AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Middle District of Florida

United States of America
v.
Roman Boss

Case No. 8:23-mj-1242 AEP

Defendant(s)

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 fall 2014 through the present in the county of Hillsborough in the Middle District of Florida, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. § 1960	Operating an unlicensed money service business
18 U.S.C. § 1956 (a)(2)	International money laundering

This criminal complaint is based on these facts:

See affidavit attached.

☑ Continued on the attached sheet.

Complainant's signature

JUSTIN R. ALLEN Special Agent, IRS-CI

Printed name and title

Sworn to before me over the telephone or other reliable electronic means and signed by me pursuant to Fed. R. Crim. P. 4.1 and 4(d).

Date: 3/9/23

Judge's signature

City and state: Tampa, Florida

Anthony E. Porcelli, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A CRIMINAL COMPLAINT

I, Justin Allen, being duly sworn, depose and state the following

1. I am employed as a Special Agent with the Internal Revenue Service–Criminal Investigation ("IRS-CI") and have been employed in this capacity since February of 2010. My responsibilities include the investigation of criminal violations of Titles 18, 26, and 31 of the United States Code, and related offenses. I earned a Bachelor of Science degree in Accounting from Florida State University in 2004 and a Masters in Accounting from Florida State University in 2005. I received my Certified Public Accountant license from the State of Florida in 2006. I have attended over 500 hours of training in various aspects of criminal investigation as well as classes dealing specifically with tax evasion, money laundering, asset seizure and forfeiture, various financial investigative techniques, and related financial investigations. I received this training from the Federal Law Enforcement Training Center in Glynco, Georgia, as well as the National Criminal Investigation Training Academy for Internal Revenue Service Special Agents, Glynco, Georgia. In my capacity as a special agent with IRS-CI, I have conducted a variety of financial, tax, narcotics, money laundering, organized crime, national security, and cybercrime investigations. I am currently assigned to the Cyber Crimes Unit in the Washington, DC Field Office.

2. I make this affidavit in support of an application for a criminal

complaint and arrest warrant for Roman BOSS. This affidavit does not set forth every fact resulting from the investigation; rather, it sets forth facts sufficient to establish probable cause to believe that BOSS has violated 18 U.S.C. § 1960, operating an unlicensed money service business and 18 U.S.C. § 1956(a)(2), international money laundering.

DEFINITIONS

3. **Virtual Currency**: Virtual currencies or cryptocurrencies are digital tokens of value circulated over the Internet as substitutes for traditional fiat currency. Virtual currencies are not issued by any government or bank like traditional fiat currencies, such as the U.S. dollar, but rather are generated and controlled through computer software. Bitcoin (or "BTC") and Ether ("ETH") are currently the most well-known virtual currencies in use.

4. **Virtual Currency Address**: Virtual currency addresses are the particular virtual locations to or from which such currencies are sent and received. A virtual currency address is analogous to a bank account number and is represented as a string of letters and numbers.

5. **Blockchain**: The code behind many virtual currencies requires that all transactions involving that virtual currency be publicly recorded on what is known as a blockchain. The blockchain is essentially a distributed public ledger, run by a decentralized network of computers, containing an immutable and historical record of every transaction utilizing that blockchain's technology. The blockchain can be

updated multiple times per hour and records every virtual currency address that has ever received that virtual currency and maintains records of every transaction and all the known balances for each virtual currency address. There are different blockchains for different types of virtual currencies.

6. **Virtual Currency Exchange ("VCE")**: VCEs are trading and/or storage platforms for virtual currencies, such as BTC and ETH. Many VCEs also store their customers' virtual currency in virtual currency wallets. As previously stated, these wallets can hold multiple virtual currency addresses associated with a user on a VCE's network. Because VCEs act as money services businesses, they are legally required to conduct due diligence of their customers (*i.e.*, Know Your Customer (or "KYC") checks) and to have anti-money laundering programs in place (to the extent they operate and service customers in the United States).

7. **Blockchain Analysis:** It is virtually impossible to look at a sole transaction on a blockchain and immediately ascertain the identity of the individual behind said transaction. That is because blockchain data generally only consists of alphanumeric strings and timestamps. That said, law enforcement can obtain leads regarding the identity of the owner of an address by analyzing blockchain data to figure out whether that same individual is connected to other relevant addresses on the blockchain. To do so, law enforcement can use blockchain explorers, as well as commercial services offered by several different blockchain-analysis companies. These companies analyze virtual currency blockchains and attempt to identify the

individuals or groups involved in transactions. "For example, when an organization creates multiple [BTC] addresses, it will often combine its [BTC] addresses into a separate, central [BTC] address (*i.e.*, a "cluster"). It is possible to identify a 'cluster' of [BTC] addresses held by one organization by analyzing the [BTC] blockchain's transaction history. Open-source tools and private software products can be used to analyze a transaction." *United States v. Gratkowski*, 964 F.3d 307, 309 (5th Cir. 2020). Through numerous unrelated investigations, law enforcement has found the information provided by these tools to be reliable.

