UNITED STATES DISTRICT COURT

for the

Eastern District of California

United States of America
v.

Kristy Lynn FELKINS

Defendant(s)

Case No. 2:20-mj-0140 CKD

SEALED

CRIMINAL COMPLAINT

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

On or about the date(s) of February 2016 through May 2016 in the county of Butte in the Eastern District of California, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. § 1958	Use of Interstate Commerce Facilities in the Commission of Murder-for-Hire

This criminal complaint is based on these facts:

(see attachment)

☒ Continued on the attached sheet.

/s/
Complainant's signature

Special Agent Aron Mann
Homeland Security Investigations
Printed name and title

Sworn to before me and signed telephonically.

Date: 9/14/2020 at 10:25 am

Judge's signature

City and state: Sacramento, California

Carolyn K. Delaney, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

I, Aron Mann, being duly sworn, hereby depose and state as follows:

I. INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with Homeland Security Investigations ("HSI") and have been so employed since June 2016. As a requirement for employment as an HSI Special Agent, I successfully completed the Criminal Investigator Training Program ("CITP") located at the Federal Law Enforcement Training Center ("FLETC") in Glynco, Georgia. At the conclusion of CITP, I completed an additional Homeland Security Investigations Special Agent Training Academy. As part of the training at FLETC, I received extensive instruction in the areas of immigration law, customs law, illegal narcotics, firearms, surveillance, and interview techniques.

2. As a Special Agent with HSI, part of my duties include investigating violations of federal criminal laws, including those related to the cybercrime and the dark web. As an HSI Special Agent, I am a "Federal Law Enforcement Officer," authorized to investigate violations of the laws of the United States and to execute search and seizure warrants issued under the authority of the United States. I have prepared, executed, and assisted in numerous search and arrest warrants, including those related to violations of federal criminal laws covering cybercrime and related activities in connection with electronic communication applications such as email.

3. Among other duties, I am currently participating in an investigation related to violations of 18 U.S.C. § 1958 (Use of Interstate Commerce Facilities in the Commission of Murder-for-Hire) (hereafter, "Subject Offense"). I personally have participated in the investigation since September 2019 and am familiar with the relevant facts and circumstances. The facts and information contained in this Affidavit are based on my knowledge and observations, my training and experience, and speaking with other federal law enforcement officers familiar with this investigation.

4. This Affidavit is intended to show only that there is sufficient probable cause for the requested arrest warrant and does not set forth all of my knowledge about this matter. Except where otherwise indicated, communications are reproduced in summary and in part. Where dates, figures, times, and/or calculations are set forth in this Affidavit, they are approximate, unless noted otherwise.

5. Based on my training and experience and the facts set forth in this Affidavit, I submit there is probable cause to believe that a violation of federal criminal law, to wit: the Subject Offense has been committed by Kristy FELKINS, and a warrant for her arrest should be issued.

II. STATUTORY FRAMEWORK

6. Murder-for-Hire occurs when (1) whoever travels in or causes another (including the intended victim) to travel in interstate or foreign commerce, or uses or causes another (including the intended victim) to use the mail or any facility of interstate or foreign commerce, (2) with intent that a murder be committed in violation of the laws of any State or the United States (3) as consideration for the receipt of, or as consideration for a promise or agreement to pay anything of pecuniary value, or who conspires to do so [violates this statute]. 18 U.S.C. § 1958.

7. Interstate Communications occur when whoever transmits in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure the person of another. 18 U.S.C. § 875(c).

III. TECHNICAL BACKGROUND

8. Based on my training and experience, I am aware of the following concepts:

a. 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. Currently operating, popular dark web marketplaces are Monopoly, Dark Market, and White House.

b. 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.

c. "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.

d. "The Onion Router," "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 the "Tor Browser," designed to access the Tor network. One of the logos, or "icons," for the 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.

e. Some software used to access the dark web does not permanently store images of the websites and or other data that are visited on the computer that is running the software.

f. 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., 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

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

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.

g. "Bitcoin" (or "BTC[2]") 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.

h. 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.

