.S.C. §§ 2261A(2) and 2.

/s/

R. Montgomery
Special Agent
Federal Bureau of Investigation

Sworn to before me over the telephone and signed by me pursuant to Fed. R. Crim. P. 4.1 and 4(d) on this 14th day of May, 2021. This application and warrant are to be filed under seal.



HONORABLE THOMAS S. HIXSON
United States Magistrate Judge