UNITED STATES DISTRICT COURT

for the

Eastern District of Kentucky

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* Information associated with Apple account associated with 919867615027 that is stored at premises controlled by Apple Inc.	Case No. 5:23-MJ-5200

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A, incorporated by reference herein

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, incorporated by reference herein

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18/1956, 1957	Money laundering
18/1960	Conducting unlicensed money transmitting business
18/371	Conspiracy

The application is based on these facts:

See attached affidavit, incorportated herein by reference.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Matthew Resch
Applicant's signature

Matthew Resch, Special Agent, FBI
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 06/07/2023

Judge's signature

City and state: Lexington, KY

Matthew A. Stinnett, United States Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF KENTUCKY

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH APPLE ACCOUNT ASSOCIATED WITH 919867615027 THAT IS STORED AT PREMISES CONTROLLED BY APPLE INC.	Case No. 5:23-MJ-5200 **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Matthew Resch, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises owned, maintained, controlled, or operated by Apple Inc. ("Apple"), an electronic communications service and/or remote computing service provider headquartered at One Apple Park Way, Cupertino, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been since December 2020. I have received training in computer intrusion investigations, to include the role of electronic communications providers and the internet in cyber-criminal

activity. I am currently assigned to the FBI Louisville Cyber Task Force to investigate computer intrusions and the infrastructure that supports them, to include cyber-enabled fraud money laundering. I was previously a Computer Scientist with the FBI, and received training in digital forensics, malware, computer operating systems, and computer networking.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 1956 and 1957, Money Laundering, 18 U.S.C. § 1960, Unlicensed Money Services Business, and 18 U.S.C. § 371, Conspiracy have been committed by known and unknown persons. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and fruits of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

6. The investigation relates to the illegal exchange of cash for virtual currency conducted on online marketplaces known for criminal activity. In April 2021, the FBI identified a vendor using the moniker "elonmuskwhm" on criminal darknet marketplaces, White House Market and Dark0de Reborn, and the peer-to-peer exchange, LocalMonero, offering to mail customers cash within the United States in return for bitcoin. The advertisements from

"elonmuskwhm" indicated he would ship cash using U.S. Postal Service Express Mail or Priority Mail with package tracking available. On Dark0de Reborn, "elonmuskwhm" had four listings for these "cash by mail" exchanges and stated he/she was the only vendor who could provide up to $1,000,000 per week. The four (4) listings were priced at $500, $1,000, $5,000, and $10,000. On White House Market, "elonmuskwhm" had five (5) listings priced at $500, $1,000, $2,000, $5,000, and $10,000, respectively, and he/she stated the shipments would be mailed from the United States. On May 4, 2021, on the criminal forum Dread, "elonmuskwhm" directed people to not pay taxes by using his/her cash-by-mail service.

7. Darknet marketplaces like White House Market and Dark0de Reborn, are marketplaces for buying and selling illegal goods and services, and money conversion services, like that offered by "elonmuskwhm," are used to promote specified unlawful activities as defined in 18 U.S.C. § 1956, and to conceal the location, source, ownership, or control of the proceeds of that activity. A money transmitting business is any business that provides "currency exchange," "money transmitting or remittance services," or that accepts "currency, funds, or value that substitutes for currency and transmits" that "by any means." 31 U.S.C. § 5330(d)(1). A cryptocurrency exchange service such as that operated by "elonmuskwhm" constitutes a money transmitting business. As such, "elonmuskwhm" must register his/her business with the Secretary of the Treasury. *Id.* at § 5330(a)(1). The database for money services business registrants contains no registration for "elonmuskwhm" or any name found on the shipping materials from "elonmuskwhm". This is a violation of 18 U.S.C. § 1960. Because "elonmuskwhm" worked with shippers in the United States to send the cash by mail, this amounts to a conspiracy in violation of 18 U.S.C. § 371.