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

j. 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

[2] As of September 1, 2020, one Bitcoin is equal to approximately $11,980.00 USD.

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[3] 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. The Trezor device offers an advanced passphrase option that incorporates a "25th seed word" that must be enabled to access potentially obscured digital currency assets.

k. 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 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

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

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.

l. 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. Such purchases and sales are often facilitated by peer-to-peer bitcoin exchangers who are not registered with the federal or a state government and who advertise their services on websites designed to facilitate such transactions. These unregistered exchangers often charge a higher transaction fee than legitimate, registered digital currency exchangers. This higher fee is essentially a premium that the unregistered exchangers charge in return for not filing reports on the exchanges pursuant to the Bank Secrecy Act, such as CTRs and SARs.

IV. BACKGROUND CONCERNING LOCALBITCOINS.COM

9. Based on my training and experience, I know the following about the website 'www.localbitcoins.com' (also referred to as "LBC"):

10. LBC is a website founded in 2012, based in Helsinki, Finland, that enables person-to-person Bitcoin trades through a variety of in-person and online means. The website allows users to post advertisements to either buy or sell Bitcoins; on these advertisements, users state their specific exchange rate and the payment methods they will accept for the transaction. Users can then respond to these advertisements and agree to meet locally in person for a face-to-face cash transaction or trade directly through a variety of online methods. Purchased or sold Bitcoins are generally placed in an escrow account by 'www.localbitcoins.com' until the completion of the

transaction and are released to a user's 'www.localbitcoins.com' web wallet upon completion. At this point, Bitcoins can be transferred out of the 'www.localbitcoins.com' wallet to any other desired location. In exchange for its services, 'www.localbitcoins.com' charges nominal fees for the transfer of Bitcoin beyond a 'www.localbitcoins.com' web wallet.

11. There are a number of anonymous or nearly anonymous ways to purchase Bitcoin through the website. For example, some users post advertisements on 'www.localbitcoins.com' offering Bitcoin in exchange for a variety of highly anonymized cash proxy methods, such as Vanilla pre-paid gift cards, Amazon.com gift cards, Walmart gift cards, Reloadit 'packs,' and numerous other methods. Other users accept anonymous cash deposits into 'funnel' type bank accounts through national banks, Western Union and MoneyGram transfers, or simple cash or cashier's checks sent via mail. I am aware that individuals do transmit cash via the U.S. Mail and/or private delivery companies such as Federal Express and in return receive Bitcoin from a seller of Bitcoin (Bitcoins are transmitted from the seller's Bitcoin wallet to the buyer's Bitcoin wallet over the internet). Other users will get contact information through the website, and then meet face to face to purchase Bitcoins using cash.

12. Once a user initiates a 'trade' on the 'www.localbitcoins.com' website in response to an advertisement, the user can engage in dialogue with the Bitcoin buyer/seller through an internal messaging service provided by 'www.localbitcoins.com.' Through this service, the user and the buyer/seller can negotiate further details of the trade or arrange a location to meet in person to complete the transaction. Once the trade is completed, users are given the option to rate the buyer/seller and provide relevant feedback regarding the experience. Some users choose to communicate through email or encrypted chat applications such as Wickr[4] after having met through the site.

