AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

District of Columbia

United States of America
v.
ROMAN STERLINGOV

Date of Birth: XXXXXXXX

Defendant(s)

Case: 1:21-mj-00400
Assigned To : Meriweather, Robin M.
Assign. Date : 4/26/2021
Description: COMPLAINT W/ ARREST WARRANT

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 October 27, 2011 to April 26, 2021 in the county of _____ in the _____ in the District of Columbia, the defendant(s) violated:

Code Section	*Offense Description*
18 USC 1960(a)	Unlicensed Money Transmission
18 USC 1956(a)(3)	Money Laundering - Sting
D.C. Code 26-1023(c)	Money Transmission without a License

This criminal complaint is based on these facts:

See attached statement of facts.

☒ Continued on the attached sheet.

Devon A Beckett

Complainant's signature

Devon Beckett, Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: 04/26/2021

Robin M. Meriweather

Judge's signature

City and state: Washington D.C.

Robin M. Meriweather, Magistrate Judge
Printed name and title

Case: 1:21-mj-00400
Assigned To : Meriweather, Robin M.
Assign. Date : 4/26/2021
Description: COMPLAINT W/ ARREST WARRANT

STATEMENT OF FACTS

Your affiant, Devon Beckett, is a Special Agent assigned to the Internal Revenue Service, Criminal Investigation (IRS-CI). As a special agent, my responsibilities include the investigation of criminal violations of the Internal Revenue Code (Title 26, United States Code), the Money Laundering Control Act (Title 18, United States Code, Sections 1956 and 1957), the Bank Secrecy Act (including relevant parts of Title 31, United States Code), and related offenses. I have experience investigating crimes involving virtual currency and the darknet, including "mixing" and "tumbling" services, as further described below. I also am experienced in analyzing and tracing virtual currency transactions. Currently, I am tasked with investigating the BITCOIN FOG darknet money laundering service. As a Special Agent, I am authorized by law or by a Government agency to engage in or supervise the prevention, detection, investigation, or prosecution of a violation of Federal criminal laws.

The facts and information contained in this Affidavit are based on my personal knowledge and observations, information provided to me by others involved in the investigation, and a review of documents and records. This Affidavit does not contain each and every fact known to the government. It contains only those facts I believe are necessary to support a finding of probable cause that ROMAN STERLINGOV, a citizen of Russia and Sweden, committed the following offenses: Laundering of Monetary Instruments, in violation of 18 U.S.C. § 1956(a)(3)(B); Operating an Unlicensed Money Transmitting Business, in violation of 18 U.S.C. § 1960(a); and Money Transmission Without a License, in violation of D.C. Code § 26-1023(c).

A. Introduction

IRS-CI and the Federal Bureau of Investigation (FBI) have been investigating an illicit Bitcoin money transmitting and money laundering service called BITCOIN FOG. BITCOIN FOG is an Internet-based service accessible from the District of Columbia and U.S. states. It can be accessed through the Tor hidden website located at http://foggeddriztrcar2.onion.[1] BITCOIN FOG functions as a Bitcoin "tumbler" or "mixer" service.[2] It allows users to send bitcoins to designated

[1] Tor is a computer network designed to facilitate anonymous communication over the Internet. The Tor network does this by routing a user's communications through a globally distributed network of relay computers, or proxies, rendering conventional Internet Protocol ("IP") address-based methods of identifying users ineffective. To access the Tor network, a user must install Tor software either by downloading an add-on to the user's web browser or by downloading the free "Tor browser bundle," which is available at www.torproject.org. When a Tor user accesses a website, only the IP address of the last relay computer (the "exit node"), as opposed to the user's actual IP address, is logged by the website. The Tor network also makes it possible for users to operate websites, called "hidden services," in a manner that conceals the true IP address of the computer hosting the website. Unlike standard Internet websites, a Tor-based web address is comprised of a series of 16 algorithm-generated characters, for example "asdlk8fs9dflku7f," followed by the suffix ".onion." As with all Tor communications, communications between users' computers and a Tor hidden-service webserver are routed through a series of intermediary computers. Accordingly, neither law enforcement nor hidden-service users can use public lookups or ordinary investigative means to determine the true IP address—and therefore the location—of a computer server that hosts a hidden service. For these reasons, hidden services are often referenced as residing on the "darknet" or "Dark Web," and ordinary Internet websites are often referenced as residing on the "clearnet."

