

AO 106 (Rev. 04/10) Application for a Search Warrant (Modified: WAWD 10-26-18)

UNITED STATES DISTRICT COURT

for the  
Western District of Washington

In the Matter of the Search of  
*(Briefly describe the property to be searched  
or identify the person by name and address)*  
(1) Information associated with 36 Google accounts that is  
stored at premises controlled by Google LLC; and  
(2) Information associated with 2 Apple accounts that is  
stored at premises controlled by Apple Inc.

Case No. MJ22-129

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachments A-1 and A-2, incorporated herein by reference.

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachments B-1 and B-2, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- evidence of a crime;
- contraband, fruits of crime, or other items illegally possessed;
- property designed for use, intended for use, or used in committing a crime;
- a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

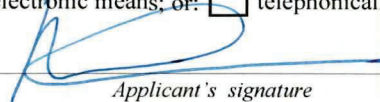
<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. § 371	Conspiracy
18 U.S.C. §§ 1343 and 1349	Wire Fraud and Wire Fraud Conspiracy
18 U.S.C. §§ 1956 and 1957	Money Laundering and Money Laundering Conspiracy

The application is based on these facts:

- See Affidavit of Federal Bureau of Investigation Special Agent Andrew Cropcho continued on the attached sheet.

Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

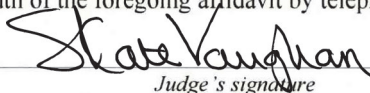
Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented:  by reliable electronic means; or:  telephonically recorded.

  
*Applicant's signature*

Andrew Cropcho, Special Agent  
*Printed name and title*

- The foregoing affidavit was sworn to before me and signed in my presence, or
- The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: April 1, 2022

  
*Judge's signature*

City and state: Seattle, Washington

Hon. S. Kate Vaughan, United States Magistrate Judge  
*Printed name and title*

**AFFIDAVIT**

STATE OF WASHINGTON )

) ss

COUNTY OF KING )

I, Andrew Cropcho, being duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts, further described below (collectively the “Accounts”), that are stored at premises owned, maintained, controlled, or operated by (a) Google LLC (“Google”), an electronic communications service and/or remote computing service provider headquartered at 1600 Amphitheater Parkway, Mountain View, California; and (b) Apple Inc. (“Apple”), an electronic communications service and/or remote computing service provider headquartered at One Apple Park Way, Cupertino, California. The information to be searched is described in the following paragraphs and in Attachments A-1 and A-2. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google and Apple to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachments B-1 and B-2. Upon receipt of the information described in Section I of Attachments B-1 and B-2, government-authorized persons will review that information to locate the items described in Section II of Attachments B-1 and B-2.

2. The Accounts to be searched are as follows:

a. **Google**

- ivan@hashcoins.com (**GOOGLE ACCOUNT 1**);
- ivan@burfa.com (**GOOGLE ACCOUNT 2**);
- ivan.turygin@polybius.io (**GOOGLE ACCOUNT 3**);
- turygin@gmail.com (**GOOGLE ACCOUNT 4**);

- 1 • sergei@hashcoins.com (**GOOGLE ACCOUNT 5**);
- 2 • sergei@burfa.com (**GOOGLE ACCOUNT 6**);
- 3 • sergei.potapenko@polybius.io (**GOOGLE ACCOUNT 7**);
- 4 • sergei.potapenko@gmail.com (**GOOGLE ACCOUNT 8**);
- 5 • nikolay@hashcoins.com (**GOOGLE ACCOUNT 9**);
- 6 • nikolay.pavlovskiy@burfa.com (**GOOGLE ACCOUNT 10**);
- 7 • pavel@hashcoins.com (**GOOGLE ACCOUNT 11**);
- 8 • pavel.tsihhotski@burfa.com (**GOOGLE ACCOUNT 12**);
- 9 • pavel.tsihhotski@polybius.io (**GOOGLE ACCOUNT 13**);
- 10 • stanislav.pavlov@hashcoins.com (**GOOGLE ACCOUNT 14**);
- 11 • stanislav.pavlov@burfa.com (**GOOGLE ACCOUNT 15**);
- 12 • vadim.tsvetikov@hashcoins.com (**GOOGLE ACCOUNT 16**);
- 13 • vadim.tsvetikov@burfa.com (**GOOGLE ACCOUNT 17**);
- 14 • vitali@hashcoins.com (**GOOGLE ACCOUNT 18**);
- 15 • vitali@burfa.com (**GOOGLE ACCOUNT 19**);
- 16 • anton.altement@polybius.io (**GOOGLE ACCOUNT 20**);
- 17 • edgar.bers@polybius.io (**GOOGLE ACCOUNT 21**);
- 18 • tatjana@burfa.com (**GOOGLE ACCOUNT 22**);
- 19 • margarita.burunova@hashcoins.com (**GOOGLE ACCOUNT 23**);
- 20 • dalmeronprojects@gmail.com (**GOOGLE ACCOUNT 24**);
- 21 • ecohousenetworks@gmail.com (**GOOGLE ACCOUNT 25**);
- 22 • admin@hashcoins.com (**GOOGLE ACCOUNT 26**);
- 23 • info@hashcoins.com (**GOOGLE ACCOUNT 27**);
- 24 • info@burfa.com (**GOOGLE ACCOUNT 28**);
- 25 • info@polybius.io (**GOOGLE ACCOUNT 29**);
- 26 • invoices@hashcoins.com (**GOOGLE ACCOUNT 30**);
- 27 • invoices@burfa.com (**GOOGLE ACCOUNT 31**);
- 28 • microsoft@hashcoins.com (**GOOGLE ACCOUNT 32**);

- 1 • cb@hashcoins.com (**GOOGLE ACCOUNT 33**);
- 2 • licenses@hashcoins.com (**GOOGLE ACCOUNT 34**);
- 3 • alerts.mining@burfa.com (**GOOGLE ACCOUNT 35**); and
- 4 • support@polybius.io (**GOOGLE ACCOUNT 36**);

5 (collectively the “**GOOGLE ACCOUNTS**”); and

6 b. **Apple**

- 7 • Sergei.potapenko@gmail.com (DSID 624556209) (“**APPLE**
- 8 **ACCOUNT 1**”) (believed to be used by SERGEI POTAPENKO); and
- 9 • Turygin@gmail.com (DSID 1931852295) (“**APPLE ACCOUNT 2**”)
- 10 (believed to be used by IVAN TURYGIN);

11 (collectively the “**APPLE ACCOUNTS**”).

12 3. I am a Special Agent with the Federal Bureau of Investigation (“FBI”) and  
13 have been since May of 2018. I am currently assigned to the Seattle Field Office. My  
14 primary duties include investigating violations of Federal law, including corporate fraud,  
15 securities fraud, government program fraud, and healthcare fraud. Part of those duties  
16 include investigating instances of wire fraud being used for financial gain at the expense of  
17 others. Before my career as an FBI Special Agent, I was employed by a large public  
18 accounting firm for over three years and, as part of my employment, I examined financial  
19 information of clients to determine their accuracy, reliability, and sources.

20 4. The facts set forth in this Affidavit are based on my own personal knowledge;  
21 knowledge obtained from other individuals during my participation in this investigation,  
22 including other law enforcement personnel; review of documents and records related to this  
23 investigation; communications with others who have personal knowledge of the events and  
24 circumstances described herein including, but not limited to, the victims in this investigation;  
25 and information gained through my training and experience.

26 5. This affidavit is intended to show merely that there is sufficient probable cause  
27 for the requested warrant and does not set forth all of my knowledge about this matter.

1           6.       Based on my training and experience, and the facts as set forth in this affidavit,  
2 there is probable cause to believe that violations of Title 18, United States Code, Sections  
3 371 (Conspiracy), 1343 (Wire Fraud), 1349 (Wire Fraud Conspiracy), 1956 (Money  
4 Laundering), and 1957 (Money Laundering—transactions over \$10,000) have been committed  
5 by IVAN TURYGIN and SERGEI POTAPENKO, individually, and by and through the use  
6 of their companies HASHCOINS OU, HASHCOINS TRADE OU, HASHCOINS LP  
7 (collectively, “HASHCOINS”); HASHFLARE LP (“HASHFLARE”); Burfa Capital OU,  
8 Burfa Media OU, Burfa Real Estate OU, Burfa Tech OU, Burfa Trade OU, Burfa Invest OU  
9 (collectively, the “BURFA Entities”); Polybius Foundation OU, Polybius Tech OU, Polybius  
10 Ventures OU, Polybius Fintech MidCo OU (collectively, “POLYBIUS”); and Dalmeron  
11 Projects LP (“DALMERON”), along with other co-conspirators, known and unknown,  
12 including identified key employees of the same companies. There is also probable cause to  
13 search the information described in Attachments A, for evidence, instrumentalities, or  
14 contraband of these crimes, as described in Attachments B.

#### JURISDICTION

15  
16           7.       This Court has jurisdiction to issue the requested warrant because it is “a court  
17 of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A)  
18 & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has  
19 jurisdiction over the offense[s] being investigated.” 18 U.S.C. § 2711(3)(A)(i).

20           8.       Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is  
21 not required for the service or execution of this warrant.

22           9.       This warrant application is to be presented electronically pursuant to Local  
23 Criminal Rule CrR 41(d)(3).

#### PROCEDURAL HISTORY

24  
25           10.      On April 3, 2020, in connection with the pendent investigation, the Honorable  
26 Brian A. Tsuchida, United States Magistrate Judge, issued a search warrant pursuant to Title  
27 18, United States Code, Sections 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), requiring  
28 Google to disclose to the government copies of certain information and records pertaining to

1 the Google Accounts and authorizing the government to seize specified information and  
2 records.<sup>1</sup> See MJ20-153. The relevant time period for the information and records subject to  
3 disclosure and seizure under the search warrant was the inception of each relevant account  
4 through the date of the search warrant.

5 11. On March 11, 2021, the Honorable John L. Weinberg, United States  
6 Magistrate Judge, issued a search warrant pursuant to Title 18, United States Code, Sections  
7 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), requiring Apple to disclose to the government  
8 copies of certain information and records pertaining to the Apple Accounts and authorizing  
9 the government to seize specified information and records. See MJ21-149. The relevant time  
10 period for the information and records subject to disclosure and seizure under the search  
11 warrant was the inception of each relevant account through the date of the search warrant.

12 12. The April 3, 2020, and March 11, 2021, search warrants are collectively  
13 referred to herein as the “Search Warrants.”

14 13. In support of its applications for the Search Warrants, the United States  
15 submitted two affidavits (collectively, the “Affidavits”). I was the affiant for both Affidavits,  
16 and I swore to the truth and accuracy of their contents.

17 14. The Affidavits are incorporated by reference herein and appended to this  
18 search warrant application.

### 19 **BACKGROUND ON VIRTUAL CURRENCY AND MINING**

20 15. Virtual currency (also known as cryptocurrency) is an asset that can be  
21 exchanged directly person to person, through a virtual currency exchange, or through other  
22 intermediaries. It can be used to buy goods and services, exchanged for “fiat currency”  
23 (currency established by government regulation or law) or other virtual currency, or held as  
24 an investment, among other applications.

25 \_\_\_\_\_  
26 <sup>1</sup> The search warrant included four additional accounts not included in the Google Accounts listed above. One of those  
27 additional accounts contained a clerical error as written, so Google did not provide any information associated with the  
28 account. The other three accounts were not associated with any information or records seized by the FBI. Accordingly,  
those four additional accounts are not included in this search warrant application.

1           16. Virtual currency is generally not issued by any government or bank. Rather, it  
2 is frequently generated and controlled through software operating on a decentralized, peer-  
3 to-peer (“P2P”) network of computers across the world. (Some types of virtual currency,  
4 however, are generated and controlled through software operating on a centralized network  
5 of computers across the world.)

6           17. There are thousands of virtual currencies in use, including Bitcoin, Ethereum,  
7 Bitcoin Cash, and Monero. Bitcoin,<sup>2</sup> the most popular form of virtual currency, can be  
8 generated through mining. According to Bitcoin.org, “Bitcoin mining is the process of  
9 making computer hardware do mathematical calculations for the Bitcoin network to confirm  
10 transactions and increase security. As a reward for their services, Bitcoin miners can collect  
11 transaction fees for the transactions they confirm, along with newly created bitcoins.”

12           18. Bitcoin mining can be conducted locally on a user’s computer or other  
13 computer hardware, or it can be conducted on another’s system via the cloud. According to  
14 the Santa Clara Law School High Technology Journal: “Cloud mining is an economic  
15 arrangement whereby a person pays another person or entity to engage in cryptocurrency  
16 mining on their behalf and receives the transaction fees, cryptocurrency or a portion thereof  
17 that is generated from such mining efforts.”

18           19. One measure for determining the effectiveness or processing power of a  
19 mining operation is to calculate the operation’s hash rate. According to Bitcoin.org: “The  
20 hash rate is the measuring unit of the processing power of the Bitcoin network. The Bitcoin  
21 network must make intensive mathematical operations for security purposes. When the  
22 network reached a hash rate of 10 Th/s, it meant it could make 10 trillion calculations per  
23 second.”

24           20. Bitcoin utilizes “public key cryptography,” a mathematical algorithm that  
25 generates a pair of unique, corresponding keys: the “public key” and the “private key.” These  
26

---

27 <sup>2</sup> Since Bitcoin is both a virtual currency and a protocol, capitalization differs. Accepted practice is to use “Bitcoin”  
28 (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 virtual currency. That practice is adopted here.

1 components form the “public address,” which is used to send and receive bitcoins and can be  
2 shared. A public address is akin to a bank account number, and a private key is akin to a  
3 Personal Identification Number (“PIN”) or password. Only the holder of a public address’s  
4 private key can authorize transfers of virtual currency from that public address to another  
5 public address.

6 21. Many virtual currencies operate via a “blockchain,” a record (or ledger) of  
7 every transaction ever conducted that is distributed throughout the computer network (as  
8 opposed to being maintained by any single administrator or entity). As to bitcoins, although  
9 the public addresses of those engaging in virtual currency transactions are recorded on a  
10 blockchain, the identities of the individuals or entities behind the public addresses are not  
11 recorded on these public ledgers. If, however, an individual or entity is linked to a public  
12 address, it may be possible to determine what transactions were conducted by that individual  
13 or entity. Bitcoin transactions are therefore sometimes described as “pseudonymous,”  
14 meaning that they are partially anonymous.

15 22. Virtual currency users typically employ a “wallet,” a tool that can be used to  
16 manage public and private keys, interface with a blockchain, and send or receive virtual  
17 currency. Wallets vary widely in terms of their format and technological sophistication. One  
18 variety, known as “hosted” (or “custodial”) wallets, are virtual-currency wallets controlled  
19 by a third party—often, a company with a cloud-based, encrypted wallet platform that may  
20 be hosted on the company’s servers. Users of hosted wallets may be able to access the  
21 company’s platform through various digital devices, much like a traditional online banking  
22 experience. Hosted wallet providers include virtual currency exchanges, which allow their  
23 customers, for a fee, to exchange virtual currency for other virtual currencies and/or fiat  
24 currencies.

25 23. Virtual currencies are sometimes launched through Initial Coin Offerings  
26 (“ICO”). An ICO is a capital raising event in which an entity offers investors a unique “coin”  
27 or “token” in exchange for consideration—most commonly in the form of established virtual  
28 currencies or fiat currency. These tokens are issued on a blockchain and are sometimes



1 listed on online platforms, called virtual currency exchanges, where they are tradable for  
2 virtual or fiat currencies. To participate in an ICO, investors are typically required to  
3 transfer virtual currencies to the issuer's address, online wallet, or other account. During an  
4 ICO, or after its completion, the issuer would typically distribute its unique "tokens" to the  
5 participant's unique address on the related virtual currency's blockchain. Similar to  
6 stockholders in an initial public offering ("IPO"), holders of tokens are entitled to certain  
7 rights related to a venture underlying the ICO, such as profits, shares of assets, use of certain  
8 services provided by the issuer, and voting rights.

### 9 STATEMENT OF PROBABLE CAUSE

#### 10 **A. Summary of Investigation**

11 24. There is probable cause to believe that Estonian nationals IVAN  
12 TURYGIN and SERGEI POTAPENKO, as well as various corporate entities they owned  
13 and/or controlled, and other co-conspirators, carried out a multi-faceted wire-fraud and  
14 money-laundering conspiracy, in violation of 18 U.S.C. §§ 371, 1343, 1349, 1956, and 1957.  
15 As discussed below, from approximately 2014 through 2018, TURYGIN, POTAPENKO,  
16 and other co-conspirators deceived and defrauded others in relation to cryptocurrency and  
17 cryptocurrency-related ventures, all for their own personal gain. They further engaged in a  
18 series of financial and monetary transactions to obfuscate the true nature and location of the  
19 fraudulently obtained funds, and to enrich themselves.

20 25. This fraud scheme had four distinct stages, which together constitute a scheme  
21 or artifice to defraud:

22 a. ***Sale of Cryptocurrency Mining Hardware and Equipment:*** In 2014, through  
23 HASHCOINS, TURYGIN and POTAPENKO sold cryptocurrency mining hardware and  
24 equipment they did not have. When the influx of contracts to purchase mining equipment far  
25 outpaced HASHCOIN's ability to fulfill the contracts, TURYGIN and POTAPENKO  
26 revised the contracts to redirect existing and new customers to a purported cloud-based  
27 platform to mine Bitcoin and other cryptocurrencies offered by HASHFLARE, which  
28 TURYGIN and POTAPENKO also owned and operated.

1           **b. *Sale of Cryptocurrency Mining Contracts:*** TURYGIN, POTAPENKO, and  
2 other co-conspirators operated HASHFLARE as a fraud and Ponzi scheme beginning in or  
3 around 2015 and continuing through mid-2018. During this time, they fraudulently induced  
4 thousands of individuals, including one or more of whom resided in the Western District of  
5 Washington, to invest in contracts that guaranteed the buyer a portion of HASHFLARE's  
6 purported cryptocurrency mining power, and thus a portion of the resulting profits. In order  
7 to avoid repaying HASHFLARE investors, TURYGIN and POTAPENKO instituted  
8 material changes to the HASHFLARE investor agreements, substantially reducing payments  
9 to investors and restricting their abilities to withdraw funds. Then, in July 2018,  
10 HASHFLARE unilaterally canceled its contracts with investors and stopped paying annual  
11 returns, claiming that cryptocurrency mining was no longer profitable.<sup>3</sup> In fact, the vast  
12 majority of annual returns HASHFLARE had paid up to that point were sourced from  
13 victims' deposits, not from cryptocurrency mining. To date, the FBI has identified at least  
14 \$175 million that victims transferred to HASHFLARE, most of which TURYGIN and  
15 POTAPENKO laundered through various shell companies, bank accounts, and  
16 cryptocurrency wallets they controlled, or otherwise used to perpetuate their fraud scheme.

17           **c. *Polybius Initial Coin Offering:*** In 2017, leveraging the apparent success of  
18 their cloud-mining operations, TURYGIN, POTAPENKO, and others perpetuated their wire-  
19 fraud scheme by using proceeds from the initial phase of the scheme—i.e., the  
20 HASHFLARE Ponzi scheme—to partially fund the launch of POLYBIUS, and the ICO of  
21 PLBT, POLYBIUS's newly minted cryptocurrency token. TURYGIN, POTAPENKO, and  
22 others induced victims to purchase tens of millions of dollars of PLBT tokens by making  
23 numerous misrepresentations about POLYBIUS and PLBT including, without limitation,  
24 that POLYBIUS would use the ICO proceeds to develop a digital bank and would pay  
25

---

26 <sup>3</sup> These material alterations and purported cancellation of mining contracts were the subject of a purported class action  
27 lawsuit filed in the Central District of California, *Baylog et al. v. Hashflare LP*, No. 18-CV0343. In defending that  
28 lawsuit, HASHFLARE continued to falsely represent in court filings that it was a legitimate enterprise and investment  
vehicle for cloud-based cryptocurrency mining.

1 dividends to holders of PLBT tokens. Not long after completion of the ICO in June 2017,  
2 POLYBIUS publicly dropped any pretext that it intended to build a digital bank. POLYBIUS  
3 transferred much of the estimated \$32 million it raised in the ICO to shell companies, bank  
4 accounts, and/or cryptocurrency wallets controlled by TURYGIN and POTAPENKO.

5 d. ***Laundering Proceeds:*** TURYGIN, POTAPENKO, and others funneled the  
6 fraudulently obtained victim funds through a convoluted network of domestic and  
7 international shell companies—including HASHCOINS, DALMERON, and the BURFA  
8 Entities—bank accounts, cryptocurrency exchanges, cryptocurrency wallets, and tangible  
9 property, all of which they owned and/or controlled, in order to conceal the nature, location,  
10 source, ownership, and control of the funds, and to promote additional fraudulent conduct.  
11 Additionally, TURYGIN and POTAPENKO used fraud proceeds to fund their lavish  
12 lifestyle, which included extensive travel on private jets, stays at luxurious international  
13 villas, and the purchase of real estate and luxury cars in Estonia. Even after ostensibly  
14 shuttering HASHFLARE, TURYGIN and POTAPENKO used fraud proceeds to purchase  
15 expensive cryptocurrency mining hardware, which they used to mine cryptocurrencies for  
16 personal gain.

17 26. The Accounts, described in more detail below, are believed to be used to  
18 facilitate the scheme and/or associated with the individual or individuals behind the scheme.

19 **B. Evidence Obtained from Previous Search Warrants**

20 27. The FBI executed the Search Warrants and reviewed the information and  
21 records provided by Google and Apple. All of the Google and Apple Accounts were  
22 associated with at least some information and records containing evidence of the wire-fraud  
23 and money-laundering scheme described above. Representative, non-exclusive examples of  
24 the relevant information and records obtained from the Search Warrants are set forth below.

25 28. Records stored by Google associated with Google Accounts 2 (TURYGIN),  
26 16 (Vadim Tsvetikov), 18 (Vitali Pavlov), and 22 (Tatjana Potapova) contained evidence of  
27 HASHFLARE's inability to provide cloud-mining services it sold to customers. Specifically,  
28 the accounts contained information and records evidencing HASHCOINS' and

1 HASHFLARE’s efforts to place a nominal amount of cryptocurrency mining equipment into  
2 service toward the end of HASHFLARE’s operations in 2018. This was the first instance  
3 since HASHFLARE began selling cloud-mining contracts in 2015 in which either  
4 HASHCOINS or HASHFLARE was associated with a datacenter housing its own  
5 cryptocurrency mining equipment.

6 29. Similarly, records stored by Google associated with Google Accounts  
7 2 (TURYGIN), 5 (POTAPENKO), and 22 (Tatjana Potapova), contained bank records for  
8 Connectum, Ltd., bank accounts being used by the BURFA and HASHCOINS entities to  
9 perpetuate the fraud schemes. Those records show that the Connectum bank accounts  
10 received what appear to be victim deposits from purchases of HASHFLARE cloud-mining  
11 contracts. Those Connectum bank accounts then sent large sums of funds to Cryptopay,  
12 Ltd.—a fiat-cryptocurrency exchange—with notations evidencing the purchase of  
13 cryptocurrency. The FBI’s independent analyses of the Bitcoin and Ether blockchains trace  
14 cryptocurrency from wallets held by Cryptopay to wallets held or controlled by TURYGIN,  
15 POTAPENKO, and their various entities, through elaborate peel chains<sup>4</sup>, and ultimately on  
16 to what appear to be victims’ wallets. This suggests that, as part of its Ponzi scheme,  
17 HASHFLARE converted victims’ funds deposited in its Connectum bank accounts into  
18 cryptocurrency, which it then used to pay back other victims.

19 30. The Connectum bank records obtained from some of the Google Accounts also  
20 show an interconnectedness among HASHCOINS, HASHFLARE, the BURFA Entities,  
21 DALMERON, and POLYBIUS, which all claim to be independent entities. The bank records  
22 contain millions of dollars of inter-entity transactions, suggesting that TURYGIN,  
23

---

24  
25 <sup>4</sup> A “peel chain” is a technique often used to launder large amounts of cryptocurrency by using a lengthy “chain” of  
26 smaller transactions. In a peel chain, a small portion of the overall amount to be transferred “peels” off from the main  
27 address in a relatively low-value transfer. (In this case, TURYGIN and POTAPENKO would “peel” off chunks of 10  
28 bitcoin for transfer into a larger HASHFLARE scam cluster.) The remaining balance of the larger cryptocurrency  
amount—the “change”—transfers to a new change address, and the process repeats itself until the desired larger transfer  
is complete. TURYGIN and POTAPENKO’s use of a peel chain here appears designed to prevent or disrupt victims  
from tracing payments they received from HASHFLARE back to the wallets that had received the initial victim deposits.

1 POTAPENKO, and others used the network of companies to move money and to conceal  
2 location, nature, source, ownership, and/or control of funds.

3 31. The Google Accounts searched by the FBI pursuant to the Search Warrants  
4 also contained informative records concerning the PLBT ICO. Google Accounts  
5 2 (TURGYIN), 24 (DALMERON), and 29 (POLYBIUS), for example, contained marketing  
6 e-mails that appear to have been sent to the public and which made representations about  
7 Polybius's business goals. Google Account 2 contained POLYBIUS internal business plans  
8 and records identifying potential victims of the PLBT ICO.

9 32. In Apple Account 1, which is associated with POTAPENKO, the FBI found  
10 records which appear to show that DALMERON purchased private jet flights to Greece for  
11 POTAPENKO and his family. POTAPENKO has previously asserted no connection with  
12 DALMERON, which the FBI learned from other records received tens of millions of dollars  
13 from HASHFLARE during the time period of the alleged Ponzi scheme, and which sent  
14 millions of dollars on to POLYBIUS.

15 33. In Apple Account 2, which is associated with TURYGIN, the FBI found  
16 records providing a summary of bank accounts associated with TURGYIN at the Tallinn  
17 Business Bank in Estonia. The summary helped the FBI determine whether it had a full  
18 accounting of records from that bank.

19 34. The FBI also located bank records illustrating how POTAPENKO and  
20 TURYGIN appear to be using shell companies to facilitate payments to themselves. For  
21 example, in Apple Account 2, the FBI found bank records showing a 30,000 Euro deposit  
22 into an Ecohouse Networks LP bank account from HASHCOINS, on July 24, 2015, with a  
23 notation that the payment was for "computational power leasing." On July 24, 2015, and  
24 August 11, 2015, a total of 29,000 Euros were transferred from the Ecohouse Networks LP  
25 bank account to TURYGIN, indicating TURYGIN used a shell company as a conduit for a  
26 passthrough payment to him disguised as a payment for computational power leasing.

27 35. Given that the Accounts contained evidence of the multi-stage fraud and  
28 money laundering conspiracy, including numerous bank records, I believe an updated search

1 of Accounts is likely to return additional evidence of the alleged violations under  
2 investigation by the FBI. In particular, up-to-date records may help the FBI identify how  
3 TURYGIN, POTAPENKO, and others continued to spend and move fraud proceeds from the  
4 dates of the earlier search warrants until the present. This may help the FBI identify the  
5 current location of any assets that could be returned to or otherwise used to compensate  
6 victims for their losses.