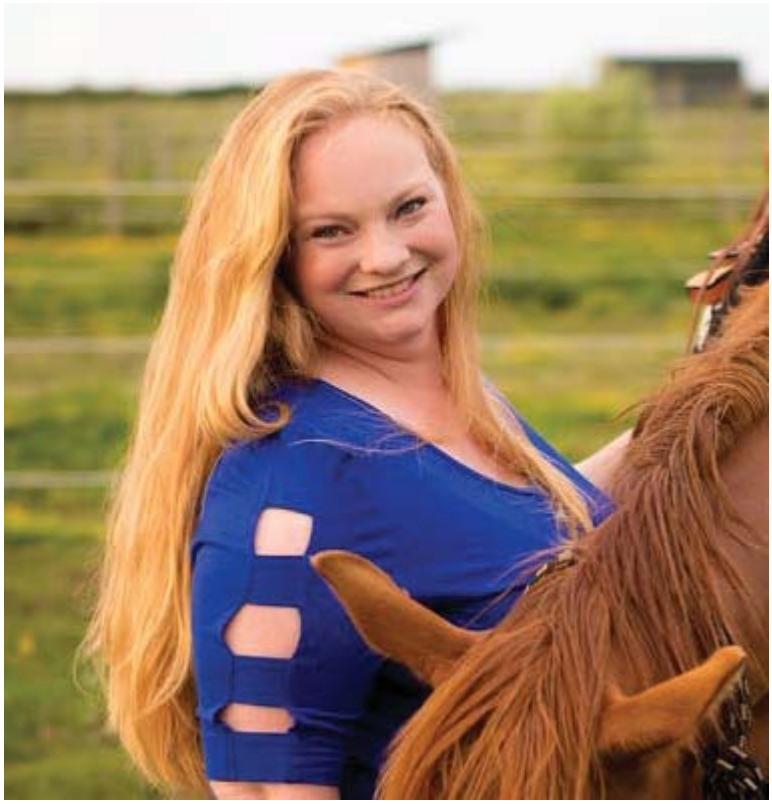
/ / /

/ / /

[4] Wickr is an end-to-end encrypted chat system primarily used on mobile devices, through which the user can set a time limit on how long the message will be viewable by the recipient. Once the message expires, it is wiped from the device.

V. FACTS ESTABLISHING PROBABLE CAUSE

13. In September 2019, your affiant, a member of the Northern California Illicit Digital Economy ("NCIDE") task force, received information that an unknown subject using the moniker "KBGMKN" placed an order on a dark web site to have her ex-husband (referred to as "VICTIM-1") murdered. VICTIM-1 resided in Durham, North Carolina when KBGMKN placed an order for his murder. As described below, there is probable cause to believe that KBGMKN was a moniker used by Kristy Lynn FELKINS, a 35-year old female currently residing in Fallon, Nevada (photo included below).



14. Before moving to Fallon, Nevada in December 2019, FELKINS and her current partner resided in Orland, California, in the Eastern District of California from approximately February 2018 to December 2019. I know this based on my review of a United States Postal Service ("USPS") Change of Address submission from December 17, 2019. According to Thomson Reuters CLEAR, an online records database used by law enforcement and government agencies to verify names and addresses, and other sources (such as bank records), I believe that Felkins

resided in Scotia, California during the relevant time period (approximately February to May 2016); she also travelled during this time period to other cities in Northern California, including Chico, California, in the Eastern District of California. Before living on the West Coast of the U.S. FELKINS resided in North Carolina with VICTIM-1. I know this based on my review of Wells Fargo bank records for accounts held by FELKINS and VICTIM-1.

15. In or about January 2019, an individual not acting on behalf of the government (referred to herein as the "CS-1") provided information to federal law enforcement agents pertaining to a murder-for-hire website which operated on the dark web (referred to herein as "WEBSITE-1"). Between in or about August 2018 and October 2018, CS-1 used a program to scrape from WEBSITE-1 messages between the site's administrator ("ADMIN") and its users. CS-1 was also able to identify the Bitcoin addresses associated with the payments made for acts of violence. In early 2019, CS-1 provided law enforcement with the contents of these scrapes of WEBSITE-1 and continues to provide information about WEBSITE-1. CS-1 provided this information to law enforcement without any promise of pecuniary gain or judicial consideration for any pending criminal case in the United States. Law enforcement has found the information provided by CS-1 to be reliable and has corroborated this information. CS-1 resides in a foreign country and was convicted of a crime in that country related to his possession of child pornography. I am unaware of CS-1 making any false statements to law enforcement or being convicted of making any false statements or perjuring himself.

