AO 91 (Rev. 11/11) Criminal Complaint (Rev. by USAO on 3/12/20) ☐ Original ☐ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Central District of California

United States of America

v.

SCOTT QUINN BERKETT,

Defendant

Case No. 2:21-mj-02521

CRIMINAL COMPLAINT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

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 of May 20, 2021 in the county of Los Angeles in the Central District of California, the defendant violated:

Code Section	*Offense Description*
18 U.S.C. § 1958	Murder for Hire

This criminal complaint is based on these facts:

Please see attached affidavit.

☒ Continued on the attached sheet.

Complainant's signature

Caitlin Bowdler, 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.

Date: 5/21/21

Judge's signature

City and state: Los Angeles, California

Hon. Margo A. Rocconi, U.S. Magistrate Judge
Printed name and title

AUSA: Axelrad x7964

AFFIDAVIT

I, Caitlin Bowdler, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI") and have been so employed since March 2017. I am currently assigned to the Los Angeles Field Division Violent Crime Squad which is responsible for investigating kidnappings, extortion, bank robberies, Hobbs Act violations, and other violent crimes. During the time I have been employed by the FBI, I have also worked on a white-collar crime squad.

2. Since becoming an FBI Special Agent, I have received formal training at the FBI Training Academy in Quantico, Virginia. This training included segments on conducting criminal investigations, narcotics identification, organized crime, and other law enforcement topics. During the time I have been employed by the FBI, I have participated in investigations relating to extortion, cybercrimes, wire fraud, mortgage fraud, identity theft, mail fraud, and various types of financial institution fraud and violent crimes. I have participated in many aspects of criminal investigations, such as, but not limited to, reviewing evidence, the issuance of subpoenas, the analysis of pen and trap and trace records, consensually monitored telephone calls, conducting physical and electronic surveillance, working with informants, and the execution of search and arrest warrants.

II. PURPOSE OF AFFIDAVIT

3. This affidavit is made in support of a criminal complaint against, and arrest warrant for, SCOTT QUINN BERKETT ("BERKETT") for a violation 18 U.S.C. § 1958 (Murder-For-Hire). This affidavit is also made in support of search warrants for the following:

a. The premises located at 301 S. El Camino Drive, Beverly Hills, California 90212 ("SUBJECT RESIDENCE") as described more fully in Attachment A-1;

b. A 2008 MERCEDES CLK 350 with California license plate 6GFE033, VIN WDBTK56F08T099038 (the "SUBJECT VEHICLE") as described more fully in Attachment A-2;

c. The person of BERKETT, as described more fully in Attachment A-3.

4. The requested search warrants seek authorization to seize evidence, fruits, or instrumentalities of violations of 18 U.S.C. § 1958 (Murder-For-Hire); 18 U.S.C. § 373 (Solicitation to Commit a Crime of Violence); and 18 U.S.C. § 371 (Conspiracy) (the "SUBJECT OFFENSES"), as described more fully in Attachment B. Attachments A-1, A-2, A-3, and B are incorporated herein by reference.

5. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint and search warrants and does not purport to set forth all of my

knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

III. TRAINING AND EXPERIENCE ON BITCOIN

6. A Bitcoin wallet is used to store cryptocurrency and can control multiple Bitcoin addresses. The wallet interfaces with the blockchain and uses private keys to restrict access to spending Bitcoin.

7. Bitcoin is a type of virtual currency, circulated over the Internet. Bitcoin are not issued by any government, bank, or company, but rather are controlled through computer software operating via a decentralized, peer-to-peer network. Bitcoin is just one of many varieties of virtual currency.

8. Bitcoin are sent to and received from Bitcoin "addresses." A Bitcoin address is somewhat analogous to a bank account number and is represented as a 26-to-35-character-long case-sensitive string of letters and numbers. Each Bitcoin address is controlled through the use of a unique corresponding private key. This key is the equivalent of a password, or PIN, and is necessary to access the funds associated with a Bitcoin address. Only the holder of an address' private key can authorize transfers of bitcoin from that address to other Bitcoin addresses. Users can operate multiple Bitcoin addresses at any given time and may use a unique Bitcoin address for each and every transaction.