[2] The virtual currency bitcoin (abbreviated "BTC") is a form of value that is able to be transacted over the Internet using Bitcoin software. This software provides all necessary services including allowing users to create "Bitcoin addresses," roughly analogous to anonymous accounts; the injection of new bitcoin into circulation; and securely

recipients in a manner designed to conceal and obfuscate the source of the bitcoins. It works by disassociating incoming bitcoin from particular Bitcoin addresses or transactions and then comingling that bitcoin with other incoming bitcoin prior to conducting any further transactions. This process allows BITCOIN FOG customers engaged in unlawful activities to launder their proceeds by concealing the nature, source, and location of their "dirty" bitcoin. BITCOIN FOG publicly advertised this service as a way to help users obfuscate the source of their bitcoin. BITCOIN FOG charges customers a fee for this service.

BITCOIN FOG was launched on or about October 27, 2011, and was still operational as of April 26, 2021. The website is one of the original Bitcoin tumbling sites on the darknet darknet (i.e., areas of the Internet that can usually only be accessed with specific software, configurations, or authorization). As described below, more than 1.2 million BTC (valued at approximately $335,809,383 at the time of the transactions) has been sent through the site from in or about October 2011 through the present. Historically, the largest senders of BTC through BITCOIN FOG have been darknet markets, such as Agora, Silk Road 2.0, Silk Road, Evolution, and AlphaBay, that primarily trafficked in illegal narcotics and other illegal goods.

BITCOIN FOG was publicly advertised on Internet forums and well-known web pages promoting darknet markets as a tool for anonymizing bitcoin transactions. The administrator of BITCOIN FOG publicly promoted the service through a clearnet site (www.bitcoinfog.com and www.bitcoinfog.info) and a Twitter page. These outlets allowed users to easily locate and access the hidden services site through simple clearnet Internet searches.

B. BITCOIN FOG Advertised Its Mixing Service Would Conceal BTC Transactions from Authorities

BITCOIN FOG's launch was announced in an October 27, 2011 posting titled "[ANNOUNCE] Bitcoin Fog: Secure Bitcoin Anonymization" on the BitcoinTalk.org online forum. The announcement was posted by a user with the pseudonym Akemashite Omedetou (Japanese for "Happy New Year") and included links to a clearnet website for BITCOIN FOG (www.bitcoinfog.com), the Tor onion site (http://foggeddriztrcar2.onion), and a Twitter feed for updates on the site (www.twitter.com/#!/@Bitcoinfog).

The announcement post described BITCOIN FOG as a tool to make it difficult for "interested parties, be it authorities or just interested researchers" to trace users' Bitcoin transactions across the Bitcoin network. The post stated that BITCOIN FOG: "mix(es) up your bitcoins in our own pool with other users…get paid back to other accounts from our mixed pool…can eliminate any chance of finding your payments and making it impossible to prove any connection between a deposit and a withdraw inside our service."

After announcing the launch of BITCOIN FOG, the pseudonym Akemashite Omedetou continued to post on BitcoinTalk.org, extolling the anonymizing features of BITCOIN FOG and providing updates on the service. For example, on or about November 11, 2011, in response to an

transferring bitcoin from one Bitcoin address to another. For security and privacy reasons, it is common for a single Bitcoin user to control numerous Bitcoin addresses, which are stored and controlled in a "wallet." Each address is controlled through the use of a unique "private key," akin to a password.

online comment that questioned a design feature of BITCOIN FOG, Akemashite stated: "should we make it easier…to do statistical analysis on our payouts…to help[ing] them start finding our bitcoin client? (that could only be done by an authority of course…) We won't make their life easier."

In another post, dated on or about February 9, 2012, Akemashite responded to a comment from a poster about using mainstream Bitcoin exchanges to mix virtual currency. Akemashite stated: "most of them [exchanges] are also run as legitimate, visible businesses, which will be forced to reveal information about your funds, should such a request be made by the authorities…us on the other hand, the authorities have to find first, which, as Silk Road have [sic] demonstrated, can prove problematic."

The Twitter account @BitcoinFog was established on or about October 27, 2011, the date on which BITCOIN FOG was launched. The @BitcoinFog account regularly posted updates regarding the status of the BITCOIN FOG hidden site, including tweeting a link on November 14, 2014 to http://foggeddriztrcar2.onion, the current hidden services address for BITCOIN FOG.