REGULATIONS REGARDING MONEY TRANSMITTING BUSINESSES

8. 18 U.S.C. § 1960(a) provides that "[w]hoever knowingly conducts, controls, manages, supervises, directs, or owns all or part of an unlicensed money transmitting business, shall be fined in accordance with this title or imprisoned not more than 5 years, or both."

9. The term "unlicensed money transmitting business" means

> 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.

18 U.S.C. § 1960(b).

10. The "regulations" referenced in 18 U.S.C. § 1960(b)(1)(B) define a "money services business" ("MSB") as "[a] person wherever located doing business, whether or not on a regular basis or as an organized or licensed business concern, wholly or in substantial part within the United States, in" one or more specific capacities—including as a "money transmitter." 31 C.F.R. § 1010.100(ff). The term "[m]oney transmitter," in turn, includes anyone who "accept[s] . . . currency, funds, or other value that substitutes for currency from one person and . . . transmit[s] . . . 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).

11. All MSBs are required to register with the Financial Crimes Enforcement Network ("FinCEN"), a division of the U.S. Department of Treasury, unless specific exemptions apply. 31 CFR § 1022.380(a)(1). In addition, MSBs are required to comply with the Bank Secrecy Act, including filing reports of suspicious transactions, 31 U.S.C. § 5318(g); 31 C.F.R. § 1022.320(a); and implementing an effective anti-money-laundering ("AML") program, 31 U.S.C. § 5318(h); 31 C.F.R. §

1022.210. An effective anti-money-laundering program is described as "one that is reasonably designed to prevent the money services business from being used to facilitate money laundering and the financing of terrorist activities." 31 C.F.R. § 1022.210(a). Under the regulations, an anti-money-laundering program must, at a minimum, "[i]ncorporate policies, procedures, and internal controls reasonably designed to assure compliance" with an MSB's obligations to verify customer identification, file reports, creating and retain records, and respond to law enforcement requests. 31 C.F.R. § 1022.210(d)(1). The obligation to verify customer identification is frequently referred to as a "know your customer," or "KYC," requirement.

12. In 2013, FinCEN issued guidance stating that the definition of a money transmitter includes an individual who offers exchange services between virtual currency and fiat currency. *See* Dep't of the Treasury FinCEN Guidance, *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*, FIN-2013-G001 (Mar. 18, 2013) (the "FinCEN Guidance"). The FinCEN Guidance stated, among other things, that those who are money transmitters because they offer exchange services between virtual currency and fiat currency also come within the regulations applicable to MSBs. That guidance was reaffirmed in May 2019. 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).

CASE BACKGROUND

13. I am familiar with the following facts based upon my personal involvement as well as information I have obtained from other law enforcement agencies, regulatory bodies, open-source materials, and reports from civilian cybersecurity research firms. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

14. Cryptonator, which can be found online at cryptonator.com, is a cryptocurrency services company whose primary offering is a cryptocurrency wallet that allows the user to exchange between various cryptocurrency offerings within the wallet (essentially acting as an integrated cryptocurrency exchange). As of January 2023, Cryptonator provided digital asset storage, peer-to-peer transactions, and exchange capabilities for individuals and online merchants.

15. Cryptonator began operation in or around December 2013, and at that time offered only a basic cryptocurrency exchange rate calculator. The domain Cryptonator.com was registered on or about December 23, 2013, by Roman BOSS. BOSS listed a physical address in Germany and the email address trucksale@gmail.com when registering the domain.

16. Investigators obtained a search warrant for the content of trucksale@gmail.com. The content included an email on or about June 2, 2016, from

contact@cryptonator.com[1] to what appears to be a financial institution. The content of the email included, "I'm Roman. CEO at Cryptonator."

17. Beginning in or around Fall 2014, Cryptonator started offering its customers the ability to exchange one cryptocurrency for another. From 2016 through June 2020, individuals could use Cryptonator to exchange cryptocurrency for USD. The Cryptonator wallet now only allows for exchange from one cryptocurrency to any other supported cryptocurrency. As of on or about January 17, 2023, Cryptonator offered support for at least the following cryptocurrencies: Bitcoin, Bitcoin Cash, Dogecoin, Tether, Ether, Dash, Litecoin, Monero, Ripple, and Zcash.

18. Cryptonator currently offers both individual and merchant accounts. Cryptonator's individual accounts offer an online, multi-currency wallet solution which provides users separate wallets for each supported cryptocurrency. Those wallets can be managed from a single personal account.

19. Individual users pay a fee to use Cryptonator's services, which varies depending on the cryptocurrency selected. Cryptonator also earns a fee for each merchant transaction conducted through the site. Merchants pay a 0.9% fee to accept cryptocurrency on the merchants' sites, and Cryptonator pays the equivalent fiat currency (Euro and USD are supported, among others) to a bank account. The

[1] Investigators believe trucksale@gmail.com was copied on the email.