### 7 **BACKGROUND CONCERNING GOOGLE**<sup>5</sup>

8 36. Google is a United States company that offers to the public through its Google  
9 Accounts a variety of online services, including email, cloud storage, digital payments, and  
10 productivity applications, which can be accessed through a web browser or mobile  
11 applications. Google also offers to anyone, whether or not they have a Google Account, a  
12 free web browser called Google Chrome, a free search engine called Google Search, a free  
13 video streaming site called YouTube, a free mapping service called Google Maps, and a free  
14 traffic tracking service called Waze. Many of these free services offer additional  
15 functionality if the user signs into their Google Account.

16 37. In addition, Google offers an operating system (“OS”) for mobile devices,  
17 including cellular phones, known as Android. Google also sells devices, including laptops,  
18 mobile phones, tablets, smart speakers, security cameras, and wireless routers. Users of  
19 Android and Google devices are prompted to connect their device to a Google Account when  
20 they first turn on the device, and a Google Account is required for certain functionalities on  
21 these devices.

22 38. Signing up for a Google Account automatically generates an email address at  
23 the domain gmail.com. That email address will be the log-in username for access to the  
24 Google Account.

---

25  
26  
27 <sup>5</sup> The information in this section is based on information published by Google on its public websites, including, but not  
28 limited to, the following webpages: the “Google legal policy and products” page available to registered law enforcement  
at lers.google.com; product pages on support.google.com; or product pages on about.google.com.

1 39. Google advertises its services as “One Account. All of Google working for  
2 you.” Once logged into a Google Account, a user can connect to Google’s full suite of  
3 services offered to the general public, described in further detail below. In addition, Google  
4 keeps certain records indicating ownership and usage of the Google Account across services,  
5 described further after the description of services below:

- 6 a. Email. Google provides email services (called Gmail) to Google Accounts  
7 through email addresses at gmail.com or enterprise email addresses hosted by  
8 Google.
- 9 b. Contacts. Google Contacts stores contacts the user affirmatively adds to the  
10 address book, as well as contacts the user has interacted with in Google  
11 products. Google Contacts can store up to 25,000 contacts. Users can send  
12 messages to more than one contact at a time by manually creating a group  
13 within Google Contacts or communicate with an email distribution list called a  
14 Google Group. Users have the option to sync their Android mobile phone or  
15 device address book with their account so it is stored in Google Contacts.  
16 Google preserves contacts indefinitely, unless the user deletes them. Contacts  
17 can be accessed from the same browser window as other Google products like  
18 Gmail and Calendar.
- 19 c. Calendar. Google provides an appointment book for Google Accounts through  
20 Google Calendar, which can be accessed through a browser or mobile  
21 application. Users can create events or RSVP to events created by others in  
22 Google Calendar. Google Calendar can be set to generate reminder emails or  
23 alarms about events or tasks, repeat events at specified intervals, track RSVPs,  
24 and auto-schedule appointments to complete periodic goals (like running three  
25 times a week). A single Google Account can set up multiple calendars. An  
26 entire calendar can be shared with other Google Accounts by the user or made  
27 public so anyone can access it. Users have the option to sync their mobile  
28 phone or device calendar so it is stored in Google Calendar. Google preserves

1 appointments indefinitely, unless the user deletes them. Calendar can be  
2 accessed from the same browser window as other Google products like Gmail  
3 and Contacts.

4 d. Maps. Google offers a map service called Google Maps which can be searched  
5 for addresses or points of interest. Google Maps can provide users with turn-  
6 by-turn directions from one location to another using a range of transportation  
7 options (driving, biking, walking, etc.) and real-time traffic updates. Users can  
8 share their real-time location with others through Google Maps by using the  
9 Location Sharing feature. And users can find and plan an itinerary using  
10 Google Trips. A Google Account is not required to use Google Maps, but if  
11 users log into their Google Account while using Google Maps, they can save  
12 locations to their account, keep a history of their Google Maps searches, and  
13 create personalized maps using Google My Maps. Google stores Maps data  
14 indefinitely, unless the user deletes it.

15 e. Messaging. Google provides several messaging services including Duo,  
16 Messages, Hangouts, Meet, and Chat. These services enable real-time text,  
17 voice, and/or video communications through browsers and mobile applications,  
18 and also allow users to send and receive text messages, videos, photos,  
19 locations, links, and contacts. Google may retain a user's messages if the user  
20 has not disabled that feature or deleted the messages, though other factors may  
21 also impact retention.

22 f. Cloud Storage. Google Drive is a cloud storage service automatically created  
23 for each Google Account. Users can store an unlimited number of documents  
24 created by Google productivity applications like Google Docs (Google's word  
25 processor), Google Sheets (Google's spreadsheet program), Google Forms  
26 (Google's web form service), and Google Slides, (Google's presentation  
27 program). Users can also upload files to Google Drive, including photos,  
28 videos, PDFs, and text documents, until they hit the storage limit. Users can set



1 up their personal computer or mobile phone to automatically back up files to  
2 their Google Drive Account. Each user gets 15 gigabytes of space for free on  
3 servers controlled by Google and may purchase more through a subscription  
4 plan called Google One. In addition, Google Drive allows users to share their  
5 stored files and documents with up to 100 people and grant those with access  
6 the ability to edit or comment. Google maintains a record of who made  
7 changes when to documents edited in Google productivity applications.  
8 Documents shared with a user are saved in their Google Drive in a folder  
9 called "Shared with me." Google preserves files stored in Google Drive  
10 indefinitely, unless the user deletes them.

11 g. Photos. Google offers a cloud-based photo and video storage service called  
12 Google Photos. Users can share or receive photos and videos with others.  
13 Google Photos can be trained to recognize individuals, places, and objects in  
14 photos and videos and automatically tag them for easy retrieval via a search  
15 bar. Users have the option to sync their mobile phone or device photos to  
16 Google Photos. Google preserves files stored in Google Photos indefinitely,  
17 unless the user deletes them.

18 h. Web Browser. Google offers a free web browser service called Google Chrome  
19 which facilitates access to the Internet. Chrome retains a record of a user's  
20 browsing history and allows users to save favorite sites as bookmarks for easy  
21 access. If a user is logged into their Google Account on Chrome and has the  
22 appropriate settings enabled, their browsing history, bookmarks, and other  
23 browser settings may be saved to their Google Account in a record called My  
24 Activity.

25 40. Google integrates its various services to make it easier for Google Accounts to  
26 access the full Google suite of services. For example, users accessing their Google Account  
27 through their browser can toggle between Google Services via a toolbar displayed on the top  
28 of most Google service pages, including Gmail and Drive. Google Hangout, Meet, and Chat

1 | conversations pop up within the same browser window as Gmail. Attachments in Gmail are  
2 | displayed with a button that allows the user to save the attachment directly to Google Drive.  
3 | If someone shares a document with a Google Account user in Google Docs, the contact  
4 | information for that individual will be saved in the user's Google Contacts. Google Voice  
5 | voicemail transcripts and missed call notifications can be sent to a user's Gmail account.  
6 | And if a user logs into their Google Account on the Chrome browser, their subsequent  
7 | Chrome browser and Google Search activity is associated with that Google Account,  
8 | depending on user settings.

9 |       41. When individuals register with Google for a Google Account, Google asks  
10 | users to provide certain personal identifying information, including the user's full name,  
11 | telephone number, birthday, and gender. If a user is paying for services, the user must also  
12 | provide a physical address and means and source of payment.

13 |       42. Google typically retains and can provide certain transactional information  
14 | about the creation and use of each account on its system. Google captures the date on which  
15 | the account was created, the length of service, log-in times and durations, the types of  
16 | services utilized by the Google Account, the status of the account (including whether the  
17 | account is inactive or closed), the methods used to connect to the account (such as logging  
18 | into the account via Google's website or using a mobile application), details about the  
19 | devices used to access the account, and other log files that reflect usage of the account. In  
20 | addition, Google keeps records of the Internet Protocol ("IP") addresses used to register the  
21 | account and accept Google's terms of service, as well as the IP addresses associated with  
22 | particular logins to the account. Because every device that connects to the Internet must use  
23 | an IP address, IP address information can help to identify which computers or other devices  
24 | were used to access the Google Account.

25 |       43. Google maintains the communications, files, and associated records for each  
26 | service used by a Google Account on servers under its control. Even after a user deletes a  
27 | communication or file from their Google Account, it may continue to be available on  
28 | Google's servers for a certain period of time.

1           44.     In my training and experience, evidence of who was using a Google account  
2 and from where, and evidence related to criminal activity of the kind described above, may  
3 be found in the files and records described above. This evidence may establish the “who,  
4 what, why, when, where, and how” of the criminal conduct under investigation, thus  
5 enabling the United States to establish and prove each element or, alternatively, to exclude  
6 the innocent from further suspicion.

7           45.     Based on my training and experience, messages, emails, voicemails, photos,  
8 videos, documents, and internet searches are often created and used in furtherance of  
9 criminal activity, including to communicate and facilitate the offenses under investigation.  
10 Thus, stored communications and files connected to a Google Account may provide direct  
11 evidence of the offenses under investigation.

12           46.     In addition, the user’s account activity, logs, stored electronic communications,  
13 and other data retained by Google can indicate who has used or controlled the account. This  
14 “user attribution” evidence is analogous to the search for “indicia of occupancy” while  
15 executing a search warrant at a residence. For example, subscriber information, email and  
16 messaging logs, documents, and photos and videos (and the data associated with the  
17 foregoing, such as geo-location, date and time) may be evidence of who used or controlled  
18 the account at a relevant time. As an example, because every device has unique hardware  
19 and software identifiers, and because every device that connects to the Internet must use an  
20 IP address, IP address and device identifier information can help to identify which computers  
21 or other devices were used to access the account. Such information also allows investigators  
22 to understand the geographic and chronological context of access, use, and events relating to  
23 the crime under investigation.

24           47.     Account activity may also provide relevant insight into the account owner’s  
25 state of mind as it relates to the offenses under investigation. For example, information on  
26 the account may indicate the owner’s motive and intent to commit a crime (*e.g.*, information  
27 indicating a plan to commit a crime), or consciousness of guilt (*e.g.*, deleting account  
28 information in an effort to conceal evidence from law enforcement).

1 48. Other information connected to the use of a Google account may lead to the  
2 discovery of additional evidence. For example, the apps downloaded from the Google Play  
3 store may reveal services used in furtherance of the crimes under investigation, such as  
4 banking institutions used by the target or services used to communicate with co-conspirators.  
5 In addition, emails, instant messages, Internet activity, documents, and contact and calendar  
6 information can lead to the identification of co-conspirators and instrumentalities of the  
7 crimes under investigation.

8 49. Therefore, Google’s servers are likely to contain stored electronic  
9 communications and information concerning subscribers and their use of Google services. In  
10 my training and experience, such information may constitute evidence of the crimes under  
11 investigation including information that can be used to identify the account’s user or users.

12 **BACKGROUND CONCERNING APPLE**<sup>6</sup>

13 50. Apple is a United States company that produces the iPhone, iPad, and iPod  
14 Touch, all of which use the iOS operating system, and desktop and laptop computers based  
15 on the Mac OS operating system.

16 51. Apple provides a variety of services that can be accessed from Apple devices  
17 or, in some cases, other devices via web browsers or mobile and desktop applications  
18 (“apps”). As described in further detail below, the services include email, instant messaging,  
19 and file storage:

- 20 a. Apple provides email service to its users through email addresses at the domain  
21 names mac.com, me.com, and icloud.com.

22  
23  
24  
25 <sup>6</sup> The information in this section is based on information published by Apple on its website, including, but not limited to,  
26 the following document and webpages: “U.S. Law Enforcement Legal Process Guidelines,” available at  
27 <https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf>; “Create and start using an Apple ID,” available  
28 at <https://support.apple.com/en-us/HT203993>; “iCloud,” available at <http://www.apple.com/icloud/>; “What does iCloud  
back up?,” available at <https://support.apple.com/kb/PH12519>; “iOS Security,” available at  
[https://www.apple.com/business/docs/iOS\\_Security\\_Guide.pdf](https://www.apple.com/business/docs/iOS_Security_Guide.pdf), and “iCloud: How Can I Use iCloud?,” available at  
<https://support.apple.com/kb/PH26502>.

- 1       b. iMessage and FaceTime allow users of Apple devices to communicate in real-  
2       time. iMessage enables users of Apple devices to exchange instant messages  
3       ("iMessages") containing text, photos, videos, locations, and contacts, while  
4       FaceTime enables those users to conduct audio and video calls.
- 5       c. iCloud is a cloud storage and cloud computing service from Apple that allows  
6       its users to interact with Apple's servers to utilize iCloud-connected services to  
7       create, store, access, share, and synchronize data on Apple devices or via  
8       icloud.com on any Internet-connected device. For example, iCloud Mail  
9       enables a user to access Apple-provided email accounts on multiple Apple  
10      devices and on iCloud.com. iCloud Photo Library and My Photo Stream can be  
11      used to store and manage images and videos taken from Apple devices, and  
12      iCloud Photo Sharing allows the user to share those images and videos with  
13      other Apple subscribers. iCloud Drive can be used to store presentations,  
14      spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud  
15      to be used to synchronize bookmarks and webpages opened in the Safari web  
16      browsers on all of the user's Apple devices. iCloud Backup allows users to  
17      create a backup of their device data. iWork Apps, a suite of productivity apps  
18      (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create,  
19      store, and share documents, spreadsheets, and presentations. iCloud Keychain  
20      enables a user to keep website username and passwords, credit card  
21      information, and Wi-Fi network information synchronized across multiple  
22      Apple devices.
- 23      d. Game Center, Apple's social gaming network, allows users of Apple devices to  
24      play and share games with each other.
- 25      e. Find My iPhone allows owners of Apple devices to remotely identify and track  
26      the location of, display a message on, and wipe the contents of those devices.  
27      Find My Friends allows owners of Apple devices to share locations.
- 28

- 1 f. Location Services allows apps and websites to use information from cellular,  
2 Wi-Fi, Global Positioning System (“GPS”) networks, and Bluetooth, to  
3 determine a user’s approximate location.
- 4 g. App Store and iTunes Store are used to purchase and download digital content.  
5 iOS apps can be purchased and downloaded through App Store on iOS  
6 devices, or through iTunes Store on desktop and laptop computers running  
7 either Microsoft Windows or Mac OS. Additional digital content, including  
8 music, movies, and television shows, can be purchased through iTunes Store  
9 on iOS devices and on desktop and laptop computers running either Microsoft  
10 Windows or Mac OS.

11 52. Apple services are accessed through the use of an “Apple ID,” an account  
12 created during the setup of an Apple device or through the iTunes or iCloud services. The  
13 account identifier for an Apple ID is an email address, provided by the user. Users can  
14 submit an Apple-provided email address (often ending in @icloud.com, @me.com, or  
15 @mac.com) or an email address associated with a third-party email provider (such as Gmail,  
16 Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including  
17 iCloud, iMessage, and FaceTime) only after the user accesses and responds to a “verification  
18 email” sent by Apple to that “primary” email address. Additional email addresses  
19 (“alternate,” “rescue,” and “notification” email addresses) can also be associated with an  
20 Apple ID by the user. A single Apple ID can be linked to multiple Apple services and  
21 devices, serving as a central authentication and syncing mechanism.

22 53. Apple captures information associated with the creation and use of an Apple  
23 ID. During the creation of an Apple ID, the user must provide basic personal information  
24 including the user’s full name, physical address, and telephone numbers. The user may also  
25 provide means of payment for products offered by Apple. The subscriber information and  
26 password associated with an Apple ID can be changed by the user through the “My Apple  
27 ID” and “iForgot” pages on Apple’s website. In addition, Apple captures the date on which  
28 the account was created, the length of service, records of log-in times and durations, the

1 types of service utilized, the status of the account (including whether the account is inactive  
2 or closed), the methods used to connect to and utilize the account, the Internet Protocol  
3 address (“IP address”) used to register and access the account, and other log files that reflect  
4 usage of the account.

5 54. Additional information is captured by Apple in connection with the use of an  
6 Apple ID to access certain services. For example, Apple maintains connection logs with IP  
7 addresses that reflect a user’s sign-on activity for Apple services such as iTunes Store and  
8 App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple’s  
9 website. Apple also maintains records reflecting a user’s app purchases from App Store and  
10 iTunes Store, “call invitation logs” for FaceTime calls, “query logs” for iMessage, and “mail  
11 logs” for activity over an Apple-provided email account. Records relating to the use of the  
12 Find My iPhone service, including connection logs and requests to remotely lock or erase a  
13 device, are also maintained by Apple.

14 55. Apple also maintains information about the devices associated with an Apple  
15 ID. When a user activates or upgrades an iOS device, Apple captures and retains the user’s  
16 IP address and identifiers such as the Integrated Circuit Card ID number (“ICCID”), which is  
17 the serial number of the device’s SIM card. Similarly, the telephone number of a user’s  
18 iPhone is linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also  
19 may maintain records of other device identifiers, including the Media Access Control  
20 address (“MAC address”), the unique device identifier (“UDID”), and the serial number. In  
21 addition, information about a user’s computer is captured when iTunes is used on that  
22 computer to play content associated with an Apple ID, and information about a user’s web  
23 browser may be captured when used to access services through icloud.com and apple.com.  
24 Apple also retains records related to communications between users and Apple customer  
25 service, including communications regarding a particular Apple device or service, and the  
26 repair history for a device.

27 56. Apple provides users with five gigabytes of free electronic space on iCloud,  
28 and users can purchase additional storage space. That storage space, located on servers

1 controlled by Apple, may contain data associated with the use of iCloud-connected services,  
2 including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream,  
3 and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork  
4 and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs  
5 and iCloud Keychain). iCloud can also be used to store iOS device backups, which can  
6 contain a user's photos and videos, iMessages, Short Message Service ("SMS") and  
7 Multimedia Messaging Service ("MMS") messages, voicemail messages, call history,  
8 contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and  
9 other data. Records and data associated with third-party apps may also be stored on iCloud;  
10 for example, the iOS app for WhatsApp, an instant messaging service, can be configured to  
11 regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on  
12 Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

13 57. In my training and experience, evidence of who was using an Apple ID and  
14 from where, and evidence related to criminal activity of the kind described above, may be  
15 found in the files and records described above. This evidence may establish the "who, what,  
16 why, when, where, and how" of the criminal conduct under investigation, thus enabling the  
17 United States to establish and prove each element or, alternatively, to exclude the innocent  
18 from further suspicion.

19 58. For example, the stored communications and files connected to an Apple ID  
20 may provide direct evidence of the offenses under investigation. Based on my training and  
21 experience, instant messages, emails, voicemails, photos, videos, and documents are often  
22 created and used in furtherance of criminal activity, including to communicate and facilitate  
23 the offenses under investigation.

24 59. In addition, the user's account activity, logs, stored electronic communications,  
25 and other data retained by Apple can indicate who has used or controlled the account. This  
26 "user attribution" evidence is analogous to the search for "indicia of occupancy" while  
27 executing a search warrant at a residence. For example, subscriber information, email and  
28 messaging logs, documents, and photos and videos (and the data associated with the



1 foregoing, such as geo-location, date and time) may be evidence of who used or controlled  
2 the account at a relevant time. As an example, because every device has unique hardware  
3 and software identifiers, and because every device that connects to the Internet must use an  
4 IP address, IP address and device identifier information can help to identify which computers  
5 or other devices were used to access the account. Such information also allows investigators  
6 to understand the geographic and chronological context of access, use, and events relating to  
7 the crime under investigation.

8         60. Account activity may also provide relevant insight into the account owner's  
9 state of mind as it relates to the offenses under investigation. For example, information on  
10 the account may indicate the owner's motive and intent to commit a crime (e.g., information  
11 indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account  
12 information in an effort to conceal evidence from law enforcement).

13         61. Other information connected to an Apple ID may lead to the discovery of  
14 additional evidence. For example, the identification of apps downloaded from App Store and  
15 iTunes Store may reveal services used in furtherance of the crimes under investigation, such  
16 as banking institutions used to commit money laundering, or services used to communicate  
17 with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and  
18 contact and calendar information can lead to the identification of co-conspirators and  
19 instrumentalities of the crimes under investigation.

20         62. Apple's servers are likely to contain stored electronic communications and  
21 information concerning subscribers and their use of Apple's services. In my training and  
22 experience, such information may constitute evidence of the crimes under investigation  
23 including information that can be used to identify the account's user or users.

24  
25 //

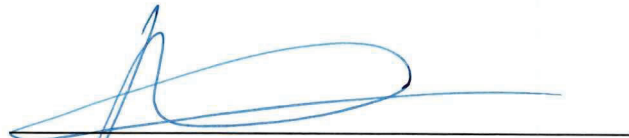
26 //

27 //

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

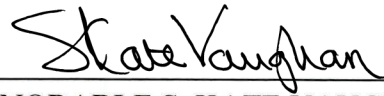
**CONCLUSION**

63. Based on the forgoing, I respectfully request that the Court issue the proposed search warrant. Accordingly, by this Affidavit and Warrant, I seek authority for the government to search all of the items specified in Section I of Attachments B (attached hereto and incorporated by reference herein) to the Warrant, and specifically to seize all of the data, documents, and records that are identified in Sections II to the same Attachments.



ANDREW CROPCHO, Affiant  
Special Agent, Federal Bureau of Investigation

The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit on the 1st day of April, 2022.



THE HONORABLE S. KATE VAUGHAN  
United States Magistrate Judge

**ATTACHMENT A-1****Accounts to be Searched**

This warrant applies to information associated with the following accounts (“the Google Accounts”) that is stored at premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043:

- ivan@hashcoins.com (**GOOGLE ACCOUNT 1**);
- ivan@burfa.com (**GOOGLE ACCOUNT 2**);
- ivan.turygin@polybius.io (**GOOGLE ACCOUNT 3**);
- turygin@gmail.com (**GOOGLE ACCOUNT 4**);
- sergei@hashcoins.com (**GOOGLE ACCOUNT 5**);
- sergei@burfa.com (**GOOGLE ACCOUNT 6**);
- sergei.potapenko@polybius.io (**GOOGLE ACCOUNT 7**);
- sergei.potapenko@gmail.com (**GOOGLE ACCOUNT 8**);
- nikolay@hashcoins.com (**GOOGLE ACCOUNT 9**);
- nikolay.pavlovskiy@burfa.com (**GOOGLE ACCOUNT 10**);
- pavel@hashcoins.com (**GOOGLE ACCOUNT 11**);
- pavel.tsihhotski@burfa.com (**GOOGLE ACCOUNT 12**);
- pavel.tsihhotski@polybius.io (**GOOGLE ACCOUNT 13**);
- stanislav.pavlov@hashcoins.com (**GOOGLE ACCOUNT 14**);
- stanislav.pavlov@burfa.com (**GOOGLE ACCOUNT 15**);
- vadim.tsvetikov@hashcoins.com (**GOOGLE ACCOUNT 16**);
- vadim.tsvetikov@burfa.com (**GOOGLE ACCOUNT 17**);
- vitali@hashcoins.com (**GOOGLE ACCOUNT 18**);
- vitali@burfa.com (**GOOGLE ACCOUNT 19**);
- anton.altement@polybius.io (**GOOGLE ACCOUNT 20**);
- edgar.bers@polybius.io (**GOOGLE ACCOUNT 21**);
- tatjana@burfa.com (**GOOGLE ACCOUNT 22**);

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

- margarita.burunova@hashcoins.com (**GOOGLE ACCOUNT 23**);
- dalmeronprojects@gmail.com (**GOOGLE ACCOUNT 24**);
- ecohousenetworks@gmail.com (**GOOGLE ACCOUNT 25**);
- admin@hashcoins.com (**GOOGLE ACCOUNT 26**);
- info@hashcoins.com (**GOOGLE ACCOUNT 27**);
- info@burfa.com (**GOOGLE ACCOUNT 28**);
- info@polybius.io (**GOOGLE ACCOUNT 29**);
- invoices@hashcoins.com (**GOOGLE ACCOUNT 30**);
- invoices@burfa.com (**GOOGLE ACCOUNT 31**);
- microsoft@hashcoins.com (**GOOGLE ACCOUNT 32**);
- cb@hashcoins.com (**GOOGLE ACCOUNT 33**);
- licenses@hashcoins.com (**GOOGLE ACCOUNT 34**);
- alerts.mining@burfa.com (**GOOGLE ACCOUNT 35**); and
- support@polybius.io (**GOOGLE ACCOUNT 36**).

**ATTACHMENT B-1**

**Particular Things to be Seized**

**I. Information to be disclosed by Google, LLC:**

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Google, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Google is required to disclose to the government for each account or identifier listed in Attachment A-1 the following information from April 4, 2020, through the present, unless otherwise indicated:

- a. All business records and subscriber information, in any form kept, pertaining to the Account, including:
  1. Names (including subscriber names, user names, and screen names);
  2. Addresses (including mailing addresses, residential addresses, business addresses, and email addresses, including alternate and recovery email addresses);
  3. Telephone numbers, including SMS recovery and alternate sign-in numbers;
  4. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol (“IP”) addresses) associated with those sessions, including log-in IP addresses;
  5. Telephone or instrument numbers or other subscriber numbers or identities, including any temporarily assigned network address, SMS recovery numbers, Google Voice numbers, and alternate sign-in numbers
  6. Length of service (including start date and creation IP) and types of service utilized;

- 1           7.     Means and source of payment (including any credit card or bank  
2                     account number); and  
3           8.     Change history.
- 4       b.     All device information associated with the Account, including but not limited  
5             to, manufacture names, model numbers, serial number, media access control  
6             (MAC) addresses, international mobile equipment identifier (IMEI) numbers,  
7             FCC ID numbers, Android IDs, and telephone numbers;
- 8       c.     Records of user activity for each connection made to or from the Account(s),  
9             including, for all Google services, the date, time, length, and method of  
10            connection, data transfer volume, user names, source and destination IP  
11            address, name of accessed Google service, and all activity logs
- 12       d.     The contents of all emails associated with the account, including stored or  
13             preserved copies of emails sent to and from the account, draft emails, and  
14             deleted emails; attachments; the source and destination addresses associated  
15             with each email; the size, length, and timestamp of each email; and true and  
16             accurate header information including the actual IP addresses of the sender and  
17             recipients of the emails;
- 18       e.     Any records pertaining to the user's contacts, including: address books; contact  
19             lists; social network links; groups, including Google Groups to which the user  
20             belongs or communicates with; user settings; and all associated logs and  
21             change history;
- 22       f.     Any records pertaining to the user's calendar(s), including: Google Calendar  
23             events; Google Tasks; reminders; appointments; invites; and goals; the sender  
24             and recipients of any event invitation, reminder, appointment, or task; user  
25             settings; and all associated logs and change history;
- 26       g.     The contents of all text, audio, and video messages associated with the  
27             account, including Chat, Duo, Hangouts, Meet, and Messages (including SMS,  
28             MMS, and RCS), in any format and however initially transmitted, including,

1 but not limited to: stored, deleted, and draft messages, including attachments  
2 and links; the source and destination addresses associated with each  
3 communication, including IP addresses; the size, length, and timestamp of each  
4 communication; user settings; and all associated logs, including access logs  
5 and change history;

- 6 h. The contents of all media associated with the account in Google Photos,  
7 including: photos, GIFs, videos, animations, collages, icons, or other data  
8 uploaded, created, stored, or shared with the account, including drafts and  
9 deleted records; accounts with access to or which previously accessed each  
10 record; any location, device, or third-party application data associated with  
11 each record; and all associated logs of each record, including the creation and  
12 change history, access logs, and IP addresses.
- 13 i. All maps data associated with the account, including Google Maps and Google  
14 Trips, including: all saved, starred, and privately labeled locations; search  
15 history; routes begun; routes completed; mode of transit used for directions;  
16 My Maps data; accounts and identifiers receiving or sending Location Sharing  
17 information to the account; changes and edits to public places; and all  
18 associated logs, including IP addresses, location data, and timestamps, and  
19 change history.
- 20 j. All Location History and Web & App Activity indicating the location at which  
21 the account was active, including the source of the data, date and time, latitude  
22 and longitude, estimated accuracy, device and platform, inferences drawn from  
23 sensor data (such as whether a user was at rest, walking, biking, or in a car),  
24 and associated logs and user settings, including Timeline access logs and  
25 change and deletion history; and
- 26 k. All Internet search and browsing history, and application usage history,  
27 including Web & App Activity, Voice & Audio History, Google Assistant, and  
28 Google Home, including: search queries and clicks, including transcribed or

1 recorded voice queries and Google Assistant responses; browsing history,  
2 including application usage; bookmarks; passwords; autofill information;  
3 alerts, subscriptions, and other automated searches, including associated  
4 notifications and creation dates; user settings; and all associated logs and  
5 change history.