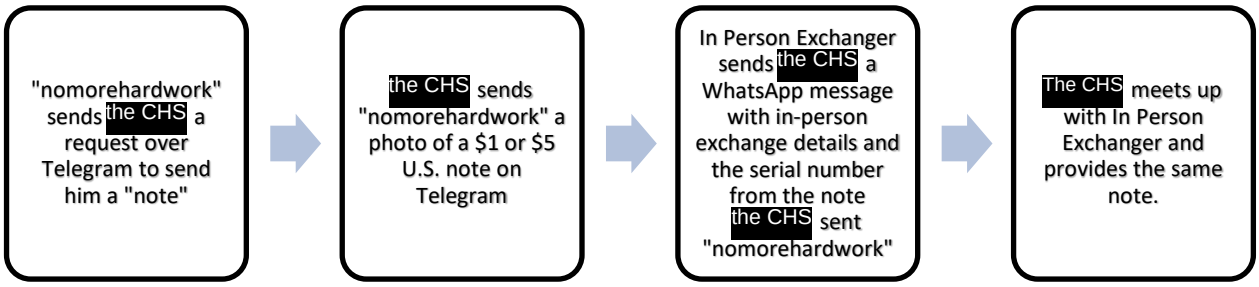
8. The FBI and United States Postal Inspection Service have conducted several controlled sales of cryptocurrency with "elonmuskwhm". Each time, "elonmuskwhm" shipped cash through the mail to a Post Office box in the Eastern District of Kentucky, in exchange for a pre-determined amount of cryptocurrency. For example, on January 3, 2023, the FBI conducted a purchase of approximately $70,000 from "elonmuskwhm." On January 4, 2023, the FBI conducted surveillance of the mailing of this purchase, and observed a known suspect, Davis Paolucci, exit his residence at [redacted], and deliver two parcels to a United States Post Office addresses to the Post Office box provided by the FBI.

9. On February 2, 2023, Paolucci was indicted for violations of 18 U.S.C. §§ 1956(h) and 371. The 18 U.S.C. § 371 offense was predicated on illegal conduct under 18 U.S.C. § 1960 (Unlicensed Money Transmitting Business). On February 7, 2023, Paolucci was arrested by the FBI. Approximately $600,000 was located during a search of his residence.

10. [redacted] A Confidential Human Source (CHS) stated he meets various individuals approximately three times a week to receive cash in amounts typically ranging between $100,000 and $300,000 at a time for the purpose of fulfilling cash shipment orders. The CHS explained that the cash exchanges are arranged via WhatsApp chats.

11. The CHS also described the tradecraft used during cash exchanges. Prior to an exchange, Telegram user "nomorehardwork", known to the CHS as the same user as "elonmuskwhm", requests that the CHS send him a picture of a "note" for pickup. The "note" is a US bank note. The CHS takes a picture of a $1 or $5 bill in his possession and sends the picture to "nomorehardwork" on Telegram. Later, a WhatsApp user contacts the CHS to set up a cash exchange (the "In-Person Exchanger"), sending him a text message with the serial number from

a bill provided to "nomorehardwork" by the CHS During the exchange, the CHS provides the original bill with matching serial number to the In-Person Exchanger, in order to receive the cash. On at least one occasion, "nomorehardwork" sent a picture to the CHS of the bill in the lap of an unknown person following an exchange. In summary, the message exchange is as follows:



12. Based on my training and experience, I know that in order to operate anonymously, cyber-criminal actors frequently utilize tradecraft to positively identify themselves and their co-conspirators to one another without providing much personally identifying information, and to verify the validity of their communications and activity. It is likely that the dollar bill tradecraft uses the serial number as a means of three-way identification for "nomorehardwork", the CHS and the In-Person Exchangers. The system relies on "nomorehardwork" communicating with both parties conducting the cash exchange.

13. The CHS reviewed his WhatsApp account and identified the WhatsApp accounts belonging to the In-Person Exchangers or those responsible for arranging cash exchanges. Among those users were +1 9293468117, who the CHS identified as the most frequent In-Person

Exchanger, and +91 7859857089, identified by the CHS as a user that arranges cash exchanges, but does not conduct them personally. Upon application of the United States, on February 8, 2023, this Court entered an order authorizing installation and use of a pen/trap device to monitor non-content information associated with these numbers, among others identified by the CHS

14. Under the guidance of the FBI, the CHS has continued to engage in cash pickups. Continued FBI surveillance of cash exchange dates and times were compared with analysis of data received through the aforementioned pen/trap device. Pen/trap data was reviewed for ten cash exchanges during which approximately $2 million was delivered. Following seven of the exchanges, within two hours following each cash exchange, WhatsApp data showed a pattern of activity in which the +1 9293468117 In-Person Exchanger sent *an image* to WhatsApp user +91 7859857089 following the exchange. That user then sent *an image* to WhatsApp user **+91 9867615027**.

15. Based on the CHS's description of the manner in which cash exchanges are conducted, and the fact that "nomorehardwork" has received an image of the exchanged bill in the past, there is probable cause to believe that an image sent immediately following a cash exchange is intended to verify that the exchange occurred according to standard procedure.

