

AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT
for the
Middle District of Florida

United States of America
v.

De Anna Marie Stinson

Defendant(s)

Case No. 8:21-mj-1955-CPT

CRIMINAL COMPLAINT

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


On or about the date(s) of July 30, 2021 to Sept. 14, 2021 in the county of Hillsborough in the Middle District of Florida, the defendant(s) violated:

| <i>Code Section</i> | <i>Offense Description</i> |
|---------------------|--|
| 18 U.S.C. § 373 | Solicitation to Commit a Crime of Violence |
| 18 U.S.C. § 1958 | Murder-for-Hire |

This criminal complaint is based on these facts:

See attached Affidavit.

Continued on the attached sheet.



Complainant's signature

Julio Fuentes, Special Agent, FBI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 41 by telephone.

Date: 09/22/2021



Judge's signature

City and state: Tampa, Florida

CHRISTOPHER P. TUIITE, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF A CRIMINAL COMPLAINT

I, Julio Fuentes, being duly sworn, deposes and states as follows:

INTRODUCTION

1. I am a Special Agent with the Federal Bureau of Investigation (FBI), United States Department of Justice, currently assigned to the Homestead Resident Agency. I have been an FBI Special Agent since June 2008 and have been assigned to the Miami Division since October 2008. My duties involve the investigation of a variety of violations of federal offenses, including violent crimes, Hobbs Act robberies, extortion, and other violations of federal law.

2. This Affidavit is submitted in support of a criminal complaint against, and arrest warrant for, De Anna Marie Stinson (“**STINSON**”) for a violation 18 U.S.C. §§ 373 (Solicitation to Commit a Crime of Violence) and 1958 (Murder-For-Hire). There is probable cause to believe that **STINSON** engaged in criminal activity using a facility of interstate and/or foreign commerce while residing in the Middle District of Florida.

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

indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

BACKGROUND ON BITCOIN

4. Bitcoin¹ (also known as “BTC”) is a type of virtual currency, circulated over the Internet. Bitcoin are not issued by any government, bank, or company, but rather are controlled through computer software operating via a decentralized, peer-to-peer network. Bitcoin is just one of many varieties of virtual currency.

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

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

¹ Since Bitcoin is both a currency and a protocol, capitalization differs. Accepted practice is to use “Bitcoin” (singular with an uppercase letter B) to label the protocol, software, and community, and “bitcoin” (with a lowercase letter b) to label units of the currency. That practice is adopted here.

restrict access to spending Bitcoin.

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

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

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

PROBABLE CAUSE

10. On or about July 30, 2021, members of an investigative media organization ("Complainants") advised the FBI they had information they believed to be a threat to life.² Law enforcement presently understands that the source of the information to the Complainants was from a website on the dark web³ that advertised

² Information provided by the Complainants has proven to be reliable in the past and has also been corroborated by law enforcement in a separate investigation.

³ 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.

murder-for-hire services (“The Website”). As law enforcement presently understands, although The Website offered murder-for-hire services, it never actually delivered on the promised services after receiving payment from its customers. To my knowledge, law enforcement officers have not had direct contact with The Website administrators.

11. I accessed The Website and observed the following statement on the homepage: “If you are looking to have someone murdered, beaten, kidnapped you have arrived at the best place.” The Website included a messaging forum open to the public. On the publicly viewable portion of The Website, agents observed a message posted on the main forum page on or about July 15, 2021 by a user named “[redacted]” (“Username-A”) titled, “Florida Job” that read, “I am looking for a quick hit in southern Florida? Is anyone available?” On or about July 20, 2021, a hitman (“Vendor-1”) on The Website responded, “Contact me.” Agents took a screenshot of this message thread to preserve it.

12. The Complainants, who have access to data stored on The Website, provided law enforcement officers with records pertaining to “Username-A”. The records included “Username-A’s” apparent subscriber information, payment and transaction details, BTC addresses associated with “Username-A’s” account on The Website, and “Username-A’s” chat communications.