The @BitcoinFog account also tweeted links to stories discussing why users should tumble bitcoins – to thwart law enforcement. For example, on or about September 13, 2017, the @BitcoinFog account tweeted a link to a story about the IRS using blockchain analysis software to track bitcoin. On or about June 11, 2019, @BitcoinFog tweeted a link to a Europol press release announcing the law enforcement takedown of Bestmixer.io, another Bitcoin mixer/tumbler, commenting: "this is why you need to use ONLY a Tor-based mixing service (Such a surprise)."

C. BITCOIN FOG Operated as an Illegal Money Transmitting and Money Laundering Service on the Darknet

While the identity of a Bitcoin address owner is generally anonymous (unless the owner opts to make the information publicly available), law enforcement can often identify the owner of a particular Bitcoin address by analyzing the blockchain.[3] The analysis can also reveal additional addresses controlled by the same individual or entity. For example, a user or business may create many Bitcoin addresses to receive payments from different customers. When the user wants to transact the bitcoin that it has received (for example, to exchange bitcoin for other currency or to purchase goods or services), it may group those addresses together to send a single transaction. Law enforcement uses commercial services offered by several different blockchain-analysis companies to investigate virtual currency transactions. These companies analyze the blockchain and attempt to identify the individuals or groups involved in the virtual currency transactions. Specifically, these companies create large databases that group transactions into "clusters" through analysis of data underlying the virtual currency transactions.

Using blockchain analysis, law enforcement confirmed that over 1.2 million BTC (valued at approximately $335,809,383 at the time of the transactions) have been sent through BITCOIN

[3] All Bitcoin transactions are recorded on what is known as the blockchain. The blockchain is essentially a distributed public ledger that keeps track of all Bitcoin transactions, incoming and outgoing, and updates approximately six times per hour. The blockchain records every address that has ever received a bitcoin and maintains records of every transaction.

FOG since the site was launched in 2011. This figure includes BTC from various sources: all direct and indirect transactions from sources such as darknet markets; funds stolen from bitcoin addresses through hacks; direct deposits and withdrawals from Bitcoin wallets; sends and receives from wallets not apparently affiliated with a known hosted service; and other unknown sources. IRS-CI cyber analysts reviewed all inputs and outputs from BITCOIN FOG to identify bitcoins sent directly to BITCOIN FOG from known darknet markets and bitcoins sent from BITCOIN FOG to known darknet markets. IRS-CI's analysis determined BITCOIN FOG received approximately 486,861.69 BTC (approximately $54,897,316.44 at the time of the transactions) *directly* from darknet markets. BITCOIN FOG sent approximately 164,931.13 BTC (approximately $23,690,956.28 at the time of the transactions) *directly* to darknet markets. In sum, BITCOIN FOG sent or received more than $78 million in transactions involving known darknet markets, counting only direct transactions.

Among these, IRS-CI cyber analysts identified direct deposits into BITCOIN FOG from at least 35 darknet markets. Below are the top five markets by U.S. dollar value of deposits:[4]

Source Market	Total Received (BTC)	Total Received (USD)
Agora Market	41,966.87	$14,398,754.73
Silk Road 2.0 Market	22,863.74	$12,518,636.97
Silk Road Marketplace	377,102.74	$9,556,159.49
Evolution Market	11,100.79	$3,199,542.15
AlphaBay Market	5,442.86	$2,907,508.67

IRS-CI cyber analysts identified funds sent directly from BITCOIN FOG to at least 51 different darknet markets. Below are the top five markets by dollar value of sends:

Destination Market	Total Sent (BTC)	Total Sent (USD)
Agora Market	26,398.12	$8,680,430.34
Silk Road 2.0 Market	11,274.21	$5,871,831.33
Silk Road Marketplace	106,522.77	$2,289,509.42
Evolution Market	6,473.24	$1,860,053.75
AlphaBay Market	3,375.90	$1,557,931.95

Based on my training and experience, including experience in other darknet investigations, darknet markets exist primarily to traffic in illegal narcotics and other illegal goods and services – a fact well-known among darknet market user and administrators, and intended by the administrators. That the darknet markets listed above primarily traffic in illegal narcotics and other illegal goods and services would be apparent to anyone using the markets because that the categories listed on each market, and the majority of specific listings, openly discuss illegal goods