16. Phone number **9867615027** was listed as a contact number on two non-immigrant visa applications for Anurag Pramod Murarka, date of birth [redacted], in July and August, 2022. The same applications listed an additional contact phone number, 8097883557, and home address [redacted] India [redacted] On one application, Murarka listed his employer as Petagma Pvt. Ltd.

17. Open-source research identified a Telegram account using phone number +918097883557 and username "elonmuskwhm", with a profile picture of a phone with a Batman

phone case and the display name "Elon". The FBI and United States Postal Inspection Service has conducted a controlled purchase and other communications with "elonmuskwhm" through a Telegram account bearing the same username, profile picture, and display name.

18. Indian Ministry of Corporate Affairs records identify Petagma Private Limited with a former director Anurag Pramod Murarka, with a new director beginning October, 2019. A website was identified for Petagma Pvt Ltd, petagma.com. The website describes the company as a land survey company and prominently features aerial drones. One of the contact phone numbers listed on the website is **+91 9867615027**.

19. On January 2, 2023, while arranging a controlled purchase, an FBI employee discussed geographic information systems (GIS) with "elonmuskwhm", who revealed a history of working in the field. The user told the FBI employee that he was knowledgeable of GIS, including aerial drones, and had been the CEO of a GIS company that he sold to his business partner approximately three years earlier.

20. PayPal records identify an account in the name Anurag Murarka, with date of birth [redacted], verified phone number **+91 9867615027**, home address [redacted] IN [redacted] The verified email address associated with the account is murarkaanurag1998@gmail.com. Thus, Murarka is the user of phone number **+91 9867615027** and Gmail account murarkaanurag1998@gmail.com**.**

21. Based on the following, there is probable cause to believe that Murarka uses an Apple account registered with Apple ID **919867615027:**

a. Google records indicate that the Google account **murarkaanurag1998@gmail.com** was accessed by three devices between November 2019 and May 2023. All three devices are Apple products: an iPad, an

iPhone, and a Mac computer. The user assigned name of the iPad device according to Google records is Anurag Murarka's iPad.

b. Between May 2 and 4, 2023, Google records show that the Google account **murarkaanurag1998@gmail.com** was accessed by the Google photos, maps, Gmail, and YouTube apps on an Apple mobile device with iOS version 16.3.1 using IP address 2401:4900:1c8e:7f92:5d0c:9457:7fa6:991.

c. Between May 2 and 4, 2023, WhatsApp records show that the same IP address was used by an Apple device to access the WhatsApp account **+91 9867615027**.

d. Apple records identify an account with Apple ID **919867615027** associated with Anurag Murarka and verified phone number **919867615027**.

e. The Apple account downloaded software updates to an iPhone with iOS version 16.3.1 from the Apple App Store on March 8, 2023 using IP address 2401:4900:1c2d:dd5d:286a:ab4a:5d8f:dfd.

f. On March 8 and 9, 2023, WhatsApp records show that the same IP address was used by an Apple device to access the WhatsApp account **+91 9867615027**.

22. WhatsApp pen/trap data identifies the device type associated with the sender of a chat message. Review of WhatsApp records associated with user **+91 9867615027** show that between February 11 and May 24, 2023, the user used WhatsApp on an iOS device to send chat messages.

23. Thus, the **murarkaanurag1998@gmail.com** Google, **919867615027** Apple, and **+91 9867615027** WhatsApp accounts, all belonging to Murarka, are accessed from an Apple mobile device accessing common IP addresses – that is, the same Apple mobile device. Additionally, Murarka used the Apple device to access his WhatsApp account to communicate

with coconspirators about the cash exchanges that comprise the basis for the offenses described herein.

24. I know, based on my training and experience, that WhatsApp conversations are encrypted end-to-end, and the only way to obtain those messages is by being a party to the exchange or obtaining a device or device backup where the messages are stored. A pattern of WhatsApp communications involving **+91 9867615027** following cash exchanges demonstrate that the user is discussing the exchanges, including likely photographic evidence that the exchanges had taken place. Because the user of **+91 9867615027** communicated over WhatsApp using an Apple device, and Apple records associate **+91 9867615027** with the Apple account **919867615027**, there is probable cause to believe that evidence of the crime, including communications regarding the cash drop offs, will be stored to the phone associated to +**91 9867615027**, and therefore also stored to the backup copy to the user's Apple account.