16. Based on my review of records from WEBSITE-1, I know that on or about February 26, 2016, KBGMKN created an account on the site. WEBSITE-1 is a now-defunct dark web site that purported to be a legitimate platform offering a variety of services, including murder, kidnapping, and assault, in exchange for cryptocurrency payments. WEBSITE-1 was actually a scam website that took users' money but never carried out the offered services.

17. When KBGMKN registered with WEBSITE-1, the user provided an email address of "ejggb133@sigaint.com."[5] The names of FELKINS's children, in order of birth, are Eme****, Jay***, and Geo*** (thus spelling out "ejg").

18. The initial conversations, beginning in February 2016, between KBGMKN and ADMIN primarily involved discussions of how KBGMKN could purchase Bitcoin and ensure that law enforcement could not trace the transaction by "mixing[6]" the Bitcoin. For example, on or about February 26, 2016, ADMIN informed KBGMKN that he/she "*can buy all bitcoins on localbitcoins.com [] you can trade with different sellers and buy the entire amount in a few days*." As described below, the Bitcoin sent by KBGMKN to WEBSITE-1 to pay for the attempted murder of VICTIM-1 were acquired from an LBC account associated with FELKINS.

19. On or about February 29, 2016, KBGMKN asked ADMIN if the site was actually providing hitman services:

> *I have found many posts, some on reddit for example, that state all hit man for hire sites are scams. Some poke fun at this specific site....*
> *Also, the [WEBSITE-1] articles really just make you look desperate ....weather it your posts or not. Any true group fighting such a thing would not include the website address.*
> *If we use a third party escrow how do I know you won't claim to have completed services when you really haven't. I can deny releasing funds but you can still claim they are owed...meaning a third party must then be involved.....*
> *How do I know you are not FBI, they do have the capability to infect ones device and trace them back to their real IP.*
> *Just being cautious*

[5] Sigaint is a now-defunct email service once available both on the regular internet and on the Tor network as a hidden service located at sigaintevyh2rzvw.onion. Sigaint catered to individuals who wished to preserve their anonymity and did not appear to maintain account records.
[6] Mixing is a process by which individuals send cryptocurrency to a wallet address held by a mixing service, which then combines those units of cryptocurrency with other inputs, and then sends them to a designated wallet address. This technique can potentially obscure the historical trail of cryptocurrency and is often used by individuals attempting to launder their funds.

20. In response to KBGMKN's message, ADMIN informed KBGMKN how to remain undetected by the FBI and also stated:

> *the post on reddit saying all hitmen sites are scams, is from undercover cop [] the [WEBSITE-1] articles are not posted by us. we do not have time to post articles [] anyway, if you don't like doing it online, you can always go in the gangs on your streets and hire a hitmen there.*
> *we don't force anyone using our services, we could not, and we do not want to[]*
> *You can even buy some cheap laptop just for this job, or declare that your laptop has been stolen, paste some duct tape on your laptop camera if you are afraid of someone hacking into your laptop, use some public wifi, and if ever caught you can say someone stole your laptop and used it to order the murder of someone you know, to frame you and to do you harm.*

21. Between March 6, 2016, and March 9, 2016, KBGMKN sent WEBSITE-1 just over twelve (12) Bitcoin, the value of which was approximately $5,000.00 at the time, for a hitman to kill VICTIM-1 and make it look like an accident. KBGMKN provided the home address of VICTIM-1 and other information such as the time he left for work, vehicle information, and locations at which VICTIM-1 could be located. After receiving Bitcoin from KBGMKN, the ADMIN acknowledged receipt of the payment and told KBGMKN that a nearby hitman would be assigned to the job.

22. On or about March 6, 2016, KBGMKN informed ADMIN that the "*order is sent*."

23. On the same day, ADMIN informed KBGMKN that he/she "*can travel out of the city on [the murder date], because our hitman won't leave any traces on stop, you want to be 100% that everybody knows they can't suspect you because you were in a different place at the time.. just in case someone might suspect you*."