13. According to the records provided by Complainants, “Username-A” joined The Website on or about June 24, 2021, and had BTC addresses associated with “Username-A’s” account. The Website records showed that “Username-A” funded

one BTC address associated with “Username-A’s” account and had conducted approximately five BTC transactions with The Website, which had a combined market value at the time of approximately \$12,307.61, to solicit and hire a “hitman” to kill VICTIM 1.

14. Specifically, “Username-A” placed an “order” for hitman services on or about June 25, 2021, which included VICTIM 1’s name, address, and a photograph of VICTIM 1. The order also included a description, “Do not do at the home. Any place else is fine. Need completed during July – preferably, between July 5th – 11th.” In addition to the “order” described above, “Username-A” placed four additional orders. Like the first order, the four subsequent orders also included the name, address, and a photograph of VICTIM 1. The orders included the following descriptions:

- a. **July 15, 2021 - Order #2.** Description: “Do not do at the home. Any place else is fine. Need completed during July. Bonus if completed by July 31st”
- b. **July 17, 2021 - Order #3.** Description: “Do you have a preferred escrow service? I am ready proceed. Can we get this done by month end?”
- c. **July 17, 2021 - Order #4.** Description: Do you have a preferred escrow service? I am ready to proceed. Can we get this done by month end? The escrow account is set up on Coinsavr. Please advise as to your Username.”
- d. **July 22, 2021 - Order #5.** Description: “Do not do at the home. Any place else is fine. Need completed during July. Bonus if completed by July 31st”

15. According to the records provided by the Complainants, on or about July 2, 2021, “Username-A” paid approximately .17740216 BTC to the BTC address

belonging to The Website, which had an estimated value of \$6,138.11 on the date of transfer, for the purpose of hiring a “hitman” to kill VICTIM 1. “Username-A” also made four additional payments on or about July 20, 2021, and on or about July 21, 2021, totaling approximately \$6,169.50 on the dates of transfer. The Website records provided by the Complainants also showed three transactions on July 20, 2021, where “Username-A” appeared to send Bitcoin to a BTC address associated with “Username-A’s” account for the purpose of funding “Username-A’s” account on The Website.

16. The Complainants also provided law enforcement officers with purported excerpts of communications on The Website between “Username-A” and The Website vendors (alleged hitmen) and administrators.⁴ These messages were not available to the public. Within these communications, on or about July 15, 2021, “Username-A” asked the administrator of The Website “Are you ready to move forward?” On or about July 17, 2021, the administrator responded that the order had been received and asked if any help obtaining Bitcoin was needed. “Username-A” responded, “I am ready to proceed. I have the bitcoin.”

17. A review of the communications between “Username-A” and the administrator revealed that “Username-A” transferred Bitcoin to a virtual currency

⁴ Law enforcement has not been able to verify these communications through direct contact with The Website. The substance of these communications, however, have been corroborated through law enforcement observations of The Website, records from a virtual currency exchange, and STINSON’s conversations with an undercover law enforcement officer in or around August and September 2021.

escrow account for the purpose of paying for the hitman service.

July 20, 2021

Username-A: I sent a test amount of \$ 100.00 to Bitcoin Escrow. It says receipt of funds still pending. I did two transactions: \$10.00 and \$ 100.00. What do you need from me to trace it? The transaction code for you to check [redacted].

I am ready to transmit today... ASAP

Username-A: Address:
[redacted BTC address]

Username-A: I did a test amount and it seems to be working. I dont see the release feature or a key code.

Username-A: The funds are in the the escrow account. Please assign to [Vendor-1].

Admin: ok i am assigning that to [Vendor-1]

July 21, 2021

Username-A: Thank you. What is the process for checking in on job status and the time frame of completion?

July 23, 2021

Username-A: Where are the instructions for releasing escrow for this site once this job has been completed?

July 27, 2021

Username-A: Its been a week. The vendor advised that it would take one week. Please advise as to how to get an update on the job

July 29, 2021

Admin: I have sent a message to the vendor asking if he has completed the job.

Once he says he completed the job, we send you a notification and that will include two links, a link to release the funds and a link to request the funds back.