6 Google is hereby ordered to disclose the above information to the government within 14 days  
7 of issuance of this warrant.

8 **II. Information to be seized by the government**

9 All information described above in Section I that constitutes fruits, contraband,  
10 evidence, and instrumentalities of violations of Title 18, United States Code, Section 1343  
11 (Wire Fraud) and Title 18, United States Code, Section 1956, and occurring after April 2015,  
12 for each of the Accounts listed on Attachment A, pertaining to the following matters:

13 a. Items, records, or information related to the operation of a  
14 cryptocurrency cloud mining Ponzi scheme;

15 b. Items, records, or information related to cryptocurrency mining, the  
16 advertisement, manufacture and sale of mining equipment, or the advertisement and sale of  
17 cloud mining contracts;

18 c. Items, records, or information related to the termination of mining  
19 contracts and the profitability of cloud mining;

20 d. Items, records, or information related to purchases of cloud mining  
21 equipment, including communications with the companies Jeltan Trading, Dalmeron  
22 Projects, Dalmeron Invest, Keleta UAB, Bitmain, Bitfury, and Inno3d;

23 e. Items, records, or information related to the transfer, purchase, sale, or  
24 disposition of cryptocurrency;

25 f. Items, records, or information related to communications with  
26 HASHFLARE or HASHCOINS investors, including complaints by investors or requests for  
27 return of funds;



1 g. Items, records, or information related to the advertisement of  
2 HASHFLARE or HASHCOINS' services;

3 h. Items, records, or information related to the owners, operators,  
4 employees, locations, assets, and business purpose of the companies HASHCOINS OU,  
5 HASHCOINS TRADE OU, HASHCOINS LP, HASHFLARE LP, Burfa Capital OU, Burfa  
6 Media OU, Burfa Real Estate OU, Burfa Tech OU, Burfa Trade OU, Burfa Invest OU,  
7 Polybius Foundation OU, Polybius Tech OU, Polybius Ventures OU, Polybius Fintech  
8 MidCo OU, Dalmeron Projects LP, Jeltan Trading, Dalmeron Invest, Keleta UAB, and  
9 OSOM Finance (collectively, the "SUBJECT ENTITIES");

10 i. Items, records, or information related to the use, creation, or operation  
11 of the "SUBJECT ENTITIES," including business plans and strategies, and the anticipated  
12 success, failure, or general validity thereof;

13 j. Items, records, or information related to the operation of hashflare.io,  
14 burfa.com, polybius.io, dalmeron.com, or hashcoins.com;

15 k. Items, records, or information concerning financial transactions  
16 associated with the operation of the SUBJECT ENTITIES, including bank accounts held by  
17 the SUBJECT ENTITIES, transfers of funds by the SUBJECT ENTITIES, expenditures of  
18 money or wealth, bank statements and other financial statements, and cryptocurrency  
19 holdings;

20 l. Items, records, or information related to cryptocurrency mining groups,  
21 cryptocurrency public keys or addresses, cryptocurrency private keys, representations of  
22 cryptocurrency wallets or their constitutive parts, to include "recovery seeds" and "root  
23 keys," which may be used to regenerate a wallet.

24 m. Items, records, or information related to the salaries or earnings of  
25 individuals employed by the SUBJECT ENTITIES.

26 n. Items, records, or information related to the payment or calculation of  
27 recruitment bonuses paid to HASHFLARE and HASHCOINS investors.  
28

1 o. Items, records, or information related to receipt of investor money,  
2 including the amount, purpose of the investment, and plans for spending that money.

3 p. Evidence indicating how and when the account was accessed or used, to  
4 determine the geographic and chronological context of account access, use, and events  
5 relating to the crime under investigation and to the email account owner.

6 q. Evidence indicating the account owner's state of mind as it relates to the  
7 crime under investigation.

8 r. The identity of the person(s) who created or used the user ID, including  
9 records that help reveal the whereabouts of such person(s).

10  
11 This warrant authorizes a review of electronically stored information, communications, other  
12 records and information disclosed pursuant to this warrant in order to locate evidence, fruits,  
13 and instrumentalities described in this warrant. The review of this electronic data may be  
14 conducted by any government personnel assisting in the investigation, who may include, in  
15 addition to law enforcement officers and agents, attorneys for the government, attorney  
16 support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete  
17 copy of the disclosed electronic data to the custody and control of attorneys for the  
18 government and their support staff for their independent review.

**ATTACHMENT A-2**

This warrant applies to information associated with the following accounts (collectively, the “Apple Accounts”) that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at One Apple Park Way, Cupertino, California:

- Sergei.potapenko@gmail.com (DSID 624556209) (“**APPLE ACCOUNT 1**”) (believed to be used by SERGEI POTAPENKO); and
- Turygin@gmail.com (DSID 1931852295) (“**APPLE ACCOUNT 2**”) (believed to be used by IVAN TURYGIN).

**ATTACHMENT B-2**

**I. Information to be disclosed by Apple Inc. (“Apple”)**

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Apple, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose for each account or identifier listed in Attachment A-2 the following information from March 12, 2021, through the present, unless otherwise indicated:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents of all emails associated with the account from March 22, 2021, through the present, including stored or preserved copies of emails sent to and from the

1 account (including all draft emails and deleted emails), the source and destination addresses  
2 associated with each email, the date and time at which each email was sent, the size and  
3 length of each email, and the true and accurate header information including the actual IP  
4 addresses of the sender and the recipient of the emails, and all attachments;

5 d. The contents of all instant messages associated with the account from March  
6 22, 2021, through the present, including stored or preserved copies of instant messages  
7 (including iMessages, SMS messages, and MMS messages) sent to and from the account  
8 (including all draft and deleted messages), the source and destination account or phone  
9 number associated with each instant message, the date and time at which each instant  
10 message was sent, the size and length of each instant message, the actual IP addresses of the  
11 sender and the recipient of each instant message, and the media, if any, attached to each  
12 instant message;

13 e. The contents of all files and other records stored on iCloud, including all iOS  
14 device backups, all Apple and third-party app data, all files and other records related to  
15 iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive,  
16 iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and  
17 iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar  
18 entries, images, videos, voicemails, device settings, and bookmarks;

19 f. All activity, connection, and transactional logs for the account (with associated  
20 IP addresses including source port numbers), including FaceTime call invitation logs,  
21 messaging and query logs (including iMessage, SMS, and MMS messages), mail logs,  
22 iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates  
23 of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple  
24 services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with  
25 web-based access of Apple services (including all associated identifiers), and logs associated  
26 with iOS device purchase, activation, and upgrades;

1 g. All records and information regarding locations where the account or devices  
2 associated with the account were accessed, including all data stored in connection with  
3 Location Services, Find My iPhone, Find My Friends, and Apple Maps;

4 h. All records pertaining to the types of service used;

5 i. All records pertaining to communications between Apple and any person  
6 regarding the account, including contacts with support services and records of actions taken;  
7 and

8 j. All files, keys, or other information necessary to decrypt any data produced in  
9 an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and  
10 fileinfolist.txt files).

11 Apple is hereby ordered to disclose the above information to the government within 14 days  
12 of issuance of this warrant.

13 **II. Information to be seized by the government**

14 All information described above in Section I that constitutes fruits, contraband,  
15 evidence, and instrumentalities of violations of Title 18, United States Code, Section 1343  
16 (Wire Fraud) and Title 18, United States Code, Section 1956, and occurring after April 2015,  
17 for each of the Accounts listed on Attachment A, pertaining to the following matters:

18 a. Items, records, or information related to the operation of a  
19 cryptocurrency cloud mining Ponzi scheme;

20 b. Items, records, or information related to cryptocurrency mining, the  
21 advertisement, manufacture and sale of mining equipment, or the advertisement and sale of  
22 cloud mining contracts;

23 c. Items, records, or information related to the termination of mining  
24 contracts and the profitability of cloud mining;

25 d. Items, records, or information related to purchases of cloud mining  
26 equipment, including communications with the companies Jeltan Trading, Dalmeron  
27 Projects, Dalmeron Invest, Keleta UAB, Bitmain, Bitfury, and Inno3d;

1 e. Items, records, or information related to the transfer, purchase, sale, or  
2 disposition of cryptocurrency;

3 f. Items, records, or information related to communications with  
4 HASHFLARE or HASHCOINS investors, including complaints by investors or requests for  
5 return of funds;

6 g. Items, records, or information related to the advertisement of  
7 HASHFLARE or HASHCOINS' services;

8 h. Items, records, or information related to the owners, operators,  
9 employees, locations, assets, and business purpose of the companies HASHCOINS OU,  
10 HASHCOINS TRADE OU, HASHCOINS LP, HASHFLARE LP, Burfa Capital OU, Burfa  
11 Media OU, Burfa Real Estate OU, Burfa Tech OU, Burfa Trade OU, Burfa Invest OU,  
12 Polybius Foundation OU, Polybius Tech OU, Polybius Ventures OU, Polybius Fintech  
13 MidCo OU, Dalmeron Projects LP, Jeltan Trading, Dalmeron Invest, Keleta UAB, and  
14 OSOM Finance (collectively, the "SUBJECT ENTITIES");

15 i. Items, records, or information related to the use, creation, or operation  
16 of the "SUBJECT ENTITIES," including business plans and strategies, and the anticipated  
17 success, failure, or general validity thereof;

18 j. Items, records, or information related to the operation of hashflare.io,  
19 burfa.com, polybius.io, dalmeron.com, or hashcoins.com;

20 k. Items, records, or information concerning financial transactions  
21 associated with the operation of the SUBJECT ENTITIES, including bank accounts held by  
22 the SUBJECT ENTITIES, transfers of funds by the SUBJECT ENTITIES, expenditures of  
23 money or wealth, bank statements and other financial statements, and cryptocurrency  
24 holdings;

25 l. Items, records, or information related to cryptocurrency mining groups,  
26 cryptocurrency public keys or addresses, cryptocurrency private keys, representations of  
27 cryptocurrency wallets or their constitutive parts, to include "recovery seeds" and "root  
28 keys," which may be used to regenerate a wallet.

1 m. Items, records, or information related to the salaries or earnings of  
2 individuals employed by the SUBJECT ENTITIES.

3 n. Items, records, or information related to the payment or calculation of  
4 recruitment bonuses paid to HASHFLARE and HASHCOINS investors.

5 o. Items, records, or information related to receipt of investor money,  
6 including the amount, purpose of the investment, and plans for spending that money.

7 p. Evidence indicating how and when the account was accessed or used, to  
8 determine the geographic and chronological context of account access, use, and events  
9 relating to the crime under investigation and to the email account owner.

10 q. Evidence indicating the account owner's state of mind as it relates to the  
11 crime under investigation.

12 r. The identity of the person(s) who created or used the user ID, including  
13 records that help reveal the whereabouts of such person(s).

14  
15 This warrant authorizes a review of electronically stored information, communications, other  
16 records and information disclosed pursuant to this warrant in order to locate evidence, fruits,  
17 and instrumentalities described in this warrant. The review of this electronic data may be  
18 conducted by any government personnel assisting in the investigation, who may include, in  
19 addition to law enforcement officers and agents, attorneys for the government, attorney  
20 support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete  
21 copy of the disclosed electronic data to the custody and control of attorneys for the  
22 government and their support staff for their independent review.



**APPENDIX 1**

**Affidavit in Support of Search Warrant MJ20-153**

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**AFFIDAVIT**

1  
2  
3 STATE OF WASHINGTON )  
4 ) ss  
5 COUNTY OF KING )

6 I, Andrew Cropcho, being duly sworn, hereby depose and state as follows:

7 **INTRODUCTION AND AGENT BACKGROUND**

8 1. I am a Special Agent with the Federal Bureau of Investigation (“FBI”) and  
9 have been since May of 2018. I am currently assigned to the Seattle Field Office. My  
10 primary duties include investigating violations of Federal law, including corporate fraud,  
11 securities fraud, government program fraud, and healthcare fraud. Part of those duties  
12 include investigating instances of wire fraud being used for financial gain at the expense of  
13 others. Before my career as an FBI Special Agent I was employed as a Certified Public  
14 Accountant for over three years and, as part of my employment, I examined financial  
15 information of clients to determine their accuracy, reliability, and sources.

16 2. The facts set forth in this Affidavit are based on my own personal knowledge;  
17 knowledge obtained from other individuals during my participation in this investigation,  
18 including other law enforcement personnel; review of documents and records related to this  
19 investigation; communications with others who have personal knowledge of the events and  
20 circumstances described herein including, but not limited to, the victims in this investigation;  
21 and information gained through my training and experience. Because this Affidavit is  
22 submitted for the limited purpose of establishing probable cause in support of the application  
23 for a search warrant, it does not set forth each and every fact that I or others have learned  
24 during the course of this investigation.

25 **PURPOSE OF AFFIDAVIT**

26 3. I make this affidavit in support of an application for a search warrant for  
27 information associated with certain accounts that are stored at premises controlled by Google  
28 LLC (“**Google**”), located at 1600 Amphitheater Parkway in Mountain View. The

1 information to be searched is described in the following paragraphs and in Attachment A,  
2 which is incorporated herein.

3 4. This affidavit is made in support of an application for a search warrant  
4 pursuant to Title 18, United States Code, Sections 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A)  
5 to require **Google** to disclose to the government copies of the information, including the  
6 content of communications, further described in Section I of Attachment B, pertaining to the  
7 following accounts:

- 8 ivan@hashcoins.com (SUBJECT ACCOUNT 1)
- 9 ivan@burfa.com (SUBJECT ACCOUNT 2)
- 10 ivan.turygin@polybius.io (SUBJECT ACCOUNT 3)
- 11 turygin@gmail.com (SUBJECT ACCOUNT 4)
- 12 scrgei@hashcoins.com (SUBJECT ACCOUNT 5)
- 13 sergei@burfa.com (SUBJECT ACCOUNT 6)
- 14 sergei.potapenko@polybius.io (SUBJECT ACCOUNT 7)
- 15 sergei.potapenko@gmail.com (SUBJECT ACCOUNT 8)
- 16 nikolay@hashcoins.com (SUBJECT ACCOUNT 9)
- 17 nikolay.pavlovskiy@burfa.com (SUBJECT ACCOUNT 10)
- 18 pavel@hashcoins.com (SUBJECT ACCOUNT 11)
- 19 pavel.tsihhotski@burfa.com (SUBJECT ACCOUNT 12)
- 20 pavel.tsihhotski@polybius.io (SUBJECT ACCOUNT 13)
- 21 stanislav.pavlov@hashcoins.com (SUBJECT ACCOUNT 14)
- 22 stanislav.pavlov@burfa.com (SUBJECT ACCOUNT 15)
- 23 vadim.tsvetikov@hashcoins.com (SUBJECT ACCOUNT 16)
- 24 vadim.tsvetikov@burfa.com (SUBJECT ACCOUNT 17)
- 25 vitali@hashcoins.com (SUBJECT ACCOUNT 18)
- 26 vitali@burfa.com (SUBJECT ACCOUNT 19)
- 27 vitali.pavlov@polybius.io (SUBJECT ACCOUNT 20)
- 28 anton.altement@polybius.io (SUBJECT ACCOUNT 21)
- edger.bers@burfa.com (SUBJECT ACCOUNT 22)

1 | edgar.bers@polybius.io (SUBJECT ACCOUNT 23)  
2 | tatjana@burfa.com (SUBJECT ACCOUNT 24)  
3 | margarita.burunova@hashcoins.com (SUBJECT ACCOUNT 25)  
4 | dalmeronprojects@gmail.com (SUBJECT ACCOUNT 26)  
5 | ecohousenetworks@gmail.com (SUBJECT ACCOUNT 27)  
6 | admin@hashcoins.com (SUBJECT ACCOUNT 28)  
7 | admin@burfa.com (SUBJECT ACCOUNT 29)  
8 | info@hashcoins.com (SUBJECT ACCOUNT 30)  
9 | info@burfa.com (SUBJECT ACCOUNT 31)  
10 | info@polybius.io (SUBJECT ACCOUNT 32)  
11 | invoices@hashcoins.com (SUBJECT ACCOUNT 33)  
12 | invoices@burfa.com (SUBJECT ACCOUNT 34)  
13 | azure@hashcoins.com (SUBJECT ACCOUNT 35)  
14 | microsoft@hashcoins.com (SUBJECT ACCOUNT 36)  
15 | cb@hashcoins.com (SUBJECT ACCOUNT 37)  
16 | licenses@hashcoins.com (SUBJECT ACCOUNT 38)  
17 | alerts.mining@burfa.com (SUBJECT ACCOUNT 39)  
18 | support@polybius.io (SUBJECT ACCOUNT 40)

19 | 5. (hereinafter, collectively the “SUBJECT ACCOUNTS”). Upon receipt of the  
20 | information described in Section I of Attachment B, government-authorized persons will  
21 | review that information to locate the items described in Section II of Attachment B. This  
22 | warrant is requested in connection with an on-going investigation in this district by the FBI.

23 | 6. Based on my training and experience, and the facts as set forth in this affidavit,  
24 | there is probable cause to believe that violations of Title 18, United States Code, Section  
25 | 1343 (Wire Fraud) have been committed by IVAN TURYGIN and SERGEI POTAPENKO,  
26 | individually, and by and through the use of their companies HASHCOINS OU (hereinafter  
27 | “HASHCOINS”), HASHCOINS TRADE OU, HASHCOINS LP, HASHFLARE LP  
28 | (hereinafter “HASHFLARE”), Burfa Capital OU, Burfa Media OU, Burfa Real Estate OU,

1 | Burfa Tech OU, Burfa Trade OU, Burfa Invest OU (collectively, the “BURFA Entities”),  
2 | Polybius Foundation OU, Polybius Tech OU, Polybius Ventures OU, Polybius Fintech  
3 | MidCo OU (collectively, “POLYBIUS”), Dalmeron Projects LP, and Ecohouse Networks  
4 | LP, along with identified key employees of the same companies. There is also probable  
5 | cause to search the information described in Attachment A, for evidence, instrumentalities,  
6 | or contraband of these crimes, as described in Attachment B.

7 | **JURISDICTION**

8 | 7. This Court has jurisdiction to issue the requested warrant because it is “a court  
9 | of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A)  
10 | & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has  
11 | jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

12 | 8. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is  
13 | not required for the service or execution of this warrant.

14 | 9. This warrant application is to be presented electronically pursuant to Local  
15 | Criminal Rule CrR 41(d)(3).

16 | **BACKGROUND ON VIRTUAL CURRENCY AND MINING**

17 | 10. Virtual currency (also known as cryptocurrency) is an asset that can be  
18 | exchanged directly person to person, through a virtual currency exchange, or through other  
19 | intermediaries. It can be used to buy goods and services, exchanged for “fiat currency”  
20 | (currency established by government regulation or law) or other virtual currency, or held as  
21 | an investment, among other applications.

22 | 11. Virtual currency is generally not issued by any government or bank. Rather, it  
23 | is frequently generated and controlled through software operating on a decentralized, peer-  
24 | to-peer (“P2P”) network of computers across the world (some types of virtual currency,  
25 | however, are generated and controlled through software operating on a centralized network  
26 | of computers across the world).

1 12. There are thousands of virtual currencies in use, including Bitcoin, Ethereum,  
2 Bitcoin Cash, and Monero. Bitcoin,<sup>1</sup> the most popular form of virtual currency, can be  
3 generated through mining. According to Bitcoin.org, “Bitcoin mining is the process of  
4 making computer hardware do mathematical calculations for the Bitcoin network to confirm  
5 transactions and increase security. As a reward for their services, Bitcoin miners can collect  
6 transaction fees for the transactions they confirm, along with newly created bitcoins.”

7 13. Bitcoin mining can be conducted locally on a user’s computer or other  
8 computer hardware, or can be conducted on another’s system via the cloud. According to the  
9 Santa Clara Law School High Technology Journal: “Cloud mining is an economic  
10 arrangement whereby a person pays another person or entity to engage in cryptocurrency  
11 mining on their behalf and receives the transaction fees, cryptocurrency or a portion thereof  
12 that is generated from such mining efforts.”

13 14. One measure for determining the effectiveness or processing power of a  
14 mining operation is to calculate the operation’s hash rate. According to Bitcoin.org: “The  
15 hash rate is the measuring unit of the processing power of the Bitcoin network. The Bitcoin  
16 network must make intensive mathematical operations for security purposes. When the  
17 network reached a hash rate of 10 Th/s, it meant it could make 10 trillion calculations per  
18 second.”

19 15. Bitcoin utilizes “public key cryptography,” a mathematical algorithm that  
20 generates a pair of unique, corresponding keys: the “public key” and the “private key.”  
21 These components form the “public address,” which is used to send and receive bitcoins and  
22 can be shared. A public address is akin to a bank account number, and a private key is akin  
23 to a Personal Identification Number (“PIN”) or password. Only the holder of a public  
24 address’s private key can authorize transfers of virtual currency from that public address to  
25 another public address.

26  
27  
28 <sup>1</sup> Since Bitcoin is both a virtual 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 virtual currency. That practice is adopted here.

1 16. Many virtual currencies operate via a “blockchain,” a record (or ledger) of  
2 every transaction ever conducted that is distributed throughout the computer network (as  
3 opposed to being maintained by any single administrator or entity). As to bitcoins, although  
4 the public addresses of those engaging in virtual currency transactions are recorded on a  
5 blockchain, the identities of the individuals or entities behind the public addresses are not  
6 recorded on these public ledgers. If, however, an individual or entity is linked to a public  
7 address, it may be possible to determine what transactions were conducted by that individual  
8 or entity. Bitcoin transactions are therefore sometimes described as “pseudonymous,”  
9 meaning that they are partially anonymous.

10 17. Virtual currency users typically employ a “wallet,” a tool that can be used to  
11 manage public and private keys, interface with a blockchain, and to send or receive virtual  
12 currency. Wallets vary widely in terms of their format and technological sophistication. One  
13 variety, known as “hosted” (or “custodial”) wallets, are virtual currency wallets controlled by  
14 a third-party—often, a company with a cloud-based, encrypted wallet platform that may be  
15 hosted on the company’s servers. Users of hosted wallets may be able to access the  
16 company’s platform through various digital devices, much like a traditional online banking  
17 experience. Hosted wallet providers include virtual currency exchanges, which allow their  
18 customers, for a fee, to exchange virtual currency for other virtual currencies and/or fiat  
19 currencies.

20 18. A more detailed description of virtual currencies, blockchains, and law  
21 enforcement techniques for investigating virtual currency transactions, is included below.

## 22 STATEMENT OF PROBABLE CAUSE

### 23 **A. Summary of Investigation**

24 19. The FBI is investigating whether two Estonian residents, IVAN TURYGIN<sup>2</sup>  
25 and SERGEI POTAPENKO, illegally operated a Ponzi scheme, in violation of 18 U.S.C. §  
26 1343, by fraudulently inducing individuals to invest in cryptocurrency mining.

27  
28 \_\_\_\_\_  
<sup>2</sup> IVAN TURYGIN’s name is also spelled Ivan Turögin.

1 20. Individuals can earn cryptocurrency by engaging in mining, which involves  
2 using computing power to solve a complicated algorithm to verify and record payments on  
3 the blockchain. Individuals are rewarded for this task by receiving newly created units of a  
4 cryptocurrency. Cryptocurrency mining typically involves the use of high-powered  
5 computers and the expenditure of large amounts of electricity.

6 21. HASHFLARE, incorporated in the UK and based in Estonia, claimed that it  
7 was engaged in cloud mining, using a cloud based platform to mine Bitcoin and alternative  
8 cryptocurrency coins. HASHCOINS, incorporated and based in Estonia, assisted  
9 HASHFLARE in this endeavor, providing technical support, development and marketing of  
10 HASHFLARE and its subdomains. In exchange for a monetary investment, individuals were  
11 told that they would receive a portion of the mining proceeds.

12 22. In July 2018, HASHFLARE stopped paying investors annual returns, claiming  
13 that cryptocurrency mining was no longer profitable. According to its terms of service,  
14 HASHFLARE informed investors that it would stop cryptocurrency mining “if the  
15 Maintenance and Electricity Fees [are] larger than the Payout.” Specifically, according to  
16 HASHFLARE’s terms, “If mining remains unprofitable for 21 consecutive days the Service  
17 is permanently terminated . . . [and] Payouts and Fees will also be temporarily stopped.”

18 23. Investors contend that, at the time HASHFLARE terminated its services,  
19 cryptocurrency mining was, in fact, profitable. After mining was terminated, investors,  
20 including those located in the United States, began identifying red flags which led them to  
21 believe that HASHFLARE was a Ponzi scheme that was not engaged in cryptocurrency  
22 mining.

23 24. In June 2019, Estonia’s Cyber Crime Bureau notified the FBI that it was  
24 investigating whether IVAN TURYGIN and SERGEI POTAPENKO were operating a Ponzi  
25 scheme. As of June 20, 2019, the Estonian authorities identified approximately \$120  
26 million<sup>3</sup> in losses sustained by HASHFLARE investors.