Cryptonator site states that it may request further information from merchant account holders who conduct large fiat withdraws; it is unclear if these additional requests for information are ever enforced.

20. Because it does not collect personal data, Cryptonator's accounts provides favorable registration terms for customers seeking to conceal their identities and sources of income. According to the site, neither merchant nor individual accounts require any identifying information from users to register an account. The only information required to open an account is providing and confirming an email address and password. Cryptonator also appears to allow a single individual user to open multiple accounts with different email addresses.

21. According to blockchain analysis tools, from in or around November 2014, to in or around January 2023, cryptocurrency addresses controlled by Cryptonator have completed more than 4 million transactions, totaling approximately $1,400,000,000. These blockchain tracing tools further revealed that Bitcoin addresses controlled by Cryptonator have directly and indirectly sent or received more than $25,000,000 to or from Darknet Marketplaces and Fraud Shops, more than $34,500,000 directly and indirectly to or from addresses associated with scams, more than $80,000,000 to or from "High-risk" Exchanges (which themselves also often do not require KYC information), more than $8,000,000 directly and indirectly to or from ransomware campaigns, more than $54,000,000 of hacked or stolen funds, more than $34,000,000 directly and indirectly to or from addresses

associated with mixers, nearly $2,000,000 directly and indirectly to or from known criminal cyber actors, and nearly $71,000,000 directly and indirectly to and from addresses sanctioned by the Treasury Department's Office of Foreign Assets Control (OFAC).

22. Blockchain analysis tools reveal that of the transactions Cryptonator has received, approximately 15% of those transactions have come directly from other exchanges. Of those exchanges, about 50% of the transactions have gone through exchanges that are U.S.-based, such as:

a. Virtual Currency Exchange Company 1 ("VCE1") – $18,000,000;

b. VCE2 – $12,000,000; and

c. VCE3 – $10,000,000.

23. Regarding VCE1 specifically, hundreds of thousands of Cryptonator transactions came from and went to VCE1, and more than 17,000 U.S.-based VCE1 customers transacted with Cryptonator. U.S.-based VCE2 customers accounted for another 15,000 customers who transacted with Cryptonator.

24. As further detailed below, my investigation has revealed that Cryptonator is accessible from United States IP addresses, and accepts customers from the United States. To my knowledge, Cryptonator is not registered with FinCEN and does not maintain KYC for its customers.

25. Cryptonator, and the servers used to operate it, are believed to be located in Germany. I know, based on my training and experience, that one of

easiest ways to prevent access from certain countries to websites, such as Cryptonator, is by blocking access from IP addresses located in those countries. Cryptonator appears to enable this function for German-based IP addresses. Investigators accessed Cryptonator from different IP addresses, primarily ones that geolocated to the United States, including the IP address used to register the account. However, when an investigator attempted to register a new Cryptonator account from an IP address that geolocated to Germany, they received the following message:

> "As instructed by the German Financial Authority (BaFin) we cannot longer offer services to German residents without obtaining a Financial License. And so we had to suspend opening new accounts for visitors from Germany until further notice."

Based on my training and experience, this message appears to demonstrate Cryptonator representative's knowledge regarding regulation of financial institutions and virtual currency exchanges in Germany, and efforts that Cryptonator undertook to abide by German regulations. Nevertheless, despite conducting a substantial amount of business with U.S. exchanges and customers, Cryptonator has taken no efforts to comply with U.S. regulations. In other words, Cryptonator could have either blocked U.S.-based customers, IP addresses, and/or transactions; or registered with FinCEN as an MSB. It has chosen to do neither.

26. Cryptonator uses a U.S.-based cloud platform for its customer service issues ("U.S.-based Cloud Provider 1")[2], and investigators obtained a search warrant for Cryptonator's U.S.-based Cloud Provider 1 account. The account name was listed as "Cryptonator," and the email address registered to the account was cryptonator.com@gmail.com. In the tickets observed, Cryptonator representatives repeatedly confirmed that it did not require identifying documents for account holders. A variety of U.S.-based Cloud Provider 1 tickets also confirmed that Cryptonator accepts U.S.-based customers.

27. Several of the U.S.-based Cloud Provider 1 tickets indicate BOSS's knowledge of his service being used for illegal activity, including purchases on darkweb marketplaces. For example, in a January 2017 ticket, a user requested that Cryptonator add Monero, a privacy coin[3], as one of the currency options for the exchange. Specifically, the user stated, "Please add Monero (XMR). This is wise as it is now being accepted on darknet marketplaces like Alphabay. Thank you." In

[2] U.S.-based Cloud Provider 1 is a U.S. cloud-based customer service platform designed to improve communication between companies and their customers. It helps support sales and customer service functions for businesses all over the globe. U.S.-based Cloud Provider 1 allows users to gather all their interactions with customers in one place on the U.S.-based Cloud Provider 1 platform. If customers have questions, they can submit them through various methods such as email, phone, messenger, or chat. Those questions are turned into tickets, assigned a number, and tracked. Tickets may be shared among customer support staff and may also be prioritized.