9. To acquire bitcoin, a typical user purchases them from a virtual currency exchange. A virtual currency exchange is a business that allows customers to trade virtual currencies for other forms of value, such as conventional fiat money (e.g., U.S. dollars, Russian rubles, euros). Exchanges can be brick-and-mortar businesses (exchanging traditional payment methods and virtual currencies) or online businesses (exchanging electronically transferred money and virtual currencies). Virtual currency exchanges doing business in the United States are regulated under the Bank Secrecy Act and must collect identifying information about their customers and verify their clients' identities.

10. To transfer bitcoin to another Bitcoin address, the sender transmits a transaction announcement, which is electronically signed with the sender's private key, across the peer-to-peer Bitcoin network. To complete a transaction, a sender needs only the Bitcoin address of the receiving party and the sender's own private key. This information on its own rarely reflects any identifying information about either the sender or the recipient. As a result, little-to-no personally identifiable information about the sender or recipient is transmitted in a Bitcoin transaction itself. Once the sender's transaction announcement is verified by the network, the transaction is added to the blockchain, a decentralized public ledger that records every Bitcoin transaction. The blockchain logs every Bitcoin address that has ever received bitcoin and maintains records of every transaction for each Bitcoin address.

11. While a Bitcoin address owner's identity is generally anonymous within the blockchain (unless the owner opts to make information about the owner's Bitcoin address publicly available), investigators can use the blockchain to identify the owner of a particular Bitcoin address. Because the blockchain serves as a searchable public ledger of every Bitcoin transaction, investigators can trace transactions to, among other recipients, Bitcoin exchangers. Because Bitcoin exchangers generally collect identifying information about their customers, as discussed above, subpoenas or other appropriate legal process submitted to exchangers can, in some instances, reveal the true identity of an individual responsible for a Bitcoin transaction.

IV. SUMMARY OF PROBABLE CAUSE

12. In May 2021, law enforcement received information that an individual purportedly solicited murder-for-hire services via a Dark Web Group. The individual provided specific directions about the requested murder and details about the target, Victim 1. This individual sent Bitcoin payments totaling approximately $14,000 to the Dark Web Group that was purchased using a debit card and bank account belonging to BERKETT. Based on this information, law enforcement contacted and interviewed Victim 1. Victim 1 confirmed a prior acrimonious relationship with BERKETT.

13. On May 19, 2021, an undercover law enforcement agent ("UC") contacted BERKETT, while impersonating the hitman BERKETT had contracted with via the Dark Web Group. During a series of

recorded conversations, BERKETT confirmed his requested murder of Victim 1, provided additional identifying details regarding Victim 1 and her location, and, on May 20, 2021, made an additional payment of $1,000 via Western Union intended for the UC.

V. STATEMENT OF PROBABLE CAUSE

A. Personal and Sexual Relationship Between BERKETT and Victim 1

14. Based on my conversations with other law enforcement agents, and my familiarity with this investigation, as well as my May 14, 2021, interview of Victim 1, I am aware of the following:

a. Victim 1 met BERKETT through a Facebook Fan Page called RWBY Nation related to a Japanese anime show. BERKETT and Victim 1 were both administrators for the site and began personally communicating in approximately July or August 2020.

b. BERKETT and Victim 1 messaged each other on the Discord messaging application and talked over the phone. BERKETT used the phone number 310-922-9623 to contact Victim 1 (hereafter, "BERKETT's Phone.")

c. On October 27, 2020, Victim 1 flew to meet BERKETT in Los Angeles, California. Victim 1 stayed in Los Angeles until October 30, 2020. Prior to this meeting, Victim 1 had never met BERKETT in person.

d. On October 27, 2020, BERKETT picked Victim 1 up at LAX in the SUBJECT VEHICLE. That same day, BERKETT took Victim 1 to the Avalon Hotel, located at 9400 W. Olympic Blvd.,

Beverly Hills, California 90212, where he paid for a room for Victim 1 to stay during the visit.

e. On or about May 17, 2021, I reviewed records provided by Avalon Hotel in Beverly Hills. These records confirmed the phone number listed for the reservation was BERKETT's Phone, the email address was scott.berkett@gmail.com, and that the room was paid for by a VISA card ending in 0715.