[4] The U.S. dollar value is calculated as of the date of each BTC transaction. Because the price of BTC has fluctuated significantly since BITCOIN FOG first became operational in or about October 2011, the tables presented above do not show a consistent exchange rate between BTC and U.S. dollars.

and services. I am familiar with each of the darknet markets listed in the tables above, and am aware that illegal narcotics and other illegal goods and services constituted the majority of items for sale on each market. Accordingly, there is probable cause to believe that the bitcoin transactions sent to and from BITCOIN FOG involved the proceeds of "specified unlawful activity," as defined in 18 U.S.C. § 1956(c)(7), such as the narcotics distribution (21 U.S.C. § 841); identity theft and the sale of stolen personally identifiable information (PII) (18 U.S.C. § 1028A); and computer fraud and abuse, including the sale of computer hacking tools and exploits (18 U.S.C. § 1030).

D. Undercover Transactions on BITCOIN FOG

1. September 2019 Undercover Transaction

On or about September 11, 2019, an IRS-CI Special Agent (SA) physically located in the District of Columbia and operating in an online undercover capacity accessed BITCOIN FOG at foggeddriztrcar2.onion through the Tor browser. The SA created an account through the registration page by creating a username, password, and entering a security text phrase pictured below the registration text boxes. The registration page of BITCOIN FOG stated: "As an anonymous service, we do not collect any additional information about you besides a user name and password."

The SA was never asked for any identifying information such as an email account, date of birth, social security number, or passport number, or for any other proof of identification, when creating the account.

On or about September 11, 2019, while physically located in the District of Columbia, the SA sent approximately 0.02488936 BTC ($249.99) from an IRS-CI controlled covert wallet ("UC Sending Wallet") into a wallet address provided by BITCOIN FOG.

On or about September 12, 2019, while physically located in the District of Columbia the SA accessed foggeddriztrcar2.onion. The SA's undercover BITCOIN FOG account showed a balance of approximately 0.02425700. The difference of approximately 0.00063236 BTC between the amount the SA deposited and the balance shown is approximately 2.5% of the total deposit. This is the service fee charged by BITCOIN FOG. On or about September 12, 2019, while physically located in the District of Columbia, the SA sent 0.02 BTC from BITCOIN FOG to an IRS-CI controlled covert wallet ("UC Receiving Wallet").

Through blockchain analysis, investigators traced bitcoin from the BITCOIN FOG deposit address to known BITCOIN FOG Bitcoin clusters identified through blockchain analysis. IRS-CI investigators also traced bitcoin sent to the UC Receiving Wallet and confirmed that the bitcoin was sourced from BITCOIN FOG clusters.

Investigators were unable to directly trace any direct link between the "UC Sending Wallet" and the "UC Receiving Wallet," confirming that BITCOIN FOG successfully tumbled the transaction by breaking the link in the blockchain between the source and ultimate destination of the funds.

2. November 2019 Undercover Transaction

On or about November 18, 2019, while physically located in the District of Columbia, an IRS-CI SA operating in an online undercover capacity sent approximately 0.01173987 BTC to BITCOIN FOG from an IRS-CI controlled undercover account on the Apollon darknet market. Apollon was a darknet market known to sell illegal narcotics, stolen PII, and other illegal items. On November 19, 2019, while physically located in the District of Columbia, the SA accessed BITCOIN FOG at foggeddriztrcar2.onion. The SA's undercover account on BITCOIN FOG showed that the account had been credited by the amount of the send transaction, less an approximately 2.32% fee.

On or about November 19, 2019, while physically located in the District of Columbia and after confirming the deposit of funds from Apollon Market had been credited to the SA's BITCOIN FOG account, the SA sent the message below to the BITCOIN FOG administrator using the messaging function on the BITCOIN FOG site, stating the funds were the proceeds of illegal narcotics sales:

On or about November 21, 2019, while physically located in the District of Columbia, the SA again accessed BITCOIN FOG operating in an online undercover capacity. There was no response to the above message posted by the SA on or about November 19, 2019. The SA then directed BITCOIN FOG to send 0.01146764 BTC from the undercover account on BITCOIN FOG to an IRS-CI controlled undercover wallet. BITCOIN FOG did so.

The IRS-CI SA clearly stated that the BTC was from the sale of ecstasy/molly, an illegal narcotic. At no point did the administrators of BITCOIN FOG prevent the deposit of funds from Apollon or prevent the withdrawal of funds after the funds were represented to be the proceeds of illegal drug sales.