[3] Privacy coins are cryptocurrencies that obfuscate information about its users, including identities and other transactional information.

response, BOSS stated that he hoped to add the coin as an option by the end of January. In a May 2017 ticket, another user requested support for withdrawing funds from a well-known darkweb marketplace account to Cryptonator. In yet another ticket, a user asked about how coins are mixed, and BOSS responded by stating that, "Cryptonator does not necessarily send it from your address, but from random addresses, to preserve users' privacy. All incoming payments are getting mixed in our vault." Tickets also indicate that Cryptonator offers API[4] keys to darknet marketplaces and the like, such as a bullet-proof hosting service,[5] and a shop selling cached credentials for credit card companies. Based on my training and experience, and my investigation to date in this case, this is important because it means that Cryptonator is offering its customers the ability to easily access criminal services.

28. On or about July 7, 2021, an FBI employee acting in an undercover capacity ("UC1"), while physically present in the Middle District of Florida, successfully registered an account on Cryptonator.com, by providing only an email

[4] An application programming interface (API) is a way for two or more computers programs to communicate with each other. It allows one computer program to use the resources of another.

[5] A bullet-proof (or bulletproof) hosting service is an online infrastructure service provided by internet services providers, which allow users of the hosting service to conduct illicit or high-risk services without being shut down. For instance, bullet-proof hosting providers allow their clients to use their servers to host criminal or high-risk activities, even after receiving online complaints or law enforcement subpoenas alerting the providers to this criminal activity, or court orders to stop the criminal activity.

address and password. During the registration process, Cryptonator sent a confirmation email that the account had been activated successfully. The email provided a brief overview of account features, including the statement that Cryptonator offered "100% Anonymity and Privacy (no ID verification required)."

29. Between on or about July 14, 2021, and on or about August 13, 2021, UC1 conducted a series of cryptocurrency transactions to and from the Cryptonator account as described above, all without providing any identity verification. UC1 deposited BTC into the account and subsequently exchanged that BTC for other supported cryptocurrencies, specifically Ether, Dogecoin, and Monero. On multiple occasions on Cryptonator.com, UC1 converted funds into Monero for the purpose of sending the Monero to fund accounts on a darkweb marketplace which specializes in brokering the sale of hacked credentials (*e.g.*, IP addresses, usernames, and passwords) to servers across the globe. In total, UC1 transacted and/or exchanged an equivalent of approximately $4,195 on Cryptonator.com without providing identity verification documents. These transactions were all conducted from the Middle District of Florida.

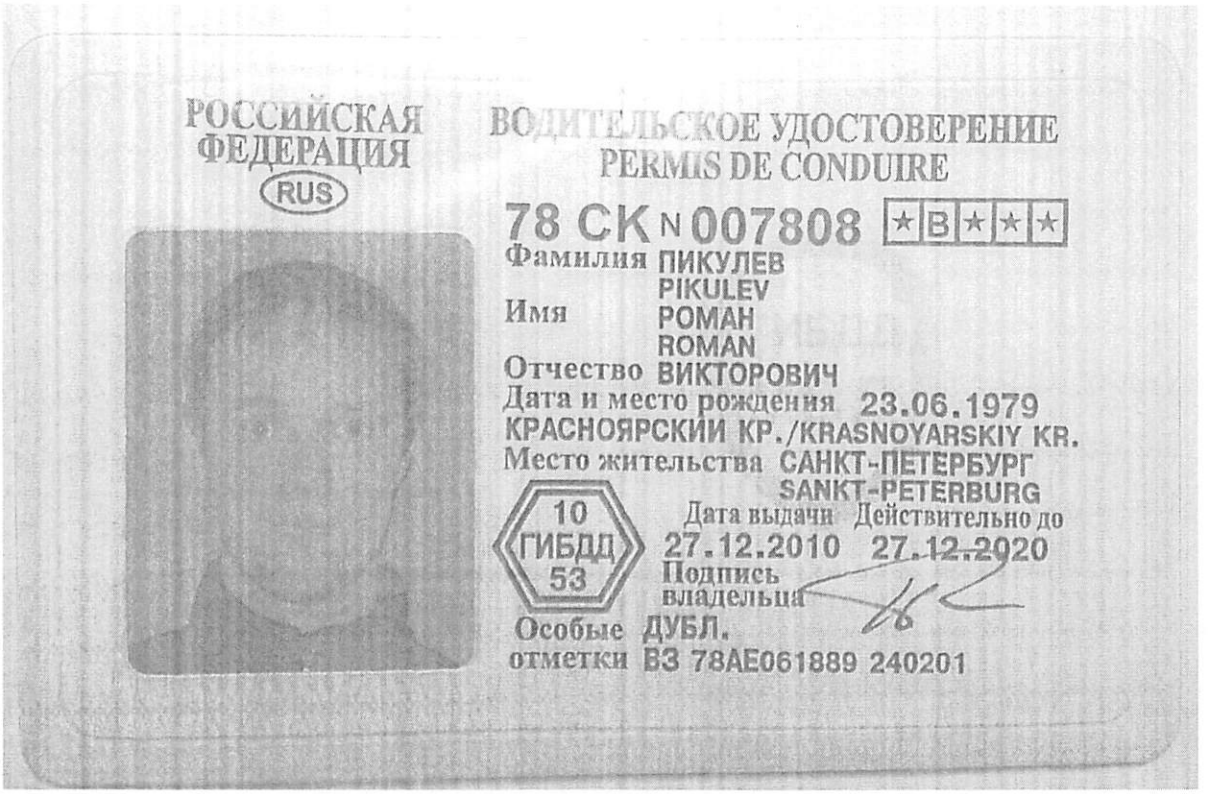
30. On or about September 17, 2021, another FBI employee acting in an undercover capacity ("UC2") successfully registered an account on Cryptonator.com by providing only an email address and password. On or about September 22, 2021, UC2's Cryptonator account received approximately 0.3336 BTC (equivalent to $14,500 USD on the date of transfer) in two transactions from a ransomware