24. KBGMKN responded on the same day: "*The sooner the better….I won't be around next week. I know it's short notice but I will be in the airport on Monday so that's the perfect alibi….*"

ADMIN states that "*monday would be too soon [] we usually need one week, to do prepaations [sic]*." In response, KBGMKN states:

> *Yeah I knew it would be too shot of a notice. I am out of town all week this coming week. If it can't be done by the end of next week, the the following Monday should be fine. But if at all possible this coming week is best, but I understand if they need more time*
> *Thanks*

25. In April 2020, your affiant obtained a federal search warrant for the email account klfelkins@yahoo.com (2:20-SW-0331-KJN). In reviewing the emails in this account, I found an email sent by FELKINS to VICTIM-1 on or about March 9, 2016 in which she states that she would be in San Francisco "next week."

26. ADMIN then informed KBGMKN that "*I have assigned the hitman [] this will be done either sunday or monday, 7 days from now*."

27. After more back and forth messages about payment, ADMIN sent the following message to KBGMKN on or about March 9, 2016:

> *Ok, we are all set.*
> *The job will be done on monday morning; please let us know if he goes to work with any other person in the car, that you don't want hurt, you need to tell us.*
> *Our man will wait him at the address of work, and when seeing him will shot him as soon as he gets down from the car; but if he is not alone bullets can hurt the other person as well.*
> *Our person will shot several times in chest and head and run; if there is someone important with him that does not need to be hurt please let us know, so the shooter is careful to hit only him*
> *Take care*

28. A few days later, on or about March 12, 2016, KBGMKN asks ADMIN if it is "*possible to make it seem like it was a mugging gone wrong? Maybe they take his wallet? I understand if that means it might not happen on Monday am, but may take an extra day or so to plan. If this*

isn't possible I understand." ADMIN responds that it would be possible to make it look like an accident, but it would cost an additional $4,000. KBGMKN tells ADMIN to just proceed as previously planned.

29. On or about March 13, 2016, ADMIN tells KBGMKN that the hit will be done on Wednesday (March 16, 2016). ADMIN advises KBGMKN to "*make sure you are in a different city and go out with several people, go shopping at mall or in public places where they have video surveillance*."

30. On or about March 16, 2016, KBGMKN asks ADMIN about the status of the hit. ADMIN states that "*the hitman is in position [] he was unable to do the shooting yesterday because he didn't saw the target*."

31. On or about March 17, 2016, KBGMKN asks ADMIN if it would help if she provides VICTIM-1's home address. She then provides the address of "*2619 Alston Ave durham nc 27713*." Based on my review of Wells Fargo bank records associated with VICTIM-1's account, I know that this was VICTIM-1's address during this time period.

32. The following day, KBGMKN asks about the status of the hit. ADMIN continues to state that the hit is on the verge of happening. The next day, on or about March 19, 2016, KBGMKN states that "*the target maybe leaving town with in the next couple days so it really needs to be done tonight or tomorrow*."

33. On or about March 20, 2016, ADMIN states that the hit will require a sniper because VICTIM-1 has not been seen alone and the hitman "*doesn't want to leave witnesses behind*." ADMIN states that a sniper would cost $9,000, which would be an additional $4,000 over what KBGMKN already paid. KBGMKN states that she has "*already borrow to the end of my limit*" and requests that the hitman just wait until VICTIM-1 leaves the house to "*shoot him in his car*." ADMIN responds that he "*will instruct the hitman to do it as you suggested*."