Through blockchain analysis, investigators traced bitcoin from the IRS-CI controlled account on Apollon Market, to the BITCOIN FOG deposit address, to known BITCOIN FOG bitcoin clusters identified through blockchain analysis. IRS-CI investigators also traced bitcoin sent to the IRS-CI controlled undercover wallet and confirmed that the bitcoin was sourced from BITCOIN FOG clusters.

E. Attribution of BITCOIN FOG to ROMAN STERLINGOV

Analysis of bitcoin transactions, financial records, Internet service provider records, e-mail records, and additional investigative information, identifies ROMAN STERLINGOV as the principal operator of BITCOIN FOG.

1. "Akemashite Omedotou" and the Shormint@hotmail.com Account

Early in the investigation, identifiers connected BITCOIN FOG to the pseudonym Akemashite Omedotou and the email account shormint@hotmail.com. As noted above, BITCOIN FOG's launch was announced in a posting on the BitcoinTalk.org forum on or about October 27, 2011 by a user called Akemashite Omedetou. Records from BitcoinTalk.org for the account associated with Akemashite Omedetou revealed that the account was created on or about October 25, 2011, using email address shormint@hotmail.com. The account registration information included the website title "Bitcoin Fog" and website URL http://www.bitcoinfog.com.

According to account details obtained from Twitter, the account @BitcoinFog was created on October 27, 2011 (the date BITCOIN FOG was announced) and was registered with email address shormint@hotmail.com.

Records from Microsoft pertaining to shormint@hotmail.com revealed that the account was created on October 7, 2011, using an apparent fake name and accessed through a Virtual Private Network (VPN) service, used to anonymize user's Internet traffic. Based on my training and experience, I know that criminals often set up "burner" accounts in order to register domains and pay for services tied to their illicit activity.

2. Connecting the BITCOIN FOG Domain to STERLINGOV

Additional investigation, as described below, connects STERLINGOV to the original BITCOIN FOG clearnet domain.

According to publicly available WhoIs information, www.bitcoinfog.com was registered through the web hosting service Highhosting.net on October 25, 2011. The WhoIs records showed that the domain was registered to "Akemashite Omedetou" using email address shormint@hotmail.com. Records from Highhosting.net revealed that Akemashite Omedetou used a Liberty Reserve[5] account (Liberty Reserve Account 1) to pay for the domain. Liberty Reserve records showed that Liberty Reserve Account 1 was registered to shormint@hotmail.com.

[5] Liberty Reserve was a Costa Rica-based digital currency exchange service that allowed users to register and transfer money to other users with only a name, e-mail address, and birth date. Deposits could be made through third parties using a credit card or bank wire, among other deposit options. Liberty Reserve did not directly process deposits or

Investigators reviewed the account activity associated with Liberty Reserve Account 1 and determined that STERLINGOV had funded the account using a series of layered transactions through multiple payment platforms, performed in close temporal proximity and apparently designed to make it difficult to trace the payment to his true identity. Specifically:

- On September 29, 2011, according to records from the virtual currency exchange Mt. Gox,[6] Roman STERLINGOV opened an account in his true name at Mt. Gox (Mt. Gox Account 1), using the email address plasma@plasmadivision.com.

- On October 3, 2011, STERLINGOV funded Mt. Gox Account 1 with 100 euros.

- On October 19, 2011, Mt. Gox Account 1 sent 36 BTC through an off-platform Bitcoin address to a second Mt. Gox Account (Mt. Gox Account 2) (registered to "nfs9000@hotmail.com").

- On October 20, 2011, Mt. Gox Account 2 sent 35 BTC to a third Mt. Gox Account (Mt. Gox Account 3) (registered to "kolbasa99@rambler.ru").

- On October 20, 2011, Mt. Gox Account 3 sent $80 USD to an account at Aurum Xchange (Aurum Xchange Account 1), another digital payment platform.

- On October 20, 2011, Aurum Xchange Account 1 sent $76 USD to Liberty Reserve Account 1.

- On October 25, 2011, Liberty Reserve Account 1 paid the domain fees for www.bitcoinfog.com to Highhosting.net.

This series of transactions is depicted in the below chart:

withdrawals. Deposited funds were then "converted" into Liberty Reserve Dollars (LRUSD) or Liberty Reserve Euros (LREUR), which were tied to the value of the U.S. dollar and the euro, respectively. The service was shut down by U.S. law enforcement in May 2013 after the founder was charged in the United States with money laundering and operation of an unlicensed money service business.