operation (hereinafter "Ransomware Group"). The Ransomware Group actors would encrypt computers on a company's network, steal their data, and extort a ransom from the company in exchange for the Ransomware Group to decrypt the victim's computers and not publish their stolen data. UC2 became an affiliate of the Ransomware Group and during an undercover operation, encrypted data from a fictitious company ("Fictitious Company 1") in order to determine how ransom payments were distributed. In other words, UC2 offered fake victim data from Fictitious Company 1 to the Ransomware Group so that UC2 would be entitled to a payment for UC2's work. Providing Fictitious Company 1's data to the Ransomware Group meant that UC2 would get paid a portion of the ransom payment (here, the payment was made by Fictitious Company 1 so that payment was actually made by the government). Being paid by the Ransomware Group meant that UC2 could gain insight into how payments were distributed and in what amount. Here, the Ransomware Group paid UC2 for UC2's cut of the ransom funds into UC2's Cryptonator account. As of on or about January 19, 2023, Cryptonator has not asked for any identification documents from UC2 nor inquired as to the source of funds.

31. As stated above, as of on or about January 17, 2023, Cryptonator offered support for at least the following cryptocurrencies: Bitcoin, Bitcoin Cash, Dogecoin, Tether, Ether, Dash, Litecoin, Monero, Ripple, and Zcash. Cryptonator offered the ability to exchange cryptocurrencies via Crytonator's platform. In order

to complete these exchange transactions, Cryptonator needed to maintain an inventory of each cryptocurrency to fulfill the exchanges. Investigators believe Cryptonator accomplished this, in part, by obtaining cryptocurrencies from other exchanges. One of those exchanges is Virtual Currency Exchange 4 ("VCE4"). Before on or about November 9, 2019, the servers used to operate VCE4 were located in the United States. After that date VCE4 moved its operations outside of the United States.

32. BOSS created an account at VCE4 on or about December 1, 2015, in the name Roman Pikulev. Investigators obtained records from VCE4. A Russian phone number and the email address contact@cryptonator.com were registered to the account. BOSS provided VCE4 with a Russian identity document to authenticate the account, displayed below.


РОССИЙСКАЯ ФЕДЕРАЦИЯ
RUS
ВОДИТЕЛЬСКОЕ УДОСТОВЕРЕНИЕ
PERMIS DE CONDUIRE
78 СК N 007808 ★B★★★
Фамилия ПИКУЛЕВ
PIKULEV
Имя РОМАН
ROMAN
Отчество ВИКТОРОВИЧ
Дата и место рождения 23.06.1979
КРАСНОЯРСКИЙ КР./KRASNOYARSKIY KR.
Место жительства САНКТ-ПЕТЕРБУРГ
SANKT-PETERBURG
10 ГИБДД 53
Дата выдачи 27.12.2010
Действительно до 27.12.2020
Подпись владельца
Особые отметки ДУБЛ.
ВЗ 78АЕ061889 240201

33. According to VCE4's records, BOSS' VCE4 account completed approximately 30,000 transactions from on or about January 29, 2016, through on or about January 17, 2023. VCE4 records indicate that the transactions did not occur through the API connection. As a result, investigators believe the trades were either manually executed or through a computer script designed to execute the trades. For example, many of these trades have the same timestamp which indicates they were likely automated. The vast majority of these transactions involved the exchange of BTC for other cryptocurrencies. BTC generally has the largest volume of daily trades of any cryptocurrency and is easier to trade due to this volume. This volume,

and number of people using it, makes BTC a favorable trading pair for cryptocurrencies. BOSS' VCE4 account received approximately $5,040,000 worth of BTC from addresses associated with Cryptonator. Investigators believe these transactions were likely to provide some of the BTC used in the exchanges.