27  
28  

---

<sup>3</sup> In this Affidavit, all references to \$ refer to US Dollars.



1 **A. HASHFLARE & HASHCOINS**

2 **a. Incorporation and Ownership**

3 25. HASHFLARE and HASHCOINS were incorporated in Estonia and the United  
4 Kingdom on the dates listed in the below chart.

5 Date	6 Corporate Name	Country	Legal Form	Directors or Beneficial Owners	Current Name	Prior Names
7 6/13/13	HASHCOINS OU	Estonia	Private Limited Company	TURYGIN & POTAPENKO	Burfa Tech OU	N/A
8 11/26/14	HASHCOINS TRADE OU	Estonia	Private Limited Company	TURYGIN & POTAPENKO	Burfa Trade OU	N/A
9 12/14/15	HASHFLARE LP	UK	Limited Partnership	Datacom Solutions Ltd & Redbone Investments Ltd.	HASHFLARE LP	Fast Consult Trade LP & HASHCOINS LP

10  
11  
12  
13  
14 26. HASHFLARE maintained the website hashflare.io while HASHCOINS  
15 maintained the website www.hashcoins.com. According to HASHCOINS' and  
16 HASHFLARE's websites, POTAPENKO is identified as a co-founder and CEO of the  
17 entities. According to public reporting, TURYGIN is a co-founder and Business  
18 Development Chairman of HASHCOINS. TURYGIN is also identified as a co-founder of  
19 HASHFLARE.

20 **b. Business Operations**

21 27. Beginning on or before April 18, 2015, HASHFLARE offered cloud mining  
22 services on its website. According to its website, HASHFLARE advertised the following:  
23 "Our service makes cryptocurrency mining available to every user. You no longer need to  
24 buy expensive equipment and spend your time setting up miners. Just select your desired  
25 capacity and earn income!" On another portion of its website, HASHFLARE advertised that  
26 "Cloud mining offers a unique option for mining with a low cost of entry as well as minimal  
27 risk and expense, which is opposite to traditional models of mining that involve  
28 procurement, maintenance and configuration of highly specialized software."

1 28. HASHFLARE advertised that it conducted this mining in collaboration with  
2 HASHCOINS. On its website, HASHFLARE explained that it offered “a new range of  
3 cloudmining services brought to you by the HASHCOINS team of cryptomining experts.”  
4 On its website, HASHCOINS claimed that it was “an Estonian based cryptocurrency mining  
5 hardware manufacturer and cloud hosted mining service provider.” HASHCOINS  
6 advertised that its users could purchase cloud mining contracts from HASHFLARE, claiming  
7 that HASHFLARE users could mine cryptocurrency using HASHCOINS’ datacenters. In its  
8 terms of service, HASHFLARE stated that “HASHCOINS OU provides technical support,  
9 development and marketing of HASHFLARE and its subdomains.”

10 29. HASHFLARE sold cloud mining contracts, allowing users to mine  
11 cryptocurrency through HASHFLARE in exchange for a return. On its website  
12 HASHFLARE explained that a user could “purchas[e] part of the mining power of hardware  
13 hosted and owned by a Cloud Mining services provider,” which “configur[es] the hardware,  
14 maintain[s] uptime and select[s] the most efficient and reliable [mining] pools.” For  
15 example, on April 18, 2015, for \$9.95, a user could buy one million hashrate (“one million  
16 hash per second” or “1 MH/s”) from HASHFLARE. For this rate, HASHFLARE advertised  
17 a “100% Scrypt Miner,” automatic accruals in Bitcoin, and a daily maintenance fee of \$0.01  
18 per 1/MH/s.

19 30. HASHFLARE’s website advertised a tool that could be used to calculate the  
20 approximate amount of profit a user would get depending on the amount of hashrate they  
21 purchased. The user would then have the option to automatically reinvest that profit or  
22 withdraw the profit if their balance was above a certain minimum threshold, which fluctuated  
23 between 0.5 bitcoin to 0.01 bitcoin throughout the existence and operation of HASHFLARE.

24 31. In addition to earning funds through cloud mining, HASHFLARE users also  
25 earned funds by recruiting others to purchase HASHFLARE contracts. HASHFLARE  
26 advertised a referral program, informing users that “as a referrer, you are eligible to receive  
27 10% referral commission bonus for every purchase made by any of your referrals, excluding  
28 reinvest and balance purchases.” As a result, HASHFLARE users could make money each

1 time one of their referred friends, family members or acquaintances purchased cloud mining  
2 contracts.

3 32. A number of individuals, including those operating in the Western District of  
4 Washington purchased mining contracts from HASHFLARE. According to financial records  
5 obtained from Fedwire, a funds transfer system operated by the United States Federal  
6 Reserve Banks, at least \$2.5 million was transferred to accounts held by HASHCOINS for  
7 what appear to be investments in HASHFLARE (examples of descriptions accompanying the  
8 transfer of money were: “HASHFLARE.io Invoice...”; “Investments...”; and “...payment  
9 for mining services”).

10 33. According to bank records obtained from Latvia, approximately \$11 million  
11 was transferred into an account held by HASHFLARE at Latvijas Pasta Banka. These  
12 transfers were made in the names of various individuals, and often referenced the terms  
13 “Invoice” and “Hashrate.” As a result, I believe that these payments were made to purchase  
14 cloud mining contracts from HASHFLARE. For example, on January 31, 2017, F.R.E.  
15 transferred \$1,708 to HASHFLARE’s account, referencing “Invoice 593395 Hashflare.io  
16 SHA-256 HASHRATE 15.” Similarly, on March 6, 2017, A.K. transferred \$5,792.72 to  
17 HASHFLARE’s account, referencing “Invoice .673156 (60TH/S SHA-256 hashrate).”

18 34. Additionally, according to information obtained from a group of approximately  
19 800 investors, a representative of which contacted law enforcement, between initial  
20 investments and re-investments of stated profits, they invested a total of \$7.5 million. It was  
21 not readily apparent how much of the \$7.5 million was contained within the amounts  
22 previously mentioned above.

### 23 c. Collapse of Mining Operations

24 35. In or around June of 2018, HASHFLARE made a number of changes to its  
25 operations. For example, HASHFLARE changed its terms of service that shortened the  
26 length of all Bitcoin mining contracts from “lifetime” contracts to “one year” contracts.  
27 Functionally speaking, under lifetime contracts purchased hashrates did not expire, whereas  
28

1 | under the new term the purchased hashrates expired after one year, requiring users to buy  
2 | additional contracts.

3 |         36. In or around July 2018, HASHFLARE also required all users to submit “Know  
4 | Your Customer” identification before they could continue using services offered on the  
5 | platform. In effect, these additional procedures reduced the ability of users to withdraw  
6 | funds earned through mining. On online forums, users complained that, even after they  
7 | submitted the necessary documentation, HASHFLARE was taking weeks or months to verify  
8 | their identities and pay balances. Other users complained that they never received their  
9 | requested balances.

10 |         37. Finally, on July 20, 2018, HASHFLARE announced that Bitcoin mining had  
11 | been unprofitable for 28 days as of July 18, 2018 and, per clause 5.5 of its Terms of Service,  
12 | all Bitcoin mining SHA-256 contracts were suspended. According to its terms of service,  
13 | HASHFLARE informed investors that it would stop cryptocurrency mining “if the  
14 | Maintenance and Electricity Fees [are] larger than the Payout.” Specifically, according to  
15 | HASHFLARE’s terms, “If mining remains unprofitable for 21 consecutive days the Service  
16 | is permanently terminated . . . [and] Payouts and Fees will also be temporarily stopped.”

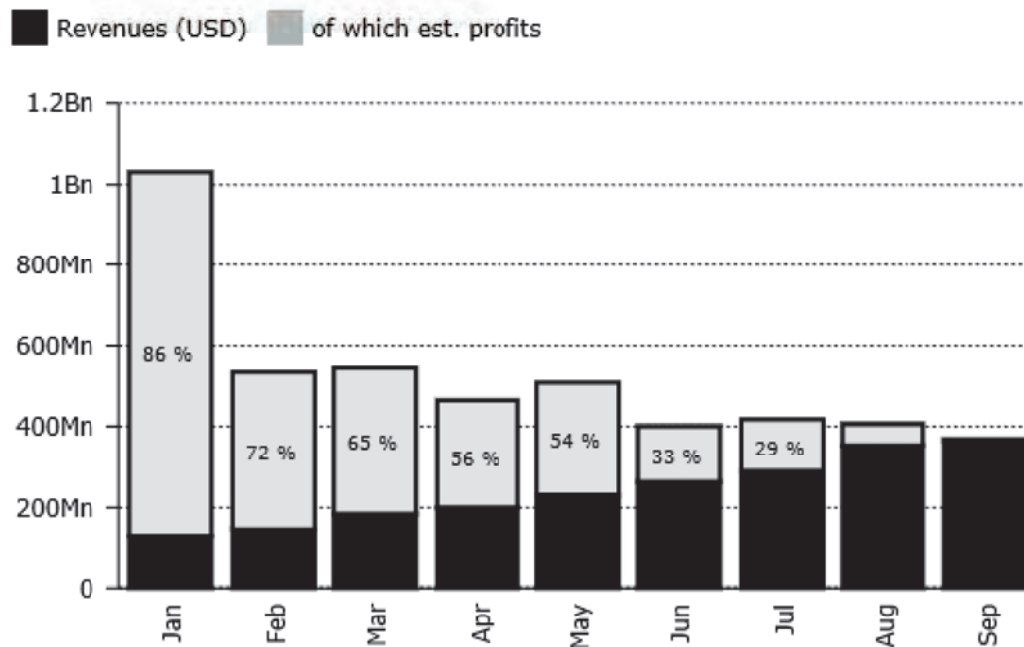
17 |         38. Interviews of three HASHFLARE investors, F.M., B.J., and F.W., revealed  
18 | that it was not possible to make any withdrawals once the Bitcoin mining contracts were  
19 | suspended, which held true through the dates of the interviews that took place in or around  
20 | September of 2019. Since then, there has been no indication from known victims that any of  
21 | the money invested was recoverable from HASHFLARE.

22 |         39. Since HASHFLARE suspended its contracts, investors, including those located  
23 | in the United States, began identifying red flags which led them to believe that  
24 | HASHFLARE was a Ponzi scheme that was not engaged in cryptocurrency mining. Instead,  
25 | they believed that HASHFLARE was profiting on fluctuations in cryptocurrency exchange  
26 | rates, using those gains and new investment proceeds to repay earlier investors. For  
27 | example, investors visited HASHFLARE’s business address in Estonia, which did not appear  
28 | to house a server farm or computing equipment consistent with cryptocurrency mining.

1 Additionally, according to these investors, the rates charged by HASHFLARE for  
 2 maintenance and electricity were above market average, and pools that were used to mine  
 3 did not produce the expected output.

4 40. Diar, which publishes a digital assets and regulations newsletter, reported that  
 5 while bitcoin mining was profitable for the first six months of 2018, with 2018 revenues  
 6 exceeding 2017 revenues by \$1.4 billion, as of the end of August and the beginning of  
 7 September, bitcoin mining was becoming unprofitable.<sup>4</sup> According to Diar, increases in  
 8 electricity costs and mining difficulty (increased hashrate) have led to this unprofitability.  
 9 For example, a chart compiled by Dial is referenced below:

10 **2018: Miners Paying Retail Electricity Prices Now Unprofitable...**



12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24 **Notes:** Profit Estimates Using S9 Miners & \$0.1/kWh, No Pool Fees or Hardware  
 25 Costs. The chart is illustrates profits if all miners paid retail electricity prices.

26  
27  
28 <sup>4</sup> Diar, *Bitcoin Miner Revenues Near \$5 Billion but Profitability Dwindles*, Volume 2, Issue 40, (Oct. 8, 2018), available at <https://diar.co/volume-2-issue-40/>.

1           41. While Diar projected that mining did not become unprofitable until late August  
2 and early September 2018, HASHFLARE contended that its mining operations became  
3 unprofitable in late June 2018. However, HASHFLARE's operations may be more costly  
4 than those profiled by Diar, which did not take pool fees or hardware costs into account.  
5 HASHFLARE's terms of service provide that users must pay the following maintenance  
6 fees: "hardware setup, data center rent, Mining Pool testing, staff salaries, future planning  
7 and proofing, software development, exchange of used and out of order parts and  
8 other expenditures required to render the service on a best-effort basis."

9           42. The FBI has been investigating whether HASHFLARE and HASHCOINS  
10 engaged in sufficient cryptocurrency mining to service the contracts that had been purchased.  
11 To do so, I have reviewed analysis conducted by Estonian authorities who analyzed 22,935  
12 transfer chains related to HASHFLARE payout wallets to determine if payouts to investors  
13 were coming from mining pools, which would be the expected source of payouts. Based on  
14 their analysis, most of the payouts came from the wallets where Bitcoin deposits were  
15 received, and only 0.8% of payouts came from mining pools. As a result, it appears that  
16 HASHFLARE may not have been engaged in substantial cryptocurrency mining, as  
17 previously advertised.

18           43. The FBI has also been investigating whether HASHFLARE and HASHCOINS  
19 possessed sufficient cryptocurrency mining equipment, in light of the number of contracts  
20 that had been purchased, and have determined the following.

21           44. On its website, HASHFLARE claimed that, when the company began in 2015,  
22 it conducted cloud mining using equipment obtained from HASHCOINS. As referenced  
23 above, investors questioned whether HASHCOINS had the capability to mine  
24 cryptocurrency, since they did not appear to have a large server location (or at least none was  
25 found). Additionally, in 2014 and 2015, HASHCOINS initially sold mining equipment, to  
26 be operated by the purchasing user. However, during that time frame, HASHCOINS  
27 claimed that it experienced supply disruptions frustrating their ability to supply Bitcoin  
28 mining equipment. On online forums, HASHCOINS users complained that purchased

1 mining equipment never arrived or that HASHCOINS claimed that shipments were  
2 substantially delayed. And while some users stated they received less powerful equipment  
3 produced by HASHCOINS, users complained that orders for more powerful mining  
4 equipment were left unfulfilled and unrefunded. In response, HASHCOINS offered its  
5 customers the opportunity to invest in HASHFLARE's cloud mining services, instead.  
6 Investors questioned whether this transition was intentional, to ensure that additional  
7 investors sent funds to HASHFLARE, and whether HASHCOINS ever had the ability to  
8 produce the more sophisticated cloud mining equipment advertised on its website.

9 45. Notably, from at least December 2015 until September 2016, HASHCOINS  
10 advertised cryptocurrency mining equipment for sale on its website. However, as of October  
11 2016, despite the above mentioned orders from users, HASHCOINS advertised on its  
12 website that "In 2015 we have changed our business model from B2C [sales to customers] to  
13 B2B [sales to businesses], working with business customers only as we mostly keep the  
14 hardware for the needs of HashFlare."

15 46. Later in its operations, HASHFLARE claimed that it was purchasing  
16 cryptocurrency mining equipment from other companies, instead of sourcing its supply from  
17 HASHCOINS.

18 47. Beginning on or before June 4, 2018, HASHFLARE appears to have  
19 advertised on its website, albeit in broken English, that it uses "equipment for mining"  
20 obtained from "Bitmain, Bitfury, Inno3d, and others." Bitmain, Bitfury, and Inno3d each  
21 manufacture cryptocurrency mining equipment. Because of the broken English, it is difficult  
22 to determine when HASHFLARE started using mining equipment supplied by these  
23 companies, but it appears that HASHFLARE advertised that it acquired this equipment in  
24 2016.<sup>5</sup>

25  
26  
27 <sup>5</sup> The language states: "HashFlare is a cloud mining service created by the specialists from HashCoins in 2015. In a short  
28 time, HashFlare became one of the largest providers of computational power for mining bitcoin, litecoin, ethereum and  
other cryptocurrencies. From 2016, HashFlare is an independent company. The variety of equipment that is used for  
mining was significantly increased on the account such companies as Bitmain, Bitfury, Inno3d and others."

48. According to banking records obtained to date,<sup>6</sup> HASHCOINS first transferred funds to Bitfury on August 14, 2017, with another transfer of more than \$900,000 in funds occurring on October 4, 2017. Records from Bitfury show that deliveries were made on October 16, 2017 and November 21, 2017.

49. Additionally, according to banking records, from January until September 2018, Burfa Media OU (described in further detail below) transferred \$12.3 million to Ask Technology Group Limited, which appears to sell Inno3d products, a cryptocurrency mining equipment manufacturer. The subject lines for each payment listed “Mining Systems” or “P106-090 Systems”—associated with cryptocurrency mining. Given the timing, it’s unclear whether these systems were ever used in connection with HASHFLARE’s operations.

50. Additionally, emails were exchanged between POTAPENKO or TURYGIN and representatives at Bitmain, Bitfury, and Inno3d. According to information obtained from Google, POTAPENKO and TURYGIN communicated with representatives from these companies during the following time periods using the following email addresses:

POTAPENKO and TURYGIN Accounts	Communicating With	Time Frame
sergei@hashcoins.com	Bitmain	9/15-3/18
	Bitfury	1/16-2/16
	Inno3d	12/17-1/19
ivan@hashcoins.com	Bitfury	6/17-1/19
sergei.potapenko@gmail.com	Bitfury	3/16-3/16
ivan@burfa.com	Bitfury	7/18-8/18
	Inno3d	12/17-1/19

51. However, HASHFLARE was advertising and selling mining contracts well before these equipment purchases from Bitfury and Inno3d. Based on financial records analyzed to date, users appeared to have begun transferring funds to HASHCOINS’ bank account to purchase HASHFLARE mining contracts in 2016 and 2017. For example, on April 7, 2017, a transfer was made with the accompanying description: “OUR PS1704077754142 Purpose: SHA-256 HASHRATE INVOICE #771551.” Those same

<sup>6</sup> The FBI is continuing to gather financial information related to this case and has, so far, obtained records from Latvia, Estonia, and the United States relating to HASHFLARE and HASHCOINS, among other entities.



1 financial records provide 28 payments made to the same HASHCOINS bank account,  
2 totaling approximately \$200,000, before any known delivery of mining equipment was made  
3 by Bitfury to HASHFLARE. Based on the above, the FBI is investigating whether  
4 HASHFLARE was soliciting and collecting investments for services it was not yet able to  
5 perform.

6 52. Between at least August 2017 and June 2018, HASHFLARE has also  
7 transferred more than € 25 million to CryptoPay Ltd., a UK company that sells Bitcoin,  
8 purchases Bitcoin in exchange for fiat currency, and sells cards that can be loaded with  
9 cryptocurrency. For example, on August 8, 2017, HASHFLARE transferred \$250,000 to  
10 CryptoPay for “digital assets purchase.” Again, on August 17, 2017 HASHFLARE  
11 transferred an additional \$250,000 for “digital assets purchase.” These payments continued  
12 through at least June 7, 2018, when HASHFLARE transferred \$800,000, also for “digital  
13 assets purchase.” Based on these purchases, and the payment references, the FBI is  
14 investigating whether HASHFLARE was paying its investors using bitcoins purchased from  
15 CryptoPay, rather than mining bitcoins as advertised.

16 53. Furthermore, based on my training and experience, and information gained  
17 during the course of this investigation, I know that Ponzi schemes operate by recruiting  
18 others, paying earlier investors with funds transferred by later investors. Ponzi schemes  
19 often involve recruitment bonuses, incentivizing earlier investors to recruit friends and  
20 family members so that funds are available to pay earlier members. As described above,  
21 HASHFLARE advertised a referral program, paying earlier investors 10% bonuses based on  
22 cloud mining contracts purchased by those they referred.

23 54. HASHFLARE and HASHCOINS have stopped selling any mining contracts  
24 and, as described below, its founders and employees appear to have moved to successor  
25 companies that continue to operate in the cryptocurrency space. Prior investors have not  
26 been able to recoup their funds and many have been unable to transfer funds held in their  
27 accounts.

1 55. I submit there is probable cause to believe HASHFLARE and HASHCOINS  
2 operated as a Ponzi scheme for at least the following reasons: (1) before its collapse,  
3 HASHFLARE appears to have been in financial distress, as evidenced by its unilateral  
4 conversion of mining contracts from lifetime contracts to year-long contracts, its use of KYC  
5 requirements to delay users' withdrawal of funds from their accounts, and its termination of  
6 mining contracts during a time when industry press considered bitcoin mining to be  
7 profitable; (2) HASHCOINS' questionable ability to manufacture cryptocurrency mining  
8 equipment, as evidenced by its 2014-15 decision to not fulfill equipment orders and instead  
9 convert purchase contracts to HASHFLARE cloud mining contracts; (3) Estonian law  
10 enforcement's analysis that HASHFLARE wasn't receiving substantial payouts from mining  
11 pools, sufficient to pay its investors; (4) HASHFLARE's purchase of mining equipment only  
12 later in its operations, beginning at the earliest in 2016 (according to its website) or 2017  
13 (according to banking information); (5) HASHFLARE's apparent purchase of "digital  
14 assets" from CryptoPay, which, among other items, sells Bitcoin, suggesting that  
15 HASHFLARE may be purchasing cryptocurrency rather than mining it; (6) HASHFLARE's  
16 inherent structure, including its referral program and lack of transparency regarding its  
17 mining pools, which is a common structure evidenced in Ponzi schemes; and (7) as described  
18 in further detail below, HASHFLARE's dissolution and the subsequent transition of its  
19 employees and co-founders, who joined new companies that continue to operate in the  
20 cryptocurrency space.

21 **d. HASHCOINS' Use of Google Services**

22 56. According to information obtained from Google, HASHCOINS uses the email  
23 domain @hashcoins.com, which is hosted by Google. HASHCOINS is a G Suite client, a  
24 Google product that provides cloud computing, productivity, and collaboration tools for  
25 business clients.

26 57. The domain @hashcoins.com was created on April 27, 2017, listing two  
27 contact emails for POTAPENKO—sergei@hashcoins.com and  
28 sergei.potapenko@gmail.com. As of February 2020, HASHCOINS used the Google

1 services Google Calendar, Google Drive, Google Docs, Gmail, Google+, Google Hangouts,  
2 Groups for Business, Hangouts Chat, Jamboard Service, Keep, Sites, and Tasks.

3 58. As of February 2020, there were fifteen email addresses associated with the  
4 domain @hashcoins.com.

Subscriber Name	Email Account	Admin	Last Login	Known Role <sup>7</sup>
HASHCOINS Admin	admin@hashcoins.com	N	5/15/19	Administrator of Account
Microsoft Azure	azure@hashcoins.com	N	11/19/18	HASHFLARE hosts its website at Microsoft
Microsoft Azure 2	microsoft@hashcoins.com	N	10/12/18	
Chargeback Check	cb@hashcoins.com	N	12/10/19	Believed to refer to payments with insufficient funds <sup>8</sup>
HASHCOINS Team	info@hashcoins.com	N	1/27/19	HASHCOINS Team
HASHCOINS Invoices	invoices@hashcoins.com	N	8/21/19	HASHCOINS Invoices
IVAN TURYGIN	ivan@hashcoins.com	N	11/12/18	Co-founder of HASHFLARE and HASHCOINS
Licenses HC	licenses@hashcoins.com	N	12/11/19	Believed to refer to hosting controller licenses
Margarita Burunova	margarita.burunova@hashcoins.com	N	7/15/19	Data Center Chief Construction Engineer at Burfa Tech
Nikolay Pavlovskiy	nikolay@hashcoins.com	Y	12/11/19	Chief Technology Officer of HASHCOINS, Vice President and Head of Business Development at HASHFLARE
Pavel Tsihhotski	pavel@hashcoins.com	N	2/17/20	Support and Community Manager for HASHCOINS

7 Obtained from HASHFLARE's or HASHCOINS' website or through public reporting.

8 A number of investors on public chat forums suggested using chargebacks to recover funds lost through the termination of HASHFLARE cloud mining contracts.

Subscriber Name	Email Account	Admin	Last Login	Known Role <sup>7</sup>
SERGEI POTAPENKO	sergei@hashcoins.com	Y	2/10/20	Co-Founder and CEO of HASHFLARE and HASHCOINS
Stanislav Pavlov	stanislav.pavlov@hashcoins.com	Y	2/19/20	Former Human Resources Manager and Customer Support for Burfa Tech OU
Vadim Tsvetikov	vadim.tsvetikov@hashcoins.com	N	2/20/20	Data Center Operation Director at BURFA CAPITAL OU
Vitali Pavlov	vitali@hashcoins.com	Y	2/18/20	Project Manager at HASHFLARE, Chief Product Officer at HASHCOINS

59. In order to gather evidence of HASHCOINS' operations, including discussions of mining cryptocurrency and providing returns to investors, the United States is seeking records from all remaining accounts associated with the HASHCOINS entity. Each account belongs to POTAPENKO, TURYGIN, or an employee that provides an important role for HASHCOINS, including data center operations, project management, and customer support. Other accounts are outward facing corporate accounts, including invoices@hashflare.com, admin@hashflare.com, or info@hashflare.com, that interact with customers, vendors, or suppliers, each of which are likely to contain evidence of additional victims and that HASHCOINS is operating as a Ponzi scheme.

## **B. Other Linked Entities**

### **1. BURFA Entities**

60. After HASHFLARE terminated its mining contracts, HASHCOINS OU changed its legal name to Burfa Tech OU and HASHCOINS TRADE OU changed its name to Burfa Trade OU. As described below, a number of HASHCOIN and HASHFLARE employees then transferred and started working for these entities.

61. Burfa Tech OU and Burfa Trade OU, are part of a conglomerate formed by TURYGIN and POTAPENKO, under the umbrella company Burfa Capital OU, incorporated in Estonia (collectively called the “BURFA Entities”). These entities are described below:

Date	Corporate Name	Country	Legal Form	Directors or Beneficial Owners	Prior Names
7/12/13	Burfa Capital OU	Estonia	Private Limited Company	TURYGIN & POTAPENKO	Starfix UU
6/27/13	Burfa Media OU	Estonia	Private Limited Company	TURYGIN & POTAPENKO	N/A
7/17/17	Burfa Real Estate OU	Estonia	Private Limited Company	Pavel Ivanov	Burfa Estate OU
6/13/13	Burfa Tech OU	Estonia	Private Limited Company	TURYGIN & POTAPENKO	HASHCOINS OU, Euro Host UU
11/26/14	Burfa Trade OU	Estonia	Private Limited Company	TURYGIN & POTAPENKO	HASHCOINS Trade OU, Habalink UU
6/27/13	Burfa Invest OU	Estonia	Private Limited Company	TURYGIN & POTAPENKO	N/A

62. According to the website for Burfa Capital, burfa.com, the various entities have the following missions:

- a. Burfa Capital OU “is a commercial organization . . . emphasizing collaboration and investment in such priority areas as IT, fintech and data processing.” Burfa Capital OU appears to be the parent corporation in the BURFA Entities conglomerate.
- b. Burfa Media OU “provides computing equipment for processing large data arrays and for any operations that require significant computing power.”
- c. Burfa Real Estate OU “is engaged in the construction of commercial and residential luxury real estate in Estonia . . . for the subsequent sale or rent.”