[6] Mt. Gox was a Bitcoin exchange based in Japan that suspended operation in April 2014 after suffering a hack that stole 850,000 bitcoins.

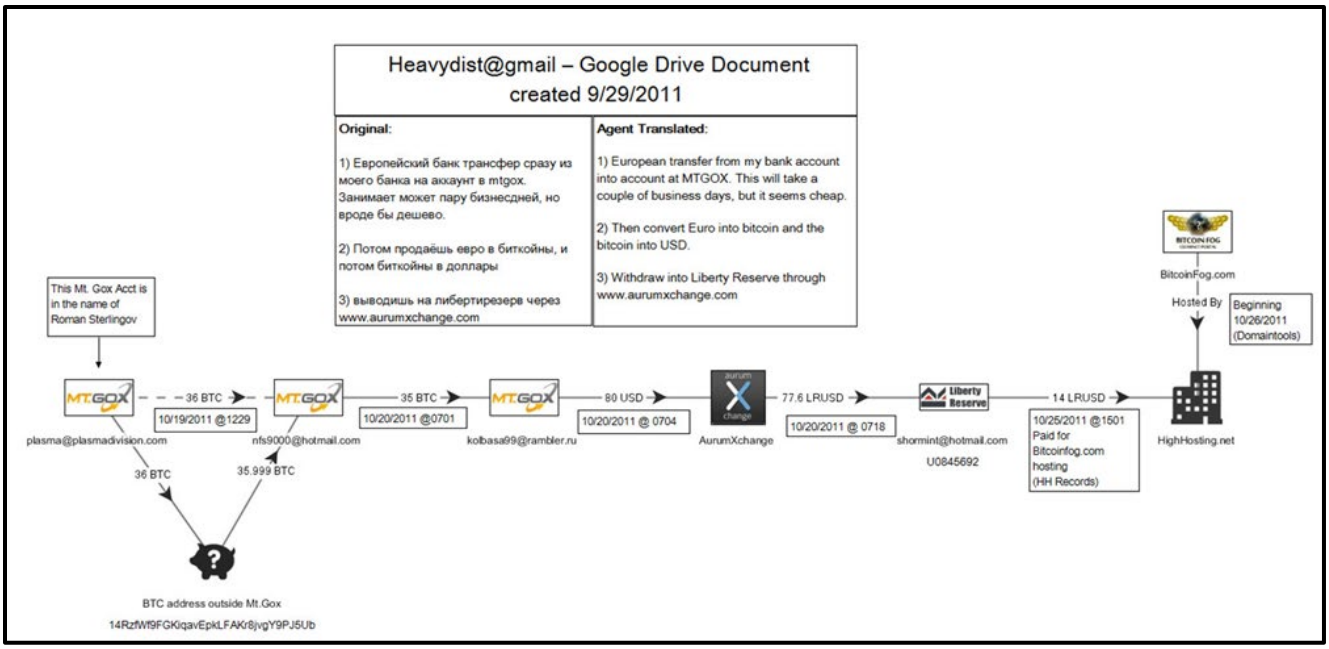
An analysis of the IP addresses used to access the above Liberty Reserve and Mt. Gox accounts confirmed that the accounts shared a common owner: STERLINGOV. For example, IP logs from Mt. Gox and Liberty Reserve showed that on November 24, 2011, a user using the IP address 212.117.160.123 logged into Mt. Gox Account 2, Mt. Gox Account 3, and Liberty Reserve Account 1, as well as another Liberty Reserve account registered to Roman STERLINGOV (Liberty Reserve Account 2). STERLINGOV was also the named account owner of a third Liberty Reserve account (Liberty Reserve Account 3) registered using the email address heavydist@gmail.com (Google Account 1).

Liberty Reserve records revealed that Liberty Reserve Account 2 was registered in STERLINGOV's true name using the email address plasma@plasmadivision.com, the same e-mail tied to Mt. Gox Account 1. The account registration information included a residential address in Gothenburg, Sweden corresponding to STERLINGOV's home address. Both Liberty Reserve Account 2 and Liberty Reserve Account 3 were registered using a Swedish telephone number, TELEPHONE NUMBER 1, which Swedish telecommunications provider records revealed is registered to STERLINGOV

On August 25, 2012, Mt. Gox Account 1 received a 180 BTC deposit sent from an account at BTC-e[7] (BTC-e Account 1). According to records from BTC-e, BTC-e Account 1 was registered to Roman STERLINGOV, using Google Account 1.