B. Victim 1 Ends Relationship with BERKETT

15. Based on my conversations with other law enforcement agents, and my familiarity with this investigation, as well as my May 14, 2021, interview of Victim 1, I am aware of the following:

a. During Victim 1's trip to Los Angeles, Victim 1 had sex with BERKETT, but felt pressured to do so. BERKETT was sexually aggressive towards Victim 1.

b. After the trip, Victim 1 tried to break up the relationship with BERKETT, but he refused to accept the break-up. BERKETT became very possessive and began constantly messaging Victim 1 on multiple social media and communications platforms. When Victim 1 did not respond to a message on one platform, BERKETT would find another way to message her.

c. Victim 1 tried to break up the relationship in December over the phone, but BERKETT refused to accept the break-up. On January 1, 2021, Victim 1 broke up with BERKETT via the text messaging application Discord. Eventually BERKETT and Victim 1 began speaking again. BERKETT became very possessive, despite Victim 1 wanting to move on. On February 7,

2021, Victim 1 confronted BERKETT, explaining that she had asked for space and he had not given it to her, and told him to back off. While BERKETT appeared to accede, approximately a month later BERKETT confronted Victim 1 about the way she had confronted him about needing space in February. BERKETT claimed that Victim 1 had used him.

d. In April 2021, Victim 1 was visiting a family member who knew that Victim 1 and BERKETT had been dating and that Victim 1 had gone to meet him in October 2020. Victim 1's family member learned that BERKETT had been sexually aggressive with Victim 1 during the California trip.

e. Victim 1's family member knew that Victim 1 had attempted to break up with BERKETT, but BERKETT continued to contact Victim 1. Victim 1's family member obtained BERKETT's father's phone number and, along with Victim 1's family member's acquaintance, called and text messaged BERKETT's father's phone number. During text messages on April 20, 2021, Victim 1's family requested that BERKETT cease contact with Victim 1 and indicated they would involve law enforcement. During the text messages, BERKETT appears to have begun using his father's phone, stating "This is Scott. I haven't spoken to [Victim 1] in over a month." After Victim 1's family demanded that BERKETT cease contact with Victim 1, BERKETT responded, "She is blocked from all social media. Will consider this matter closed."

C. BERKETT Attempts to Hire Hitman to Murder Victim 1

16. Based on a May 14, 2021 conversation with Special Agent Clay M. Anderson, I learned the following:

a. On or about May 7, 2021, members of an investigative media organization ("Complainants") advised the FBI that they had information they believed to be a threat to life. Law enforcement presently understands that the source of the information to the Complainants was a group on the Dark Web that advertised murder-for-hire services. As law enforcement presently understands, this Dark Web Group was a scam. To my knowledge, law enforcement has not had direct contact with this Dark Web Group.

b. The Complainants provided the name and address of Victim 1, who was named as a target in a murder-for-hire. The Complainants were able to provide transaction information from an unnamed source on the Dark Web ("Dark Web Group") that showed that Bitcoin payments were made with an understanding that an unknown individual would murder Victim 1.[1] The information provided was specific about the identity and location of Victim 1, as well as social media accounts, nicknames, email, and a distinctive tattoo of Victim 1.

