~~SEALED~~

s/ T. Ferris

ORDERED UNSEALED on 07/19/2021 s/ TrishaF

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA, Plaintiff, v. Lindsay Renee HENNING, Garrett Carl TUGGLE, Defendants.	Case No.: **21-MJ-2060** COMPLAINT FOR VIOLATION OF: Title 21 U.S.C.§ 841(a)(1) Distribution of a Controlled Substance (Felony); Title 21 U.S.C. §§ 841(a)(1) and 846 Conspiracy to Distribute LSD (Felony); Title 18, U.S.C., Sec. 1349 – Conspiracy; Title 18, U.S.C., Sec. 981(a)(1)(C), and Title 28, U.S.C., Sec 2461(c) – Criminal Forfeiture

The undersigned complainant being duly sworn states:

COUNT ONE

On or about June 15, 2020, within the Southern District of California, defendant, Lindsay Renee HENNING, did knowingly and intentionally distribute approximately 7 grams (0.015 pounds) of a mixture and substance containing a detectable amount of

methylenedioxymethamphetamine (MDMA), a Schedule II Controlled Substance in violation of Title 21, United States Code, Section 841(a)(1).

COUNT TWO

Beginning at a date unknown and continuing up to and including September 8, 2020, within the Southern District of California, defendant, Lindsay Renee HENNING, did knowingly and intentionally conspire together with JT and with other persons known and unknown to distribute approximately 1 gram and more, of a mixture and substance containing a detectable amount of lysergic acid diethylamide (LSD), a Schedule I Controlled Substance; in violation of Title 21, United States Code, Sections 841(a)(1) and 846 and, Title 18, United States Code, Section 2.

COUNT THREE

Beginning as early as May 31, 2020 and continuing up to present, within Southern District of California and elsewhere, defendants, Lindsay Renee HENNING and Garrett Carl TUGGLE, knowingly and intentionally conspired and agreed with others, known and unknown to the grand jury, to commit the offense of wire fraud, in violation of Title 18, United States Code, Section 1343, all in violation of Title 18, United States Code, Section 1349.

COUNT FOUR

On or about the dates set forth below, in the Southern District of California and elsewhere, during and in relation to a felony violation of Title 18, United States Code, Section 1349 (Conspiracy to Commit Wire Fraud), defendant, Lindsay Renee HENNING and Garrett Carl TUGGLE, knowingly transferred, possessed, and used, without lawful authority, the means of identification of another person as listed below, knowing that the means of identification belonged to another actual person.

//

//

//

//

Count	Defendant	Approx. Date	Actual Person	Means of Identification
4	HENNING and TUGGLE	July 10, 2020	R.D.	Name, Social Security Number, Date of Birth
5	TUGGLE	July 1, 2020 – present	T.H.	Name, Social Security Number, Date of Birth
6	TUGGLE	May 19, 2020 – Apr. 6, 2021	J.H.	Name, Social Security Number, Date of Birth

All in violation of Title 18, United States Code, Section 1028A.

FORFEITURE ALLEGATIONS

Upon conviction of one or more of the offenses alleged in Counts 1 – 6, of this Complaint and pursuant to Title 18, United States Code, Section 981 (a) (1) (C), Title 28, United States Code, Section 2461 (c), defendants Lindsay Renee HENNING and Garrett Carl TUGGLE shall forfeit to the United States any property, real and personal, which constitutes and is derived from proceeds traceable to the offenses, and any property traceable to such property, including: cash; bitcoin or cryptocurrency wallets; a 2020 Dodge Ram pickup truck (VIN 1C6SRFFT5LN163759); a 2015 Airstream Flying Cloud M-23D trailer (VIN 1STB9AG25FJ531744), both registered to Lindsay Renee HENNING; and a 2006 Mercedes Benz E55 Sedan (VIN WDBUF76J16A872178) registered to Garrett Carl TUGLE.

If any of the above-described forfeited property, as a result of any act or omission of defendant Lindsay Renee HENNING, cannot be located upon the exercise of due diligence; has been transferred or sold to, or deposited with, a third person; has been placed beyond the jurisdiction of the Court; has been substantially diminished in value; or has been commingled with other property which cannot be subdivided without difficulty, it is the intent of the United States, pursuant to Title 21, United States Code, Section 853 (p), made applicable herein by Title 18, United States Code, Section 982 (b), to seek forfeiture of any

other property of the defendant up to the value of the property described above subject to forfeiture.

All pursuant to Title 18, United States Code, Sections 981(a)(1)(C) and 982(a)(1), and Title 28, United States Code, Section 2461(c).

The complainant states that this complaint is based on the attached Affidavit incorporated herein by reference.

Sarah Duray

Special Agent Sarah Duray
Drug Enforcement Administration

Sworn and attested to under oath by telephone, in accordance with Federal Rule of Criminal Procedure 4.1, this 20th day of May, 2021.

HON. KAREN S. CRAWFORD
U. S. MAGISTRATE JUDGE

AFFIDAVIT

I Sarah Duray, being duly sworn, states:

1. I am a Special Agent (SA) Criminal Investigator for the United States (U.S.) Drug Enforcement Administration (DEA), and I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18 of the United States Code. I am empowered by law to conduct investigations and to make arrests for felony offenses. I was hired by the DEA in May of 2018, and I attended the DEA academy for approximately 18 weeks. At the DEA Academy, I was trained in the various aspects of conducting narcotics investigations. My training at the DEA Academy in Quantico, Virginia, included drug identification, detection, and interdiction, money laundering techniques, conspiracy investigations, and asset identification, seizure, and forfeiture. In September 2018, I was sworn as a DEA SA and was assigned to DEA San Diego Field Division (SDFD).

2. While with the DEA, I have participated in approximately 100 narcotics investigations and more than 50 arrests for violations of the California Health & Safety (H&S) Code and Title 21 of the U.S. Code. These investigations and arrests involved: (1) unlawful importation, exportation, manufacture, possession with intent to distribute and distribution of narcotics; (2) the laundering of narcotics proceeds and monetary instruments derived from narcotics activities; and (3) conspiracies associated with narcotics offenses. These investigations have involved debriefing defendants, witnesses and informants, conducting surveillance, assisting in court ordered interceptions, executing search warrants, seizing narcotics and narcotics-related assets and making arrests for narcotics-related offenses.

3. Upon my arrival at the DEA SDFD, I was assigned to the San

Diego County Integrated Narcotics Task Force (NTF) Team 10 and was so assigned until March 2020. NTF Team 10 is comprised of DEA SAs, Task Force Agents (TFAs) and Task Force Officers (TFOs) from Homeland Security Investigations (HSI), Federal Bureau of Investigation (FBI), California Department of Health Care Services and Detectives (federally cross sworn TFOs) from the San Diego Police Department (SDPD), who primarily investigate illegal drug trafficking organizations operating in the U.S., and internationally, including those organizations whose operations involve the distribution of wholesale and retail quantities of fentanyl, oxycodone, hydrocodone or other controlled pharmaceutical drugs, cocaine, methamphetamine, marijuana, heroin and their derivatives in and around the San Diego, California area. NTF Team 10 focuses on investigating illegal drug distribution related to drug overdose deaths in San Diego County. In March 2020, I was assigned to the DEA Tactical Diversion Squad (TDS). TDS primarily investigates the diversion of pharmaceutical pills for illicit purposes, as well as counterfeit pharmaceutical pills being manufactured and sold in the U.S.

4. In connection with this investigation I have consulted, discussed, and worked along-side of agents and investigators from a variety of agencies, including DEA agents who specialize in cyber investigation, agents with the United States Department of Labor, Office of Investigations, Labor Racketeering and Fraud (DOL-OIG), who specialize in fraud investigations, and investigators with the California Department of Corrections and Rehabilitation, U.S. Postal Inspection Service, and the California Employment Development Department (EDD), Office of the Inspector General. The agents with whom I am working include agents who are familiar with the emerging use of the "dark web" and digital currency by drug traffickers, and they have investigated

schemes of crime utilizing them in furtherance of their users' drug trafficking and money laundering activities. Those agents with whom I am working also include agents who have directed and participated in investigations involving identity theft and various types of fraud using stolen identities, including several investigations involving the fraudulent acquisition of EDD Pandemic Unemployment Assistance (PUA) benefits.

5. This affidavit supports:

i. A criminal complaint against Lindsay Renee HENNING (HENNING) for violations of Title 21, United States Code, Section 841 (distribution of methylenedioxymethamphetamine (MDMA)), and Title 21, United States Code, Sections 841 and 846 (conspiracy to distribute lysergic acid diethylamide (LSD)) (the Target Offenses as to HENNING); and against both HENNING and Garrett Carl TUGGLE (TUGGLE) for violations of Title 18, United States Code, Section 1349, Conspiracy to Commit Wire Fraud, and Title 18, United States Code, Section 1028A(a)(1) (aggravated identity theft) (the Target Offenses as to HENNING and TUGGLE), and warrants for HENNING's and TUGGLE's arrest.

ii. An application for a warrant directing T-Mobile to provide real-time tracking and geo-location information (e.g., Global Positioning Satellite and/or cell site information) for cellular phone number 619 317 7926 and subscribed to Lindsay HENNING at P.O. Box 402, 3952 Clairmont Mesa Boulevard, Box D-402, San Diego, CA, 92117 (the Subject Device). Based on information below, I have probable cause to believe that the requested tracking information will reveal the location of a person to be arrested pursuant to Federal Rule of Criminal Procedure 41(c)(4).

iii. An application to search 2782 Escala Circle, San Diego, California, the **Target Location**, as further described in Attachment A-1, for evidence of violations of the Target Offenses and fruits of the Target Offenses, as set forth in Attachment B.

iv. An application to search a grey Mercedes model E55 sedan with VIN No. WDBUF76J16A872178, registered to Garrett Carl TUGGLE (**Target Vehicle 1**), as described in Attachment A-2, for evidence of violations of the Target Offenses and fruits of the Target Offenses, as set forth in Attachment B.