25. Cyber actors frequently use multiple encrypted messaging services to communicate with various co-conspirators. In this case, "elonmuskwhm" is known to have used Wickr, WhatsApp, and Telegram to communicate with customers and co-conspirators. Because "elonmuskwhm" communicated money laundering transaction details using Telegram and Wickr, and is the user of the Apple account **919867615027**, there is probable cause to believe that evidence of the crime, including communications regarding customer transactions, will be stored to the phone associated to +**91 9867615027**, and therefore also stored to the backup copy to the user's Apple account.

26. Apple records indicate that the account with Apple ID **919867615027** has iCloud Backup, Bookmarks, Calendars, iCloud Photos, Contacts, iCloud Drive, iCloud Reminders, Messages in iCloud, Notes, and Sign in with Apple features enabled. These services are

configured to backup to the iCloud account. The account also has the Advanced Data Protection setting, which is capable of encrypting these backups, disabled.

27. IP address information from WhatsApp and cryptocurrency traced from controlled purchases has identified multiple connections between the "elonmuskwhm" moniker and users in India. Additionally, IP addresses associated to the WhatsApp messages are located in a different geographic region within India than the IP addresses obtained from the cryptocurrency tracing. Thus, it appears that the different elements of this scheme within India – i.e., those organizing the money launderers in the United States and those receiving cryptocurrency – are in a different region than the cryptocurrency recipients. This could perhaps be due to the use of VPNs. This application seeks location information to discover evidence into the connections between these elements of the scheme, whether the co-conspirators are using VPNs, and to help identify the true location and identity of the **+91 9867615027** WhatsApp user. Additionally, location information provides evidence into the elements of an 18 U.S.C. § 1956(a)(2) offense, which requires that monetary instruments or funds from the United States to or through a place outside the United States, or vice versa.

28. Based on my training and experience, money launderers have a need to maintain a contact list of co-conspirators and customers in order to conduct their money laundering scheme. They also have a need to maintain a financial ledger of transactions. These contacts and financial ledgers may also be backed up to an iCloud account in the form of Apple iWork documents, such as Pages or Notes, iCloud Drive, and iCloud Backup services, which Apple records indicate are enabled for the account, or as other types of files backed up to the account in association with specific third-party applications.

29. Based on the above, it is evident that the user of **919867615027** manages a

significant volume of international cash and cryptocurrency transactions. The investigation has observed approximately two to three cash drops per week over a multi-month period, during which hundreds of thousands of dollars have been exchanged. It is logical that organizing these kinds of logistics require a calendar. In my training and experience, I am aware that the Apple calendar app attempts to or automatically updates itself when hotel and airline reservations are sent to an email account and when possible, meetings are detected over email. The calendar can also be synchronized with multiple third-party calendar services to organize calendar events in one location. Apple records indicate that the account has the Calendars service enabled, which allows the user's calendar to be synchronized to iCloud for backup and use across multiple devices. Maintaining a calendar that tracks the criminal activity is relevant evidence to both determine the method of operation and provides insight into the *mens rea* of the actors.

30. Most major cryptocurrencies and cryptocurrency exchanges can be accessed or interacted with via a mobile app. As with a mobile banking app, these applications may contain the details of cryptocurrency transactions or other financial instruments involved in the money laundering scheme. They may also contain the keys required to access that cryptocurrency. These details may also be backed up to an iCloud account. Google email header records for the account murarkaanurag1998@gmail.com show emails received from the Coinbase, Paxful, and Binance cryptocurrency exchanges. Accounts at each exchange can be accessed via iOS mobile application, or via web browser on an Apple device.

31. Based on my training and experience, I know that internet browsing data can provide evidence of the state of mind of a cyber-criminal actor, their location, and their identity or the identities of their co-conspirators. This evidence can take the form of browser history, tabs, and bookmarks, which identify websites visited by the actor in order to facilitate criminal

activity, such as to conduct research on potential customers or access accounts used in commission of the crime.

32. On May 25, 2023, Apple was served a 2703(f) request for preservation of all records associated with the account **919867615027** for a period of 90 days. Apple confirmed preservation of records on May 26, 2023.

BACKGROUND CONCERNING APPLE[1]

33. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

34. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct audio and video calls.