1 d. Burfa Tech OU is reported to be “a leader in the field of data center  
2 design and maintenance for the industrial sector . . . specializ[ing] in high-performance  
3 computing and turnkey data center solutions.” Like HASHCOINS, Burfa Tech OU is  
4 reported publicly to be “an IT company operating in Estonia mainly in the field of equipment  
5 for cryptocurrency mining.”

6 e. Burfa Trade OU “is engaged in the wholesale trade of timber materials.”

7 f. Burfa Invest OU “is a globally recognized brand with three main vectors  
8 of development”—trade, real estate, and construction.

9 63. As described in the chart below, a number of the individuals employed by the  
10 BURFA Entities appear to have been formerly employed by HASHCOINS or  
11 HASHFLARE.

<b>Name</b>	<b>Role in HASHCOINS or HASHFLARE</b>	<b>Role in BURFA Entities</b>
SERGEI POTAPENKO	Co-Founder and CEO of HASHFLARE and HASHCOINS	Board Member & Co-Founder of Burfa Capital OU
IVAN TURYGIN	Co-founder of HASHFLARE and HASHCOINS	Board Member & Co-Founder of Burfa Capital OU
Nikolay Pavlovskiy	Chief Technology Officer of HASHCOINS, Vice President and Head of Business Development at HASHFLARE	Chief Technology Officer for Burfa Capital OU
Vitali Pavlov	Project Manager at HASHFLARE, Chief Product Officer at HASHCOINS	Chief Product Officer at Burfa Capital OU
Vadim Tsvetikov	Associated with HASHCOINS, as described above	Data Center Operation Director for Burfa Capital OU
Pavel Tsihhotski	Support and Community Manager for HASHCOINS	Head of Support for Burfa Capital OU
Stanislav Pavlov	Associated with HASHCOINS, as described above	Former Human Resources Manager and Customer Support for Burfa Tech OU
Tatjana Potapova	Chief Financial Officer for HASHCOINS	Chief Financial Officer for Burfa Media OU
Edger Bers	Public Relations Business Development Manager for HASHCOINS	Associated with BURFA Entities—possesses @burfa.com email address

12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
64. Additionally, around the time the Bitcoin mining contracts were suspended, HASHFLARE transferred substantial assets to the BURFA Entities. For example, according

1 to bank records gathered during the course of this investigation, two different bank accounts  
 2 held in the name of HASHFLARE transferred approximately \$15.5 million to a bank account  
 3 held in the name of Burfa Media OU throughout the year in 2018.

4 65. According to information obtained from Google, the BURFA Entities use the  
 5 email domain @burfa.com, which is hosted by Google. The billing address for this domain  
 6 is Burfa Media OU, in the care of SERGEI POTAPENKO. Burfa Media OU is a G Suite  
 7 client, a Google product that provides cloud computing, productivity, and collaboration tools  
 8 for business clients.

9 66. The @burfa.com domain was established on August 22, 2017, listing two  
 10 contact email addresses—admin@burfa.com and sergei@hashcoins.com (associated with  
 11 POTAPENKO). As of December 2019, the Burfa entities used the Google services Google  
 12 Calendar, Google Drive, Google Docs, Gmail, Google+, Google Hangouts, Groups for  
 13 Business, Hangouts Chat, Jamboard Service, Keep, Sites, and Tasks.

14 67. As of December 2019, there were 42 email addresses associated with the  
 15 domain @burfa.com. Those identified as most relevant to this investigation are included  
 16 below:

Subscriber Name	Email Account	Admin	Last Login	Known Role
Admin Burfa	admin@burfa.com	Y	5/15/19	Administrator
Alerts Mining	alerts.mining@burfa.com	N	12/14/19	Mining Alerts
Info Burfa	info@burfa.com	N	10/9/19	Public Facing Information Email Address
Burfa Media	invoices@burfa.com	N	8/21/19	Invoices
Edger Bers	edger.bers@burfa.com	N	12/3/19	Product Development for BURFA Tech OU
IVAN TUROGIN	ivan@burfa.com	N	11/26/19	Board Member & Co-Founder of BURFA Capital OU
Nikolay Pavlovskiy	nikolay.pavlovskiy@burfa.com	N	12/4/19	Chief Technology Officer for BURFA Capital OU
Pavel Tsihhotski	pavel.tsihhotski@burfa.com	N	12/4/19	Head of Support for BURFA Capital OU

Subscriber Name	Email Account	Admin	Last Login	Known Role
SERGEI POTAPENKO	sergei@burfa.com	N	12/3/19	Board Member & Co-Founder of BURFA Capital OU
Stanislav Pavlov	stanislav.pavlov@burfa.com	Y	12/14/19	Former Human Resources Manager and Customer Support for Burfa Tech OU
Tatjana Potapova	tatjana@burfa.com	N	12/8/19	Chief Financial Officer for Burfa Media OU
Vadim Tsvetikov	vadim.tsvetikov@burfa.com	N	12/11/19	Data Center Operation Director for BURFA Capital OU
Vitali Pavlov	vitali@burfa.com	N	12/8/19	Chief Product Officer at BURFA Capital OU

68. In order to gather evidence of the BURFA Entities' operations as successor companies to HASHFLARE and HASHCOINS, including discussions of ongoing cryptocurrency mining, or the location of corporate assets and evidence, the United States is seeking records from the above BURFA accounts associated with the former HASHFLARE or HASHCOINS employees or current BURFA Tech OU employees, which is the successor corporation of HASHCOINS. The United States also seeks records from the BURFA Entities' outward facing corporate accounts, including invoices@burfa.com, admin@burfa.com, alerts.mining@burfa.com, or info@burfa.com, which interact with customers, vendors, or suppliers, each of which are likely to contain evidence that BURFA is the successor entity to HASHCOINS, and has subsumed its operations and assets.

### **C. Polybius Foundation**

69. In addition to HASHCOINS, HASHFLARE, and the BURFA Entities, TURYGIN and POTAPENKO have also formed a second conglomerate, comprised of four entities—Polybius Foundation OU, Polybius Tech OU, Polybius Ventures OU, and Polybius Fintech MidCo OU (collectively, referred to as "POLYBIUS").

70. Each of these entities was incorporated in Estonia, as listed below:



Date	Corporate Name	Country	Legal Form	Directors or Beneficial Owners
2/13/17	Polybius Foundation OU	Estonia	Private Limited Company	TURYGIN, POTAPENKO & Anton Altement
2/1/18	Polybius Tech OU	Estonia	Private Limited Company	TURYGIN, POTAPENKO, Anton Altement & Vadim Gerassimov
2/8/18	Polybius Ventures OU	Estonia	Private Limited Company	TURYGIN, POTAPENKO & Anton Altement
4/25/18	Polybius Fintech MidCo OU	Estonia	Private Limited Company	TURYGIN, POTAPENKO, Anton Altement & Mathieu Hardy

71. According to the website for POLYBIUS, Polybius.io, and public reporting, the various entities have the following missions:

a. Polybius Tech OU created a cryptocurrency wallet called OSOM Finance, designed to hold both Bitcoin and alternative coins.

b. Polybius Ventures OU and Polybius Fintech MidCo OU are not separately described but are both subsidiaries in the POLYBIUS ecosystem.

c. Polybius Foundation, according to its Prospectus (also known as a “Whitepaper”), is “a team of financial, security, legal and technical experts” who are raising funds to start Polybius Bank. The intent was for Polybius Bank to be a “fully digital bank accessible everywhere at any time. It will have all the functions of a classical bank, but will not host any branches, nor any physical front-offices and will rely fully on the latest digital technologies.” The front of the prospectus reads, in part: “Polybius POWERED BY HASHCOINS.”

72. According to an article written by Forbes on October 29, 2018, POLYBIUS raised approximately \$32 million dollars during its Initial Coin Offering (“ICO”) in the summer of 2017. The symbol for the POLYBIUS coins is PLBT. As of the date of the writing of the article, no tangible product had been launched. In fact, it announced that it abandoned the prospect of opening a bank, and that it would develop a mobile app instead.

73. A cursory review of the POLYBIUS tokens was discussed in a law review article published by the Columbia Law Review in April of 2019, entitled “Coin-Operated Capitalism.” In the article, the authors note that a “development team can unilaterally change the [POLYBIUS] tokens purchased by investors—or sometimes, propose changes that

1 | will not be adopted if a certain percentage of users do not object.” The authors opine that the  
 2 | latter type of proposed changes that may be detrimental to investors may automatically take  
 3 | effect with no knowledge of the investor because (1) the default vote is inherently set to  
 4 | “yes,” and (2) the investing public as a whole does not have the technical skills to monitor or  
 5 | understand the proposed changes a development team may make to the POLYBIUS tokens.  
 6 | To date, it is unknown whether any such changes occurred.

7 | 74. On November 17, 2018, POLYBIUS released a blog post announcing it was  
 8 | releasing a new personal finance management service called “OSOM.” Later in 2019,  
 9 | POLYBIUS released instructions about how to transfer PLBT tokens from an investor’s  
 10 | POLYBIUS Wallet to their OSOM Wallet. According to POLYBIUS, transfer of the PLBT  
 11 | tokens to the OSOM Wallet was important because the POLYBIUS Wallet would eventually  
 12 | no longer be functioning.

13 | 75. A simple search of Apple’s “App Store” and Google’s “Play Store” for  
 14 | “POLYBIUS” and “OSOM” yields no relevant results.

15 | 76. The POLYBIUS coin is still available for purchase as of today, and both the  
 16 | OSOM website and POLYBIUS website are making assertions that a product is being  
 17 | developed.

18 | 77. According to banking records, POLYBIUS has received substantial payments  
 19 | from the BURFA Entities. For example, in June 2018, Burfa Media OU transferred more  
 20 | than € 2 million to accounts held by Polybius Foundation OU.

21 | 78. As with the BURFA Entities, some of the individuals employed by  
 22 | POLYBIUS appear to have been formerly employed by HASHCOINS or HASHFLARE or  
 23 | the BURFA entities. As a result, it appears that POLYBIUS is a successor entity of  
 24 | HASHCOINS and HASHFLARE.

Name	Role in HASHCOINS, HASHFLARE or BURFA	Role in POLYBIUS
SERGEI POTAPENKO	Co-Founder and CEO of HASHFLARE and HASHCOINS	Co-Founder of POLYBIUS
IVAN TURYGIN	Co-founder of HASHFLARE and HASHCOINS	Co-Founder of POLYBIUS

<b>Name</b>	<b>Role in HASHCOINS, HASHFLARE or BURFA</b>	<b>Role in POLYBIUS</b>
Edgar Bers	Public Relations Business Development Manager for HASHCOINS	Communications and Media Manager for POLYBIUS
Pavel Tsihhotski	Support and Community Manager for HASHCOINS	Associated with POLYBIUS (possesses @polybius.io email address)
Anton Altement	Associated with BURFA Entities (possesses @burfa.com email address)	CEO & Co-Founder of POLYBIUS
Vitali Pavlov	Project Manager at HASHFLARE, Chief Product Officer at HASHCOINS	Product Manager POLYBIUS

79. According to information obtained from Google, POLYBIUS uses the email domain @polybius.io, which is hosted by Google. Based on publicly available domain name searches, it appears that POLYBIUS is a G Suite client, a Google product that provides cloud computing, productivity, and collaboration tools for business clients.

80. During the course of this investigation, law enforcement has identified at least seven email addresses associated with the domain @polybius.io. Those identified as most relevant to this investigation are included below:

<b>Suspected Owner</b>	<b>Email Account</b>	<b>Known Role</b>
POLYBIUS Support	support@polybius.io	Support
POLYBIUS Information	info@polybius.io	Information
Anton Altement	anton.altement@polybius.io	CEO & Co-Founder of POLYBIUS
Edger Bers	edgar.bers@polybius.io	Communications and Media Manager for POLYBIUS
IVAN TURYGIN	ivan.turygin@polybius.io	Co-Founder of POLYBIUS
SERGEI POTAPENKO	sergei.potapenko@polybius.io	Co-Founder of POLYBIUS
Pavel Tsihhotski	pavel.tsihhotski@polybius.io	Unknown
Vitali Pavlov	vitali.pavlov@polybius.io	Product Manager POLYBIUS

81. In order to gather evidence of POLYBIUS's operations as a successor company to HASHFLARE and HASHCOINS, including discussions of ongoing cryptocurrency management, or the location of corporate assets and evidence, the United

1 States is seeking records from the above POLYBIUS accounts associated with the former  
 2 HASHFLARE or HASHCOINS employees or current POLYBIUS executives, which  
 3 continues to operate in the cryptocurrency sphere. The United States also seeks records from  
 4 POLYBIUS's outward facing corporate accounts, including support@polybius.io and  
 5 info@polybius.io, which interact with customers and the public, each of which are likely to  
 6 contain evidence that POLYBIUS is the successor entity to HASHCOINS, and has  
 7 subsumed its operations and assets.

8 **D. Dalmeron Projects & Ecohouse Networks**

9 82. During the course of this investigation, law enforcement has learned that an  
 10 account held by HASHFLARE transferred over € 40 million to an account held by Dalmeron  
 11 Projects LP in Latvia. Dalmeron Projects LP transferred a significant portion of those funds  
 12 to accounts held by Burfa Media OU, Polybius Foundation OU, and HASHCOINS.

13 83. Similarly, law enforcement has learned that HASHCOINS has transferred over  
 14 € 900,000 to accounts held by Ecohouse Networks LP in Latvia. Ecohouse Networks  
 15 transferred a portion of those funds to an account held by Burfa Media OU in Estonia.

16 84. Dalmeron Projects LP was incorporated in Canada, as described below.  
 17 Ecohouse Networks was incorporated in the United Kingdom. Dalmeron Projects LP appears  
 18 to operate the website www.dalmeron.com, advertising "cryptocurrency cloud mining  
 19 solutions for corporate clients." The website explained "we offer hashing power to  
 20 companies working with cryptocurrencies, hashing algorithms or private blockchain-based  
 21 networks using the newest ASIC hardware and GPU rigs."

Date	Corporate Name	Country	Legal Form	Directors or Beneficial Owners
3/8/16	Dalmeron Projects LP	Canada	Limited Partnership	Unknown
11/17/14	Ecohouse Networks	UK	Limited Partnership	No persons with Significant Control Listed

22  
 23  
 24  
 25  
 26 85. As described below, despite their separate corporate forms, both entities appear  
 27 to be linked to IVAN TURYGIN.  
 28

1 86. According to information obtained from Google, the account  
2 dalmeronprojects@gmail.com was created on October 24, 2016, listing the subscriber name  
3 as “Dalmeron Projects.” The recovery email listed on the account was  
4 ecohousenetworks@gmail.com. The services associated with the account were: Web & App  
5 Activity, Gmail, Google Hangouts, YouTube, Google Calendar, Android Partner, and  
6 Google My Maps.

7 87. The dalmeronprojects@gmail.com account is linked by cookies to the  
8 ecohousenetworks@gmail.com, ivan.turygin@polybius.com, ivan@burfa.com, and  
9 turygin@gmail.com email addresses. A cookie is a text file that a web browser places on a  
10 user’s computer or machine. Cookies are used for a variety of purposes, including  
11 authentication, security, storing website information and preferences, advertising, and  
12 analytics. Based on my training and experience, I know if accounts are linked by cookies it  
13 suggests that they were accessed and owned by a common user.

14 88. According to information obtained from Google, the account  
15 ecohousenetworks@gmail.com was created on March 9, 2015, listing the subscriber name as  
16 “Ecohouse Networks.” The recover email listed on the account was turygin@gmail.com,  
17 which as explained below is associated with TURYGIN. The services associated with the  
18 account were: Web & App Activity, Gmail, Google Hangouts, YouTube, Google Calendar,  
19 Android Partner, and Google My Maps.

20 89. The ecohousenetworks@gmail.com account is also linked by cookies to the  
21 dalmcronprojects@gmail.com, ivan.turygin@polybius.io, ivan@burfa.com, and  
22 turygin@gmail.com accounts.

23 90. In order to determine the business purpose of these transfers, or to gather  
24 evidence that these transfers were a continuation of the HASHFLARE Ponzi operation or a  
25 money laundering transaction, designed to conceal assets stolen from HASHFLARE and  
26 HASHCOINS investors, the United States seeks records for both accounts belonging to  
27 Ecohouse Networks LP and Dalmeron Projects LP.  
28

1 | **E. Personal Email Addresses**

2 | 91. In addition to corporate email addresses, TURYGIN and POTAPENKO both  
3 | use personal email addresses hosted at Google.

4 | 92. On May 10, 2006, the email address sergei.potapenko@gmail.com was  
5 | registered, listing the subscriber name as “Sergei Pt.” The recovery email associated with  
6 | the account was sergei@hashcoins.com. The services associated with the account include:  
7 | Account Activity, Android, Contacts, Gmail, Google Calendar, Google Chrome Sync,  
8 | Google Docs, Google Drive, Google Hangouts, Google Keep, Google Maps Engine, Google  
9 | Mobile, Google My Maps, Google Payments, Google Photos, Google Play, Google Search  
10 | Console, Google+, Location History, YouTube and iGoogle.

11 | 93. According to Google, the sergei.potapenko@gmail.com account is linked by  
12 | cookies to sergei@burfa.com and sergei@hashcoins.com.

13 | 94. On February 25, 2005, the email address turygin@gmail.com was registered,  
14 | listing the subscriber name as IVAN TURYGIN. The recovery email associated with the  
15 | account was ivan@burfa.com. The services associated with the account include: Android,  
16 | Google Calendar, Google Chrome Sync, Google Docs, Google Drive, Google Hangouts,  
17 | Google Maps, Google Maps Engine, Google My Maps, Google Photos, Google Voice,  
18 | Location History, Web & App Activity, YouTube, and iGoogle.

19 | 95. According to Google, the turygin@gmail.com account is linked by cookies to  
20 | dalmeronprojects@gmail.com, ecohousenetworks@gmail.com, ivan.turygin@polybius.io,  
21 | and ivan@burfa.com.

22 | 96. As described below, although these email addresses end with the domain  
23 | @gmail.com, both POTAPENKO and TURYGIN used them to communicate regarding  
24 | corporate matters tied to HASHFLARE, HASHCOINS, the BURFA Entities, and  
25 | POLYBIUS.

26 | **F. Emails Sent and Received**

27 | 97. POTAPENKO and TURYGIN use their @hashcoins.com, @burfa.com,  
28 | @polybius.io, and @gmail.com email addresses virtually interchangeably to communicate

with other employees of their corporations. For example, POTAPENKO and TURYGIN have used the following accounts to communicate with the following employees:

POTAPENKO and TURYGIN Accounts	Entity	Communicating With <sup>9</sup>
sergei@hashcoins.com	HASHCOINS	vitali@hashcoins.com accounts@hashcoins.com job@hashcoins.com pavel@hashcoins.com vadim.tsetikov@hashcoins.com invoices@hashcoins.com irina.rusakova@hashcoins.com ivan@hashcoins.com simon.inkin@hashcoins.com alexandr@hashcoins.com pavel.borozdin@hashcoins.com mihkel@hashcoins.com hctinvoices@hashcoins.com arkadi.zaitzev@hashcoins.com dan.but@hashcoins.com admin@hashcoins.com management@hashcoins.com info@hashcoins.com stanilov.pavlov@hashcoins.com margarita.burunova@hashcoins.com job+managers@hashcoins.com anna.vesselko@hashcoins.com maksim.stadnik@hashcoins.com simon@hashcoins.com cfbot@hashcoins.com nikolay.pavlovskiy@hashcoins.com jira@hashcoins.com konstantin.kalakauskas@hashcoins.com roman.kononov@hashcoins.com sales@hashcoins.com roman.sadovski@hashcoins.com cb@hashcoins.com ervin.bazin@hashcoins.com rena@hashcoins.com support@hashcoins.com adim.tsvetikov@hashcoins.com aleksandr@hashcoins.com allan.rumjantsev@hashcoins.com

<sup>9</sup> As a to, from, or co-cc'd address.

1 POTAPENKO and TURYGIN 2 Accounts	3 Entity	4 Communicating With <sup>9</sup>
		allan.vaino@hashcoins.com andrei@hashcoins.com anton@hashcoins.com artur.kutsenko@hashcoins.com christine@hashcoins.com it+noreply@hashcoins.com julia.dolzenkova@hashcoins.com julia.odnodvortseva@hashcoins.com kirill.tserjukanov@hashcoins.com lev.malinovski@hashcoins.com lev.mozhaev@hashcoins.com licenses@hashcoins.com matt.morozov@hashcoins.com natalia.levinzon@hashcoins.com nikolai@hashcoins.com roman@hashcoins.com tatjana@hashcoins.com valentin@hashcoins.com vityal@hashcoins.com wordpress@hashcoins.com
	BURFA Entities	ivan@burfa.com tatjana@burfa.com pavel@burfa.com anton.altement@burfa.com julia.karpa@burfa.com margarita.burunova@burfa.com karmella@burfa.com vitali@burfa.com info@burfa.com vadim.tsvetikov@burfa.com sergei@burfa.com anton@burfa.com admin@burfa.com anton.fjodorov@burfa.com invoices@burfa.com irina.rusakova@burfa.com ivan.turygin@burfa.com
	POLYBIUS	anton.altement@polybius.io edgar.bers@polybius.io mathieu.hardy@polybius.io ivan.turygin@polybius.io sergei.potapenko@polybius.io support@polybius.io



POTAPENKO and TURYGIN Accounts	Entity	Communicating With <sup>9</sup>
		jerome.dickinson@polybius.io info@polybius.io vadim.gerassimov@polybius.io gunther.debacker@polybius.io pavel.tsihhotski@polybius.io andrius.verseckas@polybius.io dmitri.troskov@polybius.io igor.rusovitch@polybius.io dilnoza.shaumaroova@polybius.io etienne.goffin@polybius.io mykhailo.riabokon@polybius.io
	DALMERON PROJECTS	dalmeronprojects@gmail.com
	TURYGIN	turygin@gmail.com
	HASHFLARE	alex@hashflare.io info@hashflare.io support@hashflare.io legal@hashflare.io alerts@hashflare.io
ivan@hashcoins.com	HASHCOINS	job@hashcoins.com vitali@hashcoins.com sergei@hashcoins.com vadim.tsvetikov@hashcoins.com nikolay@hashcoins.com margarita.burunova@hashcoins.com management@hashcoins.com job+managers@hashcoins.com stanislav.pavlov@hashcoins.com arkadi.zaitsev@hashcoins.com cfbot@hashcoins.com simon.inkin@hashcoins.com pavel.borozdin@hashcoins.com edgar@hashcoins.com pavel@hashcoins.com info@hashcoins.com alexandr@hashcoins.com irina.rusakova@hashcoins.com rena@hashcoins.com sales@hashcoins.com support@hashcoins.com aleksandr@hashcoins.com andrei@hashcoins.com anton@hashcoins.com

1 POTAPENKO and TURYGIN 2 Accounts	Entity	Communicating With <sup>9</sup>
		invoices@hashcoins.com it+noreply@hashcoins.com iv.an@hashcoins.com konstantin.kalakauskas@hashcoins.com nikolay.pavlovskiy@hashcoins.com roman@hashcoins.com tatjana@hashcoins.com valentin@hashcoins.com vitaly@hashcoins.com
	BURFA Entities	tatjana@burfa.com vadim.tsvetikov@burfa.com anton.altement@burfa.com ivan@burfa.com julia.karpa@burfa.com margarita.burunova@burfa.com sergei@burfa.com
	POLYBIUS	support@polybius.io anton.altement@polybius.io info@polybius.io edgar.bers@polybius.io
	HASHFLARE	legal@hashflare.io
sergei.potapenko@gmail.com	HASHCOINS	dev@hashcoins.com edgar@hashcoins.com info@hashcoins.com invoices@hashcoins.com mihkel@hashcoins.com nikolay@hashcoins.com partners@hashcoins.com pavel.borozdin@hashcoins.com pavel@hashcoins.com sales@hashcoins.com sergei@hashcoins.com simon.inkin@hashcoins.com stanislav.pavlov@hashcoins.com support@hashcoins.com vadim@hashcoins.com vitali@hashcoins.com
	BURFA Entities	ivan@burfa.com pavel@burfa.com info@burfa.com tatjana@burfa.com karmella@burfa.com margarita.burunova@burfa.com

POTAPENKO and TURYGIN Accounts	Entity	Communicating With <sup>9</sup>
		nikolay.pavlovskiy@burfa.com sergei@burfa.com vitali@burfa.com
	POLYBIUS	support@polybius.io anton.altement@polybius.io info@polybius.io
	HASHFLARE	info@hashflare.io alex@hashflare.io alerts@hashflare.io support@hashflare.io invoices@hashflare.io
turygin@gmail.com	HASHCOINS	invoices@hashcoins.com simon.inkin@hashcoins.com edgar@hashcoins.com info@hashcoins.com cloud@hashcoins.com ivan@hashcoins.com pavel.borozdin@hashcoins.com
	BURFA Entities	irina.rusakova@burfa.com vitali@burfa.com
	POLYBIUS	anton.altement@polybius.io
	HASHFLARE	info@hashflare.io support@hashflare.io
sergei@burfa.com	HASHCOINS	vitali@hashcoins.com invoices@hashcoins.com irina.rusakova@hashcoins.com alexandr@hashcoins.com nikolay@hashcoins.com arkadi.zaitsev@hashcoins.com pavel@hashcoins.com vadim.tsvetikov@hashcoins.com info@hashcoins.com pavel.borozdin@hashcoins.com anna.vesselko@hashcoins.com ivan.turygin@hashcoins.com sergei.potapenko@hashcoins.com sergei@hashcoins.com margarita.burunova@hashcoins.com ivan@hashcoins.com nikolay.pavlovskiy@hashcoins.com
	BURFA Entities	ivan@burfa.com anton.altement@burfa.com vitali@burfa.com