6. The facts set forth in this affidavit are based on my own personal knowledge, knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers, witness interviews, review of documents, and computer records related to this investigation, communications with others who have personal knowledge of the events and circumstances described herein, and information gained through my training and experience. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the Criminal Complaint and the requested warrants, it does not set forth every fact that I or others have learned during this investigation.

PROBABLE CAUSE

Background to the CARES Act and PUA benefits

7. In response to the COVID-19 pandemic and the massive unemployment that resulted from the pandemic, on March 27, 2020, Congress Passed and the President signed the Coronavirus Aid, Relief, and Economic Security (CARES) Act. The CARES Act expanded unemployment benefits to include self-employed persons, independent contractors, and part time workers previously excluded from such benefits. In order to qualify for

Pandemic Unemployment Assistance (PUA), an applicant must complete an online application with the applicant's name, date of birth, social security number, and other personal information. The applicant can then file for benefits by certifying online that he/she is unemployed and eligible for benefits. To be eligible, an applicant must have been employed in a qualifying position immediately prior to the period being claimed. Claims are commonly paid out through electronic debit cards that are sent to the claimant through U.S. Mail to a physical address. In California, PUA benefits are administered through the California Employment Development Department (EDD).

Background to Bitcoin and Dark Web Marketplaces

8. Based on my training and experience and my conversations with other agents who specialize in crypto currency investigations, I am aware of the following concepts:

a. "Dark web marketplaces," also sometimes called "dark net marketplaces" refer to 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. Cellular "smart phones" can connect to the internet, including the

dark web, and can be utilized to manage a drug vendor account as well as conduct digital currency transactions.

b. "Vendors" are the dark web's sellers of goods and services, often of an illicit nature, and they do so through the creation and operation of "vendor accounts." Customers, meanwhile, operate "customer accounts." It is possible for the same person to operate one or more customer accounts and one or more vendor accounts at the same time.

c. The "Tor network," or simply "Tor," is a special network of computers on the Internet, distributed around the world, that is designed to conceal the true Internet Protocol ("IP") addresses of the computers accessing the network, and, thereby, the locations and identities of the network's users. Tor likewise enables websites to operate on the network in a way that conceals the true IP addresses of the computer servers hosting the websites, which are referred to as "hidden services" on the Tor network. Such "hidden services" operating on Tor have complex web addresses, generated by a computer algorithm, ending in ".onion" and can only be accessed through specific web browser software, including a major dark-web browser known as "Tor Browser," designed to access the Tor network. One of the logos, or "icons," for Tor Browser is a simple image of the Earth with purple water and bright green landmasses with bright green concentric circles wrapping around the planet to look like an onion.

d. Digital currency (also known as crypto-currency or virtual currency)[1] is generally defined as an electronic-sourced unit of value that can be used as a substitute for fiat currency (i.e.,

[1] For purposes of this affidavit, "digital currency," "crypto-currency," and "virtual currency" address the same concept.

currency created and regulated by a government). Digital currency exists entirely on the Internet and is not stored in any physical form. Digital currency is not issued by any government, bank, or company and is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Digital currency is not illegal in the United States and may be used for legitimate financial transactions. However, digital currency is often used for conducting illegal transactions, such as the sale of controlled substances.

e. "Bitcoin" (or "BTC") is a type of online digital currency that allows users to transfer funds more anonymously than would be possible through traditional banking and credit systems. Bitcoins are a decentralized, peer-to-peer form of electronic currency having no association with banks or governments. Users store their bitcoins in digital "wallets," which are identified by unique electronic "addresses." A digital wallet essentially stores the access code that allows an individual to conduct Bitcoin transactions on the public ledger. To access Bitcoins on the public ledger, an individual must use a public address (or "public key") and a private address (or "private key"). The public address can be analogized to an account number while the private key is like the password to access that account. Even though the public addresses of those engaging in Bitcoin transactions are recorded on the public ledger, the "Blockchain," the true identities of the individuals or entities behind the public addresses are not recorded. If, however, a real individual or entity is linked to a public address, it would be possible to determine what transactions were conducted by that

individual or entity. Bitcoin transactions are, therefore, described as "pseudonymous," meaning they are partially anonymous.

f. Although they are legal and have known legitimate uses, bitcoins are also known to be used by cybercriminals for money-laundering purposes, and are believed to be the most oft-used means of payment for illegal goods and services on "dark web" websites operating on the Tor network. By maintaining multiple bitcoin wallets, those who use bitcoins for illicit purposes can attempt to thwart law enforcement's efforts to track purchases within the dark web marketplace.

g. Bitcoin is one example of a digital currency; other digital currencies, such as Etherium and Monero, also exist and are used by darknet actors. The technology underlying these currencies are similar, though these currencies provide more privacy and anonymity of the users.

h. Exchangers and users of cryptocurrencies store and transact their cryptocurrency in a number of ways, as wallet software can be housed in a variety of forms, including on a tangible, external device ("hardware wallet"), downloaded on a PC or laptop ("desktop wallet"), with an Internet-based cloud storage provider ("online wallet"), as a mobile application on a smartphone or tablet ("mobile wallet"), printed public and private keys ("paper wallet"), and as an online account associated with a cryptocurrency exchange. Because these desktop, mobile, and online wallets are electronic in nature, they are located on mobile devices (e.g., smart phones or tablets) or at websites that users can access via a computer, smart phone, or any device that can search the Internet. Moreover, hardware wallets are located on some type of external or removable media device, such

as a USB thumb drive or other commercially available device designed to store cryptocurrency (e.g. Trezor, Keepkey, or Nano Ledger). In addition, paper wallets contain an address and a QR code[2] with the public and private key embedded in the code. Paper wallet keys are not stored digitally. Wallets can also be backed up into, for example, paper printouts, USB drives, or CDs, and accessed through a "recovery seed" (random words strung together in a phrase) or a complex password. Additional security safeguards for cryptocurrency wallets can include two-factor authorization (such as a password and a phrase). I also know that individuals possessing cryptocurrencies often have safeguards in place to ensure that their cryptocurrencies become further secured in the event that their assets become potentially vulnerable to seizure and/or unauthorized transfer.

i. Some companies offer cryptocurrency wallet services which allow users to download a digital wallet application onto their smart phone or other digital device. A user typically accesses the wallet application by inputting a user-generated PIN code or password. Users can store, receive, and transfer cryptocurrencies via the application; however, many of these companies do not store or otherwise have access to their users' funds or the private keys that are necessary to access users' wallet applications. Rather, the private keys are stored on the device on which the wallet application is installed (or any digital or physical backup private key that the user creates). As a result, these companies generally cannot assist in seizing or otherwise restraining their users' cryptocurrency. Nevertheless, law enforcement could seize

[2] A QR code is a matrix barcode that is a machine-readable optical label.

cryptocurrency from the user's wallet directly, such as by accessing the user's smart phone, accessing the wallet application, and transferring the cryptocurrency therein to a law enforcement-controlled wallet. Alternatively, where law enforcement has obtained the recovery seed for a wallet (see above), law enforcement may be able to use the recovery seed phrase to recover or reconstitute the wallet on a different digital device and subsequently transfer cryptocurrencies held within the new wallet to a law enforcement-controlled wallet.

9. Darknet marketplaces often only accept payment through digital currencies, such as Bitcoin, and operate an escrow whereby customers provide the digital currency to the marketplace, who in turn provides it to the vendor after a transaction is completed. Accordingly, large amounts of Bitcoin sales or purchases by an individual can be an indicator that the individual is involved in drug trafficking or the distribution of other illegal items. Individuals intending to purchase illegal items on Silk Road-like websites need to purchase or barter for Bitcoins. Further, individuals who have received Bitcoins as proceeds of illegal sales on Silk Road-like websites need to sell their Bitcoins to convert them to fiat (government-backed) currency.

Summary of Facts Supporting Probable Cause

10. The crimes described in this affidavit arose after September 2020 traffic stop revealed that throughout the Spring and Summer of 2020, HENNING was distributing drugs through the mail and working in concert with TUGGLE to fraudulently obtain Pandemic Unemployment Assistance (PUA) benefits from the California EDD. Evidence of HENNING's distribution and conspiracy to distribute drugs is based on drugs and paraphernalia found in HENNING's vehicles, combined with a court-

authorized search of messages stored on HENNING's cell phone. These show distributing drugs, both through the mail and in-person, including messages in which HENNING explicitly references drugs and photographs of the drugs that she mails to her co-conspirator.

11. Those same stored messages, combined with hand-written documents found in HENNING's vehicle, and EDD and bank records, show that HENNING and TUGGLE were working in concert to use other persons' personal identifying information (PII) such as dates of birth and social security numbers, to fraudulently obtain PUA benefits from EDD. Specifically, the same PII found on handwritten sheets of paper in HENNING's vehicle was used to apply for, and receive, PUA benefits from the EDD for approximately one dozen people. The EDD issued debit cards on those applications to an address that HENNING and TUGGLE discussed using. HENNING possessed the security codes[3] for those cards and ATM photographs show HENNING's boyfriend withdrawing money from those cards.