[1] The "dark web," also sometimes called the "darknet," "dark net" or "deep web," is a colloquial name for a number of extensive, sophisticated, and widely used criminal marketplaces operating on the Internet, which allow participants to buy and sell illegal items, such as drugs, firearms, and other hazardous materials with greater anonymity than is possible on the traditional Internet (sometimes called the "clear web" or simply "web"). These online black market websites use a variety of technologies, including the Tor network (defined below) and other encryption technologies, to ensure that communications and transactions are shielded from interception and monitoring. A famous dark web marketplace, Silk Road, operated similar to legitimate commercial websites such as Amazon and eBay, but offered illicit goods and services. Law enforcement shut down Silk Road in 2013.

c. Also provided by the Complainants were purported excerpts of communications on the Dark Web between a user, "Ula77" and the Dark Web Group. Within these communications[2], on approximately April 22, 2021, Ula77 was asked, "hi, are u looking for a hitman?" to which Ula77 responded, "Saving up for a simple hit. Ill be putting the job in as soon as I have the BTC." Based on my training and experience, as well as my familiarity with this investigation, I believe "BTC" was a reference to Bitcoin.

d. On April 27, 2021, Ula77 states, "Hello, I was hoping you would be the person to contact if I had questions on what sort of information I would need to have ahead of time when placing a hit if I dont have the address, and if I can make small requests for once the hits been carried out IE: Make sure to destroy the phone of the target."

e. On April 28, 2021, following the payment of Bitcoin, Ula77 submitted their "order," providing the information, "OrderName: [Victim 1's name]" and Order Description, "I'd like it to look like an accident, but robbery gone wrong may work better. So long as she is dead. I'd also like for her phone to be retrieved and destroyed irreparably in the process." On that same day, Ula77 stated, "I would like proof of her death sent to me. She has a distinctive tattoo on one of her forearms that I know the image of, so a photo of her

[2] As discussed below, while law enforcement has not been able to verify these communications through direct contact with the Dark Web Group, the substance of these communications has been verified through BERKETT's extensive conversations with an undercover law enforcement officer on May 19 and 20, 2021.

corpse and a photo of her tattoo for identification would work. I'll refrain from sending a picture of the tattoo to avoid doctored photos. If possible, letting me know if she was in Arizona or Idaho wuld also be appreciated so I can also verify via the obituaries."

f. On May 9, 2021, Ula77 stated, "Ive updated the order so that the bounty matches with what you informed me the hitman was requesting for the job: 2000 extra to check both locations and 2000 extra to destroy the phone, and the original 9000 bounty, for a total of 13000. I look forward to receiving communications that will let me know when, approximately, to prepare my alibi."

17. Based on my training and experience, and conversations with other law enforcement officers and agents, as well as my personal familiarity with this investigation, I am aware of the following:

a. Information provided by the Complainants described the time of the transaction as well as the receiving Bitcoin wallet belonging to the Dark Web Group. The information indicated that Bitcoin payments for the murder of Victim 1 were made on April 25, 26, and 28, and May 5, 2021.

b. Based on an analysis of the Bitcoin blockchain used in the transaction, law enforcement was able to determine that the Bitcoin wallets used to pay the Dark Web Group were CoinBase wallets. CoinBase is a Bitcoin exchange service.

c. CoinBase provided the owner of the Bitcoin wallets that the Complainants indicated were responsible for

paying the Dark Web Group, as well as the transaction history for those wallets, which I reviewed. The information provided by CoinBase shows BERKETT listed as the owner of the Coinbase Wallets and shows the transactions between BERKETT and the entity behind the murder for hire sought by BERKETT -- believed to be the Dark Web Group.

d. CoinBase also provided the registration information for the CoinBase wallets associated with payment to what is believed to be the Dark Web Group, which included the name associated with the account, "Scott Berkett," with the address listed as the SUBJECT RESIDENCE, and the date of birth, driver's license number, social security number, and phone number associated with BERKETT.

e. Coinbase further provided the Bank of America savings account and Mastercard debit card used to purchase the Bitcoin. Both are registered in BERKETT's name.