1 POTAPENKO and TURYGIN 2 Accounts	3 Entity	4 Communicating With <sup>9</sup>
		5 nikolay@burfa.com 6 tatjana@burfa.com 7 sergei.potapenko@burfa.com 8 pavel@burfa.com 9 irina.rusakova@burfa.com 10 alexandr.gromov@burfa.com 11 anton@burfa.com 12 ivan.turygin@burfa.com 13 kiikri@burfa.com 14 karmella@burfa.com 15 julia.karpa@burfa.com 16 margarita.burunova@burfa.com 17 andrei.koshmanov@burfa.com 18 vadim.tsvetikov@burfa.com 19 nikolay.pavlovskiy@burfa.com 20 pavel.tsihhotski@burfa.com 21 accounts@burfa.com 22 anna.vesselko@burfa.com 23 info@burfa.com 24 dan.but@burfa.com 25 stanislav.pavlov@burfa.com 26 anton.fjodorov@burfa.com 27 ekaterina.gatovskaia@burfa.com 28 invoices@burfa.com iturygin@burfa.com ivan.turogin@burfa.com npavlovskiy@burfa.com spotapenko@burfa.com
	POLYBIUS	mathieu.hardy@polybius.io jerome.dickinson@polybius.io vadim.gerassimov@polybius.io edgar.bers@polybius.io maksim.stadnik@polybius.io
	HASHFLARE	info@hashflare.io ivan.turygin@hashflare.io sergei.potapenko@hashflare.io support@hashflare.io legal@hashflare.io nikolay.pavlovskiy@hashflare.io
ivan@burfa.com	HASHCOINS	sergei@hashcoins.com vitali@hashcoins.com nikolay@hashcoins.com vadim.tsvetikov@hashcoins.com

1 POTAPENKO and TURYGIN 2 Accounts	Entity	Communicating With <sup>9</sup>
		irina.rusakova@hashcoins.com edgar@hashcoins.com alexandr@hashcoins.com margarita.burunova@hashcoins.com info@hashcoins.com invoices@hashcoins.com pavel.borozdin@hashcoins.com sergei.potapenko@hashcoins.com arkadi.zaitsev@hashcoins.com ivan.turygin@hashcoins.com pavel@hashcoins.com vadim@hashcoins.com vitali.pavlov@hashcoins.com nikolay.pavlovskiy@hashcoins.com konstantin.kalakauskas@hashcoins.com anna.vesselko@hashcoins.com ivan@hashcoins.com simon.inkin@hashcoins.com stanislav.pavlov@hashcoins.com lev.mozhaev@hashcoins.com nikolai@hashcoins.com adim.tsvetikov@hashcoins.com allan.rumjantsev@hashcoins.com allan.vaino@hashcoins.com artur.kutsenko@hashcoins.com cfbot@hashcoins.com christine@hashcoins.com dan.but@hashcoins.com ervin.bazin@hashcoins.com julia.dolzenkova@hashcoins.com julia.odnodvortseva@hashcoins.com kirill.tserjukanov@hashcoins.com lev.malinovski@hashcoins.com maksim.stadnik@hashcoins.com mihkel@hashcoins.com natalia.levinzon@hashcoins.com roman.sadovski@hashcoins.com sales@hashcoins.com
	BURFA Entities	tatjana@burfa.com sergei@burfa.com pavel@burfa.com anton.altement@burfa.com kiikri@burfa.com

1 POTAPENKO and TURYGIN 2 Accounts	3 Entity	4 Communicating With <sup>9</sup>
5 6 7 8 9 10 11 12 13 14 15 16 17		julia.karpa@burfa.com karmella@burfa.com vitali@burfa.com margarita.burunova@burfa.com info@burfa.com irina.rusakova@burfa.com nikolay@burfa.com ivan.turygin@burfa.com anton@burfa.com nikolay.pavlovskiy@burfa.com alexandr.gromov@burfa.com vadim.tsvetikov@burfa.com sergei.potapenko@burfa.com invoices@burfa.com andrei.koshmanov@burfa.com iturygin@burfa.com npavlovskiy@burfa.com spotapenko@burfa.com anna.vesselko@burfa.com anton.fjodorov@burfa.com pavel.tsihhotski@burfa.com kiikri+managers@burfa.com press@burfa.com tatjana.potapova@burfa.com tech@burfa.com vitali.pavlov@burfa.com
18 19 20 21 22 23 24 25 26 27 28	POLYBIUS	anton.altement@polybius.io support@polybius.io edgar.bers@polybius.io mathieu.hardy@polybius.io sergei.potapenko@polybius.io info@polybius.io jerome.dickinson@polybius.io vadim.gerassimov@polybius.io andrius.verseckas@polybius.io dmitri.troskov@polybius.io emc@polybius.io igor.rusovitch@polybius.io pavel.tsihhotski@polybius.io etienne.goffin@polybius.io ivan.turygin@polybius.io vitali.pavlov@polybius.io

POTAPENKO and TURYGIN Accounts	Entity	Communicating With <sup>9</sup>
	DALMERON PROJECTS	dalmeronprojects@gmail.com
	POTAPENKO	sergei.potapenko@gmail.com
dalmeronprojects@gmail.com	HASHCOINS	sergei@hashcoins.com
	BURFA Entities	ivan@burfa.com sergei@burfa.com
	POLYBIUS	support@polybius.io info@polybius.io
ecohousenetworks@gmail.com	HASHCOINS	info@hashcoins.com
	BURFA Entities	ivan@burfa.com info@burfa.com
	POLYBIUS	support@polybius.io info@polybius.io
	HASHFLARE	info@hashflare.io

98. POTAPENKO and TURYGIN also used their various accounts to communicate with cryptocurrency providers or mining companies, as indicated below:

POTAPENKO and TURYGIN Accounts	Communicating With
sergei@hashcoins.com	marc.taverner@bitfury.com anna@bitmain.com info@bitmaintech.com sharif.allayarov@bitmaintech.com kirill@inno3d.com alexey.s@cryptopay.me dmitry@cryptopay.me george@cryptopay.me nikolai@cryptopay.me nickolay.s@cryptopay.me info@cryptopay.me pavel@cryptopay.me
ivan@hashcoins.com	evgeniy.pavlov@bitfury.com marc.taverner@bitfury.com mk@bitfury.com claus.pedersen@bitfury.com aymen.elalfy@bitfury.com daan.mcgrath@bitfury.com bing.feng@bitfury.com auke.russchen@bitfury.com georgy.zabadaev@bitfury.com

POTAPENKO and TURYGIN Accounts	Communicating With
	sales@bitfury.com rodrigo.marques@bitfury.com george@cryptopay.me
sergei.potapenko@gmail.com	marc.taverner@bitfury.com george@cryptopay.me support@cryptopay.me
sergei@burfa.com	nikolai@cryptopay.me support@cryptopay.me
ivan@burfa.com	georgy.zabadaev@bitfury.com kirill@inno3d.com support@cryptopay.me eric@cryptopay.me george@cryptopay.me help@cryptopay.me

99. Finally, POTAPENKO and TURYGIN used sergei@hashcoins.com, sergei.potapenko@gmail.com, turygin@gmail.com, sergei@burfa.com, ivan@burfa.com, and dalmeronprojects@gmail.com to communicate with financial representatives where HASHFLARE, HASHCOINS, and other entities held accounts. And POTAPENKO and TURYGIN used sergei@hashcoins.com, sergei.potapenko@gmail.com, turygin@gmail.com, and sergei@burfa.com to communicate with representatives of CloudFlare and/or Microsoft, where HASHFLARE and the BURFA Entities host their websites.

100. Based on the above, there is probable cause to believe that information contained in the **SUBJECT ACCOUNTS** could reveal, among other things: (1) the plans and strategies formed by the users of the **SUBJECT ACCOUNTS** to defraud investors and customers, (2) the actions taken to execute those plans, (3) the operations and relationship between the various entities, including assets transferred between those entities; (4) the extent and capacity of mining operations at HASHCOINS and HASHFLARE; (5) the location of assets paid by investors to HASHCOINS and HASHFLARE; and (6) information on where HASHFLARE and HASHCOINS store their server data, including data on the identity and investment of each HASHFLARE subscriber. Therefore, the United States seeks records and information from Google related to each of the **SUBJECT ACCOUNTS**.



**BACKGROUND CONCERNING ONLINE ACCOUNTS**

101. As explained herein, information stored in connection with an online account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion.

102. In my training and experience, the information stored in connection with an online account can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time.

103. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user’s account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email).

104. Stored electronic data may provide relevant insight into the email account owner’s state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner’s motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

## 1. Google's Services

105. In my training and experience, I have learned that Google provides a variety of online services, including electronic mail ("email") access and instant messaging (otherwise known as "chat" messaging), to the general public. Google provides subscribers email and chat accounts at the domain name "@gmail.com." Google also allows subscribers to register a custom domain name and set up Google services such as chat and email using that domain name instead of "@gmail.com."

### A. Subscriber Records and Account Content

106. Subscribers obtain an account by registering with Google. When doing so, email providers like Google ask the subscriber to provide certain personal identifying information. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users, and to help establish who has dominion and control over the account.

107. Email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google's websites), and other log files that reflect usage of the account. In addition, email providers often have records of the IP address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

108. In some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing

1 | inquiries, or complaints from other users. Email providers typically retain records about  
2 | such communications, including records of contacts between the user and the provider's  
3 | support services, as well records of any actions taken by the provider or user as a result of  
4 | the communications. In my training and experience, such information may constitute  
5 | evidence of the crimes under investigation because the information can be used to identify  
6 | the account's user or users.

7 |       109. In general, an email that is sent to a Google subscriber is stored in the  
8 | subscriber's "mail box" on Google's servers until the subscriber deletes the email. When the  
9 | subscriber sends an email, it is initiated at the user's computer, transferred via the Internet to  
10 | Google servers, and then transmitted to its end destination. Google often maintains a copy of  
11 | received and sent emails. Unless the sender specifically deletes an email from the Google  
12 | server, the email can remain on the system indefinitely. Even if the subscriber deletes the  
13 | email, it may continue to be available on Google's servers for some period of time.

14 |       110. A sent or received email typically includes the content of the message, source  
15 | and destination addresses, the date and time at which the email was sent, and the size and  
16 | length of the email. If an email user writes a draft message but does not send it, that message  
17 | may also be saved by Google but may not include all of these categories of data.

18 |       111. In addition to email and chat, Google offers subscribers numerous other  
19 | services including: Android, Blogger, Google Alerts, Google Calendar, Google Chrome  
20 | Sync, Google Cloud Print, G-Suite, Google Developers Console, Google Drive, Google  
21 | Hangouts, Google Maps, Google Payments, Google Photos, Google Search Console, Google  
22 | Voice, Google+, Google Profile, Location History, Web & Activity, Search, and YouTube,  
23 | among others. Thus, a subscriber to a Google account can also store files, including address  
24 | books, contact lists, calendar data, photographs and other files, on servers maintained and/or  
25 | owned by Google. For example, Google Calendar is a calendar service that users may utilize  
26 | to organize their schedule and share events with others. Google Drive may be used to store  
27 | data and documents, including spreadsheets, written documents (such as Word or Word  
28 | Perfect) and other documents. Google Photos can be used to create photo albums, store

1 | photographs, and share photographs with others and “You Tube,” allows users to view, store  
2 | and share videos. Google Search Console records a Google account user’s search queries.  
3 | And Google Web & Activity records certain browsing history depending on whether the  
4 | account holder is logged into their account. Google Keep is a note-taking service, offering a  
5 | variety of tools for taking notes, including text, lists, images, and audio. Google Hangouts  
6 | enables users to communicate with each other using instant messaging (including text, video,  
7 | and voice), including through an application or within a Gmail browser window. Instant  
8 | messages sent and received using these services are often saved within a user’s account and  
9 | accessible through Gmail. Google Voice offers a VOIP telephone number and records and  
10 | transcribes voicemails. Groups for Business allow companies to create group discussions  
11 | through emails, which are archived by Google. Like many internet service companies  
12 | (including the companies discussed below), the services Google offers are constantly  
13 | changing and evolving.

14 |       112. Based upon my training and experience, all of these types of information may  
15 | be evidence of crimes under investigation. Stored communications, documents, and Google  
16 | account activity not only may contain evidence of the crimes, but also help identify the  
17 | participants in those crimes. For example, address books and contact lists may help identify  
18 | both the owner of the account and locate co-conspirators. Similarly, photographs and videos  
19 | stored in the account may help identify the account owner’s true identity or document  
20 | evidence of the crimes under investigation, including pictures of cryptocurrency mining  
21 | equipment or screenshots of corporate websites. Documents (such as Google Docs used to  
22 | store investor information or mining efforts), may identify the scope of the criminal activity,  
23 | including containing important business documents, profits and loss statements, or  
24 | communications with investors. And calendar data may reveal the timing and extent of  
25 | criminal activity, including the timing of establishing corporate entities or the termination of  
26 | bitcoin mining contracts. Search and browsing history may also constitute direct evidence of  
27 | the crimes under investigation to the extent the browsing history or search history might  
28 |

1 include searches and browsing history related to bitcoin mining, purchasing cryptocurrency,  
2 or identifying the victims.

3 113. Google is also able to provide information that will assist law enforcement in  
4 identifying other accounts associated with the **SUBJECT ACCOUNTS**, namely,  
5 information identifying and relating to other accounts used by the same subscriber. This  
6 information includes any forwarding or fetching accounts<sup>10</sup> relating to the **SUBJECT**  
7 **ACCOUNTS**, all other Google accounts linked to the **SUBJECT ACCOUNTS** because  
8 they were accessed from the same computer (referred to as “cookie overlap”), all other  
9 Google accounts that list the same SMS phone number as the **SUBJECT ACCOUNTS**, all  
10 other Google accounts that list the same recovery email addresses<sup>11</sup> as do the **SUBJECT**  
11 **ACCOUNTS**, and all other Google accounts that share the same creation IP address as the  
12 **SUBJECT ACCOUNTS**. Information associated with these associated accounts will assist  
13 law enforcement in determining who controls the **SUBJECT ACCOUNTS** and will also  
14 help to identify other email accounts relevant to the investigation.

#### 15 **B. Google Location History and Location Reporting**

16 114. According to Google’s website, “Location Reporting” allows Google to  
17 periodically store and use a device’s most recent location data in connection with the Google  
18 Account connected to the device. “Location History” allows Google to store a history of  
19 location data from all devices where a user is logged into their Google Account and have  
20 enabled Location Reporting. According to Google “[w]hen you turn on Location Reporting  
21 for a device like your iPhone or iPad, it lets Google periodically store and use that device’s  
22 most recent location data in connection with your Google Account.” How often Location  
23 Reporting updates location data is not fixed. Frequency is determined by factors such as  
24

25 <sup>10</sup> A forwarding or fetching account related to one of the **SUBJECT ACCOUNTS** would be a  
26 separate e-mail account that can be setup by the user to receive copies of all of the e-mail sent to the  
27 Target Account.

28 <sup>11</sup> The recovery e-mail address is an additional e-mail address supplied by the user that is used by  
Google to confirm your username after you create an e-mail account, help you if you are having  
trouble signing into your Google account or have forgotten your password, or alert you to any  
unusual activity involving user’s Google e-mail address.

1 | how much battery life the device has, if the device is moving, or how fast the device is  
2 | moving. Google's location services may use GPS, Wi-Fi hotspots, and cellular network  
3 | towers to determine an account holder's location.

4 |       115. Based on the above, I know that if a user of the **SUBJECT ACCOUNTS**  
5 | utilizes a mobile device to access the respective account identified in Attachment A-1 and  
6 | has not disabled location services on his or her device/s or through the Google account  
7 | settings, Google may have detailed records of the locations at which the account holder(s)  
8 | utilized the mobile device(s). This type of evidence may further assist in identifying the  
9 | account holder(s), and lead to the discovery of other evidence of the crimes under  
10 | investigation. For example, in the present case, HASHFLARE and HASHCOINS own  
11 | several bank accounts held overseas. Location data could identify countries where additional  
12 | accounts were opened or accessed.

13 |       116. I know that Google's Android service collects and stores identifying  
14 | information about an Android smart phone used to access the Google account, including the  
15 | International Mobile Equipment Identifier (IMEI), International Mobile Subscriber Identity  
16 | (IMSI), telephone number and mobile carrier code. In addition, Google may collect and  
17 | store certain data related to applications used on Android smart phones, and in certain  
18 | instances, Google may allow a user to backup settings, app data, communications, and other  
19 | data stored on an Android device. I know that Google's Location History service  
20 | periodically queries the physical location of a device that is currently accessing a Google  
21 | account through the device's GPS, nearby Wi-Fi network IDs and cellular tower information  
22 | and records a history of device movements in Google's servers. Because of the complicated  
23 | nature of the successive corporate structures, the overlapping employees at each entity, and  
24 | the existence of foreign bank accounts, I believe the founders of HASHCOINS,  
25 | HASHFLARE, the BURFA Entities, and POLYBIUS have made a concerted effort to  
26 | disguise their assets and corporate structures, I am requesting Google to provide information  
27 | from the Android service and Location History service from the **SUBJECT ACCOUNTS**.

**INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

117. Pursuant to Title 18, United States Code, Section 2703(g), this application and affidavit for a search warrant seeks authorization to require Google, and their agents and employees, to assist agents in the execution of this warrant. Once issued, the search warrant will be presented to Google with direction that it identifies the accounts described in Attachment A to this affidavit, as well as other subscriber and log records associated with the accounts, as set forth in Section I of Attachment B to this affidavit.

118. The search warrant will direct Google to create an exact copy of the specified account and records.

119. I, and/or other law enforcement personnel will thereafter review the copy of the electronically stored data and identify from among that content those items that come within the items identified in Section II to Attachment B for seizure.

120. Analyzing the data contained in the forensic copy may require special technical skills, equipment, and software. It could also be very time-consuming. Searching by keywords, for example, can yield thousands of “hits,” each of which must then be reviewed in context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant “hit” does not end the review process. Keywords used originally need to be modified continuously, based on interim results. Certain file formats, moreover, do not lend themselves to keyword searches, as keywords, search text, and many common email, database and spreadsheet applications do not store data as searchable text. The data may be saved, instead, in proprietary non-text format. And, as the volume of storage allotted by service providers increases, the time it takes to properly analyze recovered data increases, as well. Consistent with the foregoing, searching the recovered data for the information subject to seizure pursuant to this warrant may require a range of data analysis techniques and may take weeks or even months. All forensic analysis of the data will employ only those search protocols and methodologies reasonably designed to identify and seize the items identified in Section II of Attachment B to the warrant.

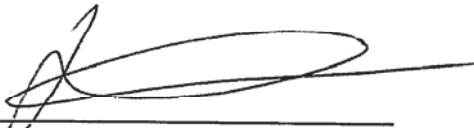
1           121. Based on my experience and training, and the experience and training of other  
2 agents with whom I have communicated, it is necessary to review and seize a variety of e-  
3 mail communications, chat logs and documents, that identify any users of the subject account  
4 and e-mails sent or received in temporal proximity to incriminating e-mails that provide  
5 context to the incriminating communications.  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28




1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**CONCLUSION**

122. Based on the forgoing, I respectfully request that the Court issue the proposed search warrant. Accordingly, by this Affidavit and Warrant I seek authority for the government to search all of the items specified in Section I, Attachment B (attached hereto and incorporated by reference herein) to the Warrant, and specifically to seize all of the data, documents and records that are identified in Section II to that same Attachment.

  
\_\_\_\_\_  
Andrew Cropcho, Affiant  
Special Agent

The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit on the 3 day of April, 2020.

  
\_\_\_\_\_  
THE HONORABLE BRIAN A. TSUCHIDA  
United States Magistrate Judge

**ATTACHMENT A**

**Google Accounts to be Searched**

The electronically stored data, information and communications contained in, related to, and associated with, including all preserved data associated with Google accounts:

- ivan@hashcoins.com (SUBJECT ACCOUNT 1)
- ivan@burfa.com (SUBJECT ACCOUNT 2)
- ivan.turygin@polybius.io (SUBJECT ACCOUNT 3)
- turygin@gmail.com (SUBJECT ACCOUNT 4)
- sergei@hashcoins.com (SUBJECT ACCOUNT 5)
- sergei@burfa.com (SUBJECT ACCOUNT 6)
- sergei.potapenko@polybius.io (SUBJECT ACCOUNT 7)
- sergei.potapenko@gmail.com (SUBJECT ACCOUNT 8)
- nikolay@hashcoins.com (SUBJECT ACCOUNT 9)
- nikolay.pavlovskiy@burfa.com (SUBJECT ACCOUNT 10)
- pavel@hashcoins.com (SUBJECT ACCOUNT 11)
- pavel.tsihhotski@burfa.com (SUBJECT ACCOUNT 12)
- pavel.tsihhotski@polybius.io (SUBJECT ACCOUNT 13)
- stanislav.pavlov@hashcoins.com (SUBJECT ACCOUNT 14)
- stanislav.pavlov@burfa.com (SUBJECT ACCOUNT 15)
- vadim.tsvetikov@hashcoins.com (SUBJECT ACCOUNT 16)
- vadim.tsvetikov@burfa.com (SUBJECT ACCOUNT 17)
- vitali@hashcoins.com (SUBJECT ACCOUNT 18)
- vitali@burfa.com (SUBJECT ACCOUNT 19)
- vitali.pavlov@polybius.io (SUBJECT ACCOUNT 20)
- anton.altement@polybius.io (SUBJECT ACCOUNT 21)
- edger.bers@burfa.com (SUBJECT ACCOUNT 22)
- edgar.bers@polybius.io (SUBJECT ACCOUNT 23)

1 | tatjana@burfa.com (SUBJECT ACCOUNT 24)

2 | margarita.burunova@hashcoins.com (SUBJECT ACCOUNT 25)

3 | dalmeronprojects@gmail.com (SUBJECT ACCOUNT 26)

4 | ecohousenetworks@gmail.com (SUBJECT ACCOUNT 27)

5 | admin@hashcoins.com (SUBJECT ACCOUNT 28)

6 | admin@burfa.com (SUBJECT ACCOUNT 29)

7 | info@hashcoins.com (SUBJECT ACCOUNT 30)

8 | info@burfa.com (SUBJECT ACCOUNT 31)

9 | info@polybius.io (SUBJECT ACCOUNT 32)

10 | invoices@hashcoins.com (SUBJECT ACCOUNT 33)

11 | invoices@burfa.com (SUBJECT ACCOUNT 34)

12 | azure@hashcoins.com (SUBJECT ACCOUNT 35)

13 | microsoft@hashcoins.com (SUBJECT ACCOUNT 36)

14 | cb@hashcoins.com (SUBJECT ACCOUNT 37)

15 | licenses@hashcoins.com (SUBJECT ACCOUNT 38)

16 | alerts.mining@burfa.com (SUBJECT ACCOUNT 39)

17 | support@polybius.io (SUBJECT ACCOUNT 40)

18 |  
19 | (the "Accounts") that are stored at a premises controlled by Google LLC, a company  
20 | that accepts service of legal process at 1600 Amphitheatre Parkway in Mountain  
21 | View, California.  
22 |  
23 |  
24 |  
25 |  
26 |  
27 |  
28 |

**ATTACHMENT B**

**Particular Things to be Seized**

**I. Information to be disclosed by Google, LLC:**

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, LLC (“Google”), including any data, messages, records, files, logs, or information that has been deleted but is still available to Google, or has been preserved pursuant to a request made under Title 18, United States Code, Section 2703(f), Google is required to disclose the following information to the government for each Account or identifier listed in Attachment A, from Account inception to the present:

a. The contents of all emails associated with the account from April 2015 to the present, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. all contact lists;

d. all Google Calendar content;

e. all Google Drive content (including backups of any apps stored on Google Drive);

f. all Google Docs content;

g. all Google Maps content;

h. all Google Photos content;

i. all Google Keep content;

- 1 j. all Google Search Console content;
- 2 k. all Google Web & Activity content;
- 3 l. all Google Chrome Sync content;
- 4 m. all Google Location History content;
- 5 n. all Google Voice content;
- 6 o. all Android content, including, but not limited to active content and
- 7 backups;
- 8 p. all Android Device console content;
- 9 q. all Android Market content;
- 10 r. all Google Hangouts content;
- 11 s. all Groups for Business content;
- 12 t. all Google Profile content, including all Google+ content;
- 13 u. all account history, including any records of communications between
- 14 Google and any other person about issues relating to the accounts, such as technical
- 15 problems, billing inquiries, or complaints from other users about the specified account. This
- 16 to include records of contacts between the subscriber and the provider's support services, as
- 17 well as records of any actions taken by the provider or subscriber in connection with the
- 18 service.

19 Google is hereby ordered to disclose the above information to the government within  
20 **14 days** of service of this warrant.

21  
22 **II. Information to be seized by the government**

23 All information described above in Section I that constitutes fruits, contraband,  
24 evidence, and instrumentalities of violations of Title 18, United States Code, Section 1343  
25 (Wire Fraud), and occurring after April 2015, for each of the Accounts listed on Attachment  
26 A, pertaining to the following matters:

- 27 a. Items, records, or information related to the operation of a
- 28 cryptocurrency cloud mining Ponzi scheme;

1           b.     Items, records, or information related to cryptocurrency mining, the  
2 advertisement, manufacture and sale of mining equipment, or the advertisement and sale of  
3 cloud mining contracts;

4           c.     Items, records, or information related to the termination of mining  
5 contracts and the profitability of cloud mining;

6           d.     Items, records, or information related to purchases of cloud mining  
7 equipment, including communications with the companies Bitmain, Bitfury, and Inno3d;

8           e.     Items, records, or information related to the transfer, purchase, sale, or  
9 disposition of cryptocurrency;

10          f.     Items, records, or information related to communications with  
11 HASHFLARE or HASHCOINS investors, including complaints by investors or requests for  
12 return of funds;

13          g.     Items, records, or information related to the advertisement of  
14 HASHFLARE or HASHCOINS' services;

15          h.     Items, records, or information related to the owners, operators,  
16 employees, locations, assets, and business purpose of the companies HASHCOINS OU,  
17 HASHCOINS TRADE OU, HASHCOINS LP, HASHFLARE LP, Burfa Capital OU, Burfa  
18 Media OU, Burfa Real Estate OU, Burfa Tech OU, Burfa Trade OU, Burfa Invest OU,  
19 Polybius Foundation OU, Polybius Tech OU, Polybius Ventures OU, Polybius Fintech  
20 MidCo OU, Dalmeron Projects LP, and Ecohouse Networks LP (collectively, the  
21 "SUBJECT ENTITIES");

22          i.     Items, records, or information related to the use, creation, or operation  
23 of the "SUBJECT ENTITIES," including business plans and strategies, and the anticipated  
24 success, failure, or general validity thereof;

25          j.     Items, records, or information related to the operation of hashflare.io,  
26 burfa.com, polybius.io, or hashcoins.com;

27          k.     Items, records, or information concerning financial transactions  
28 associated with the operation of the SUBJECT ENTITIES, including bank accounts held by

1 the SUBJECT ENTITIES, transfers of funds by the SUBJECT ENTITIES, expenditures of  
2 money or wealth, bank statements and other financial statements, and cryptocurrency  
3 holdings;

4 l. Items, records, or information related to cryptocurrency mining groups,  
5 cryptocurrency public keys or addresses, cryptocurrency private keys, representations of  
6 cryptocurrency wallets or their constitutive parts, to include “recovery seeds” and “root  
7 keys,” which may be used to regenerate a wallet.

8 m. Items, records, or information related to the salaries or earnings of  
9 individuals employed by the SUBJECT ENTITIES.