Records from Google pertaining to Google Account 1 revealed that the account was registered to "Roman Heavydist" and was linked to TELEPHONE NUMBER 1, identified above as STERLINGOV's phone number. Investigators obtained the contents of Google Account 1 pursuant to a lawfully authorized search warrant. Google Account 1's Google Drive folder contained Russian language document titled Ввод денег ("Putting Money"), dated September 29, 2011 (less than a month prior to the launch of BITCOIN FOG). A translation of the document showed that the document appeared to be notes taken by STERLINGOV describing how to layer funds. The steps outlined in the document match the steps that STERLINGOV took to pay for the domain www.bitcoinfog.com. The below chart displays the relevant text of the document overlayed on the transaction path used by STERLINGOV to pay for the BitcoinFog.com domain.

[7] BTC-e was cryptocurrency exchange that was shut down in July 2017 when the exchange founder was indicted in the United States for money laundering and the servers were seized by U.S. law enforcement.



3. STERLINGOV's Connections to Early BITCOIN FOG Test Transactions

Blockchain analysis of the earliest transactions associated with BITCOIN FOG's activity on the blockchain revealed a series of small value transactions, beginning in early October 2011, approximately two weeks before BITCOIN FOG was officially launched on October 27, 2011. The transactions appeared to be test transactions conducted to beta test the BITCOIN FOG mixer before it went live. These transactions originated from Mt. Gox Account 1, registered in STERLINGOV's true name.

As shown by Mt. Gox records and blockchain analysis, on October 13, 2011, Mt. Gox Account 1 sent approximately two BTC to Bitcoin cluster 12NSB5. This deposit was then broken into smaller amounts through a series of four Bitcoin transactions. Subsequently, the bitcoin was deposited into two new bitcoin wallets, 1KWMex (0.41 BTC) and 1NeWNP (1.57 BTC). The transaction pattern within cluster 12NSB5 is consistent with mixing/tumbling transactions, including those seen from BITCOIN FOG.

Wallet 1KWMex held its 0.41 bitcoin idle, while wallet 1NeWNP transferred its bitcoin to a new address. Through blockchain analysis, investigators traced the outflow of the balance of 1.57 BTC from wallet 1NeWNP to BITCOIN FOG.

Based on my training and experience, I know that software and web developers typically beta-test new software and websites prior to launching them. Beta testing is conducted to confirm that a site's features work and, in the case of a mixer such as BITCOIN FOG, to ensure the tumbler's algorithm is properly working. Law enforcement has observed on numerous occasions darknet market site administrators conduct beta testing prior to launching darknet platforms to the public. Based on my training and experience, including previous investigations of Bitcoin mixers, I believe that the activity described above is consistent with beta testing the BITCOIN FOG

platform. I am aware that such beta testing would typically only be conducted an individual involved in administrating a website or service.

4. STERLINGOV's Receipt of Proceeds from BITCOIN FOG

BITCOIN FOG charges a variable fee of 2% to 2.5% on each deposit. Blockchain analysis revealed that these fees are retained within the BITCOIN FOG cluster, and that the administrator made periodic withdrawals from the BITCOIN FOG cluster to pay himself. These withdrawals occur sporadically and in the same manner as a regular user. The withdrawals appear to be concealed to blend in with regular mixing transactions in order to protect the site administrator from scrutiny. Based on BITCOIN FOG's transaction activity over time, STERLINGOV would have made approximately $8 million in commissions from BITCOIN FOG transactions if he had cashed out the administrative fees near the time that the transactions occurred. Due to the significant increase in value of bitcoin over the course of BITCOIN FOG's operation – from a low of approximately $2 shortly after BITCOIN FOG launched in fall 2011 to a current value of $50,000 – STERLINGOV has been able to reap significant appreciation from his profits that were kept in bitcoin. The current value of the BITCOIN FOG cluster – including customer funds in STERLINGOV's control and STERLINGOV's own money – is nearly $70 million.

Investigators obtained records of STERLINGOV's true-name accounts at several cryptocurrency exchanges. Analysis of STERLINGOV's accounts revealed the vast majority of cryptocurrency deposited into his accounts was originally sourced and traced back to BITCOIN FOG clusters. This activity continued through at least 2019.