34. KBGMKN informed ADMIN later that day that "*it appears [VICTIM-1] is leaving for the airport late tomorrow night or early Tuesday morning*." The next day, KBGMKN asks

about the status of the hit. ADMIN informs her that "*nothing happened today*" and recommends that KBGMKN pay the additional money for a sniper. ADMIN also asks KBGMKN to explain "*the reason for the murder*." KBGMKN responds:

> *I do stand to get money from this but that isn't the reason behind my motivation....*
> *This man mentally, physically, sexually and emotionally abused me. I ran, and then he took my children away from me. He now mentally abuses my children and threatens their physical well being. He is quite the snake and master manipulater.....*
> *I know I can get the 4000 in 4-5 weeks. And right now the children are visiting grandparents so they aren't at risk of witnessing or possibly being involved. They are safe and comfortable.*
> *My family and friends are not people to have a lot of money, and I have already borrowed from them all they can give trying to settle things with him legally with lawyers. The money I have already sent to you was the last I had to pay the lawyers for the next battle we are up against*
> *My bank accounts are bare from running, relocating, starting over and Lawyers. [] Not to mention I stand to get his retirement, our house and possibly a large life insurance payout.*

35. Divorce papers filed in North Carolina confirm that FELKINS and VICTIM-1 formally received a divorce on January 29, 2016—just before KBGMKN began communicating with ADMIN to have VICTIM-1 murdered. Specifically, your affiant has reviewed a Wake County, North Carolina divorce filing (15-CVD-15540) from January 29, 2016 in which VICTIM-1 is the Plaintiff and Kristy FELKINS is the Defendant. The divorce complaint provides that VICTIM-1 and FELKINS were married on or about June 19, 2004 in Butte County, California, and resided together until their separation on or about November 8, 2014. The complaint also states that VICTIM-1 and FELKINS have two children together, while FELKINS has a third child with a different partner. At the time of the January 29, 2016 marriage dissolution, a claim of equitable distribution (15-CVD-0768) was pending in Durham County, North Carolina.

36. I also found in FELKINS' Yahoo account an email message she sent to a second male she met from a Craigslist personal advertisement. In this email, FELKINS describes how

VICTIM-1 mentally abused her throughout their marriage and finally physically abused her near the end of the relationship, at which time she knew she needed to leave the marriage. This statement is similar to what KBGMKN stated to ADMIN in the message above.

37. The email account also contained email messages between FELKINS and VICTIM-1 in which they discuss their divorce proceedings.

38. In response to KBGMKN's explanation for why she wants VICTIM-1 murdered, ADMIN states that they will agree to have a sniper do the job and KBGMKN can make full payment at a later time when KBGMKN receives the insurance money. KBGMKN then states the following:

> *Ok, he Flys out of the rdu airport early Tuesday morning. He will be gone for almost 2 weeks and when he gets back he will have my kids again. I really hope the current guy can get it done tomorrow I really wanted this to happen while the kids weren't with him. I can't wait for this to be over. I will offer 2000$ bonus to the current hitman if he gets this done tomorrow.*

39. On the same day, on or about March 21, 2016, KBGMKN also states:

> *If the current hitman can't get it done is there anyway to get a sniper in tonight to do it? He could get him when he leaves early tomorrow morning.*
> *I did a little research I believe he will be leaving his house around 4 am maybe a half hr earlier or later, to go to the airport. He will have his girlfriend with him so they probably will be in her white honda.*

40. In response, ADMIN states:

> *I don't think the sniper hitman will be able to get ready and go there so fast; however if the current sniper won't be able to do it; he will follow them to the airport and will bribe someone to find out where he is going, eventually he will buy a last minute flight with the same plane to the same location to stay with him.*

He will leave his gun at the car tough, as no guns can pass through the airport gate

He will fly towards the same location, and when landed he will steal a car, he is good at it. He will steal a truck or some solid jeep, and will run him over by car, making it look like an accident.

41. KBGMKN then tells ADMIN: "*I am pretty sure he is flying into San Francisco. [] He is landing at 11 on the west coast [and] then plans to drive up the coast. I will send as much info as I can get*." KBGMKN also states that "*I live on the west coast but I am hours away from San Francisco and have no ties down there. If it looked like an accident that would be better if done in San Francisco.*"

42. I have reviewed travel records from Southwest Airlines for VICTIM-1. The records revealed that on Tuesday, March 22, 2016, VICTIM-1 traveled from Raleigh-Durham International Airport to San Francisco International Airport, as KBGMKN stated above.