D. BERKETT Confirms His Desire to Have Victim 1 Murdered During Conversation with Undercover Law Enforcement Agent

18. Based on my training and experience, my participating in the investigation, conversations with the undercover agent, and my review of WhatsApp messages and recorded telephone calls, I am aware of the following:

a. On May 19, 2021, a law enforcement undercover agent ("UC") contacted BERKETT via the WhatsApp communications application, purporting to be the hitman BERKETT had contracted using the Dark Web. The UC sent BERKETT photos via WhatsApp of Victim 1 in a Walmart store. The UC also sent the message,

"Call me." Based on the conversation that followed, I believe that BERKETT was the user of Ula77 during the communications with the Dark Web Group.

b. On May 19, 2021, at approximately 9:55 p.m., the UC spoke with BERKETT using BERKETT's Phone. During this initial call, BERKETT claimed to not have received the photos sent to him by the UC and asked that the photos be resent. Shortly thereafter, the UC resent the photos of Victim 1 and, at approximately 9:59 p.m., the UC called BERKETT back via WhatsApp at the same number.

c. During this call, the UC confirmed that BERKETT had received the photos of Victim 1 and represented to BERKETT that he was the hitman hired to fulfill the murder-for-hire contract BERKETT had sought via the Dark Web and paid for using Bitcoin. Specifically, BERKETT and the UC had the following exchange:

UC: "Hi. You got the pictures?"

BERKETT: "Yup."

UC: "Yeah. So, I'm following up on uh, something that was started a little while ago. Um. I'm just making contact with you."

BERKETT: "Okay. I was actually surprised to get, get that through WhatsApp."

UC: "I know. We switch things up every once in a while. We'll pick another one after this."

BERKETT: "Okay, sounds good. Yeah, it seems to be the person. Uh, can't recognize them about, can't recognize

them as well because of the graininess but, yeah that looks, that looks like them."

UC: "That's, that's her, right?"

BERKETT: "Yeah, that's her."

d. The UC then confirmed again that the photos of the victim were BERKETT's intended target and that BERKETT had used a Bitcoin payment to obtain her murder. Specifically, BERKETT and the UC had the following exchange:

UCE: "Confirming that's the person that we talked about on the uh, on the other piece, right?"

BERKETT: "Yeah."

UCE: "Okay. And you've already made, you're already made the uh, the uh… the B payment, right?"

BERKETT: "Yeah, I've already done that."

UCE: "Okay, good."

BERKETT: "That was confirmed by uh… yeah."

e. Based on my training and experience, as well as my familiarity with this investigation, I believe the "other piece" was a reference by the UC to the dark web and that "B payment" was a reference by the UC to the Bitcoin payment made to the dark web site by Ula77. BERKETT's response appears to confirm his understanding of these references.

f. The UC and BERKETT then discussed details of the murder, namely, how the murder should be made to appear, i.e. as a robbery or accident. During this portion of the discussion, BERKETT expressed concern that the murder not be traced back to him. BERKETT also confirmed his desire for proof-of-death, that

is, a photograph of the victim's distinctive tattoo.

Specifically, BERKETT and the UCE had the following exchange:

UC: "Good. Alright, so my understanding is what has to get done is this has to get done, uh we're looking at some kind of accident or robbery to have gone wrong, right?"

BERKETT: "Yeah."

UC: "Okay."

BERKETT: "That way it doesn't get traced."

UC: "Right, and then we need to work on making sure your alibi is good. Um, and then we need some, you want some kind of proof, and there's, if I'm, if I'm getting the information right, it's some kind of phone that needs to be taken care of as well, right?"

BERKETT: "Yeah."

UC: "Okay."

BERKETT: "Uh, proof of the uh tattoo on her, one of her forearms."

UC: "Okay. Do you want, is there, do you want that tattoo? Is that part of this?"

BERKETT: "Just need a picture of it to verify."

UC: "Okay, do you, do you want it? Do you, is that, what kind of souvenir do you need, or do you need one?"

BERKETT: "Uh, just the photo…"

UC: "Just the photo."

BERKETT: "…of the tattoo."