12. Approximately 108 additional PUA claims were made for addresses connected to TUGGLE. EDD issued debit cards to those addresses for 78 of those claims, for a total payout of approximately 1,6 million dollars. TUGGLE is connected to those addresses through messages discussing those addresses with HENNING, or through ATM photographs of cards sent to those addresses showing TUGGLE withdrawing funds from those cards.

13. Additional messages and financial records show that HENNING and TUGGLE invested the proceeds of drug dealing (as to HENNING) and fraudulent PUA benefits (as to both HENNING and TUGGLE) into crypto currency accounts or virtual "wallets."

[3] A three-digit number printed on the back of the EDD-issued debit card.

The September 8, 2020 Traffic Stop

14. On September 8, 2020, Officers of the San Diego Police Department initiated a traffic stop on HENNING as she was driving a 2020 Dodge Ram pickup truck (VIN 1C6SRFFT5LN163759); pulling a 2015 Airstream Flying Cloud M-23D trailer (VIN 1STB9AG25FJ531744) after noticing that the trailer's registration tags had expired, and being informed that HENNING was driving on a suspended license. The truck and trailer were stopped on a bridge over Interstate 8 in a position that partially impeded traffic. Officers searched the truck and trailer based on: 1) the need to conduct an inventory of the contents of the truck and trailer prior to towing the vehicles; and 2) probable cause that the vehicles contained controlled substances based on information received through confidential sources and surveillance of the vehicles and HENNING. Throughout the truck officers found several plastic and aluminum containers along with numerous Ziploc style baggies containing: 2.9 grams of a mixture of MDMA[4] and cocaine; 2.5 grams of methamphetamine; 1.9 grams of powder cocaine; 20.3 grams of ketamine; 48 MDMA tablets; 1.075 grams of LSD;[5] and 7.4 grams of cocaine. Officers also found four digital scales, notebooks that contained a list of drugs and their corresponding prices, and a digital money counter. Inside the trailer officers found a drug-testing kit, vacuum sealing machines, various items of dominion and control for HENNING and Salvatore COMPILATI, her boyfriend, and a list of instructions on how to make GHB.

[4] MDMA (also known as Methylenedioxymethamphetamine) and MDA (also known as Methylenedioxyamphetamine) are psychedelic hallucinogenic drug and empathogen/entactogen of the phenethylamine family and are commonly referred to under the generic name "ecstasy." Both are Schedule I controlled substances.

[5] LSD (also known as (lysergic acid diethylamide or "acid") is a hallucinogenic drug and a Schedule I controlled substance.

15. Also in the truck agents found a cellular phone (HENNING's former phone, **HFP**), an Apple iPad, and numerous documents containing the Personal Identifying Information (PII) of several individuals. **HFP** was found on the driver's seat, powered on and plugged into the truck at the time of the traffic stop.

The Court-Authorized Search of HFP

16. Based on the items found in the truck and trailer, on October 21, 2020 agents obtained a search warrant issued by the California Superior Court, County of San Diego, to search **HFP** for evidence of narcotics sales and fraud in connection with Pandemic Unemployment Assistance (PUA) benefits.

17. The search revealed that HENNING used an application called Signal to distribute controlled substances and fraudulently obtain PUA benefits. Signal is a messaging service that encrypts users' communications and makes them virtually impossible to intercept. However, HENNING saved the unencrypted archives of her messages on **HFP**. HENNING can be identified as the user of this phone throughout these chats based on: her self-identification in the messages – her communications are addressed to "Lindsay;" on several "selfie" photos of herself that she messages, and on distinctive jewelry that she wears that appears in several photos that she sends.

Archived messages in HFP show HENNING selling narcotics and investing the proceeds in bitcoin

18. HENNING's saved messages show she was a prolific narcotics dealer. For example, on May 27, 2020, a contact who goes by "Greg," messaged HENNING saying that he liked "that Crystal" referencing a prior delivery of methamphetamine and asking whether he could order more from HENNING. HENNING asks him: "what do you need." "Greg" asked "Can I talk

on here." HENNING affirms and assures him: "yeah totally . . . its encrypted. Speak Freely." "Greg" then requests: "2 8 balls [two 3.5 gram orders][6] and 5g of meth." HENNING clarifies that he is ordering 7 grams of cocaine and 5 grams of methamphetamine: "Coke in the 7g? N 5 of the go fast, gotcha." Greg confirms: "Yes please." HENNING agrees to deliver the drugs and "Greg" provides his address. HENNING agrees to be there in half an hour.

19. Additional messages in **HFP** show that JL[7] is an Arizona resident and sub-distributor of narcotics. On June 3, 2020, HENNING thanked JL for a deal they had just completed and recommended that JL branch out to sell Ketamine, and cocaine: "Yeah thank you let me know if You need anything in the future or if any of ur people want that kitty. . . [Ketamine] I'm still in town n have kitty n coke [cocaine]. . . There's decent profit margins in both of your wanted to pick some up." JL replied that he would see if his/her customers were interested.

20. On June 10, 2020, J.L. asked HENNING, "How much for another quad of molly? [1/4 ounce of MDMA] I have 500 [dollars] on it rn [right now] if that's good again" HENNING responded, "Yah that's perf . . . Just cash me n I'll send it out today or tomorrow 100% . . . Do you have a preference on color . . . Also need an address n don't worry I package discreetly." Anticipating further sales, on June 12, 2020, HENNING turned the discussion to the terms of payment. She expressed a preference for bitcoin to conceal the transaction and avoid law enforcement

[6] My interpretation of coded language is set forth in brackets and is based on my training, experience, knowledge of this investigation, and my conversations with other agents and confidential sources who are experienced in drug transactions.

[7] Agents identified JL after /she provided his true name and address in response to HENNING's question about where to send a package of drugs.

scrutiny:

> I can tell you're good people so as long as we can keep a steady thing going I'm good with all of it. I may have you hang on to the money tho cuz I don't know I trust all the transfers . . . N then I'll come grab it or you can put it in bitcoin or something . . . They def watch how money moves … I ain't worried . . . Let's make you some money . . . Imma give you good prices, just figure out a way to pay me easily I think bitcoin fed the best . . . Def . . . Like u buy it at atm n then send me pic of the code[8] . . . Or... idk I don't want there to be a trail.

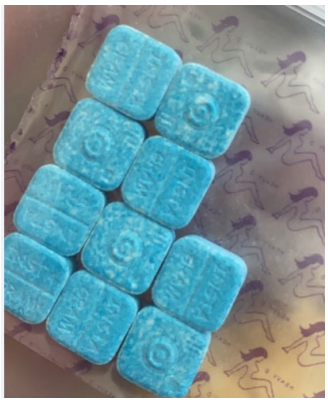
J.L. responded, "You can convert bitcoin through cash app . . . You can't track bitcoin if it's converted online at all."

21. HENNING and J.L. discussed J.L.'s order over the next several days. On June 12, 2020, HENNING texted, "So I have : 7g Miranda [MDMA] 500 paid, 7g Miranda (450), Pressy [manufactured pills] x10 (150), 3g dmt (360), Acid 1/2 sheet (225) Look legit to you? . . . Acid gellies" HENNING then sent JL two photographs. The first photo shows a small, clear Ziploc baggie containing a yellow/amber, coarse powder.

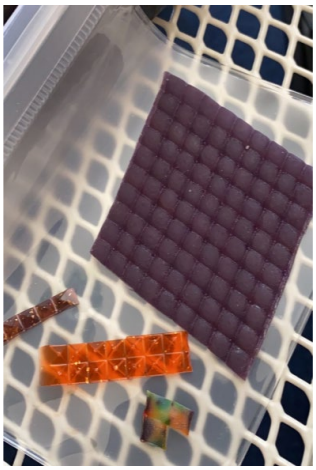
22. The second photo is another clear Ziploc baggie with a repeating design of a silhouetted female. The baggie contains 10 square blue tablets with white specks and unknown markings pressed into the tablets with an Instagram logo (identical blue tablets seized from

[8] Bitcoin can be exchanged through transmission of a QR code.

HENNING's truck tested positive for MDA).



23. HENNING then asked, "You want all one kind Miranda [MDMA] or some white [Cocaine]?" J.L. responded, "holy shit those are fucking dope!! And some of the white would be ideal." HENNING then sent J.L. a photograph of a clear plastic folder, similar to a wallet insert for IDs, which contains a sheet of purple square consisting of 90 doses of suspected LSD, an orange strip consisting of 14 squares, and two other connected strips or squares.