34. The VCE4 records also showed another group of transactions involving the exchange of ETH for BTC. Investigators believe this is likely due to customers exchanging cryptocurrencies for Ether. Based on my training and experience, I know that ETH generally has the second highest volume of cryptocurrency trades, which like BTC, makes it an attractive trading pair. BOSS' VCE4 account also received approximately $7,350,000 worth of ETH from addresses clustered to Cryptonator. Based on my training and experience, and my investigation to date in this case, the Ether from these transactions was in turn exchanged for BTC in BOSS' VCE4 account to then exchange the BTC for other cryptocurrencies.

35. Transactions with BOSS' VCE4 account—and withdrawals to Cryptonator addresses—facilitated BOSS' criminal conduct of running an unlicensed money service business. Similar to how narcotics traffickers need to purchase or rent vehicles to transport narcotics, BOSS needed an inventory of various cryptocurrencies in order to fulfill transactions on Cryptonator. BOSS obtained that inventory, in part, from VCE4. On or about the dates listed below, BOSS caused the transmission and transfer, of a monetary instrument and funds, in the amounts described below, from a place in the United States, to or through a place outside the

United States, with the intent to promote the carrying on of specified unlawful activity, that is, running an unlicensed money service business.

36. On April 9, 2018, BOSS' VCE4 account exchanged BTC for Bitcoin Cash ("BCH") in 6 separate trades with the same timestamp for 63 BCH (see table below). One minute later, BOSS' VCE4 account sent 32.65 BCH to address ending PGyS which is associated with Cryptonator.

Amount BCH	Timestamp
2.98459721	4/9/18 19:26
0.01	4/9/18 19:26
28.74	4/9/18 19:26
2.98459721	4/9/18 19:26
0.01	4/9/18 19:26
28.74	4/9/18 19:26
63.46919442	

37. On May 23, 2019, BOSS' VCE4 account exchanged BTC for Ripple ("XRP") in 8 separate trades with the same timestamp for 81,967 XRP (see table below.) One minute later, BOSS' VCE4 account sent 40,902 XRP to address ending EhkB. One minute after that, address ending EhkB sent the same about to Cryptonator. Additionally, address ending EhkB sent 100% of its funds to Cryptonator.

Amount XRP	Timestamp
425.4744682	5/23/19 3:33
27,116.69	5/23/19 3:33
13,428.33	5/23/19 3:33

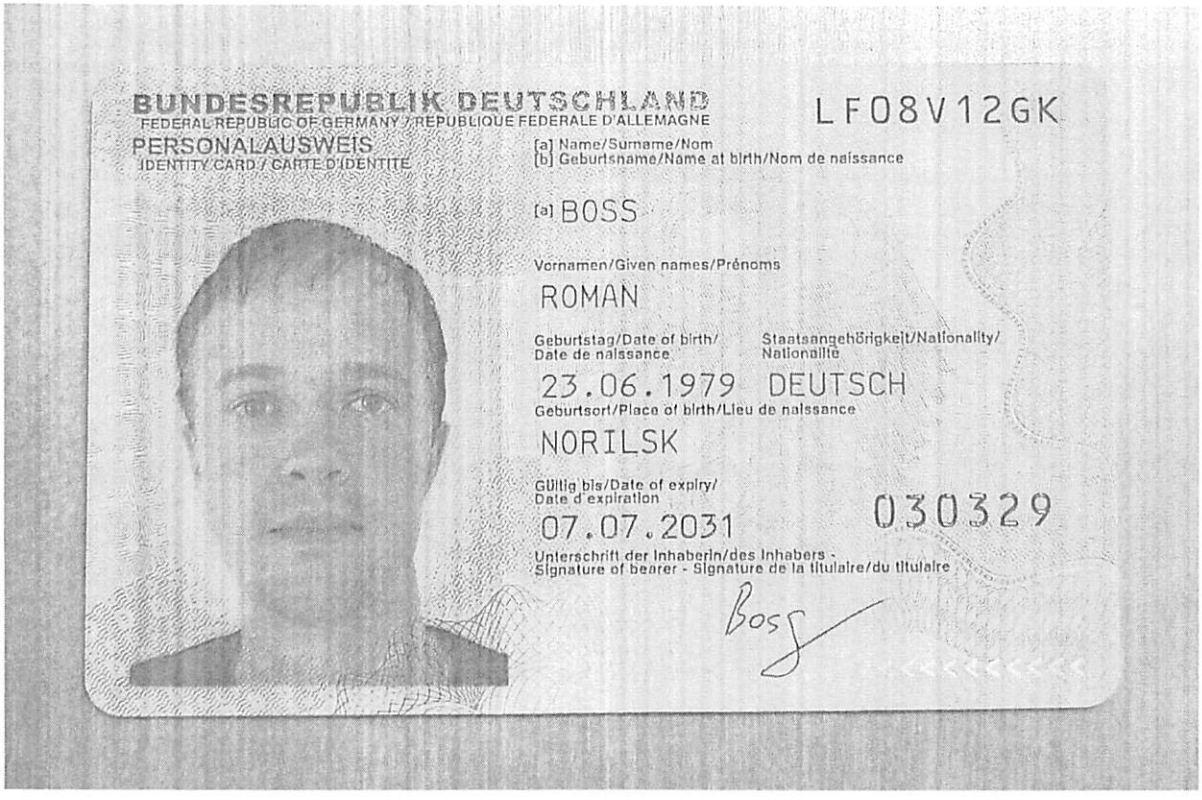
Amount XRP	Timestamp
11.2204887	5/23/19 3:33
1.89189739	5/23/19 3:33
425.4744682	5/23/19 3:33
27,116.69	5/23/19 3:33
13,428.33	5/23/19 3:33
11.2204887	5/23/19 3:33
1.89189739	5/23/19 3:33
81,967.21371	