UC: "Okay, so"

BERKETT: "It's distinctive enough that I don't need a

souvenir."

g. The UC then asked BERKETT what sort of proof of death he required. Specifically, BERKETT and the UC had the following exchange:

UC: "Okay. What, is there any part of it, so, do you wanna see? Do you want a video of her not breathing? What do, what do you want to see?"

BERKETT: "Um, picture of the corpse and a picture of the tattoo, of the tattoo, to make, to verify . . ."

UCE: "Okay."

BERKETT: ". . . Just so that way, cuz there were warnings of like, hey, make sure it's not photo-shopped."

h. The UC asked BERKETT to provide additional payment to complete the murder of Victim 1, stating "if you could just send me, can you, can you float a grand or half a grand to a Western Union to get this thing done?" The UC then provide specific information as to where and to whom to send the money. The UC also texted BERKETT this information via WhatsApp.

i. BERKETT and the UC then discussed BERKETT developing an alibi for Victim 1's death, with BERKETT stating, "Uh, there's a, okay. There's a few places nearby maybe that, that uh can put me on camera." BERKETT and the UC then discussed locations where BERKETT's car could be seen on camera, with BERKETT describing his car as "an old Mercedes." The SUBJECT VEHICLE is a 2008 Mercedes that BERKETT was observed driving as recently as May 13, 2021, and has been observed on

the curb in front of the garage of the SUBJECT RESIDENCE on May 19 and 20, 2021.

j. The UC then asked for any additional information about Victim 1, to which BERKETT responded that she has a dog, that her family has a gun, and that Victim 1 "Uh . . . has weak heart, so probably would be very e . . ., so any uh, any drunk, any feigning a drunk driver situation would probably be very easy to pull off, off probably, would and, wouldn't have as high of a survival chance. Uh . . ."

19. Based on the conversations between Victim 1 and law enforcement, the details provided by BERKETT to the UC align with Victim 1. Victim 1 stated that she has a dog and the dog has come up in conversation with BERKETT. Additionally, Victim 1 has confirmed that her family does have a gun at their residence and Victim 1 recalled a conversation with BERKETT where this was discussed.

E. BERKETT Makes Western Union Money Transfer For Murder of Victim 1

20. Based on my training and experience, and conversations with other law enforcement officers and agents, as well as my personal familiarity with this investigation, I am aware of the following:

a. On May 19, 2021, BERKETT was instructed by the UC to make a Western Union Money Transfer of $1,000 to an individual in Scottsdale, Arizona, as payment for the murder-for-hire. The next day, May 20, 2021, the UC messaged BERKETT on WhatsApp asking for an update and, at approximately 3:11

p.m., BERKETT responded that he "started to move the funds. Shouldn't take more than an hour. I'll let you know if there's an issue.

b. On May 20, 2021, following BERKETT's discussion with the UC, I conducted surveillance of the SUBJECT RESIDENCE during which law enforcement observed BERKETT leave the house and walk to the Rite Aid located at 463 N. Bedford Drive, Beverly Hills 90210. A Western Union kiosk is located inside this Rite Aid. While inside the Rite Aid, at approximately 5:25 p.m., I observed BERKETT at the Western Union booth and on the Western Union phone. BERKETT then went to the Rite Aid cashier to pay for the transaction. I observed BERKETT present the cashier with cash.

c. Following this transaction, FBI SA Sarah Corcoran received a Rite Aid Corporation Detail Journal Report from a Rite Aid employee that showed a $1,000 Western Union transaction with Rite Aid and $31 fee had been paid by BERKETT.

d. At approximately 5:45 p.m., BERKETT messaged the UC on WhatsApp, "Done. 5350546096." Based on my training and experience, as well as my familiarity with this investigation, I believe this message from BERKETT to the UC was confirmation that he had made the Western Union transfer for the murder and was providing the proof of transfer code to the UC.

e. On May 21, 2021, I was able to confirm through Western Union's website using the "5350546096" tracking code provided by BERKETT, that the money was transferred and was ready for pick up.