You will check if he completed the job, if not, you can click the link in message to release the funds back

Alternatively if he fails to complete the job, we can either assign you a different hitman to do the job or you can just withdraw the btc from it to your external wallet

Username-A: Thank you for explaining the escrow process. I will give them until the 31st. BTW, what is the new website? Does [Vendor-1] normally come through? Do you have another vendor suggestion if [Vendor-1] doesnt work out?

July 31, 2021

Username-A: I havent heard from the vendor. Please reassign the job to someone who has a history of getting jobs done. Let me know who youve reassigned the job to. I need this done ASAP

18. While “Username-A” communicated with The Website administrators, “Username-A” also communicated with vendors who held themselves out to be hitmen. Specifically, between on or about July 17, 2021 and July 30, 2021, “Username-A” and Vendor-1 engaged in the following conversation:

Username-A: What is your turn around time for job completion?

Vendor-1: About one week. is this ok?

Username-A: Yes. Since I don't have access to the escrow you use Florida, and Bitcoin escrow is not safe, what trusted site can I use to set up this escrow? I am ready to get this done ASAP. Also, I will do bonus if we can get this done by month end.

Username-A: Did you receive the assignment? Is anything else needed?

Vendor-1: Yes, I received the assignment. Everything is ok.

Username-A: How do we communicate regarding job status updates and estimated time of completion of job?

Username-A: Any updates?

Username-A: Please provide an update ASAP

Username-A: Please advise. It has been over one week

Username-A: What happened with my job? I got no update and it wasn't completed.

19. On or about July 30, 2021, the FBI began investigating the above-described alleged criminal activity on The Website. Agents interviewed VICTIM 1 and learned that STINSON had a previous romantic relationship with VICTIM 1's current spouse.

20. Law enforcement officers also conducted an analysis of the Bitcoin blockchain used in the transactions described above and determined that some of the BTC addresses used to pay The Website belonged to a specific U.S. based virtual currency exchange.

21. A subpoena to the virtual currency exchange yielded records for a registered account that had sent bitcoin to The Website or BTC addresses associated

with The Website. The exchange responded to the subpoena and provided business records associated with the account, which I reviewed. The records provided revealed that the account was registered to “DeAnna Stinson” at her residence in Tampa, Florida, and had been created on or about March 15, 2021 (“the STINSON Virtual Exchange Account”). The registration information for the STINSON Virtual Exchange Account also included the email address “dmariestinson@gmail.com,” the date of birth, driver’s license number, social security number, and phone number associated with **STINSON**. The exchange service also provided a copy of **STINSON**’s driver’s license and “selfie” styled photo of **STINSON** that were submitted to verify the STINSON Virtual Exchange Account.

22. The STINSON Virtual Exchange Account also contained the following bank account details:

- a. A savings account issued by Chase, believed to be Chase Bank, in **STINSON**’s name.
- b. A checking account issued by JP Morgan Chase in the name of WOE Consulting, Inc.

A check of the Florida Division of Corporations revealed WOE Consulting, Inc. is registered to **STINSON** at residence in Tampa, Florida.

23. In response to the subpoena for business records, the virtual currency exchange also provided a transactional log for the STINSON Virtual Exchange Account. I reviewed the records and observed a transaction dated July 2, 2021, where the STINSON Virtual Exchange Account sent approximately .17743084 BTC (valued

at approximately \$5,983.12 on the date of the transaction) to a BTC address the Complainants advised was assigned with The Website. This transaction is consistent with the transaction reflected in The Website records provided by the Complainants as described above in paragraph 15.⁵

24. Records for STINSON Virtual Exchange Account also show the following transactions dated July 17, 2021:

- a. Approximately .00315515 BTC (valued at approximately \$100.15 on the date of the transaction) was sent to a BTC address that, based on the Bitcoin blockchain, appears to be controlled The Website.
- b. Approximately .14500091 BTC (valued at approximately \$4,595.40 on the date of the transaction) was sent to a BTC address that, based on the Bitcoin blockchain, appears to be controlled by The Website.