38. On August 9, 2019, BOSS' VCE4 account exchanged BTC for Dash ("DASH") in 16 separate trades with the same timestamp for 227 DASH (see table below.) Two minutes later, BOSS' VCE4 account sent 113 DASH to address ending rhM2 which is associated with Cryptonator.

Amount DASH	Timestamp
12.68743309	8/9/19 18:18
16.766	8/9/19 18:18
12.6773	8/9/19 18:18
14	8/9/19 18:18
34.39725344	8/9/19 18:18
22.91707373	8/9/19 18:18
0.191	8/9/19 18:18
0.00030338	8/9/19 18:18
12.68743309	8/9/19 18:18
16.766	8/9/19 18:18
12.6773	8/9/19 18:18
14	8/9/19 18:18
34.39725344	8/9/19 18:18
22.91707373	8/9/19 18:18
0.191	8/9/19 18:18
0.00030338	8/9/19 18:18

Amount DASH	Timestamp
227.2727273	

39. BOSS created an account at VCE2 on or about November 26, 2013, in the name Roman BOSS. A German phone number and the email address trucksale@gmail.com were registered to the account. BOSS provided VCE2 with German and Russian identity documents to authenticate the account. The German identity document is displayed below.



40. From March 18, 2021, through May 8, 2022, BOSS' VCE1 account received $146,343 worth of ETH directly from addresses clustered as Cryptonator in 39 different transactions. The transactions are displayed in a chart below.

TIMESTAMP	USD
3/18/21 4:19	$1,811.57
3/24/21 10:25	$5,153.25
3/24/21 11:18	$3,293.45
4/22/21 8:13	$7,726.17
5/24/21 9:05	$2,814.35
6/1/21 15:02	$2,597.77
6/2/21 14:49	$2,721.92
6/18/21 4:19	$2,331.39
6/23/21 11:40	$2,946.54
7/2/21 9:23	$2,107.95
7/9/21 3:29	$2,099.62
7/15/21 5:55	$9,515.67
8/2/21 2:15	$7,691.48
8/4/21 4:16	$4,951.31
8/9/21 17:49	$8,343.29
8/16/21 9:26	$9,678.19
9/19/21 12:17	$335.60
9/20/21 16:21	$3,234.68
9/24/21 16:29	$4,419.20
10/6/21 7:20	$2,763.61
10/14/21 5:20	$3,746.16
11/2/21 12:56	$4,510.70
11/9/21 12:29	$4,753.21
11/16/21 11:28	$4,271.35
11/24/21 4:22	$4,288.99
12/12/21 8:01	$3,842.70
12/21/21 0:02	$1,878.90
12/24/21 17:09	$4,068.18
1/9/22 15:51	$3,152.25
1/17/22 6:08	$3,267.66
1/26/22 14:37	$2,434.33
2/8/22 6:40	$1,548.76
2/16/22 9:10	$1,540.44
3/1/22 8:38	$2,633.47
3/9/22 9:05	$1,375.74
3/28/22 15:07	$3,377.74

TIMESTAMP	USD
4/9/22 7:22	$6,430.34
4/29/22 13:14	$1,398.72
5/8/22 5:05	$1,285.60
	$146,342.25

41. According to records from VCE1, BOSS has a VCE1 debit card linked to his account. VCE1 debit cards allow users to use the card at any retailer that accepts Visa. VCE1 debit cards can be funded with cryptocurrencies and allow users to spend their cryptocurrency anywhere a credit card is accepted. BOSS spent approximately $281,161 from on or about March 18, 2021, through on or about January 27, 2023, with his VCE1 debit card. BOSS used his VCE1 card to pay for lifestyle expenses, including what appears to be travel to the United States, Brazil, Mexico, Italy, and Egypt.