10 n. Items, records, or information related to the payment or calculation of  
11 recruitment bonuses paid to HASHFLARE and HASHCOINS investors.

12 o. Items, records, or information related to receipt of investor money,  
13 including the amount, purpose of the investment, and plans for spending that money.

14 p. Evidence indicating how and when the email account was accessed or  
15 used, to determine the geographic and chronological context of account access, use, and  
16 events relating to the crime under investigation and to the email account owner.

17 q. Evidence indicating the email account owner’s state of mind as it relates  
18 to the crime under investigation.

19 r. The identity of the person(s) who created or used the user ID, including  
20 records that help reveal the whereabouts of such person(s).

21  
22 This warrant authorizes a review of electronically stored information, communications, other  
23 records and information disclosed pursuant to this warrant in order to locate evidence, fruits,  
24 and instrumentalities described in this warrant. The review of this electronic data may be  
25 conducted by any government personnel assisting in the investigation, who may include, in  
26 addition to law enforcement officers and agents, attorneys for the government, attorney  
27 support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete  
28 copy of the disclosed electronic data to the custody and control of attorneys for the  
government and their support staff for their independent review.

**APPENDIX 2**

**Affidavit in Support of Search Warrant MJ21-149**

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28



**AFFIDAVIT**

1  
2  
3 STATE OF WASHINGTON )  
4 ) ss  
5 COUNTY OF KING )

6 I, Andrew Cropcho, being duly sworn, hereby depose and state as follows:

7 **INTRODUCTION AND AGENT BACKGROUND**

8 1. I am a Special Agent with the Federal Bureau of Investigation (“FBI”) and  
9 have been since May of 2018. I am currently assigned to the Seattle Field Office. My  
10 primary duties include investigating violations of Federal law, including corporate fraud,  
11 securities fraud, government program fraud, and healthcare fraud. Part of those duties  
12 include investigating instances of wire fraud being used for financial gain at the expense of  
13 others. Before my career as an FBI Special Agent I was employed as a Certified Public  
14 Accountant for over three years and, as part of my employment, I examined financial  
15 information of clients to determine their accuracy, reliability, and sources.

16 2. The facts set forth in this Affidavit are based on my own personal knowledge;  
17 knowledge obtained from other individuals during my participation in this investigation,  
18 including other law enforcement personnel; review of documents and records related to this  
19 investigation; communications with others who have personal knowledge of the events and  
20 circumstances described herein including, but not limited to, the victims in this investigation;  
21 and information gained through my training and experience. Because this Affidavit is  
22 submitted for the limited purpose of establishing probable cause in support of the application  
23 for a search warrant, it does not set forth each and every fact that I or others have learned  
24 during the course of this investigation.

25 **PURPOSE OF AFFIDAVIT**

26 3. I make this affidavit in support of an application for a search warrant for  
27 information associated with certain accounts that are stored at premises controlled by Apple,  
28 Inc. (“Apple”), located at One Apple Park Way, Cupertino, California 95014. The

1 information to be searched is described in the following paragraphs and in Attachment A,  
2 which is incorporated herein.

3 4. This affidavit is made in support of an application for a search warrant  
4 pursuant to Title 18, United States Code, Sections 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A)  
5 to require Apple to disclose to the government copies of the information, including the  
6 content of communications, further described in Section I of Attachment B, pertaining to the  
7 following accounts:

8 a. Sergei.potapenko@gmail.com (DSID 624556209) (“**SUBJECT**  
9 **ACCOUNT 1**”) (believed to be used by SERGEI POTAPENKO); and

10 b. Turygin@gmail.com (DSID 1931852295) (“**SUBJECT ACCOUNT**  
11 **2**”) (believed to be used by IVAN TURYGIN);

12 (hereinafter, collectively the “**SUBJECT ACCOUNTS**”). Upon receipt of the information  
13 described in Section I of Attachment B, government-authorized persons will review that  
14 information to locate the items described in Section II of Attachment B. This warrant is  
15 requested in connection with an ongoing investigation in this district by the FBI.

16 5. Based on my training and experience, and the facts as set forth in this affidavit,  
17 there is probable cause to believe that violations of Title 18, United States Code, Section  
18 1343 (Wire Fraud) have been committed by IVAN TURYGIN and SERGEI POTAPENKO,  
19 individually, and by and through the use of their companies HASHCOINS OU (hereinafter  
20 “HASHCOINS”), HASHCOINS TRADE OU, HASHCOINS LP, HASHFLARE LP  
21 (hereinafter “HASHFLARE”), Burfa Capital OU, Burfa Media OU, Burfa Real Estate OU,  
22 Burfa Tech OU, Burfa Trade OU, Burfa Invest OU (collectively, the “BURFA Entities”),  
23 Polybius Foundation OU, Polybius Tech OU, Polybius Ventures OU, Polybius Fintech  
24 MidCo OU (collectively, “POLYBIUS”), and Dalmeron Projects LP, along with identified  
25 key employees of the same companies. There is also probable cause to search the  
26 information described in Attachment A, for evidence, instrumentalities, or contraband of  
27 these crimes, as described in Attachment B.

**JURISDICTION**

6. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

7. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

8. This warrant application is to be presented electronically pursuant to Local Criminal Rule CrR 41(d)(3).

**BACKGROUND ON VIRTUAL CURRENCY AND MINING**

9. Virtual currency (also known as cryptocurrency) is an asset that can be exchanged directly person to person, through a virtual currency exchange, or through other intermediaries. It can be used to buy goods and services, exchanged for “fiat currency” (currency established by government regulation or law) or other virtual currency, or held as an investment, among other applications.

10. Virtual currency is generally not issued by any government or bank. Rather, it is frequently generated and controlled through software operating on a decentralized, peer-to-peer (“P2P”) network of computers across the world (some types of virtual currency, however, are generated and controlled through software operating on a centralized network of computers across the world).

11. There are thousands of virtual currencies in use, including Bitcoin, Ethereum, Bitcoin Cash, and Monero. Bitcoin,<sup>1</sup> the most popular form of virtual currency, can be generated through mining. According to Bitcoin.org, “Bitcoin mining is the process of making computer hardware do mathematical calculations for the Bitcoin network to confirm

<sup>1</sup> Since Bitcoin is both a virtual 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 virtual currency. That practice is adopted here.

1 transactions and increase security. As a reward for their services, Bitcoin miners can collect  
2 transaction fees for the transactions they confirm, along with newly created bitcoins.”

3 12. Bitcoin mining can be conducted locally on a user’s computer or other  
4 computer hardware, or can be conducted on another’s system via the cloud. According to  
5 the Santa Clara Law School High Technology Journal: “Cloud mining is an economic  
6 arrangement whereby a person pays another person or entity to engage in cryptocurrency  
7 mining on their behalf and receives the transaction fees, cryptocurrency or a portion thereof  
8 that is generated from such mining efforts.”

9 13. One measure for determining the effectiveness or processing power of a  
10 mining operation is to calculate the operation’s hash rate. According to Bitcoin.org: “The  
11 hash rate is the measuring unit of the processing power of the Bitcoin network. The Bitcoin  
12 network must make intensive mathematical operations for security purposes. When the  
13 network reached a hash rate of 10 Th/s, it meant it could make 10 trillion calculations per  
14 second.”

15 14. Bitcoin utilizes “public key cryptography,” a mathematical algorithm that  
16 generates a pair of unique, corresponding keys: the “public key” and the “private key.”  
17 These components form the “public address,” which is used to send and receive bitcoins and  
18 can be shared. A public address is akin to a bank account number, and a private key is akin  
19 to a Personal Identification Number (“PIN”) or password. Only the holder of a public  
20 address’s private key can authorize transfers of virtual currency from that public address to  
21 another public address.

22 15. Many virtual currencies operate via a “blockchain,” a record (or ledger) of  
23 every transaction ever conducted that is distributed throughout the computer network (as  
24 opposed to being maintained by any single administrator or entity). As to bitcoins, although  
25 the public addresses of those engaging in virtual currency transactions are recorded on a  
26 blockchain, the identities of the individuals or entities behind the public addresses are not  
27 recorded on these public ledgers. If, however, an individual or entity is linked to a public  
28 address, it may be possible to determine what transactions were conducted by that individual

1 or entity. Bitcoin transactions are therefore sometimes described as “pseudonymous,”  
2 meaning that they are partially anonymous.

3 16. Virtual currency users typically employ a “wallet,” a tool that can be used to  
4 manage public and private keys, interface with a blockchain, and to send or receive virtual  
5 currency. Wallets vary widely in terms of their format and technological sophistication.  
6 One variety, known as “hosted” (or “custodial”) wallets, are virtual currency wallets  
7 controlled by a third-party—often, a company with a cloud-based, encrypted wallet platform  
8 that may be hosted on the company’s servers. Users of hosted wallets may be able to access  
9 the company’s platform through various digital devices, much like a traditional online  
10 banking experience. Hosted wallet providers include virtual currency exchanges, which  
11 allow their customers, for a fee, to exchange virtual currency for other virtual currencies  
12 and/or fiat currencies.

13 17. A more detailed description of virtual currencies, blockchains, and law  
14 enforcement techniques for investigating virtual currency transactions, is included below.

15 **STATEMENT OF PROBABLE CAUSE**

16 **A. Summary of Investigation**

17 18. The FBI is investigating whether two Estonian residents, IVAN TURYGIN<sup>2</sup>  
18 and SERGEI POTAPENKO, illegally operated a Ponzi scheme, in violation of 18 U.S.C. §  
19 1343, by fraudulently inducing individuals to invest in cryptocurrency mining.

20 19. Individuals can earn cryptocurrency by engaging in mining, which involves  
21 using computing power to solve a complicated algorithm to verify and record payments on  
22 the blockchain. Individuals are rewarded for this task by receiving newly created units of a  
23 cryptocurrency. Cryptocurrency mining typically involves the use of high-powered  
24 computers and the expenditure of large amounts of electricity.

25 20. HASHFLARE LP (“HASHFLARE”), incorporated in the UK and based in  
26 Estonia, claimed that it was engaged in cloud mining, using a cloud-based platform to mine  
27

28 \_\_\_\_\_  
<sup>2</sup> IVAN TURYGIN’s name is also spelled Ivan Turögin.

1 Bitcoin and alternative cryptocurrency coins. HASHCOINS OU (“HASHCOINS”),  
2 incorporated and based in Estonia, assisted HASHFLARE in this endeavor, providing  
3 technical support, development and marketing of HASHFLARE and its subdomains. In  
4 exchange for a monetary investment, individuals were told that they would receive a portion  
5 of the mining proceeds.

6 21. In July 2018, HASHFLARE stopped paying investors annual returns, claiming  
7 that cryptocurrency mining was no longer profitable. According to its terms of service,  
8 HASHFLARE informed investors that it would stop cryptocurrency mining “if the  
9 Maintenance and Electricity Fees [are] larger than the Payout.” Specifically, according to  
10 HASHFLARE’s terms, “If mining remains unprofitable for 21 consecutive days the Service  
11 is permanently terminated . . . [and] Payouts and Fees will also be temporarily stopped.”

12 22. Investors contend that, at the time HASHFLARE terminated its services,  
13 cryptocurrency mining was, in fact, profitable. After mining was terminated, investors,  
14 including those located in the United States, began identifying red flags which led them to  
15 believe that HASHFLARE was a Ponzi scheme that was not engaged in cryptocurrency  
16 mining.

17 23. In June 2019, Estonia’s Cyber Crime Bureau notified the FBI that it was  
18 investigating whether IVAN TURYGIN and SERGEI POTAPENKO were operating a Ponzi  
19 scheme. As of June 20, 2019, the Estonian authorities identified approximately \$120  
20 million<sup>3</sup> in losses sustained by HASHFLARE investors.

## 21 **B. HASHFLARE & HASHCOINS**

### 22 **a. Incorporation and Ownership**

23 24. HASHFLARE and HASHCOINS were incorporated in Estonia and the United  
24 Kingdom on the dates listed in the below chart.

25  
26  
27  
28  

---

<sup>3</sup> In this Affidavit, all references to \$ refer to US Dollars.

Date	Corporate Name	Country	Legal Form	Directors or Beneficial Owners	Current Name	Prior Names
6/13/13	HASHCOINS OU	Estonia	Private Limited Company	TURYGIN & POTAPENKO	Burfa Tech OU	N/A
11/26/14	HASHCOINS TRADE OU	Estonia	Private Limited Company	TURYGIN & POTAPENKO	Burfa Trade OU	N/A
12/14/15	HASHFLARE LP	UK	Limited Partnership	Malter Capital LTD & MS-Proxy Services LTD	HASHFLARE LP	Fast Consult Trade LP & HASHCOINS LP

25. HASHFLARE maintained the website hashflare.io, while HASHCOINS maintained the website www.hashcoins.com. According to HASHCOINS' and HASHFLARE's websites, POTAPENKO was identified as a co-founder and CEO of the entities. According to public reporting, TURYGIN was a co-founder and Business Development Chairman of HASHCOINS. TURYGIN was also identified as a co-founder of HASHFLARE.

**b. Business Operations**

26. Beginning on or before April 18, 2015, HASHFLARE offered cloud mining services on its website. According to its website, HASHFLARE advertised the following: "Our service makes cryptocurrency mining available to every user. You no longer need to buy expensive equipment and spend your time setting up miners. Just select your desired capacity and earn income!" On another portion of its website, HASHFLARE advertised that "Cloud mining offers a unique option for mining with a low cost of entry as well as minimal risk and expense, which is opposite to traditional models of mining that involve procurement, maintenance and configuration of highly specialized software."

27. HASHFLARE advertised that it conducted this mining in collaboration with HASHCOINS. On its website, HASHFLARE explained that it offered "a new range of cloudmining services brought to you by the HASHCOINS team of cryptomining experts." In turn, on its website, HASHCOINS claimed that it was "an Estonian based cryptocurrency

1 mining hardware manufacturer and cloud hosted mining service provider.” HASHCOINS  
2 advertised that its users could purchase cloud mining contracts from HASHFLARE, claiming  
3 that HASHFLARE users could mine cryptocurrency using HASHCOINS’ datacenters. In its  
4 terms of service, HASHFLARE stated that “HASHCOINS OU provides technical support,  
5 development and marketing of HASHFLARE and its subdomains.”

6 28. HASHFLARE sold cloud mining contracts, allowing users to mine  
7 cryptocurrency through HASHFLARE in exchange for a return. On its website,  
8 HASHFLARE explained that a user could “purchas[e] part of the mining power of hardware  
9 hosted and owned by a Cloud Mining services provider,” which “configur[es] the hardware,  
10 maintain[s] uptime and select[s] the most efficient and reliable [mining] pools.” For  
11 example, on April 18, 2015, for \$9.95, a user could buy one million hashrate (“one million  
12 hash per second” or “1 MH/s”) from HASHFLARE. For this rate, HASHFLARE advertised  
13 a “100% Scrypt Miner,” automatic accruals in Bitcoin, and a daily maintenance fee of \$0.01  
14 per 1/MH/s.

15 29. HASHFLARE’s website advertised a tool that could be used to calculate the  
16 approximate amount of profit a user would get depending on the amount of hashrate the user  
17 purchased. The user would then have the option to automatically reinvest that profit or  
18 withdraw the profit if their balance was above a certain minimum threshold, which fluctuated  
19 between 0.5 bitcoin to 0.01 bitcoin throughout the existence and operation of HASHFLARE.

20 30. In addition to earning funds through cloud mining, HASHFLARE users also  
21 earned funds by recruiting others to purchase HASHFLARE contracts. HASHFLARE  
22 advertised a referral program, informing users that “as a referrer, you are eligible to receive  
23 10% referral commission bonus for every purchase made by any of your referrals, excluding  
24 reinvest and balance purchases.” As a result, HASHFLARE users could make money each  
25 time one of their referred friends, family members or acquaintances purchased cloud mining  
26 contracts.

27 31. A number of individuals, including those operating in the Western District of  
28 Washington purchased mining contracts from HASHFLARE. According to financial records



1 | obtained from Fedwire, a funds transfer system operated by the United States Federal  
2 | Reserve Banks, at least \$2.5 million was transferred to accounts held by HASHCOINS for  
3 | what appear to be investments in HASHFLARE (examples of descriptions accompanying the  
4 | transfer of money were: “HASHFLARE.io Invoice...”; “Investments...”; and “...payment  
5 | for mining services”).

6 |       32. According to bank records obtained from Latvia, approximately \$11 million  
7 | was transferred into an account held by HASHFLARE at Latvijas Pasta Banka. These  
8 | transfers were made in the names of various individuals, and often referenced the terms  
9 | “Invoice” and “Hashrate.” As a result, I believe that these payments were also made to  
10 | purchase cloud mining contracts from HASHFLARE. For example, on January 31, 2017,  
11 | F.R.E. transferred \$1,708 to HASHFLARE’s account, referencing “Invoice 593395  
12 | Hashflare.io SHA-256 HASHRATE 15.” Similarly, on March 6, 2017, A.K. transferred  
13 | \$5,792.72 to HASHFLARE’s account, referencing “Invoice .673156 (60TH/S SHA-256  
14 | hashrate).

15 |       33. Additionally, according to information obtained from a group of approximately  
16 | 800 investors, a representative of which contacted law enforcement, between initial  
17 | investments and re-investments of stated profits, they invested a total of \$7.5 million. It was  
18 | not readily apparent how much of the \$7.5 million was contained within the amounts  
19 | previously mentioned above.

20 |       34. A search of email accounts affiliated with HASHFLARE and HASHCOINS  
21 | revealed a bank statement, with a date range from January 1, 2017 through September 21,  
22 | 2018, showing approximately \$120 million of deposits into a bank account with the account  
23 | owner name of “Hashflare LP”. The description of most of the deposits was: “Payment from  
24 | VISA/Mastercard, card processing dd...” A substantial amount of the deposits stopped in or  
25 | around June of 2018. Based on the same email account review, I know the statements  
26 | related to a main bank account that received deposits from users of the mining services.

1                   **c. Collapse of Mining Operations**

2           35.    In or around August of 2017, HASHFLARE made a number of changes to its  
3 operations. For example, HASHFLARE changed its terms of service that shortened the  
4 length of all Bitcoin mining contracts from “lifetime” contracts to “one year” contracts.  
5 Functionally speaking, under lifetime contracts purchased hashrates did not expire, whereas  
6 under the new term the purchased hashrates expired after one year, requiring users to buy  
7 additional contracts.

8           36.    In or around July 2018, HASHFLARE also required all users to submit “Know  
9 Your Customer” identification before they could continue using services offered on the  
10 platform. In effect, these additional procedures reduced the ability of users to withdraw  
11 funds earned through mining. On online forums, users complained that, even after they  
12 submitted the necessary documentation, HASHFLARE was taking weeks or months to verify  
13 their identities and pay balances. Other users complained that they never received their  
14 requested balances.

15           37.    Finally, on July 20, 2018, HASHFLARE announced that Bitcoin mining had  
16 been unprofitable for 28 days as of July 18, 2018 and, per clause 5.5 of its Terms of Service,  
17 all Bitcoin mining SHA-256 contracts were suspended. According to its terms of service,  
18 HASHFLARE informed investors that it would stop cryptocurrency mining “if the  
19 Maintenance and Electricity Fees [are] larger than the Payout.” Specifically, according to  
20 HASHFLARE’s terms, “If mining remains unprofitable for 21 consecutive days the Service  
21 is permanently terminated . . . [and] Payouts and Fees will also be temporarily stopped.”

22           38.    One week later, on July 27, 2018, HASHFLARE informed the public that  
23 SHA-256 would resume on July 28, 2018. However, a review of archived copies of the  
24 HASHFLARE website showed SHA-256 mining contract remained “Out of Stock” over a  
25 year later.

26           39.    Furthermore, interviews of three HASHFLARE investors, F.M., B.J., and  
27 F.W., revealed that it was not possible to make any withdrawals once the Bitcoin mining  
28 contracts were suspended, which held true through the dates of the interviews that took place

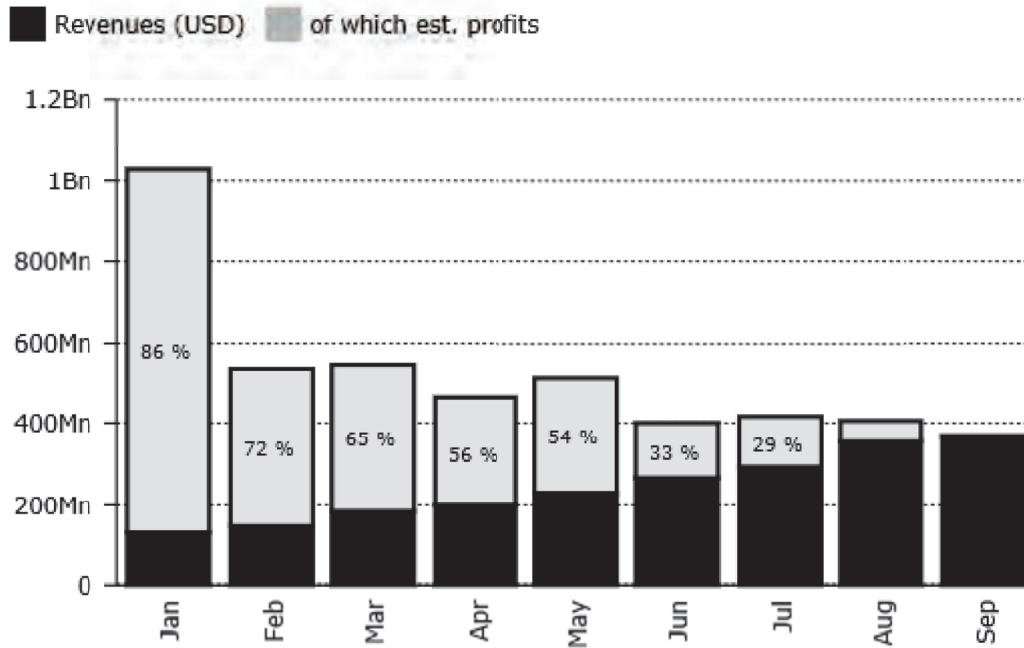
1 in or around September of 2019. Since then, there has been no indication from known  
2 victims that any of the money invested was recoverable from HASHFLARE.

3 40. Since HASHFLARE suspended its contracts, investors, including those located  
4 in the United States, began identifying red flags which led them to believe that  
5 HASHFLARE was a Ponzi scheme that was not engaged in cryptocurrency mining. Instead,  
6 they believed that HASHFLARE was profiting on fluctuations in cryptocurrency exchange  
7 rates, using those gains and new investment proceeds to repay earlier investors. For  
8 example, investors visited HASHFLARE's business address in Estonia, which did not appear  
9 to house a server farm or computing equipment consistent with cryptocurrency mining.  
10 Additionally, according to these investors, the rates charged by HASHFLARE for  
11 maintenance and electricity were above market average, and pools that were used to mine  
12 did not produce the expected output.

13 41. Diar, which publishes a digital assets and regulations newsletter, reported that  
14 while bitcoin mining was profitable for the first six months of 2018, with 2018 revenues  
15 exceeding 2017 revenues by \$1.4 billion, as of the end of August and the beginning of  
16 September, bitcoin mining was becoming unprofitable.<sup>4</sup> According to Diar, increases in  
17 electricity costs and mining difficulty (increased hashrate) have led to this unprofitability.  
18 For example, a chart compiled by Dial is referenced below:

19  
20  
21  
22  
23  
24  
25  
26  
27  
28 <sup>4</sup> Diar, *Bitcoin Miner Revenues Near \$5 Billion but Profitability Dwindles*, Volume 2, Issue 40, (Oct. 8, 2018), available  
at <https://diar.co/volume-2-issue-40/>.

**2018: Miners Paying Retail Electricity Prices Now Unprofitable...**



**Notes:** Profit Estimates Using S9 Miners & \$0.1/kWh, No Pool Fees or Hardware Costs. The chart is illustrates profits if all miners paid retail electricity prices.

42. While Diar projected that mining did not become unprofitable until late August and early September 2018, HASHFLARE contended that its mining operations became unprofitable in late June 2018. However, HASHFLARE’s operations may be more costly than those profiled by Diar, which did not take pool fees or hardware costs into account. HASHFLARE’s terms of service provide that users must pay the following maintenance fees: “hardware setup, data center rent, Mining Pool testing, staff salaries, future planning and proofing, software development, exchange of used and out of order parts and other expenditures required to render the service on a best-effort basis.”

43. Estonian authorities analyzed 22,935 transfer chains related to HASHFLARE payout wallets to determine if payouts to investors were coming from mining pools, which would be the expected source of payouts. Based on their analysis, most of the payouts came from the wallets where Bitcoin deposits were received, and only 0.8% of payouts came from

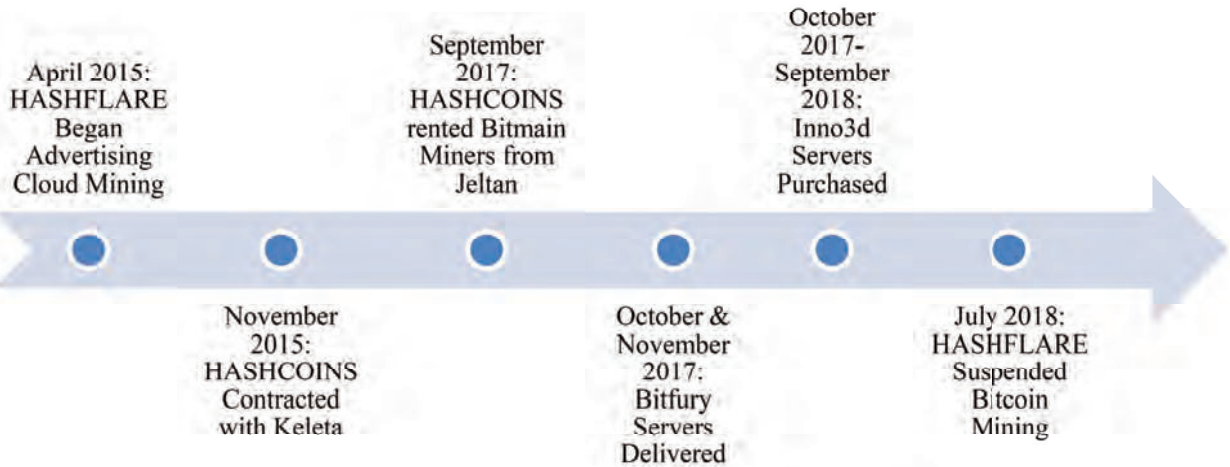
1 mining pools. As a result, it appears that HASHFLARE may not have been engaged in  
2 substantial cryptocurrency mining, as previously advertised.

3 **d. HASHFLARE's and HASHCOINS' Cloud Mining Capabilities**

4 44. The FBI has been investigating whether HASHFLARE and HASHCOINS  
5 possessed sufficient mining equipment to service the contracts that had been purchased. On  
6 its website, HASHFLARE claims that, when the company began in 2015, it conducted cloud  
7 mining using equipment obtained from HASHCOINS. As referenced above, investors  
8 questioned whether HASHCOINS had the capability to mine cryptocurrency, since they did  
9 not appear to have a large server location (or at least none was found).