24. On June 14, 2020, HENNING messaged J.L., "Hey keep this between us but so one of Noel's friends, Shane is gonna grab some molly and possibly some dmt from you . . . So when u get my pkg just hit him up n he will pay u directly . . . So there's less trail . . . He's hella

cool, air traffic controller." JL responded, "Sic and no problem will he just wanna roll by?" HENNING responded, "Idk ima give u his number . . . U can work it out with him . . . I charge him 80/g on the molly . . . Prob $150-175/g on the dmt he won't argue don't worry . . . (480) 228-3083 . . . Shane . . . Signal. Always. I gave ur number too. So he's expecting u when u get the pkg which will go out Monday." J.L. responded, "Sounds good thanks"

25. When she prepared the mailing label, HENNING asked where she should send the package. J.L. replied with his name, [J.L.], and his address. On June 16, 2020, HENNING said, "Getting that label right now stand by for tracking." J.L. responded, "Okay perfect." HENNING then sent him a photo of a Priority Mail label.[9]

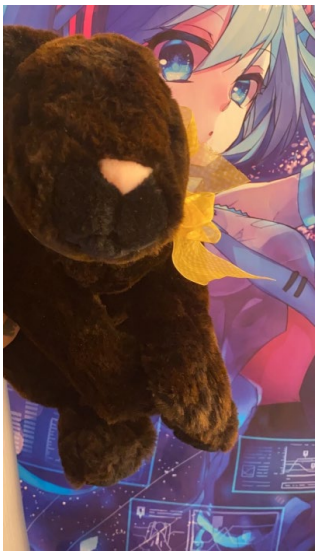
26. HENNING asked, "good?" JL responded, "Good . . . and no worries" HENNING then said, "I gotta tape it all up but ya . . . I normally overnight but they're closed so I can't cuz don't have this special thing they use I think it should be fine don't you? It's gonna be in a metal box so they won't be able to see in it." J.L. said, "I believe so, if anything I've heard overnight mail is usually more sketchy." HENNING responded, "N is already vacuum sealed in like a coffee

[9] Agents recognize the small skull ring in this photograph as one HENNING was wearing at the time of her arrest on September 8, 2020.

bag." HENNING then sent J.L. a photograph of an unknown substance in a sealed plastic bag.

The steering wheel in the background is from HENNING's Dodge Ram truck. J.L. responded, "Okay sicc yeah we should be good AF then."

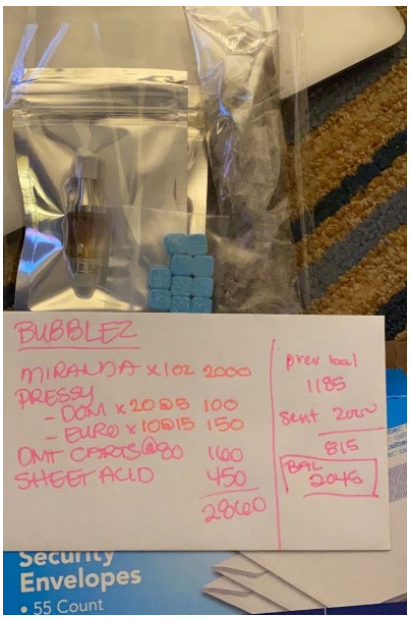
27. J.L. confirmed receipt of the drugs on June 24, 2020, when he sent HENNING a photograph of a brown stuffed bunny doll and the message, "Got the bunny!!"



HENNING responded, "Yesssss . . . Omg that was stressing me out."

28. HENNING and J.L. continued to discuss drug sales throughout the month of July 2020. On July 17, 2020, HENNING sent J.L. a photograph depicting controlled substances ready for shipping and a photograph of an invoice addressed to J.L.'s alias, "Bubblez," showing his purchases,

payments, and amount still owed, $2,046: "Miranda X 1oz 2000; Pressy, Dom X 20 @ 5 100 Euro X 10 @ 15 150; DMT Carts @ 80 160; Sheet Acid 450 for a total of $2,860; Previous balance 1,185, sent 2,000, new balance 2,046."



HENNING and TUGGLE conspire to commit wire fraud by using other persons' PII to obtain PUA benefits

29. The September 8, 2020 inventory search of HENNING's truck revealed several notebooks and loose papers on the rear passenger seat. The loose papers included thirteen pages, each containing the name of an individual and accompanying PII for that individual, as well as EDD account usernames and passcodes, debit card numbers and security codes for the debit cards. EDD investigators queried EDD databases using the names of suspected identity theft victims found in HENNING's notebook and found evidence of over thirteen distinct claims corresponding to the names and PII in HENNING's notebook. Saved messages between HENNING and TUGGLE show TUGGLE introducing HENNING to the fraudulent scheme, including discussions in which they discuss HENNING's success in submitting information for at least 5 of the 13 victims mentioned by

name.

i. HENNING and TUGGLE discuss efforts to defraud the EDD over Signal App Messages on HFP

30. **HFP** contained extensive chat messages with TUGGLE, using the screen name "GARTH5551,"[10] discussing their ongoing efforts to process fraudulent EDD UI claims.

31. Messages in **HFP** show HENNING supplying TUGGLE with drugs and introducing TUGGLE to one of her suppliers for drugs in mid-June 2020. On June 18, 2020, HENNING explained that she can supply TUGGLE with a variety of drugs:

> I Am for the most part very well connected. If it's drugs, to typically i can get it within 24 hours but a lot of times a lot faster. Molly [MDMA], acid [LSD], ketamine, mushrooms, etc... all day . Typically clear [methamphetamine] n chach [cocaine] to but lately not as easy

32. On June 28, 2020, HENNING asked TUGGLE where he is and TUGGLE indicated that he was in a downtown San Diego hotel. TUGGLE expressed frustration at the person who supplies him with drugs: "I just woke up out of nowhere. Watching my buddy "look" for my dope." HENNING replied, "I got coke [cocaine] n meth [methamphetamine] n kitty [ketamine] molly

[10] Agents base their identification of "GARTH5551" as TUGGLE on the following evidence. First, on July 6, 2020, GARTH5551 messages HENNING that he is going in for a lasik eye appointment and he texts her a selfie showing TUGGLE wearing a surgical mask. Second, on August 8, 2020, HENNING meets GARTH5551 at the Anaheim Marriott. Over chats, HENNING tells GARTH5551 that she needs to list the guests name to enter the parking lot and GARTH5551 responds "Tuggle." Third, TUGGLE used the Mission Center Road address described below not only for HENNING's fraudulent EDD claims but also for a series of fraudulent EDD claims unconnected to HENNING, and for which he is photographed on ATM video cashing out EDD cards, as set forth below. In addition, "GARTH5551" also references using the address 830 East Vista Way Suite 221 for fraudulent EDD claims. TUGGLE is photographed on ATM video cashing out EDD cards sent to that address as well.

[MDMA] . . . N I'm with the dude that was getting the hgh [human growth hormone[11]] . . . so he's gonna talk to you about that when i get there . . . is that cool." TUGGLE agreed to the meeting, after confirming that it would be just HENNING and one other person.

33. TUGGLE assisted HENNING to find customers for drugs and HENNING reimbursed TUGGLE for that help. On July 20, 2020, HENNING asked TUGGLE: "Did your homie pay on the molly [MDMA][?] . . . He only have the 600 for addy [$600 for Adderall[12]] when i was there, I was gonna split that with you . . . The molly [MDMA] money." TUGGLE replied: "Nk" [I believe this is a typographical error for "ok"].

34. On June 18, 2020, HENNING informed TUGGLE, "I need my unemployment to come thru." HENNING described problems dealing with EDD's customer service representative. TUGGLE replied: "I've done many many applications for people and I've seen everything. I follow all the forums online about what's going on and it's just ridiculous."

35. Over the next two weeks, TUGGLE began to advise HENNING over how to submit fraudulent EDD claims. On July 6, 2020, TUGGLE wrote: "Hey, so I forgot to mention that the edd had specific filing times . . . between 10pm and 2am you cant file But you can do all kinds of other stuff like prepare." HENNING replied, "Wow ya that's interesting Gonna tonight prepare."

36. On July 9, 2020, HENNING and TUGGLE were sharing the same San

[11] HGH is not controlled under the Controlled Substances Act (CSA). However, the distribution of HGH for any use other than treatment of a disease or medical condition is criminalized aunder the Food, Drug, and Cosmetic's Act , 21 U.S.C. § 333(e)(1), and pursuant to section 333(e)(3) such a conviction shall be considered a felony violation of the Controlled Substances Act.

[12] Adderall is a stimulant and is a Schedule II controlled substance.

Diego hotel room.[13] She wrote that she purchased an iPad, keyboard, pen, "N other shit to organize the [EDD application] process a bit . . . Imma head back there now n start doing it may need your login for jstash[14] . . . I talked to a edd [Employment Development Department] lady today n she said pandemic deadline is in dec n no deadline otherwise."

37. HENNING asked TUGGLE: "Hey could u send me the addy [address] that I can send the things to." TUGGLE responded by texting a photo of the UPS store business card, 5694 Mission Center Road Suite 409, with a hand written not of "409" for the box number, which is the same as the address listed with EDD for PUA claims associated with nine of the thirteen names found in the notebook in HENNING's truck.

38. On July 10, 2020, HENNING told TUGGLE that she was in her

[13] HENNING indicated that she was in the room and asked TUGGLE whether he could pick up a pizza order she placed, he said he was still in out in El Cajon and could not pick up her order. TUGGLE booked that room under the name T.H. As explained below, TUGGLE stole that identity, the real T.H. resides in a different state and is employed as a medical professional.

[14] "Jstash" refers to "Joker's Stash." For most of 2020, Joker's Stash was an internet dark-web marketplace for buying and selling stolen cards, including credit cards and identity cards. On December 18, 2020, the FBI and Interpol seized several servers operated by Joker's Stash, temporarily disrupting the sites activity. The site announced it was permanently closing in February 2021.

