UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	:	
	:	
v.	:	**CRIMINAL NO. 21-cr-399 (RDM)**
	:	
ROMAN STERLINGOV,	:	
	:	
Defendant.	:	

DECLARATION BY LUKE SCHOLL

I, Luke Scholl, depose and state as follows:

1. I am a Staff Operations Specialist with the Department of Justice, Federal Bureau of Investigation (FBI) and have been so employed since 2015. I am currently detailed to the Department of Justice's National Cryptocurrency Enforcement Team. I was previously assigned to an intelligence squad and embedded on a Cyber Criminal Squad in FBI Newark Division. I have investigative experience in cases involving virtual currency, money laundering, the darknet, and computer intrusions. In the course of these investigations, I have reviewed legal returns from Virtual Asset Service Providers (VASPs), such as Kraken and LocalBitcoins. I have operational experience with undercover cryptocurrency transactions and cryptocurrency seizure. I have been a member of the FBI's Virtual Currency Response Team since its inception in 2020. I have used blockchain analysis software tools since 2016. I have received training from Chainalysis Inc., including "Advanced Chainalysis Training", obtained a Chainalysis Cryptocurrency Fundamentals Course Certification, and currently possess a Chainalysis Reactor Certification.

2. This report is based on my review of the following cryptocurrency accounts associated with Roman Sterlingov ("STERLINGOV") including

a. Records obtained from Payward Ventures, Inc. dba Kraken ("Kraken")[1] including two accounts opened by STERLINGOV: account #[redacted] DGMY, held in the name of Roman Sterlingov ("TARGET ACCOUNT 1"); and account #[redacted] KQ5Y, held in the name of TO THE MOON LTD | ROMAN ("TARGET ACCOUNT 2").

b. Records obtained from LocalBitcoins[2] associated with the following account: account username: gothecoin held in the name of Roman Sterlingov ("LOCALBITCOINS ACCOUNT 1").

3. In addition, I reviewed records documenting undercover transactions conducted by IRS-CI during the course of their investigation into STERLINGOV and BITCOIN FOG.

Section A – Attribution of the BITCOIN FOG Cluster

4. According to the IRS-CI documents, on or about 9/11/2019 an IRS-CI Special Agent conducted an undercover transaction to BITCOIN FOG. The IRS-CI Special Agent accessed BITCOIN FOG via its Tor Hidden Service address on the darkweb at foggedriztrcar2.onion and received a Bitcoin address[3] (the UNDERCOVER DEPOSIT ADDRESS) to deposit funds to their BITCOIN FOG account.

[1] Kraken was a cryptocurrency exchange located in the United States and offering custodial wallet services.

[2] LocalBitcoins was a peer-to-peer cryptocurrency exchange located in Finland and offering custodial wallet services.

[3] 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, a cryptographic equivalent of a password needed to access the address. Only the holder of an address' private key can authorize any transfers from that address to another Bitcoin address.

5. Analysis I conducted identified additional addresses controlled by BITCOIN FOG through the use of WalletExplorer.com, a reputable open source blockchain analysis tool. According to WalletExplorer.com, its algorithm groups Bitcoin addresses into wallets based on co-spending[4]. On or about 8/19/2022, a search of the UNDERCOVER DEPOSIT ADDRESS, on WalletExplorer.com revealed that the UNDERCOVER DEPOSIT ADDRESS belonged to a wallet which contained approximately 244,975 additional Bitcoin addresses. Furthermore, WalletExplorer.com had attributed this wallet independently to BITCOIN FOG.

6. The FBI has access to software tools that analyze financial transactions on the Bitcoin Blockchain[5]. I have found these tools to be reliable in numerous previous investigations. Multiple tools corroborated the attribution of the UNDERCOVER DEPOSIT ADDRESS to BITCOIN FOG. One such software tool identified a cluster of approximately 925,000 Bitcoin addresses attributed to BITCOIN FOG (the BITCOIN FOG CLUSTER), which contained the UNDERCOVER DEPOSIT ADDRESS. The analysis contained in this report relied upon attribution of addresses in the BITCOIN FOG CLUSTER provided by this software tool in the determination of the source of funds in all three STERLINGOV accounts.

Section B – Tracing Funds in STERLINGOV Accounts to Bitcoin Fog

LOCALBITCOINS ACCOUNT 1

7. According to records provided by LocalBitcoins, STERLINGOV opened LOCALBITCOINS ACCOUNT 1 with the username "gothecoin" in the name of ROMAN

[4] Co-Spending is when two or more bitcoin addresses are used as inputs to the same transaction, which indicates that a single entity holds the private keys for all of the addresses used as inputs to this transaction. This is the most common way to attribute addresses as being contained in the same cryptocurrency wallet and belonging to the same entity. This relationship is transitive such that if Address A and Address B co-spend in one transaction, and Address B and Address C co-spend in a second transaction, it can be deduced the same entity controls addresses A, B, and C.