F. Investigation of SUBJECT RESIDENCE and SUBJECT VEHICLE

21. Based on my training and experience, and conversations with other law enforcement officers and agents, as well as my personal familiarity with this investigation, I am aware of the following:

a. On or about May 14, 2021, I reviewed records obtained from the California Department of Motor Vehicles and learned that SUBJECT VEHICLE is currently registered to BERKETT's father, who also lives at the SUBJECT RESIDENCE. According to Victim 1, BERKETT was driving SUBJECT VEHICLE when he picked her up from LAX in October 2020.

b. On or about May 14, 2021, I submitted an Emergency Disclosure Request ("EDR") for subscriber information and records for BERKETT's Phone. In response to the EDR, the contact name on the account was provided: "Scott Berkett." BERKETT's father was also listed on the account. Also, in response to the EDR, Verizon provide information that on or about May 14-16, 2021, BERKETT's phone number was pinging consistently in the vicinity of SUBJECT RESIDENCE.

c. Based on my conversations with Victim 1, during her trip to Los Angeles in October 2020 to visit BERKETT, she visited the SUBJECT RESIDENCE. According to Victim 1, BERKETT has a room within this residence.

d. On May 17, 2021, Victim 1 was provided photos of the SUBJECT VEHICLE and she confirmed this was the vehicle that BERKETT drove during her trip.

e. On or about May 14, 16, 19, and 20, 2021, I conducted physical surveillance of the SUBJECT RESIDENCE. At that time, the SUBJECT VEHICLE was parked on the curb in front of the garage for the residence.

f. Based on the foregoing, I believe that BERKETT currently lives at the SUBJECT RESIDENCE and has access to and operates the SUBJECT VEHICLE.

G. Probable Cause to Believe Evidence of the SUBJECT OFFENSES Will be Found in SUBJECT RESIDENCE, SUBJECT VEHICLE, and on BERKETT's Person

22. Based on my training and experience investigating stalking and threat-to-life cases, I know that individuals engaged in such conduct commonly use fake or anonymized accounts, false identifications or identities, or stolen identifications, in order to avoid detection and to hide their true identities. These individuals often also keep evidence related to these accounts and identifiers in secure, easily-accessible places, like their homes, cars, and on their person.

23. Based on the foregoing, as well as my training, experience, and knowledge of this investigation, I also believe that electronic devices, including computers, laptops, tablets, and cellular telephones capable of making telephone calls and accessing the internet as discussed above -- and that were likely used by BERKETT during the activities described herein -- will be found at the SUBJECT RESIDENCE, in the SUBJECT VEHICLE, and on BERKETT's person. Based on BERKETT's use of the internet, and other digital devices, I also believe digital and physical evidence related to the SUBJECT OFFENSES (including

evidence related to identity) will be found at the SUBJECT RESIDENCE, in the SUBJECT VEHICLE, and on BERKETT's person.

VI. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

24. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable

data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

25. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which

may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

26. The search warrant requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when

a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

c. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress BERKETT's thumb and/or fingers on the device(s); and (2) hold the device(s) in front of BERKETT's face with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

//

//

VII. CONCLUSION

27. For all the reasons described above, there is probable cause to believe that BERKETT has solicited the murder of Victim 1 in violation of 18 U.S.C. § 1958 (Murder-For-Hire). Further, there is probable cause to believe that evidence of violations of the SUBJECT OFFENSES, as described above and in Attachment B of this affidavit, will be found in a search of the SUBJECT RESIDENCE, the SUBJECT VEHICLE, and on BERKETT's person as further described above and in Attachments A-1, A-2, A-3, to this affidavit.

Caitlin Bowdler, Special Agent
FBI

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this ___ day of May, 2021.

UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A-1

PREMISES TO BE SEARCHED

The premises located at 301 S. El Camino Drive, Beverly Hills, California 90212, the residence of SCOTT BERKETT ("SUBJECT RESIDENCE"). The SUBJECT RESIDENCE is a two-story single-family residence, as depicted in the photograph below.