Airstream trailer at that time: "I'm gonna go to someone's house to use WiFi right now n do this . Trailer is so frustrating so much going on n can't concentrate for shit." HENNING then turned the discussion to fraudulent identification cards that she and TUGGLE were planning to get: "In going tomorrow to my photographers pad to get photo taken. Would the Chinese put the photo on like 2-3 id at same time? That's a good idea huh? Order several so we can get more." TUGGLE replied, "Yeah that's how your supposed to do it." HENNING asked whether TUGGLE wanted to come with her to the photographer. He replied, "I only ordered one because I was still trying to find the right vendor that did almost perfect fakes for Cali."

39. HENNING then commented that the Jstash site for fraudulent PII was down for maintenance (after she put $50.00 on the site) and she asked TUGGLE whether he had a backup: "Guck i just put 50 on jstash n refresh n it's closed for maintenance. Do you have another site for that kinda shit." TUGGLE replied by suggesting several dark-web internet sites selling PII: "Ssn24.me," "Nova search," and "robocheck.cc." TUGGLE said that "Nova search" was "$9" for each identity and "robocheck.cc" offered PII at $3.50 per identity.

40. TUGGLE then asked HENNING, "How is it coming along?" HENNING replied, "Omg I finally fetting one to go thru. [she then names R.D.] The rest were like not eligible or whatever."

41. R.D. is the name written on one of the pages from HENNING's notebook, along with that person's SSN and date of birth, the associated EDD account number, debit card number, the debit-card pin and the 3-digit security code printed on the back of the debit-card. R.D. is a real person who did not authorize the use of his identity for HENNING to collect UI benefits. TUGGLE replies asking: "It went through. How do

u know already?" HENNING responded: "I mean i got a conf numver lol i guess i dont know shit" TUGGLE then asks HENNING: "Is that the first one you've done?" HENNING responds: "The 6 other ones ive done werent elegible or they fuckin worked in the last 18 mo . I was getting so frusyrated . But can i cash app you n u send more bitcoin if i get u a addresso" TUGGLE responds: "So getting it completed is one thing… U have to keep checking every 24hrs to see if it worked." In telling TUGGLE that the other six identities she attempted to use were not eligible because they had recently worked and did not show up unemployed, HENNING demonstrates a knowledge that the PII she was using belonged to real people.

42. HENNING then confirms that she will pay TUGGLE for the successful claim that went through profits on drug sales, reflecting an agreement that HENNING would pay TUGGLE for the identities he sent her: "ok I got to go deliver drugs quick I'll get money in my act n then send you some, or you want cash?"

43. On July 11, 2020, HENNING messaged TUGGLE that she certified for J.J. HENNING states, "That one going to mission center. [the address TUGGLE provided on the business card] [R.D.] is also mine. So i owe u $3000" TUGGLE responds: "Nice. Good job lindz," to which HENNING responds: "Still goin haha." TUGGLE then says "Nice. Getting the hang of it no," to which HENNING responds: "Ya totally."

44. On July 15, 2020, HENNING confirms with TUGLLE that she certified for 6 people, which resulted in over $100,000 in proceeds. HENNING messaged TUGGLE that she will pay him $9,000 for those 6 claims, which further reflects their agreement that HENNING would pay TUGGLE $1,500 per successful claim. On July 15, 2020, HENNING confirms with TUGGLE: "So far I've certified for 6 ppl n they are all 17550 [each

claim is worth $17,550] except for one, so thats over 100k. So I'm giving you 9000 for those 6." Agents have confirmed that EDD approved claims for six of the identities found in the loose papers on the rear seat of HENNING's truck, and that the card numbers, CVV security codes written on the back of the cards, and PII found on those papers correspond to the same information in EDD's databases for those six PUA claims. Agents have further established that all those claims are fraudulent. Agents confirmed through interviews and EDD databases that none of those individuals submitted unemployment claims to EDD.

45. ATM video still-shots from the withdrawals for five of the identities found in HENNING's notebook show that on August 30, 2020, HENNING's boyfriend, COMPILLATI, withdrew funds from five different EDD debit cards issued in connection with those fraudulent claims. PII for a sixth individual also found in HENNING's truck, although not in that notebook, was also associated with a fraudulent EDD claim. ATM video for that claim shows TUGGLE[15] withdrawing funds from the debit card issued on that account on September 30, 2020.

46. Agents have identified at least sixty additional fraudulent EDD claims that are either connected to an address used by TUGGLE or which are connected to ATM withdrawals in which TUGGLE is photographed. In total, these claims exceed one million dollars.

47. The messages in **HFP** also provide cause to believe that TUGGLE owns a gun. On July 23, 2020, TUGGLE messaged HENNING, "can your man fix my gun you think? Or help me with jt." HENNING replied, "Sammmy can fix guns." HENNING then sent TUGGLE a photo of a screen shot of her phone showing a photo of the top of a Glock pistol. TUGGLE replied, "I

[15] Although the subject in the photos is masked, agents recognize TUGGLE based on his eyes and eyebrows, his hat, and a leather bag with a distinctive red and black striped strap.

want a glock that looks like that. Shits fucking rad."

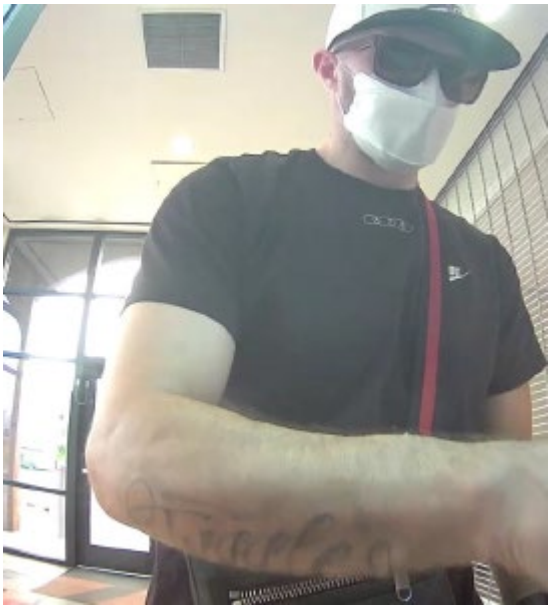
48. TUGGLE is linked to more than 108 EDD UI claims which have paid out more than $1.6 million dollars. TUGGLE is connected to these claims through a combination of his links to the claimant address, through his communications with other co-conspirators, or through ATM photos in which TUGGLE is withdrawing money from the claimant account. In these photos, TUGGLE is identified through his face, his tattoos, his vehicle, or an item of clothing or an accessory (satchel or watch) that appears across photos from several different claimant ATM card withdrawals. The claims linked to TUGGLE are summarized as follows:

Claimant Address	No. of Claims/No. Claims Paid	Amount Paid
1255 East Vista Way, No. 178	14 Claims/9 Paid	$185,000
1530 Noran Avenue	18 Claims/14 Paid	$295,000
2537 Northside Drive, Apt 623	13 Claims/8 Paid	$195,000
5694 Mission Center Rd. Suite 602, Box 409	14 Claims/12 Paid	$268,000
2307 Fenton Parkway N 107-125	4 Claims/2 Paid	$46,000
7514 Girard Ave. Suite 1254	19 Claims/14 Paid	$280,000
830 East Vista Way, Suite 221	26 Claims/19 Paid	$346,000
Total Claims: 108; Total Claims Paid: 78; Total Amount Paid $1,615,000		

49. There is evidence connecting TUGGLE to each of these addresses and/or claims. As noted, on July 9, 2020, TUGGLE sent HENNING a photo of a business card bearing the address 5694 Mission Center Rd Suite 602, Box 409. On August 10, 2020, TUGGLE messages HENNING: "is 830 e vista way ste 221 an address I gave you ever?" HENNING replies, "No never . . .I've only had mission center." Utilities for the address on Northside

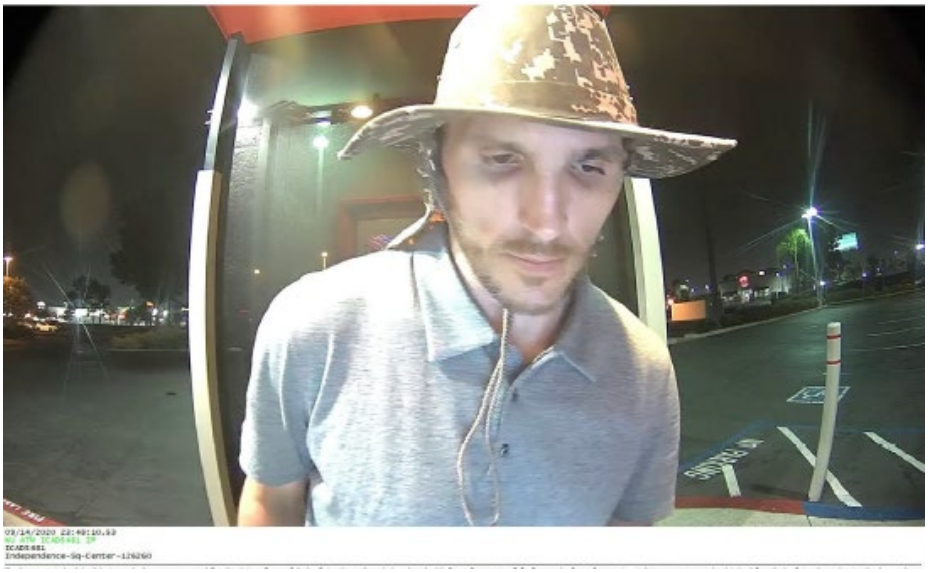
Drive were subscribed to the name T.H., an alias that connected to TUGGLE, as set forth below. The Girard Ave. address is a retail mailbox store that rents post office boxes. TUGGLE rented a box in his own name at that store, and also indicated that T.H. (TUGGLE's alias) could receive mail at that location. Agents interviewed employees at that store who described the tenant to that box as a person resembling TUGGLE who carried a small dog that resembles a dog appearing in photos that TUGGLE has emailed.