[5] A blockchain is a ledger organized into a series of chronological, interlinked data blocks and secured by cryptography. Many virtual assets rely on public blockchains, which allow anyone to see a record of every transaction on the network.

STERLINGOV on 9/20/2012. According to these records, from account opening through 1/13/2022, LOCALBITCOINS ACCOUNT 1 received 73 deposits totaling approximately 259.81 BTC.

8. Blockchain analysis I conducted based on the deposit addresses belonging to LOCALBITCOINS ACCOUNT 1 identified in these records indicated that LOCALBITCOINS ACCOUNT 1 received a total of approximately 259.67 BTC in approximately 80 deposits[6], valued at approximately $870,941[7]. In addition to transactions recorded on the Bitcoin Blockchain, the LocalBitcoins records indicated a single transaction internal to LocalBitcoins.com occurred on or about 9/25/2017 of approximately 0.15 Bitcoin, valued at approximately $553. The total value deposited to the account was approximately 259.82 BTC, valued at approximately $871,494. Blockchain analysis indicated that deposits to LOCALBITCOINS ACCOUNT 1 traceable to the BITCOIN FOG CLUSTER totaled approximately 99.23 BTC, valued at approximately $629,923 as detailed below.

9. Approximately nine deposits to LOCALBITCOINS ACCOUNT 1 came directly from the BITCOIN FOG CLUSTER totaling approximately 64.33 BTC, valued at approximately $585,804. These deposits occurred from on or about 12/11/2017 to on or about 10/17/2018.

[6] The difference of seven transactions between the LocalBitcoins records and the blockchain analysis appeared to result from grouped transactions in the LocalBitcoins records in 2012 and 2013. The LocalBitcoins records listed two deposits in this time period without a corresponding transaction hash with deposit addresses and deposit values matching the sum of multiple deposits recorded on the Bitcoin blockchain to those addresses.

[7] USD value calculations of bitcoin deposits throughout this report are based on the average daily Bitcoin price on the date of each deposit.

10. Approximately 29 deposits to LOCALBITCOINS ACCOUNT 1 were indirectly traceable[8] to the BITCOIN FOG CLUSTER totaling approximately 34.92 BTC, valued at approximately $44,192. These deposits occurred from on or about 10/29/2015 to 9/27/2019.

TARGET ACCOUNT 1

11. According to records provided by Kraken, STERLINGOV opened TARGET ACCOUNT 1 in the name of Roman Sterlingov on or about March 18, 2014. According to these records, from account opening through on or about 5/24/2021, TARGET ACCOUNT 1 received 29 deposits totaling approximately 111.39 BTC and one deposit of approximately 9.56 Bitcoin Cash (BCH).[9]

12. Blockchain analysis I conducted based on the deposit addresses belonging to TARGET ACCOUNT 1 identified in these records indicated TARGET ACCOUNT 1 received approximately 29 deposits totaling approximately 111.39 BTC, valued at approximately $418,394.[10] In addition, TARGET ACCOUNT 1 received a single Bitcoin Cash (BCH) deposit of 9.56 BCH valued at approximately $12,670. The total USD value deposited to the account was approximately $431,064. The majority of these deposits, both in the number of Bitcoin and in

[8] "Indirectly traceable" indicates that the transactions on the Bitcoin Blockchain can provably show a path of multiple transactions that moved specific funds between two addresses or clusters. This path necessarily includes one or more intermediary Bitcoin addresses.

(Example: If Address A sends 1 BTC to Address B in Transactions 1, then Address B sends the same 1 BTC to Address C in Transactions 2, the funds deposited to address C would be indirectly traceable to Address A.)

In contrast, direct transactions are those in which funds are sent directly between two addresses or clusters in a single transaction recorded on the Bitcoin Blockchain (without any intermediary addresses).

[9] Bitcoin Cash is a separate cryptocurrency which forked from the Bitcoin network on or about August 1st, 2017.

[10] These figures differ from those previously reported by IRS-CI investigators in the seizure warrant affidavit for TARGET ACCOUNT 1 and TARGET ACCOUNT 2. I assess that this difference was likely caused by the inclusion of Kraken withdrawal addresses associated with TARGET ACCOUNT 1 in the IRS-CI accounting. The analysis in this document included only those addresses reported by Kraken as deposit addresses of TARGET ACCOUNT 1.

USD value, came directly from withdrawals from LOCALBITCOINS ACCOUNT 1 or were indirectly traceable to the BITCOIN FOG CLUSTER as detailed below.