The SUBJECT RESIDENCE includes any and all storage units, containers, attachments, attics, safes, carports, garages, vehicles, outbuildings, and all other areas within the curtilage.

ATTACHMENT A-2

VEHICLE TO BE SEARCHED

A red Mercedes Benz sedan with California license plate 6GFE033, and Vehicle Identification number WDBTK56F08T099038 ("SUBJECT VEHICLE"), as depicted in the photograph below.

ATTACHMENT A-4

PERSON TO BE SEARCHED

The person of SCOTT BERKETT ("BERKETT"), date of birth April 22, 1997, with California Driver's License Number F7005190. BERKETT's California Department of Motor Vehicle records lists him as standing 6'0" tall with brown hair and green eyes.

The search of BERKETT shall include any and all clothing and personal belongings, digital devices, backpacks, wallets, briefcases, purses, and bags that are within BERKETT's immediate vicinity and control at the location where the search warrant is executed. The search shall not include a strip search or a body cavity search.

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. § 1958 (Murder-For-Hire); 18 U.S.C. § 373 (Solicitation to Commit a Crime of Violence); and 18 U.S.C. § 371 (Conspiracy) (the "SUBJECT OFFENSES"), namely:

a. Messages, documents, communications, photographs, records or digital media regarding Victim 1, the dark net, the dark web, or similar Tor network, soliciting murder, soliciting a crime of violence, bitcoin, and cryptocurrency;

b. Records and information related to victim, including but not limited to photographs, videos, drawings, depicting the likenesses of the victim, their relatives, neighbors, co-workers, or friends;

c. Records or internet searches or activity regarding murder, murder-for-hire, alibis, hitman, bitcoin, cryptocurrency, the dark web, and the dark net;

d. Records and information related to threats to commit, or the commission of acts of sexual or other physical violence against others;

e. Records and information relating to the purchase, possession, or use of digital devices, including smartphones, "burner" phones, desktop computers, laptop computers, encryption software/services, virtual Private Network ("VPN") subscription services, and identity alteration or modulation devices, programs and software;

f. Records and information relating to accounts used or controlled by BERKETT with any telephone service provider, internet service provider, or other online communication service;

g. Records and information related to the use of instant and social media messages (such as Discord, Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp), SMS text, email communications, or other text or written communications sent to or received from any digital device in connection with the SUBJECT OFFENSES;

h. Records and information related to the use of the dark net and any accounts used or controlled by BERKETT on the dark web or dark net;

i. Records and information related to call logs, including all telephone numbers dialed from any of the digital devices seized and all telephone numbers accessed through any push-to-talk functions, as well as all received or missed incoming calls;

j. Records and information sufficient to show address book information, including all stored or saved telephone numbers;

k. Records and information sufficient to show indicia of occupancy, residency or ownership of the SUBJECT RESIDENCE and the property to be seized pursuant to the warrants, including forms of personal identification, records

relating to utility bills, telephone bills, loan payment receipts, rent receipts, trust deeds, lease of rental agreements, addressed envelopes, escrow documents, keys, letters, mail, canceled mail envelopes, or clothing;

l. Global Positioning System ("GPS") coordinates and other information or records identifying travel routes, destinations, origination points, and other locations from October 2019 to the present; and

m. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the SUBJECT OFFENSES, and forensic copies thereof.

n. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal

digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURE FOR DIGITAL DEVICES

4. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) and/or forensic image(s) thereof beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

c. The search team will not seize contraband or evidence relating to other crimes outside the scope of the items to be seized without first obtaining a further warrant to search for and seize such contraband or evidence.

d. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

5. The review of the electronic data obtained pursuant to this warrant 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 investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

6. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

7. During the execution of this search warrant, law enforcement is permitted to: (1) depress BERKETT's thumb and/or fingers onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of BERKETT's face with his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

8. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.