50. Included among those claimants is a claim for P.B. which was submitted to EDD on July 2, 2020, with an address at 2307 Fenton Parkway, later updated to 7514 Girard Ave. Suite 1254 on July 10, 2020 (the debit card was mailed to the Fenton Parkway address on July 3, 2020). EDD paid out $23,700 on PB's claim. At all relevant times P.B. was an inmate in a California state prison. Below is a photo from an ATM machine showing TUGGLE withdrawing money on September 6, 2020 at a bank in La Jolla, California from the debit card issued to P.B. TUGGLE is identified by the tattoo "G Tuggle" on his right forearm.



Since TUGGLE used a debit card sent to the Girard Ave address, I infer that TUGGLE is connected the other cards and applications using that address.

51. Also included among those claims is a claim by M.T., submitted on June 14, 2020, and residing at an address on 1255 East Vista Way, Suite 176. EDD paid out $19,200 to M.T. At all relevant times M.T. was an inmate in a California state prison. Below is a photo of TUGGLE withdrawing money on September 14, 2020 from a bank in the Kearny Mesa neighborhood using an EDD debit card issued to M.T.



52. Also included among the claims linked to TUGGLE is a claim for J.H., submitted on May 19, 2020 and using the address, 830 East Vista Way Suite 221 (the same address that TUGGLE messaged to HENNING inquiring whether she was using that address). EDD has paid out $17,430 on that card. At all relevant times JH has been an inmate in a California state prison. Records maintained by the California Department of Corrections and Rehabilitation (CDCR) show that TUGGLE maintains an account by which

he can transmit money to prisoners. On November 13, 2020 and April 6, 2021, TUGGLE transferred $300 to J.H., for a total of $600. At all relevant times J.H. has been an inmate in a California state prison. The April 6, 2021 payment was also accompanied by an email from TUGGLE to J.H.:

> hey bubba hope your alright. not sure if u get the News out there but shit is fucked up out here. I can not take your calls no matter how much I want to answer. things are very stressful out here. im straight up shook right now. I prolly won't be around when u get out. Whats up with your cases? you gonna get some action or what? if you feel the need to call. you must must keep it appropriate. I hope you catch my drift. because it's raining shackles in California right now and I prefer to stay free of those forever. 619-500-9111

53. TUGGLE frequently uses various vehicles to withdraw funds from EDD debit cards. For example, on June 25, 2020 he was photographed driving a grey Mercedes sedan to a drive-up ATM machine. California DMV records indicate that TUGGLE has one Mercedes sedan registered under his name, a Mercedes model E55 sedan with VIN No. WDBUF76J16A872178 (**Target Vehicle 1**).

54. As noted above, to facilitate the fraud, at various times during the commission of the fraud TUGGLE assumed the identity of a person named "T.H." DEA databases show the real T.H. resides in a state outside of California and is a health care worker who is licensed to prescribe medication. Several sources indicate that TUGGLE has assumed T.H.'s name and identity, including his SSN and date of birth, in furtherance of the Target Offenses. First, Subpoenas to a San Diego Hotel show that T.H. booked hotel room 916 at a Marriott Hotel in San Diego on July 7 and 8, 2020. messages indicate that on July 7 and 8, 2020, when HENNING and TUGGLE were preparing to submit fraudulent EDD

applications, they were staying in hotel room number 916.[16] Second, on July 11, 2020, T.H. subscribed to phone number 858 500 2055 serviced by AT&T. AT&T subscriber records indicate that the financially responsible party for that number is "Garrett Tuggle" with a home address at the Target Location, and with the contact phone number 619 852 5866, the same number that TUGGLE uses when messaging HENNING. On January 9, 2021, T.H. switched to phone number 619 673 5880, also serviced by AT&T, with "Garrett Tuggle" still listed as the billing contact and still using the Target Location as his address. Third, utilities at the Target Location are subscribed to T.H., using the real T.H.'s SSN and Date of Birth. As set forth below, agents have recently observed TUGGLE exit the Target Location and TUGGLE has messaged photos of three Mercedes vehicles, parked on a street near the Target Location, one of which appears to be **Target Vehicle 1**. Fourth, T.H. was also the subscriber to utilities at another residence at 2537 Northside Dr. Apt. 623, San Diego California. TUGGLE is also associated with this residence. An EDD application for "NJ" issued EDD debit cards to that address and a person resembling TUGGLE appears on ATM photos withdrawing money from those debit cards on September 13 and 18, 2020, and December 6, 2020. Finally, on July 7, 2020, TUGGLE messaged HENNING that he was contacted by a person who asked for pay stubs in connection with a residence he was moving to. HENNING replied, "Good job mr [T.H. surname] ur adulting hard today." Also on July 7, 2020, HENNING messages TUGGLE about the purchase of certain Apple tablets that they needed to prepare and submit EDD UI applications. HENNING suggests, "Maybe [T.H.'s first name] should sign up for Apple credit card," suggesting that TUGGLE should use the T.H.

[16] Between 9:20 pm and 9:40 pm TUGGLE and HENNING exchange several messages regarding the room. Tuggle states that he has the room keys to access hotel parking and that they are staying in room 916.

alias to sign up for a credit card to purchase the Apple tablet. TUGGLE replied, "That's a no go." In the same series of messages HENNING asks TUGGLE, "Does [T.H.'s first name] have a passport." TUGGLE replies, "No passport." These messages indicate that HENNING was aware that TUGGLE was using the T.H. identity.

Ongoing Criminal Activity

55. There is probable cause to believe that HENNING and TUGGLE continue to engage in criminal activity. EDD records indicate that neither HENNING nor TUGGLE were employed in California at any time in 2020 or 2021. As noted above, as recently as April 6, 2021, TUGGLE sent $300 to J.H., an inmate in a California state prison whose EDD benefit card was mailed to an address linked to TUGGLE. TUGGLE also wrote an email to J.H. and asked J.H. to stop calling him because it was "raining shackles in California" and TUGGLE did not want to be arrested.

56. Bank records further establish that accounts held in the names of TUGGLE and/or T.H. (TUGGLE's alias) are linked to 25 bank-issued credit cards which were used to either purchase Bitcoin or conducted peer-to-peer financial transactions. At this time, investigators have linked 13 of those 25 cards to identities that received EDD PUA benefits at the above-described addresses linked to TUGGLE. Those bank records concern transactions occurring between November 2, 2020 and March 10, 2021.

57. Based on my training and experience and conversations with other agents I know that people who earn money through drug sales and fraud will often conceal that illicit income as casino winnings. According to records maintained by a San Diego County casino, HENNING cashed in $2,483 and cashed out $2,933 on April 15, 2021. She returned the next day, April 16, 2021, and cashed in $4,642 and sashed out $4,603.

This activity by someone who has no reported income is consistent with concealing illicit income and leads me to conclude that HENNNING's involvement in criminal activity is ongoing.

HENNING's Connection to the Subject Device

58. A subpoena served on T-Mobile revealed that Lindsay Henning in the subscriber to the Subject Device as of April 4, 2021 and continuing through as recently as at least May 5, 2021.

TUGGLE's Connection to the Target Location and the Target Vehicle

59. On May 5, 2021, agents observed TUGGLE leaving the Target Location riding a motorcycle wearing a helmet with a clear face-shield. Utilities for the Target Location are subscribed to T.H. As set forth above, T.H. is one of the aliases that TUGGLE uses. Also, as described above, on several occasions TUGGLE has been photographed withdrawing money from ATM machines using EDD debit cards issued to other persons. On numerous occasions, TUGGLE is driving a grey Mercedes sedan, visible in the background of the ATM photo (believed to be **Target Vehicle 1**). On April 6, 2021, TUGGLE emailed a photo of an identical grey Mercedes sedan to JH, an inmate, along with two other Mercedes sedans. The background of the photos was the street at the Target Location.

TUGGLE and HENNING put the proceeds of their crimes into Bitcoin

60. Messages on **HFP** also show that both TUGGLE and HENNING conceal the proceeds of their crimes by directing payment in Bitcoin or by converting cash proceeds into Bitcoin. As set forth above, on June 10, 2020, HENNING asks J.L. to pay for drugs in Bitcoin: "just figure out a way to pay me easily I think bitcoin fed the best . . . I don't want there to be a trail."