13. Approximately four deposits to TARGET ACCOUNT 1 came directly from LOCALBITCOINS ACCOUNT 1 and totaled approximately 15.75 BTC, valued at approximately $164,885. These transactions occurred between on or about 5/26/2017 and on or about 9/23/2019.

14. Approximately 16 deposits to TARGET ACCOUNT 1 included funds indirectly traceable to the BITCOIN FOG CLUSTER totaling approximately 83.84 BTC, valued at approximately $247,396. These deposits occurred from on or about 9/23/2014 to on or about 11/17/2020.

15. These two sources of funds combined accounted for approximately 89% of the total Bitcoin and 96% of the total USD value deposited to TARGET ACCOUNT 1.

TARGET ACCOUNT 2

16. According to records provided by Kraken, STERLINGOV opened TARGET ACOUNT 2 in the name of TO THE MOON LTD | ROMAN on or about December 16, 2015. According to these records, from account opening through on or about 5/24/2021 TARGET ACCOUNT 2 received approximately 15 deposits totaling approximately 14.37 BTC.

17. Blockchain analysis I conducted based on the deposit addresses belonging to TARGET ACCOUNT 2 identified in these records revealed that TARGET ACCOUNT 2 received approximately 15 deposits totaling approximately 14.37 BTC, valued at approximately $13,158. The majority of these deposits, both in the number of Bitcoin deposited and in USD value, came directly from withdrawals from LOCALBITCOINS ACCOUNT 1 or were indirectly traceable to the BITCOIN FOG CLUSTER as detailed below.

18. A single deposit to TARGET ACCOUNT 2 came directly from LOCALBITCOINS ACCOUNT 1 of approximately 0.57 BTC, valued at approximately $946. This transaction occurred on or about 5/9/2017.

19. Approximately six deposits to TARGET ACCOUNT 2 included funds indirectly traceable to the BITCOIN FOG Cluster totaling approximately 11.47 BTC, valued at approximately $7,871. These transactions occurred from on or about 4/5/2016 to on or about 11/12/2017.

20. These two sources of funds combined accounted for approximately 83% of the total Bitcoin and 67% of the total USD value deposited to TARGET ACCOUNT 2.

Characterization of Indirect Transfers of Funds from the BITCOIN FOG CLUSTER to Accounts Belonging to STERLINGOV

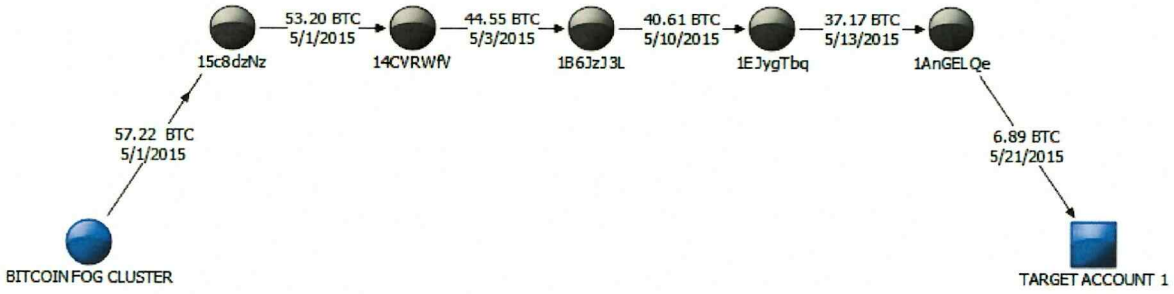
21. Blockchain analysis documented in this report identified many separate paths funds took from the BITCOIN FOG CLUSTER to STERLINGOV accounts including both direct and indirect paths. In many cases, the indirect paths consisted of two transactions and single intermediary address, as shown in the example below.

Example:

22. In other cases, the indirect paths included multiple transactions and intermediary addresses. Indirect paths ranged from as few as one intermediary address to approximately 40 intermediary addresses. Generally, most of these indirect paths consisted of transactions forming

what are known as peel chains[11]. In the example below, and other cases in this analysis, based on my training and experience I believe it is likely that all of the intermediary addresses in the peel chain are contained in a single Bitcoin wallet and controlled by the same entity. The peel chain addresses in the example below are designated by gray circles.

Example:



I declare under penalty of perjury that the foregoing is true and correct.

LUKE SCHOLL
STAFF OPERATIONS SPECIALIST
FEDERAL BUREAU OF INVESTIGATION

August 25, 2022

[11] A peel chain is a pattern of Bitcoin transactions that occurs when a relatively large amount of Bitcoin is gradually spent in multiple, sequential transactions such that each transaction has two outputs; one output constituting a payment to a separate entity, and one output consisting of the "change" (or the remainder of the initial value) sent to a new Bitcoin address which is controlled by the same entity as the original address. Blockchain analysis is required to assess which output represents a payment and which output represents the "change" and is therefore controlled by the original entity.