43. In addition, your affiant reviewed statements for shared Wells Fargo bank accounts and debit cards owned by FELKINS and VICTIM-1 during this time period. The statements showed that the debit card associated with VICTIM-1 ending in *6313 began conducting transactions in the specified area KBGMKN said VICTIM-1 would be visiting, i.e. Northern California. Prior to and after this visit to California, the debit card ending in *6313 was primarily used in VICTIM-1's home state of North Carolina.

44. The following day, on or about March 22, 2016, KBGMKN tells ADMIN the following:

I would still greatly appreciate it if this can be done tomorrow early morning if at all possible. All I know is he is landing on the west coast at 11. I am assuming he is flying in to San Francisco based on flight times, and the little bit I know about his plans. I don't know where he plans to rent a car, etc. I am afraid the hit man will not be able to find him and get this done, or that we will run into the same issue with too many other people being around. I feel like tomorrow early am on his way to the airport may be the best option 1) we have a decent idea of where he will be and when 2) it will be dark 3) limited

people/ traffic around because it's so early. His girlfriend will be with him tomorrow but she will be with him for his while trip on the coast. FYI...I have no problems if she gets harmed, etc....

I will still pay the extra 4000 if it is done tomorrow....which puts us in the make it look like an accident bracket, I don't care if it looks like an accident (though that would be great) I just need this done.

If it can't be done tomorrow am then San Francisco is fine but I really need it done no later then this coming Friday.

Thank you

45. After more discussion about payment, KBGMKN states that "*he lands 11 am san Francisco, I believe southwest airlines*." She also states that "*I will see if I can get any information that may be of use*." ADMIN then claims that the hitman was unable to locate VICTIM-1; KBGMKN states that "*I believe he was headed to Fort bragg, I will try to find out*." About an hour later, KBGMKN states that VICTIM-1 "*is no longer in Fort bragg that's all I know*." The next day, on or about March 24, 2016, ADMIN asks for more information about VICTIM-1's location. In response, KBGMKN states:

I am going to be able to get his location and hopefully an idea of his remaining travel plans tomorrow so try to keep an eye on messages. He's in the willits California area tonight, I don't know if he plans to continue north from there or head south towards Chico California

46. Bank records for the above-described debit card ending in *6313 show purchases made by VICTIM-1 in Willits, California on March 23, 2016.

47. KBGMKN then states that "*[VICTIM-1] is in chico CA. I will try to find out where he is staying. He will be in that area through this weekend*." The following day, on or about March 25, 2016, KBGMKN states that VICTIM-1 is "*staying at 111 handy ln. Cohasset ca. Which is a rural town outside of chico. Handy ln is off limpach rd, which is off Cohasset hwy.*"

48. The 111 Handy Ln. address referenced above is associated to both FELKINS and VICTIM-1 dating back to 2007 according to public records found on Thomson Reuters CLEAR.

49. ADMIN continues to claim that the hitman cannot locate VICTIM-1. KBGMKN provides additional locations for VICTIM-1, including, on or about March 26, 2016, "*at Starbucks at 4 on Monday*" in Chico, California. After more back and forth about VICTIM-1's location, KBGMKN begins to grow frustrated with ADMIN. She states on or about March 28, 2016, that "*if you guys can't do as promised then it's time for me to stop wasting my time [sic] get a refund and figure out another solution*."

50. After more discussion, KBGMKN agrees to continue using ADMIN's services. She states on or about March 29, 2016, that VICTIM-1 "*will be back in NC Sunday and back to a regular work schedule monday*."