61. HENNING also used bitcoin to pay suppliers of narcotics. On May 30, 2020, in archived messages with a contact saved as "Pat," HENNING

places a wholesale order for narcotics: "I need like 50 blues [counterfeit 30mg Oxycodone pills commonly laced with Fentanyl] n 2 zips [2 ounces of narcotics] . . . Can you handle." She follows up, "Find me drugs pls" and says she is "outside." "Pat" replies, "Be rite there." On June 3, 2020, HENNING asks "Pat" "What's the word with clear [methamphetamine] right now." "Pat" replies "I'm headed over to dude's now to get a P [a pound of methamphetamine] for someone eles . . . Cash app me the money." Cash App is an online money transfer app. HENNING replies that sh only has $300.00 in Cash App and she indicates she will pay the balance in bitcoin: "let me transfer some bit coin." "Pat" agrees: "Ok ima be at the spot in 10 mins." HENNING states that she is transferring bitcoin to him at that moment: "Bitcoin taking forever . . . You have to confirm my payments." "Pat" replies, "At dudes pad waiting for funds to clear."

62. HENNING also indicates that she will pay TUGGLE his share of the fraudulent EDD proceeds in Bitcoin. On July 11, 2020, after HENNING announces success in certifying a fraudulent application for R.D., HENNING tells TUGGLE that she will pay TUGGLE to convert the proceeds to Bitcoin: "can i cash app you n u send more bitcoin if i get u a addresso."

63. On May 31, 2020, HENNING messages a different co-conspirator that she is going to put invest all her fraudulent EDD proceeds in Bitcoin. The co-conspirator asks, "767 a week?" referring to the amount they could realize in EDD benefits. HENNING replies, "Yes . . . on a card . . . Imma put all mine in bitcoin."

Basis for Items to Be Seized from the Target Location

64. "Computer" as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(l) as an electronic, magnetic, optical, electrochemical, or

other high speed data processing device performing logical, arithmetic, or storage functions, including desktop computers, notebook or laptop computers, cellular or mobile telephones, smart phones, tablets, server computers, network hardware, and electronic storage devices (as that term is defined below).

65. Based on my knowledge, training, and experience, I know that cellular telephones, including smart phones, offer a broad range of capabilities comparable to computers. In addition to enabling voice communications, cellular telephones have capabilities including, but not limited to: (a) storing names and phone numbers in electronic "address books;" (b) sending, receiving, and storing text messages, emails, and other electronic communications; (c) taking, sending, receiving, and storing still photographs and videos; (d) storing and playing back audio files; (e) storing dates, appointments, and other information on personal calendars; and (f) accessing and downloading information and applications from the Internet. Cellular telephones may also include GPS technology for determining the location of the device. This search warrant is intended to cover such content if discovered.

66. "Electronic storage devices," as used herein, includes any physical objects or devices on which computer data can be recorded or saved. Examples include SIM cards, hard disks, RAM, floppy disks, flash memory, CD-ROMs, DVDs, ZIP discs, back-up tapes, printer or memory buffers, smart cards, PC cards, and other magnetic or optical media.

67. "Records" and "documentation," as used herein, include all of the following items of evidence in whatever form and by whatever means they may have been created or stored, including any electrical, electronic, or magnetic form (such as any information on an electronic or magnetic storage device, including computers, tablet devices, floppy

disks, hard disks, ZIP disks, CD-ROMs, flash drives, optical discs, backup tapes, printer buffers, smart cards, servers, memory calculators, pagers, cell phones, personal digital assistants such as Palm Pilot computers, as well as printouts or readouts from any magnetic storage device); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies).

68. Based on my knowledge, training, and experience, I know that in the commission of wire fraud co-conspirators generally need to communicate with each other in order to plan and execute their criminal activity, especially when it involves an ongoing conspiracy involving access device fraud. Meetings and locations of the planned drop offs, cash exchanges and other monetary transfers, and other activities need to be coordinated and communicated amongst co-conspirators and is often done with computers and electronic devices. As such, it is likely that co-conspirators were communicating with their cellular telephones.

69. Based on my knowledge, training, and experience, I know that individuals who commit wire fraud and identity theft use computers and other electronic devices to file fraudulent claims or access fraudulently obtained accounts online.

70. Based on my knowledge, training, and experience, I know that individuals engaged in wire fraud and identity theft have access to their victims' names, dates of birth, social security numbers, driver's license numbers, credit/debit card numbers, and bank account information among other personal identifying information. These individuals will often commit assorted types of access device fraud with that information, including tax fraud, credit card fraud, unemployment fraud, and bank

account takeovers. In addition, these individuals will also often perform identity checks on their victims in order to determine whether credit cards can be obtained in their victims' names, and in order to obtain additional personal information about their victims. Further, individuals engaged in access device fraud and identity theft are also known to use cryptocurrency, including Bitcoin, to buy and sell personal identifying information.

71. Based on my knowledge, training, experience, and discussions with other members of law enforcement, I also know that personal identifying information is a valuable commodity to individuals engaged in access device fraud and identity theft. These individuals are therefore unlikely to dispose of such information even if they are not using it at a particular time. Rather, they will maintain such information either in hard copy or electronically in computers and electronic storage devices in order to use it in the future. Individuals engaged in access device fraud and identity theft will also often sell such information to their co-conspirators, but will still often retain a copy of the information.

72. Based on my knowledge, training, and experience, I know that individuals engaged in wire fraud and identity theft possess and/or have access to programs and devices designed to hide, falsify, or otherwise obstruct the display or production of an IP address, or designed to allow the sharing of Internet access by multiple people while making it appear that all users come from the same IP address.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

73. Based on my knowledge, training, and experience, I know that computers and electronic storage devices can store information for long periods of time. Similarly, things that have been viewed via the Internet

are typically stored for some period of time on the devices. This information can sometimes be recovered with forensics tools.

74. There is probable cause to believe that records might be on the computers and on electronic storage devices because based on my knowledge, training, and experience, I know that electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on an electronic device, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

75. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space for long periods of time before they are overwritten. In addition, an electronic device's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

76. Wholly apart from user-generated files, an electronic device generally contains electronic evidence of how it was used, what it was used for, and who used it. This evidence includes operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files; electronic device users often do not delete such information.

77. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache," which users often do not delete.

78. Forensic evidence: As further described in Attachment B, this

application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the computers and electronic storage devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the computers and electronic storage devices because:

79. Data on computers and electronic storage devices can provide evidence of deleted or partially deleted files. Virtual memory paging systems can leave traces of information on computers and electronic storage devices that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals or other electronic storage devices, and the times the electronic device was in use. Electronic device file systems can record information about the dates files were created and the sequence in which they were created, although it is possible to falsify this info1mation.

80. Forensic evidence on an electronic device can also indicate who has used or controlled the electronic device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, chats, instant messaging logs, photographs, the presence or absence of malware, and correspondence, together with the data associated with the foregoing, such as file creation and last-accessed dates, may be evidence of who used or controlled the electronic device

at a relevant time.

81. A person with appropriate familiarity with how an electronic device works can, after examining this forensic evidence in its proper context, draw conclusions about how the electronic device was used, the purpose of its use, who used it, and when.

82. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on an electronic device, which are necessary to draw an accurate conclusion, is a dynamic process. While it is possible to specify in advance the records to be sought, electronic device evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on an electronic device is evidence may depend on other information stored on the electronic device and the application of knowledge about how an electronic device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

83. Further, in finding evidence of how an electronic device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on an electronic device. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

84. Nature of examination: Based on the foregoing, and consistent with Federal Rule of Criminal Procedure 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying the computers and electronic storage devices that reasonably appear to contain some or all of the evidence described in the wan-ant, and would authorize a later review of the media or information consistent with the

warrant. The later review may require techniques, including, but not limited to, computer-assisted scans of the entire medium, which might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

85. Because several people may share the SUBJECT PREMISES as a residence, it is possible that the SUBJECT PREMISES will contain computers and electronic storage devices that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that it is possible that the things described in this warrant could be found on any of those computers and electronic storage devices, the warrant applied for would permit the seizure and review of those items as well.

CELL PHONE SEARCH WARRANT METHODOLOGY

Procedures For Electronically Stored Information

86. It is not possible to determine, merely by knowing the cellular telephone's make, model and serial number, the nature and types of services to which the device is subscribed, and the nature of the data stored on the device. Cellular devices today can be simple cellular telephones and text message devices, can include cameras, can serve as personal digital assistants and have functions such as calendars and full address books and can be mini-computers allowing for electronic mail services, web services and rudimentary word processing. An increasing number of cellular service providers now allow for their subscribers to access their device over the internet and remotely destroy all of the data contained on the device. For that reason, the device may only be powered in a secure environment or, if possible, started in "flight mode" which disables access to the network. Unlike typical computers, many cellular telephones do not have hard drives or hard

drive equivalents and store information in volatile memory within the device or in memory cards inserted into the device. Current technology provides some solutions for acquiring some of the data stored in some cellular telephone models using forensic hardware and software. Even if some of the stored information on the device may be acquired forensically, not all of the data subject to seizure may be so acquired. For devices that are not subject to forensic data acquisition or that have potentially relevant data stored that is not subject to such acquisition, the examiner must inspect the device manually and record the process and the results using digital photography. This process is time and labor intensive and may take weeks or longer.

87. Following the issuance of this warrant, I will collect the subject cellular telephone and subject it to analysis. All forensic analysis of the data contained within the telephone and its memory cards will employ search protocols directed exclusively to the identification and extraction of data within the scope of this warrant.

88. Based on the foregoing, identifying and extracting data subject to seizure pursuant to this warrant may require a range of data analysis techniques, including manual review, and, consequently, may take weeks or months. The personnel conducting the identification and extraction of data will complete the analysis within one hundred and twenty (120) days of the date the warrant is signed, absent further application to this court.