---

[1] The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf; "Create and start using an Apple ID," available at https://support.apple.com/en-us/HT203993; "iCloud," available at http://www.apple.com/icloud/; "What does iCloud back up?," available at https://support.apple.com/kb/PH12519; "iOS Security," available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and "iCloud: How Can I Use iCloud?," available at https://support.apple.com/kb/PH26502.

c. iCloud is a cloud storage and cloud computing service from Apple that allows its users to interact with Apple's servers to utilize iCloud-connected services to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on iCloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iCloud Backup allows users to create a backup of their device data. That **919867615027** has this service activated demonstrates the account has been backed up. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

d. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

e. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

f. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

g. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

35. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. The account identifier for an Apple ID is an email address, provided by the user. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

36. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means

of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

37. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

38. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition,

information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

39. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

40. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when,

where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

41. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. Elonmuskwhm posted advertisements for his services on the darknet and the clear net. He participated in clear net forum discussions. In my experience and training, I am aware that peer-to-peer cryptocurrency exchangers constantly check the cryptocurrency price indexes available through the internet to maximize profits. Additionally, I am aware that a service-based criminal activity often requires the actors to research their clientele before engaging in transactions, which would involve the use of internet searches. Specific to this international criminal organization, where the preceding paragraphs have discussed travel, it is likely that the conspirators used the internet to search for hotels and flights to support their travel needs. For these reasons, there is probable cause to believe that internet search history would provide valuable evidence of the actors' criminal activity and state of mind.

42. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant

time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

43. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

44. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

45. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

CONCLUSION

46. Based on the forgoing, I request that the Court issue the proposed search warrant.

47. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

/s/ Matthew Resch

Matthew Resch
Special Agent
Federal Bureau of Investigation

Transmitted via email and attested to by telephone in accordance with Fed. R. Crim. P. 4.1 on this 7th day of June, 2023.

Honorable Matthew A. Stinnett
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with Apple ID 919867615027 that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at One Apple Park Way, Cupertino, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple Inc. ("Apple")

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Apple, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on May 8, 2023, Apple is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses), subscriber identifiers, verification information for primary registered email addresses[2], the date on which the account was created, the length of service, the IP address used to register the account, account status, language used, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers

[2] Note, this should not include verification information for the alternate, rescue, and notification email addresses.

("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

d. All records pertaining to the types of service used;

e. Identification of all account that are linked to the account by cookies, recovery e-mail addresses, or telephone numbers;

f. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

g. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

h. For the period from April 1, 2021 to the present:

i. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages sent to and from the account (including all draft and deleted messages), using third-party applications WhatsApp, Telegram, and Wickr, the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

ii. Information about each communication sent or received by the Account through Mail, iMessage, or FaceTime, including the date and time of the communication, the method of communication, and the source and destination of the communication (such as sender and recipient phone numbers, IP addresses, and telephone numbers);

iii. The contents of all files and other records stored on iCloud, including all iOS device backups, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iCloud Keychain, Calendar, and all address books, contact and buddy lists, notes, images, videos, and voicemails;

iv. All internet browser data, including iCloud Tabs, bookmarks, and Safari browsing history;

v. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

Apple is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C. §§ 1956 and 1957, Money Laundering, 18 U.S.C. § 1960, Unlicensed Money Services Business, and 18 U.S.C. § 371, Conspiracy, those violations involving the user of the 919867615027 Apple account and occurring after April 1, 2021, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) Evidence of the use of the dark net;

(b) Evidence of the conversion or transmission of any funds (including cryptocurrency) in any manner;

(c) Evidence of underlying criminal activities that are the source of funds sent to/from "elonmuskwhm";

(d) Evidence of solicitation to engage in criminal activity;

(e) Communications between 919867615027 or other usernames/phone numbers associated to the 919867615027 accountholder and potential money services clients;

(f) Evidence of financial instruments, including bank accounts, cryptocurrency exchange accounts, credit cards, and other financial entity records;

(g) Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the account owner;

(h) Evidence indicating the account owner's state of mind as it relates to the crime under investigation;

(i) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s);

(j) The identity of the person(s) who communicated with the account holder about matters relating to the conversion and transmission of funds, or the source of those funds, including records that help reveal their whereabouts; and

(k) Cryptocurrency or virtual tokens (including any and all representations of cryptocurrency wallets of their constitutive parts), and public keys, private keys, root keys, or seed phrases.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Apple Inc. ("Apple"), and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Apple. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Apple, and they were made by Apple as a regular practice; and

b. such records were generated by Apple's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Apple in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Apple, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date	Signature

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means ❒ Original ❒ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Eastern District of Kentucky

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* Information associated with Apple account associated with 919867615027 that is stored at premises controlled by Apple Inc.	)	Case No. 5:23-MJ-5200

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Northern District of California *(identify the person or describe the property to be searched and give its location)*:

See Attachment A, incorporated by reference herein.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B, incorporated by reference herein.