25. The transaction log contained within the STINSON Virtual Exchange Account records also included Internet Protocol (“IP”) addresses used while accessing STINSON Virtual Exchange Account. On or about July 8, 2021, an IP address registered to Hawaii Telecom was used to purchase \$5,100.00 worth of Bitcoin. On or about August 16, 2021, I received travel records from Delta Airlines indicating **STINSON** traveled from Tampa, Florida, to Honolulu, Hawaii, on or about July 5, 2021, and returned on or about July 11, 2021. These travel dates correspond with the preferred dates requested on the “order” placed on The Website.

⁵ There appears to be a small discrepancy from the U.S. dollar amounts provided by the Complainants and the STINSON Virtual Exchange Account records. While I am uncertain of the exact reason for the discrepancy, based on my training and experience it is possibly attributable to transaction fees and the volatility of Bitcoins value on the market.

26. The IP log contained within the STINSON Virtual Exchange Account records also revealed that on or about July 17, 2021, an IP address registered to Charter Communications was used to purchase \$325.00 worth of Bitcoin. On or about September 20, 2021, I received subscriber records from Charter Communications for the IP address used to make this purchase. According to Charter Communications the IP address at the specific date of time of the purchase was subscribed to **STINSON** at her residence in Tampa.

27. On or about August 24, 2021, I took staged photographs of VICTIM 1 exiting VICTIM 1's residence, which is located in the Southern District of Florida. On or about August 27, 2021, an undercover law enforcement agent ("UC") contacted **STINSON** while impersonating "the hitman" **STINSON** had contracted with via The Website. The UC sent a message using WhatsApp, an encrypted messaging application, to a WhatsApp account associated with the telephone number listed on the STINSON Virtual Exchange Account. The WhatsApp profile associated with **STINSON** had a profile picture that matched **STINSON**'s driver's license photo. The UC sent **STINSON** the staged photograph I had taken along with the photograph **STINSON** sent to The Website to identify VICTIM 1. In the text string, the UC asked **STINSON** to confirm the person in the staged photograph is the same person **STINSON** was seeking to have killed. **STINSON** responded, "Looks right."

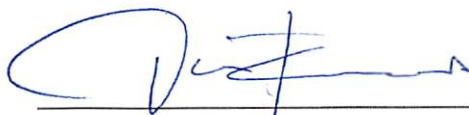
28. On or about September 1, 2021, the UC obtained **STINSON**'s number from the STINSON Virtual Exchange Account records and called **STINSON** using

the WhatsApp application. The UC called from the same number used to send **STINSON** the photographs of VICTIM 1. During the call, which was recorded, the UC stated that the UC was going to stage the murder as a robbery and that the UC would need to purchase a revolver. The UC asked **STINSON** if she was willing to send the UC money via Western Union to which **STINSON** responded, "I can't send you Western Union, I don't want it traced." The UC then asked if she could send Bitcoin to which **STINSON** responded, "Yeah that's fine." The UC told **STINSON** that some people have second thoughts and then asked **STINSON** if she was sure she wanted this done. **STINSON** responded, "yes." The UC told **STINSON** the UC would reach out if the UC needed the money.

29. On or about September 12, 2021, the UC, using the WhatsApp application, sent **STINSON** a unique BTC address and asked her to send \$350. On September 13, 2021, I checked the Bitcoin account created solely for the purposes of this investigation and observed a transfer of 0.0077 BTC (approximately \$350.00 at time of transfer).


CONCLUSION

30. Based on the foregoing, there is probable cause to believe that STINSON committed a violation of 18 U.S.C. §§ 373 (Solicitation to Commit a Crime of Violence) and 1958 (Murder-For-Hire).



Julio Fuentes, Special Agent
Federal Bureau of Investigation

Affidavit submitted by email and attested to me as true and accurate by telephone consistent with Fed. R. Crim. P. 4.1 before me this 22 day of September, 2021.



THE HONORABLE CHRISTOPHER P. TUITE
United States Magistrate Judge