51. On or about April 9, 2016, KBGMKN, before agreeing to provide additional funds to ADMIN, requests that the hired hitman take a picture of a street sign in North Carolina to verify that the hitman is actually conducting surveillance on VICTIM-1. KBGMKN requests that the photo of the street sign also include the photographer's finger on the right hand side of the image. Eventually ADMIN sends the requested photo, but KBGMKN notes that "*this is obviously a Google Street view with a photo shopped finger added in*." For the next few days, ADMIN continues to string along KBGMKN and fails to provide her with the requested photo. The final message between ADMIN and KBGMKN was on or about April 19, 2016.

52. In addition to reviewing the messages from WEBSITE-1, your affiant also obtained information on the LBC account "kl85coins." This account sent funds to the Bitcoin account of KBGMKN on WEBSITE-1, which was subsequently used to pay for the murder of VICTIM-1. The account name includes the letters "k" and "l", which are the first and middle initials of FELKINS. In addition, based on my review of California Department of Motor Vehicles records for FELKINS, I know that she was born in March 1985. Thus, the "k" and "l" combined with "85" correspond to FELKINS' personal identifiers.

53. The LBC account was created on or about February 26, 2016, which corresponds to the time frame of the WEBSITE-1 discussions referenced above. The username listed on the account is "Kristy L Felkins" and has an associated email of klfelkins@yahoo.com (the same email account referenced above for which I obtained a search warrant).

54. In addition, the user-provided phone number for the LBC account is (919) 799-8551. I know that this was FELKINS' phone number during the relevant time period based on my review of FELKINS' Yahoo email account, in which she references this phone number in numerous emails. In addition, according to Thomson Reuters CLEAR, this number is associated with FELKINS when she resided in Scotia, California.

55. The LBC records also indicate that this phone number was verified by LBC using text message verification. The phone number verification was done on the same day that the account was registered with LBC. In addition, the LBC records show that the last IP address to access the account was 23.126.183.142. This IP address is part of a block of IP addresses assigned to AT&T Internet Services. Emails from FELKINS' Yahoo account reveal that she was using AT&T Internet Services during the relevant time period.

56. While conducting a review of emails found in the klfelkins@yahoo.com search warrant return, your affiant observed an email from on or about February 25, 2016 from Craigslist confirming the posting of an advertisement created by FELKINS. Your affiant viewed the full email header information for this email and observed that the IP address that created the advertisement was the same as the last IP address that accessed the LBC account: 23.126.183.142.

```
MIME-Version: 1.0
X-Mailer: MIME-tools 5.502 (Entity 5.502)
From: "craigslist - automated message, do not reply" <robot@craigslist.org>
To: klfelkins@yahoo.com
Subject: POST/EDIT/DELETE: Beautiful female puppy (pets)
Date: Thu, 25 Feb 2016 01:17:47 +0000 (GMT)
X-CL-Originating-Ip: 23.126.183.142
```

VI. REQUEST FOR SEALING

57. Finally, your affiant respectfully requests that this Court issue an order sealing, until further order of the Court, documents filed in this case, to include, the Application and Arrest Warrant. Based upon my training and experience, your affiant has learned that online criminals actively search for criminal affidavits and warrants via the Internet and disseminate them to others actively seeking out information over the Web and other sources concerning law enforcement activity in this arena. Accordingly, premature disclosure of the contents of this Affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

[CONTINUED ON NEXT PAGE]

VII. CONCLUSION

58. Based on the facts set forth in this Affidavit, I believe there is probable cause that Kristy FELKINS committed a violation of 18 U.S.C. § 1958 (Use of Interstate Commerce Facilities in the Commission of Murder-for-Hire). I therefore request that a warrant for her arrest be issued.

I swear, under the penalty of perjury, that the foregoing information is true and correct to the best of my knowledge, information, and belief.

/s/

Aron Mann
Special Agent
Homeland Security Investigations

Approved as to form:

/s/Grant B. Rabenn
Grant B. Rabenn
Assistant United States Attorney

Sworn and Subscribed to me telephonically on September 14, 2020

Honorable Carolyn K. Delaney
United States Magistrate Judge
Eastern District of California