YOU ARE COMMANDED to execute this warrant on or before June 21, 2023 *(not to exceed 14 days)*

❒ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Matthew A. Stinnett.

(United States Magistrate Judge)

❒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

❒ for _____ days *(not to exceed 30)* ❒ until, the facts justifying, the later specific date of _____.

Date and time issued: **3:32 PM, Jun 7, 2023**

Judge's signature

City and state: Lexington, KY

Matthew A. Stinnett, United States Magistrate Judge

Printed name and title

Return

Case No.: 5:23-MJ-5200	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF KENTUCKY

INFORMATION ASSOCIATED WITH APPLE ACCOUNT ASSOCIATED WITH 919867615027 THAT IS STORED AT PREMISES CONTROLLED BY APPLE INC.	Case No. 5:23-MJ-5200 **Filed Under Seal**

APPLICATION FOR ORDER COMMANDING APPLE INC. NOT TO NOTIFY ANY PERSON OF THE EXISTENCE OF WARRANT

The United States requests that the Court order Apple Inc. ("Apple") not to notify any person (including the subscribers and customers of the account(s) listed in the warrant of the existence of the attached warrant for one year.

Apple is a provider of an electronic communication service, as defined in 18 U.S.C. § 2510(15), and/or a remote computing service, as defined in 18 U.S.C. § 2711(2). Pursuant to 18 U.S.C. § 2703, the United States obtained the attached warrant, which requires Apple to disclose certain records and information to the United States. This Court has authority under 18 U.S.C. § 2705(b) to issue "an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order." *Id.*

In this case, such an order would be appropriate because the attached warrant relates to an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation, and its disclosure may alert the targets to the ongoing investigation. Accordingly, there is reason to believe that notification of the existence of the attached warrant will seriously jeopardize the investigation or unduly delay a trial, including by giving targets an opportunity to

flee or continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, intimidate potential witnesses, or endanger the life or physical safety of an individual. *See* 18 U.S.C. § 2705(b). Some of the evidence in this investigation is stored electronically. If alerted to the existence of the warrant, the subjects under investigation could destroy that evidence, including information saved to their personal computers.

WHEREFORE, the United States respectfully requests that the Court grant the attached Order directing Apple not to disclose the existence or content of the attached warrant for one year, except that Apple may disclose the attached warrant to an attorney for Apple for the purpose of receiving legal advice.

The United States further requests that the Court order that this application and any resulting order be sealed until further order of the Court. As explained above, these documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Executed on 5/24/2023.

Kathryn M. Dieruf
Assistant United States Attorney
United States Attorney's Office
Eastern District of Kentucky
260 W. Vine Street
Lexington, KY 40507
(859)685-4885
Kathryn.Dieruf@usdoj.gov

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF KENTUCKY

INFORMATION ASSOCIATED WITH APPLE ACCOUNT ASSOCIATED WITH 919867615027 THAT IS STORED AT PREMISES CONTROLLED BY APPLE INC.	Case No. 5:23-MJ-5200 **Filed Under Seal**

ORDER

The United States has submitted an application pursuant to 18 U.S.C. § 2705(b), requesting that the Court issue an Order commanding Apple Inc. ("Apple"), an electronic communication service provider and/or a remote computing service, not to notify any person (including the subscribers and customers of the account(s) listed in the warrant) of the existence of the attached warrant for one year from the date of this order.

The Court determines that there is reason to believe that notification of the existence of the attached warrant will seriously jeopardize the investigation or unduly delay a trial, including by giving targets an opportunity to flee or continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, intimidate potential witnesses, or endanger the life or physical safety of an individual. *See* 18 U.S.C. § 2705(b).

IT IS THEREFORE ORDERED under 18 U.S.C. § 2705(b) that Apple shall not disclose the existence of the attached warrant, or this Order of the Court, to the listed subscriber or to any other person, for a period of one year from the date of this order, unless this non-disclosure period is extended by further order of the Court, except that Apple may disclose the attached warrant to an attorney for Apple for the purpose of receiving legal advice.

IT IS FURTHER ORDERED that the application and this Order are sealed for a period of one year from the date of this order.

Entered the 7th day of June, 2023.

MATTHEW A. STINNETT
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF KENTUCKY