F. BITCOIN FOG Is Not Registered with FinCEN or Licensed in the District of Columbia

Records from the Financial Crimes Enforcement Network ("FinCEN"), a division of the U.S. Department of Treasury, revealed that neither ROMAN STERLINGOV nor BITCOIN FOG was registered as a Money Services Business under federal law, despite conducting transactions with U.S. based customers. Similarly, records from the District of Columbia Department of Insurance and Banking (DISB) revealed that neither ROMAN STERLINGOV nor BITCOIN FOG was licensed as a Money Transmitter under District of Columbia law, despite conducting transactions with persons based in the District of Columbia.

Based on my training and experience, I am aware that the Bank Secrecy Act requires anyone who owns or controls a money transmitting business to register with the Secretary of the Treasury. *See* 31 U.S.C. § 5330(a)(1). I am further aware that federal regulations issued pursuant to the Bank Secrecy Act define "money services business" ("MSBs"), which include "money transmitter[s]." 31 C.F.R. § 1010.100(ff)(5). Money transmitters are defined broadly, and include anyone who "accept[s] . . . currency, funds, or other value that substitutes for currency from one person and . . . transmi[ts] . . . currency, funds, or other value that substitutes for currency to another location or person by any means," as well as "[a]ny other person engaged in the transfer of funds." 31 C.F.R. § 1010.100(ff)(5)(i)(A)-(B). MSBs are required to register with the FinCEN, unless specific exemptions apply. 31 C.F.R. § 1022.380(a)(1). MSBs are required to establish

and maintain anti-money laundering programs, to detect and report suspicious transactions, and to collect certain records of customers and customer transactions.

I am further aware that, in the District of Columbia, anyone engaging in the "business of money transmission" is generally required to obtain a license from the Superintendent of the Office of Banking and Financial Institutions of the District of Columbia. D.C. Code § 26-1002(a). "Money transmission" is defined as "the sale or issuance of payment instruments or engaging in the business of receiving money for transmission or transmitting money within the United States, or to locations abroad, by any and all means, including but not limited to payment instrument, wire, facsimile, or electronic transfer." D.C. Code § 26-1001(10). Under District of Columbia code, engaging in the business of money transmission without a license is punishable as a felony. D.C. Code § 26-1023(c).

I am further aware that Bitcoin "mixers" or "tumblers" such as BITCOIN FOG are considered to be MSBs under federal law, and they are also considered to be money transmitting businesses under District of Columbia law. *See* U.S. Dep't of the Treasury FinCEN Guidance, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*, FIN-2019-G001 (May 9, 2019), at 19-20; *United States v. Harmon*, 474 F. Supp. 3d 76 (D.D.C. 2020).

CONCLUSION

Based on the foregoing, your affiant submits that there is probable cause to believe that ROMAN STERLINGOV violated 18 U.S.C. § 1956(a)(3)(B), which makes it a crime to conduct or attempt to conduct a financial transaction involving property represented to be the proceeds of specified unlawful activity, or property used to conduct or facilitate specified unlawful activity, with the intent to conceal or disguise the nature, location, source, ownership, or control of property believed to be the proceeds of specified unlawful activity.

Your affiant submits there is also probable cause to believe that ROMAN STERLINGOV violated 18 U.S.C. § 1960(a), which makes it a crime to knowingly conduct, control, manage, supervise, direct, or own all or part of an "unlicensed money transmitting business," defined as a money transmitting business which affects interstate or foreign commerce in any manner or degree and (A) is operated without an appropriate money transmitting license in a State where such operation is punishable as a misdemeanor or a felony under State law, whether or not the defendant knew that the operation was required to be licensed or that the operation was so punishable; (B) fails to comply with the money transmitting business registration requirements under section 5330 of title 31, United States Code, or regulations prescribed under such section; or (C) otherwise involves the transportation or transmission of funds that are known to the defendant to have been derived from a criminal offense or are intended to be used to promote or support unlawful activity.

Finally, your affiant submits there is probable cause to believe ROMAN STERLINGOV violated D.C. Code § 26-1023(c), which makes it a crime to engage in the business of money transmission without a license.

Devon A. Beckett
Special Agent
IRS-Criminal Investigation

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone, this 26th day of April 2021.

ROBIN M. MERIWEATHER
U.S. MAGISTRATE JUDGE