COMPUTER SEARCH WARRANT METHODOLOGY

Procedures For Electronically Stored Information

89. With the approval of the Court in signing this warrant, agents executing this search warrant will employ the following procedures regarding computers and other electronic storage devices, including

electronic storage media, that may contain data subject to seizure pursuant to this warrant:

Forensic Imaging

90. After securing the premises, or if sufficient information is available pre-search to make the decision, the executing agents will determine the feasibility of obtaining forensic images of electronic storage devices while onsite. A forensic image is an exact physical copy of the hard drive or other media. A forensic image captures all the data on the hard drive or other media without the data being viewed and without changing the data. Absent unusual circumstances, it is essential that a forensic image be obtained prior to conducting any search of the data for information subject to seizure pursuant to this warrant. The feasibility decision will be based upon the number of devices, the nature of the devices, the volume of data to be imaged, the need for and availability of computer forensics specialists, the availability of the imaging tools required to suit the number and nature of devices found, and the security of the search team. The preference is to image onsite if it can be done in a reasonable amount of time and without jeopardizing the integrity of the data and the agents' safety. The number and type of computers and other devices and the number, type, and size of hard drives are of critical importance. It can take several hours to image a single hard drive - the bigger the drive, the longer it takes. As additional devices and hard drives are added, the length of time that the agents must remain onsite can become dangerous and impractical.

91. If it is not feasible to image the data on-site, computers and other electronic storage devices, including any necessary peripheral devices, will be transported offsite for imaging. After verified images have been obtained, the owner of the devices will be notified and the

original devices returned within forty-five (45) days of seizure absent further application to this court.

Identification and Extraction of Relevant Data

92. After obtaining a forensic image, the data will be analyzed to identify and extract data subject to seizure pursuant to this warrant. Analysis of the data following the creation of the forensic image can be a highly technical process requiring specific expertise, equipment and software. There are thousands of different hardware items and software programs, and different versions of the same programs, that can be commercially purchased, installed, and custom-configured on a user's computer system. Computers are easily customized by their users. Even apparently identical computers in an office or home environment can be different with respect to configuration, including permissions and access rights, passwords, data storage, and security. It is not unusual for a computer forensic examiner to have to obtain specialized hardware or software, and train with it, in order to view and analyze imaged data.

93. Analyzing the contents of a computer or other electronic storage device, even without significant technical challenges, can be very challenging. Searching by keywords, for example, often yields many thousands of hits, each of which must be reviewed in its context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant hit does not end the review process for several reasons. The computer may have stored metadata and other information about a relevant electronic record – e.g., who created it, when and how it was created or downloaded or copied, when it was last accessed, when it was last modified, when it was last printed, and when it was deleted. Keyword searches may also fail to discover relevant

electronic records, depending on how the records were created, stored, or used. For example, keywords search text, but many common electronic mail, database, and spreadsheet applications do not store data as searchable text. Instead, the data is saved in a proprietary non-text format. Documents printed by the computer, even if the document was never saved to the hard drive, are recoverable by forensic programs because the printed document is stored as a graphic image. Graphic images, unlike text, are not subject to keyword searches. Similarly, faxes sent to the computer are stored as graphic images and not as text. In addition, a particular relevant piece of data does not exist in a vacuum. To determine who created, modified, copied, downloaded, transferred, communicated about, deleted, or printed the data requires a search of other events that occurred on the computer in the time periods surrounding activity regarding the relevant data. Information about which user had logged in, whether users share passwords, whether the computer was connected to other computers or networks, and whether the user accessed or used other programs or services in the time period surrounding events with the relevant data can help determine who was sitting at the keyboard.

94. It is often difficult or impossible to determine the identity of the person using the computer when incriminating data has been created, modified, accessed, deleted, printed, copied, uploaded, or downloaded solely by reviewing the incriminating data. Computers generate substantial information about data and about users that generally is not visible to users. Computer-generated data, including registry information, computer logs, user profiles and passwords, web-browsing history, cookies and application and operating system metadata, often provides evidence of who was using the computer at a relevant

time. In addition, evidence such as electronic mail, chat sessions, photographs and videos, calendars and address books stored on the computer may identify the user at a particular, relevant time. The manner in which the user has structured and named files, run or accessed particular applications, and created or accessed other, non-incriminating files or documents, may serve to identify a particular user. For example, if an incriminating document is found on the computer but attribution is an issue, other documents or files created around that same time may provide circumstantial evidence of the identity of the user that created the incriminating document.

95. Analyzing data has become increasingly time-consuming as the volume of data stored on a typical computer system and available storage devices has become mind-boggling. For example, a single megabyte of storage space is roughly equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is roughly equivalent of 500,000 double-spaced pages of text. Computer hard drives are now being sold for personal computers capable of storing up to 2 terabytes (2,000 gigabytes) of data. And, this data may be stored in a variety of formats or encrypted (several new commercially available operating systems provide for automatic encryption of data upon shutdown of the computer). The sheer volume of data also has extended the time that it takes to analyze data. Running keyword searches takes longer and results in more hits that must be individually examined for relevance. And, once reviewed, relevant data leads to new keywords and new avenues for identifying data subject to seizure pursuant to the warrant.

96. Based on the foregoing, identifying and extracting data subject to seizure pursuant to this warrant may require a range of data analysis techniques, including hashing tools to identify data subject

to seizure pursuant to this warrant, and to exclude certain data from analysis, such as known operating system and application files. The identification and extraction process, accordingly, may take weeks or months. The personnel conducting the identification and extraction of data will complete the analysis within one-hundred eighty (180) days of this warrant, absent further application to this court.

97. All forensic analysis of the imaged data will employ search protocols directed exclusively to the identification and extraction of data within the scope of this warrant.

Genuine Risks of Destruction

98. Based upon my experience and training, and the experience and training of other agents with whom I have communicated, electronically stored data can be permanently deleted or modified by users possessing basic computer skills. In this case, only if the subject receives advance warning of the execution of this warrant, will there be a genuine risk of destruction of evidence.

Prior Attempts to Obtain Data

99. The United States has not attempted to obtain this data by other means.

REQUEST FOR DELAYED NOTICE OF TRACKING WARRANT

100. Pursuant to Fed. R. Crim. P. 41(f)(2)(C) and (f)(3), and 18 USC 3103a, I request permission to delay service of the tracking warrant on the user or subscriber of the Subject Device for 30 days after T-Mobile's provision of real-time tracking information has ended, because there is reasonable cause to believe that providing immediate notice of the warrant may have an adverse result as defined by 18 USC section 2705. As noted above, following her September 2020 arrest HENNING asked a co-conspirator to execute an order to erase all data on her tablet

and cellular phone. She was successful in erasing data on her tablet but the data on her cellular phone was preserved by storing it in a container that would block external radio signals. This provides cause to believe that if HENNING were to discover that agents are tracking her to execute an arrest warrant, she will flee or destroy evidence to obstruct that warrant. For the same reasons, pursuant to 18 USC section 2705(b), I request that the court direct T-Mobile not to notify any other person of the existence of the warrant.

101. No tangible property, or wire or electronic communications, shall be seized pursuant to the warrant. To the extent the requested real-time tracking (GPS, cell site, or other) information may constitute stored electronic information under 18 USC 2701-2711, it is believed 18 USC 2703(c)(1)(A) expressly authorizes the provision (by the service provider) and retention ("seizure") by agents of such information. To the extent it may not, there is reasonable necessity for the "seizure" of such information. 18 USC 3103a(b)(2). Not allowing agents to retain the information so they may identify the user of the target phone and their location would defeat the only purpose of the warrant and render the warrant useless. No stored wire or electronic information shall otherwise be seized pursuant to the warrant.

REQUEST FOR SEALING

102. This is an ongoing investigation of which the targets are unaware. I therefore request that this affidavit, and all attachments and filings related hereto (other than a copy of the search warrant itself, which will be served on a person present at the Target Location) be sealed until such time as the Court orders otherwise. For the reasons set forth above, disclosure of the affidavit at this time would seriously jeopardize the ongoing investigation; as such disclosure may provide an

opportunity to destroy evidence, change patterns of behavior, or flight from prosecution thereby seriously jeopardizing the success of the investigation. As noted, following her September 2020 arrest HENNING did successfully order the remote erasure of all data from an iPad and cell phone. She successfully erased the iPad data but was unable to erase data on her cell phone because agents stored it in a secure container that blocked external radio signals. This affidavit also contains information regarding crime victims and appropriate notifications must be made to the victims before this information is released to the public.

//

//

//

//

//

//

//

//

//

//

//

//

//

//

CONCLUSION

103. Based on the foregoing, I respectfully submit there is (i) probable cause to support the accompanying complaints and arrest warrants, (ii) the warrant directing T-Mobile to provide real-time tracking or geo-location information for the Subject Device, and (iii) to believe that in the Target Location, and the curtilage thereof, together with all electronic devices found therein belonging to TUGGLE, as more fully described in Attachment A-1, and in the Target Vehicle, as described in Attachment A-2, there exist, as further described in Attachment B, evidence of violations and attempted violations of Title 18 United States Code, Sections 1349 (Conspiracy to Commit Wire Fraud); and 1028A(a)(l) (Aggravated Identity Theft).

Sarah Duray

Sarah Duray
Special Agent, DEA

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone this 21ST day of May, 2021.

HONORABLE KAREN S. CRAWFORD
UNITED STATES MAGISTRATE JUDGE