42. BOSS also used the VCE1 debit card to make monthly payments that promoted the ability to operate Cryptonator and facilitated the criminal conduct of operating an unlicensed money service business. Some of those payments included:

a. Payments to U.S.-based Cloud Provider 1, from in or around March 2021 through in or around January 2022, for a total $942;

b. Payments to a Germany-based hosting provider,[6] from in or around March 2021 through in or around May 2022, for a total $1,395; and

c. Payments to a U.S.-based Internet service provider ("U.S.-based ISP 1")[7], from in or around April 2021 through in or around January 2023, for a total $6,151.

43. VCE1's servers are located in the United States. BOSS does not appear to have informed VCE1 that he was using VCE1 to transfer his proceeds from operating Cryptonator, an unlicensed money service business. On or about the dates listed above, BOSS caused the transmission and transfer, of a monetary instrument and funds, in the amounts described above, from a place in the United States, to or through a place outside the United States.

[6] Evidence reveals that at least some of the servers used to operate Cryptonator are hosted at a web hosting service provider located in Germany.

[7] U.S.-based ISP 1 acts as a reverse proxy for its customer's websites. Instead of going directly to their customer's websites, the traffic goes through U.S.-based ISP 1's servers. U.S.-based ISP 1 provides a service where they scan incoming traffic and attempt to filter our malicious activity.

CONCLUSION

44. Based on the foregoing facts, there is probable cause to believe that Roman Boss has violated 18 U.S.C. § 1960, operating an unlicensed money service business and 18 U.S.C. § 1956(a)(2), international money laundering.

Respectfully submitted,

JUSTIN R. ALLEN
Special Agent, IRS-CI

Affidavit submitted by email and sworn to before me over the telephone or other reliable electronic means and signed by me pursuant to Fed. R. Crim. P. 4.1 and 4(d) before me on March 1st, 2023.

ANTHONY E. PORCELLI
United States Magistrate Judge

SUPPLEMENTAL AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A CRIMINAL COMPLAINT IN CASE NUMBER 8:23-mj-1242-AEP

I, Justin Allen, being duly sworn, depose and state the following

1. I am employed as a Special Agent with the Internal Revenue Service–Criminal Investigation ("IRS-CI") and have been employed in this capacity since February of 2010. My responsibilities include the investigation of criminal violations of Titles 18, 26, and 31 of the United States Code, and related offenses. I earned a Bachelor of Science degree in Accounting from Florida State University in 2004 and a Masters in Accounting from Florida State University in 2005. I received my Certified Public Accountant license from the State of Florida in 2006. I have attended over 500 hours of training in various aspects of criminal investigation as well as classes dealing specifically with tax evasion, money laundering, asset seizure and forfeiture, various financial investigative techniques, and related financial investigations. I received this training from the Federal Law Enforcement Training Center in Glynco, Georgia, as well as the National Criminal Investigation Training Academy for Internal Revenue Service Special Agents, Glynco, Georgia. In my capacity as a special agent with IRS-CI, I have conducted a variety of financial, tax, narcotics, money laundering, organized crime, national security, and cybercrime investigations. I am currently assigned to the Cyber Crimes Unit in the Washington, DC Field Office.

2. I make this supplemental affidavit to correct an error in a previous affidavit in support of an application for a criminal complaint and arrest warrant for

Roman BOSS, matter number 8:23-mj-1242-AEP. This supplemental affidavit does not set forth every fact resulting from the investigation; rather, it sets forth facts sufficient to establish probable cause to believe that BOSS has violated 18 U.S.C. § 1960, operating an unlicensed money service business and 18 U.S.C. § 1956(a)(2).

CORRECTION

3. The previous affidavit matter number 8:23-mj-1242-AEP is incorporated entirely herein for reference.

4. Paragraph 27 of the previous affidavit stated: "U.S.-based VCE2 customers accounted for another 15,000 customers who transacted with Cryptonator." I received the number of U.S.-based customers that transacted with VCE2 during a phone call with a Legal Projects Coordinator from VCE2. Subsequently, VCE2 provided records about the number of customers who transacted with Cryptonator. That number was lower much lower than the anticipated 15,000.

5. Subsequent communications with the same Legal Projects Coordinator from VCE2 revealed the error was due to a miscommunication. VCE2 believed there were 15,000 transactions with U.S.-based customers, not 15,000 customers. VCE2 has responded that they will provide an updated amount of U.S.-based and non-

U.S.-based customers that transacted with Cryptonator. However, they are unable to provide those numbers immediately due to an audit. Undersigned felt it important, however, to clarify this error for the Court as soon as possible.

Respectfully submitted,

JUSTIN R. ALLEN
Special Agent, IRS-CI

Sworn to and subscribed before me this 23 day of March, 2023.

ANTHONY E. PORCELLI
United States Magistrate Judge