10 45. Additionally, in 2014, HASHCOINS initially sold mining equipment, to be  
11 operated by the purchasing user. However, during that time frame, HASHCOINS claimed  
12 that it experienced supply disruptions, frustrating its ability to supply Bitcoin mining  
13 equipment. As a result, HASHCOINS offered its customers the opportunity to invest in  
14 HASHFLARE's cloud mining services, instead. Investors questioned whether this transition  
15 was intentional, to ensure that additional investors sent funds to HASHFLARE, and whether  
16 HASHCOINS had the ability to produce cloud mining equipment.

17 46. Law enforcement has reviewed various financial records, along with email  
18 records, to determine what cloud mining resources were purchased by HASHFLARE. Based  
19 on these records, it appears that, at various times, HASHCOINS or HASHFLARE contracted  
20 with Keleta UAB, Bitmain, Bitfury, and Inno3d vendors to provide cloud mining services.  
21 These services at described below and depicted in the following visual chart.



47. In 2015, it appears that HASHCOINS entered into a Mining Hardware Rent Agreement with a Lithuanian company named Keleta UAB. Specifically, on October 31, 2015, HASHCOINS entered into a contract with Keleta UAB for the purpose of renting SHA-256 Protocol cryptocurrency mining hardware. Pursuant to the terms of this contract, over the course of one year, HASHCOINS obtained € 600,000 worth of hashrate. The service was set to start on November 1, 2015. A further search of the email accounts provided a HASHCOINS bank statement, with a date range of January 1, 2015 through February 24, 2017, showing that HASHCOINS transferred \$575,000 to Keleta UAB. Attached to certain email were six invoices, issued from Keleta UAB to HASHCOINS, which totaled € 575,000.

48. Of note, there is no publicly available information regarding Keleta UAB that confirms that this company actually provides mining hardware. According to public databases, the address listed on the cryptocurrency mining contract for Keleta UAB also serves as the registered address for numerous other Lithuanian companies. Based on my training and experience, and information gained during the course of this investigation, I know that incorporation companies often register multiple companies, including shell companies, using the same business address.

49. In 2017, HASHFLARE and HASHCOINS entered into contracts with Bitmain, Bitfury, and Inno3d cloud mining vendors. This is consistent with HASHFLARE's website, where beginning on or before June 4, 2018, HASHFLARE advertised, albeit in broken

1 English, that it uses “equipment for mining” obtained from “Bitmain, Bitfury, Inno3d, and  
2 others.” Bitmain, Bitfury, and Inno3d each manufacture cryptocurrency mining equipment.  
3 Because of the broken English, it is difficult to determine when HASHFLARE started using  
4 mining equipment supplied by these companies, but it appears that HASHFLARE advertised  
5 that it acquired this equipment in 2016.<sup>5</sup>

6 50. While law enforcement has not identified evidence that HASHFLARE  
7 purchased mining equipment from Bitmain, Bitfury, or Inno3d in 2016, it has located  
8 evidence that a limited amount of funds was transferred to these vendors in 2017, during the  
9 final months of HASHCOINS’ and HASHFLARE’s operations.

10 51. First, according to an email sent to TURYGIN, on September 1, 2017,  
11 HASHCOINS entered into a contract with a UK company named Jeltan Trading LP for the  
12 purpose of renting Bitmain Antminer L3+ hardware. Pursuant to the terms of this contract,  
13 HASHCOINS purchased \$1,000,000 worth of hashrate over the course of a year. According  
14 to bank records HASHCOINS transferred € 918,000 to Jeltan Trading LP between  
15 September 19, 2017, and November 13, 2017.

16 52. Of note, there is no publicly available information regarding Jeltan Trading LP  
17 that confirms that this company actually owns or rents mining hardware. According to  
18 public databases, the address listed on the cryptocurrency mining contract for Jeltan Trading  
19 LP also serves as the registered address for numerous other UK companies. Based on my  
20 training and experience, and information gained during the course of this investigation, I  
21 know that incorporation companies often register multiple companies, including shell  
22 companies, using the same business address.

23 53. Second, according to information obtained from Bitfury, on August 3, 2017,  
24 Bitfury entered into an agreement to sell HASHCOINS ten “Bitfury B8 server[s] with  
25 proprietary BitFury hardware (16 nm) capable of producing up to 43 TH/s (±5%) of SHA  
26

---

27 <sup>5</sup> The language states: “HashFlare is a cloud mining service created by the specialists from HashCoins in 2015. In a short  
28 time, HashFlare became one of the largest providers of computational power for mining bitcoin, litecoin, ethereum and  
other cryptocurrencies. From 2016, HashFlare is an independent company. The variety of equipment that is used for  
mining was significantly increased on the account such companies as Bitmain, Bitfury, Inno3d and others.”

1 256 hashing power ('Hashing Power') and consuming 6.4 KW ( $\pm 5\%$ ) of electricity" for  
2 \$52,000. Additionally, on September 25, 2017, Bitfury entered into a contract to sell  
3 HASHCOINS 462 "Bitfury Europe configured B8 server[s] with proprietary Bitfury  
4 hardware (16 nm) capable of producing up to 43 TH/s ( $\pm 5\%$ ) of SHA 256 hashing power  
5 ('Hashing Power') and consuming 6.4 KW ( $\pm 5\%$ ) of electricity." In exchange for these  
6 servers, HASHCOINS paid Bitfury \$984,984.<sup>6</sup> Records from Bitfury show that shipments  
7 of these servers were made on October 16, 2017 and November 21, 2017. A review of  
8 emails between HASHCOINS and a representative of the Borealis Data Center (the final  
9 destination of the equipment), showed that the equipment was still in transit as of December  
10 4, 2017.

11 54. Furthermore, on October 12, 2017, TURYGIN and a HASHCOINS  
12 representative exchanged emails with a Bitfury representative, discussing a "4M order next  
13 week right after IM." The HASHCOINS representative explained that "the 4M order is . . .  
14 not yet confirmed." Based on the context of this email, I believe 4M to refer to 4 Megawatts.  
15 I have seen no evidence suggesting that such a large purchase was completed, which would  
16 likely amount to nearly \$4 million (the first round of purchases from BitFury resulted in 1  
17 Megawatt of equipment being purchased for approximately \$1 million). Rather, according to  
18 banking records obtained to date,<sup>7</sup> HASHCOINS first transferred funds to Bitfury on August  
19 14, 2017, with another transfer of funds occurring on October 4, 2017. These funds transfers  
20 were consistent with the amounts identified in the above-mentioned contracts.

21 55. Thirdly, bank statements for both HASHCOINS and Burfa Media show that,  
22 between October of 2017 and September of 2018, approximately \$13 million was transferred  
23 to ASK Technology, which sells Inno3d-branded products. A search of email accounts  
24 belonging to Burfa Media personnel contained a summary of 23 invoices due to ASK  
25 Technology Group Limited, which totaled approximately € 16 million. Based on the  
26

27 <sup>6</sup> Bitfury also entered into subsequent agreements, in 2018, to sell equipment to HASHCOINS' successor, BURFA  
28 MEDIA OU.

<sup>7</sup> The FBI is continuing to gather financial information related to this case and has, so far, obtained records from Latvia,  
Estonia, and the United States relating to HASHFLARE and HASHCOINS, among other entities.



1 | discrepancy between payments made to ASK Technology and the invoice totals that were  
2 | compiled by Burfa Media, the amount of product purchased from ASK Technology was  
3 | unclear.

4 |         56. In addition to Bitfury, Bitmain, and Inno3d, law enforcement has identified  
5 | evidence suggesting that payments were made to other cryptocurrency mining providers.

6 |         57. For example, in January 2018, HASHCOINS transferred € 79,415.87 to BDC  
7 | Mining EHF. According to publicly available information, BDC Mining EHF is based in  
8 | Iceland.

9 |         58. Additionally, HASHFLARE transferred funds to Dalmeron Projects for “SHA-  
10 | 256” and “According to a Computational Power Rent Agreement from 16.02.2018.”

11 | According to documents located in email accounts used by HASHFLARE and HASHCOINS  
12 | personnel, Anatoli Sheipak serves as the “ultimate beneficial owner” of Dalmeron Projects.

13 | However, for the following reasons, it appears that the owners of HASHFLARE and  
14 | HASHCOINS are the true beneficial owners of Dalmeron Projects. First, on August 1, 2017,  
15 | TURYGIN emailed an incorporation company, requesting that a related company, Dalmeron  
16 | Invest, be incorporated, listing Anatoli Sheipak as the director and owner of the entity.

17 | Additionally, on a document dated August 31, 2017 and entitled “MINING HARDWARE  
18 | RENT AGREEMENT – AMENDMENT 1,” between HASHCOINS and Dalmeron Projects,  
19 | LP, the signatory for Dalmeron Projects was TURYGIN. Also, on October 26, 2017,

20 | GoDaddy sent POTAPENKO an email recommending that he renew the domain registration  
21 | for dalmeron.com. Anatoli Sheipak was also listed as the sole subscriber for

22 | HASHFLARE’s Microsoft account, suggesting that he is affiliated with HASHFLARE.

23 | And, finally, TURYGIN’s email account, turygin@gmail.com, is linked by cookies to  
24 | dalmeronprojects@gmail.com. Accordingly, based on my training and experience, and  
25 | information gained during the course of this investigation, I believe that Dalmeron Projects is  
26 | a subsidiary or is otherwise associated with HASHFLARE and HASHCOINS, rather than an  
27 | independent company providing cloud mining services.

1           59.     Similar to Dalmeron Projects, HASHCOINS transferred funds to another  
2 company named Ecohouse Networks LP, for “Computation power rent SHA-256(GH/s)”,  
3 according to invoices dated as early as January of 2016, which were located in email  
4 accounts used by HASHFLARE and HASHCOINS personnel. However, on January 18,  
5 2017, a bank application was sent via email by the representative of a payment processing  
6 company to TURYGIN, asking TURYGIN to see if the attached application was accurate.  
7 The bank application named Ecohouse Networks LP as the customer and named TURYGIN  
8 as the payment card user and sole beneficial owner. Additionally, a “HARDWARE LEASE  
9 CONTRACT” contract dated July 15, 2015, named HASHCOINS as the Tenant, represented  
10 by POTAPENKO, and Ecohouse Networks LP as the Lessor, represented by TURYGIN; the  
11 contract was not executed by either party. Accordingly, based on my training and  
12 experience, and information gained during the course of this investigation, I believe that  
13 Ecohouse Networks LP is a subsidiary or is otherwise associated with HASHFLARE and  
14 HASHCOINS, rather than an independent company providing cloud mining services.

15           60.     As described above, HASHCOINS and HASHFLARE began purchasing or  
16 renting cryptocurrency mining equipment from third parties in November 2015, with the  
17 bulk of their purchases occurring in the final months of their operations (September 2017  
18 through June 2018). Based on financial records analyzed to date, users appeared to have  
19 begun transferring funds to HASHCOINS’ bank accounts to purchase HASHFLARE mining  
20 contracts in or before November 2015. For example, on November 29, 2015, a transfer was  
21 made to an account held by HASHCOINS TRADE OU with the accompanying description:  
22 “Invoice #32789 ivanovdmi3i@list.ru HashFlare.io SHA-256 hashrate 300GH/s.” These  
23 transfers were made before any known delivery of mining equipment was made by these  
24 vendors to HASHFLARE or HASHCOINS. Based on the above, the FBI is investigating  
25 whether HASHFLARE was soliciting and collecting investments for services it was not yet  
26 able to sufficiently perform.

1           61.     Additionally, since neither Jeltan Trading LP nor Keleta UAB have any  
2 appreciable public presence online, the FBI is also investigating whether those entities are  
3 legitimate, providing actual services to HASHFLARE or HASHCOINS.

4           62.     Between at least August 2017 through June 2018, HASHFLARE and  
5 HASHCOINS had collectively transferred more than € 74 million to CryptoPay Ltd., a UK  
6 company that sells Bitcoin, purchases Bitcoin in exchange for fiat currency, and sells cards  
7 that can be loaded with cryptocurrency. For example, on August 7, 2017, HASHFLARE  
8 transferred € 250,000 to CryptoPay Ltd. for “digital assets purchase.” Again, on August 14,  
9 2017, HASHFLARE transferred an additional € 250,000 for “digital assets purchase.” These  
10 payments continued through at least June 15, 2018, when HASHFLARE transferred €  
11 2,000,000, also for “digital assets purchase.” Based on these purchases, and the payment  
12 references, the FBI is investigating whether HASHFLARE was paying its investors using  
13 bitcoins purchased from CryptoPay, rather than mining bitcoins as advertised.

14           63.     Furthermore, based on my training and experience, and information gained  
15 during the course of this investigation, I know that Ponzi schemes operate by recruiting  
16 others, paying earlier investors with funds transferred by later investors. Ponzi schemes  
17 often involve recruitment bonuses, incentivizing earlier investors to recruit friends and  
18 family members so that funds are available to pay earlier members. As described above,  
19 HASHFLARE advertised a referral program, paying earlier investors 10% bonuses based on  
20 cloud mining contracts purchased by those they referred.

21           64.     HASHFLARE and HASHCOINS have stopped selling any mining contracts  
22 and, as described below, its founders and employees appear to have moved to successor  
23 companies that continue to operate in the cryptocurrency space. Prior investors have not  
24 been able to recoup their funds and many have been unable to transfer funds held in their  
25 accounts.

26           65.     On December 29, 2020, an Estonian news company “DV” published an article  
27 describing a police investigation of POTAPENKO and TURYGIN. The article provided, in  
28

1 part, that POTAPENKO and TURYGIN were being investigated for fraud that was  
2 facilitated through HASHFLARE's purported cloud-mining operations.

3 66. As part of this article, TURYGIN wrote to DV asserting that a Scottish firm,  
4 Fast Consult LP, bought the HASHFLARE cloud-mining operations in March 2016.  
5 According to TURYGIN, Fast Consult LP renamed itself to HASHCOINS LP, and later  
6 HASHFLARE. TURYGIN explained that HASHCOINS, a company he and POTAPENKO  
7 own, but which was distinguishable from HASHCOINS LP, which TURYGIN and  
8 POTAPENKO did not own, provided IT services and technical support to HASHFLARE for  
9 two years after its sale.

10 67. On December 31, 2020, TURYGIN published his own article in DV in  
11 response to the December 29, 2020, article, further claiming that HASHCOINS TRADE OU  
12 assisted HASHCOINS LP with accepting funds until the Fall of 2016, but after that  
13 HASHCOINS LP began to independently accept its own funds into their own accounts.

14 68. TURYGIN's assertions are not supported by the evidence gathered to date in  
15 this investigation. For example, an E-shop Agreement for payment card acceptance was  
16 signed by TURYGIN on or around May 24, 2017, which named IVAN TUROGIN as the  
17 authorized representative of HASHCOINS LP. According to the terms of the agreement,  
18 reports would be sent to the email address sergei@hashcoins.com, associated with  
19 POTAPENKO. The E-shop Agreement also provided that, while the legal address for  
20 HASHCOINS LP was listed as 44/46 Morningside Road, Suite 3, Edinburgh, EH10 4BF,  
21 Scotland, United Kingdom, the actual address provided was Tartu Mnt 43, 10128 Estonia –  
22 the address utilized by Burfa, HASHCOINS, and Polybius, as well as TURYGIN's own  
23 Apple registration address. Furthermore, in an email dated January 30, 2017, POTAPENKO  
24 explained to the representative of a payment processing company that HASHCOINS LP  
25 operates in Estonia and not the United Kingdom.

26 69. I submit there is probable cause to believe HASHFLARE and HASHCOINS  
27 operated as a Ponzi scheme for at least the following reasons: (1) before its collapse,  
28 HASHFLARE appears to have been in financial distress, as evidenced by its unilateral

1 conversion of mining contracts from lifetime contracts to year-long contracts, its use of KYC  
2 requirements to delay users' withdrawal of funds from their accounts, and its termination of  
3 mining contracts during a time when industry press considered bitcoin mining to be  
4 profitable; (2) HASHCOINS' questionable ability to manufacture cryptocurrency mining  
5 equipment, as evidenced by its 2014 decision to not fulfill equipment orders and instead  
6 convert purchase contracts to HASHFLARE cloud mining contracts; (3) Estonian law  
7 enforcement's analysis that HASHFLARE wasn't receiving substantial payouts from mining  
8 pools, sufficient to pay its investors; (4) HASHFLARE's apparent purchase of "digital  
9 assets" from CryptoPay, which, among other items, sells Bitcoin, suggesting that  
10 HASHFLARE may be purchasing cryptocurrency rather than mining it; (5) HASHFLARE's  
11 inherent structure, including its referral program and lack of transparency regarding its  
12 mining pools, which is a common structure evidenced in Ponzi schemes; (6) TURYGIN's  
13 public attempt to mask true ownership of the now-defunct cloud-mining company; and (7) as  
14 described in further detail below, HASHFLARE's dissolution and the subsequent transition  
15 of its employees and co-founders, who joined new companies that continue to operate in the  
16 cryptocurrency space.

17 **C. Other Linked Entities**

18 **a. BURFA Entities**

19 70. After HASHFLARE terminated its mining contracts, HASHCOINS OU  
20 changed its legal name to Burfa Tech OU and HASHCOINS TRADE OU changed its name  
21 to Burfa Trade OU. As described below, a number of HASHCOINS and HASHFLARE  
22 employees then transferred and started working for these entities.

23 71. Burfa Tech OU and Burfa Trade OU are part of a conglomerate formed by  
24 TURYGIN and POTAPENKO, under the umbrella company Burfa Capital OU, incorporated  
25 in Estonia (collectively called the "BURFA Entities"). These entities are described below:  
26  
27  
28

Date	Corporate Name	Country	Legal Form	Directors or Beneficial Owners	Prior Names
7/12/13	Burfa Capital OU	Estonia	Private Limited Company	TURYGIN & POTAPENKO	Starfix UU
6/27/13	Burfa Media OU	Estonia	Private Limited Company	TURYGIN & POTAPENKO	N/A
7/17/17	Burfa Real Estate OU	Estonia	Private Limited Company	Pavel Ivanov	Burfa Estate OU
6/13/13	Burfa Tech OU	Estonia	Private Limited Company	TURYGIN & POTAPENKO	HASHCOINS OU, Euro Host UU
11/26/14	Burfa Trade OU	Estonia	Private Limited Company	TURYGIN & POTAPENKO	HASHCOINS Trade OU, Habalink UU
6/27/13	Burfa Invest OU	Estonia	Private Limited Company	TURYGIN & POTAPENKO	N/A

72. According to the website for Burfa Capital, burfa.com, the various entities have the following missions:

- a. Burfa Capital OU “is a commercial organization . . . emphasizing collaboration and investment in such priority areas as IT, fintech and data processing.” Burfa Capital OU appears to be the parent corporation in the BURFA Entities conglomerate.
- b. Burfa Media OU “provides computing equipment for processing large data arrays and for any operations that require significant computing power.”
- c. Burfa Real Estate OU “is engaged in the construction of commercial and residential luxury real estate in Estonia . . . for the subsequent sale or rent.”
- d. Burfa Tech OU is reported to be “a leader in the field of data center design and maintenance for the industrial sector . . . specializ[ing] in high-performance computing and turnkey data center solutions.” Like HASHCOINS, Burfa Tech OU is reported publicly to be “an IT company operating in Estonia mainly in the field of equipment for cryptocurrency mining.”
- e. Burfa Trade OU “is engaged in the wholesale trade of timber materials.”

1 f. Burfa Invest OU “is a globally recognized brand with three main vectors  
2 of development”—trade, real estate, and construction.

3 73. As described in the chart below, a number of the individuals employed by the  
4 BURFA Entities appear to have been formerly employed by HASHCOINS or  
5 HASHFLARE.

Name	Role in HASHCOINS or HASHFLARE	Role in BURFA Entities
SERGEI POTAPENKO	Co-Founder and CEO of HASHFLARE and HASHCOINS	Board Member & Co-Founder of Burfa Capital OU
IVAN TURYGIN	Co-founder of HASHFLARE and HASHCOINS	Board Member & Co-Founder of Burfa Capital OU
Nikolay Pavlovskiy	Chief Technology Officer of HASHCOINS, Vice President and Head of Business Development at HASHFLARE	Chief Technology Officer for Burfa Capital OU
Vitali Pavlov	Project Manager at HASHFLARE, Chief Product Officer at HASHCOINS	Chief Product Officer at Burfa Tech OU
Vadim Tsvetikov	Associated with HASHCOINS, as described above	Data Center Operation Director for Burfa Tech OU
Pavel Tsihhotski	Support and Community Manager for HASHCOINS	Former Head of Support for Burfa Capital OU
Stanislav Pavlov	Associated with HASHCOINS, as described above	Former Human Resources Manager and Customer Support for Burfa Tech OU
Tatjana Potapova	Chief Financial Officer for HASHCOINS	Chief Financial Officer for Burfa Media OU
Edger Bers	Public Relations Business Development Manager for HASHCOINS	Associated with BURFA Entities—possesses @burfa.com email address

20 74. Additionally, around the time the Bitcoin mining contracts were suspended,  
21 HASHFLARE transferred substantial assets to the BURFA Entities. For example, according  
22 to bank records gathered during the course of this investigation, two different bank accounts  
23 held in the name of HASHFLARE transferred approximately \$15.5 million to a bank account  
24 in the name of Burfa Media OU throughout the year in 2018.

25 75. The @burfa.com domain was established on August 22, 2017, listing two  
26 contact email addresses—admin@burfa.com and sergei@hashcoins.com (associated with  
27 POTAPENKO).  
28

**b. POLYBIUS**

76. In addition to HASHCOINS, HASHFLARE, and the BURFA Entities, TURYGIN and POTAPENKO have also formed a second conglomerate, comprised of four entities—Polybius Foundation OU, Polybius Tech OU, Polybius Ventures OU, and Polybius Fintech MidCo OU (collectively, referred to as “POLYBIUS”).

77. Each of these entities was incorporated in Estonia, as listed below:

Date	Corporate Name	Country	Legal Form	Directors or Beneficial Owners
2/13/17	Polybius Foundation OU	Estonia	Private Limited Company	TURYGIN, POTAPENKO & Anton Altement
2/1/18	Polybius Tech OU	Estonia	Private Limited Company	TURYGIN, POTAPENKO, Anton Altement & Vadim Gerassimov
2/8/18	Polybius Ventures OU	Estonia	Private Limited Company	TURYGIN, POTAPENKO & Anton Altement
4/25/18	Polybius Fintech MidCo OU	Estonia	Private Limited Company	TURYGIN, POTAPENKO, Anton Altement & Mathieu Hardy

78. According to the website for POLYBIUS, Polybius.io, and public reporting, the various entities have the following missions:

a. Polybius Tech OU created a cryptocurrency wallet called OSOM Finance, designed to hold both Bitcoin and alternative coins.

b. Polybius Ventures OU and Polybius Fintech MidCo OU are not separately described but are both subsidiaries in the POLYBIUS ecosystem.

c. Polybius Foundation, according to its Prospectus (also known as a “Whitepaper”), is “a team of financial, security, legal and technical experts” who are raising funds to start Polybius Bank. The intent was for Polybius Bank to be a “fully digital bank accessible everywhere at any time. It will have all the functions of a classical bank, but will not host any branches, nor any physical front-offices and will rely fully on the latest digital technologies.” The front of the prospectus reads, in part: “Polybius POWERED BY HASHCOINS.”

79. According to an article written by Forbes on October 29, 2018, POLYBIUS raised approximately \$32 million dollars during its Initial Coin Offering (“ICO”) in the summer of 2017. The symbol for the POLYBIUS coins is PLBT. As of the date of the



1 | writing of the article, no tangible product had been launched. In fact, it announced that it  
2 | abandoned the prospect of opening a bank, and that it would develop a mobile app instead.

3 | 80. A cursory review of the POLYBIUS tokens was discussed in a law review  
4 | article published by the Columbia Law Review in April of 2019, entitled “Coin-Operated  
5 | Capitalism.” In the article, the authors note that a “development team can unilaterally  
6 | change the [POLYBIUS] tokens purchased by investors—or sometimes, propose changes that  
7 | will not be adopted if a certain percentage of users do not object.” The authors opine that the  
8 | latter type of proposed changes that may be detrimental to investors may automatically take  
9 | effect with no knowledge of the investor because (1) the default vote is inherently set to  
10 | “yes,” and (2) the investing public as a whole does not have the technical skills to monitor or  
11 | understand the proposed changes a development team may make to the POLYBIUS tokens.  
12 | To date, it is unknown whether any such changes occurred.

13 | 81. On November 17, 2018, POLYBIUS released a blog post announcing it was  
14 | releasing a new personal finance management service called “OSOM.” Later in 2019,  
15 | POLYBIUS released instructions about how to transfer PLBT tokens from an investor’s  
16 | POLYBIUS Wallet to their OSOM Wallet. According to POLYBIUS, transfer of the PLBT  
17 | tokens to the OSOM Wallet was important because the POLYBIUS Wallet would eventually  
18 | no longer be functioning.

19 | 82. While the American versions of Apple’s “App Store” and Google’s “Play  
20 | Store” have no results when searching for “POLYBIUS” and “OSOM,” the same search on  
21 | the United Kingdom versions shows that Polybius Tech Launched OSOM Finance in or  
22 | around October of 2019. The App Store’s version of OSOM Finance has about five reviews,  
23 | and the Play Store’s version of OSOM Finance has about 74 reviews. According to a  
24 | description of OSOM Finance, the app is advertised as an “all-in-one crypto portfolio  
25 | management app.”

26 | 83. The POLYBIUS coin is still available for purchase as of today, and both the  
27 | OSOM website and POLYBIUS website are still in existence.  
28 |

84. As with the BURFA Entities, some of the individuals employed by POLYBIUS appear to have been formerly employed by HASHCOINS or HASHFLARE or the BURFA entities. As a result, it appears that POLYBIUS is a successor entity of HASHCOINS and HASHFLARE.

Name	Role in HASHCOINS, HASHFLARE or BURFA	Role in POLYBIUS
SERGEI POTAPENKO	Co-Founder and CEO of HASHFLARE and HASHCOINS	Co-Founder of POLYBIUS
IVAN TURYGIN	Co-founder of HASHFLARE and HASHCOINS	Co-Founder of POLYBIUS
Edgar Bers	Public Relations Business Development Manager for HASHCOINS	Product Manager for POLYBIUS
Pavel Tsihhotski	Support and Community Manager for HASHCOINS	Associated with POLYBIUS (possesses @polybius.io email address)
Anton Altement	Associated with BURFA Entities (possesses @burfa.com email address)	CEO & Co-Founder of POLYBIUS
Vitali Pavlov	Project Manager at HASHFLARE, Chief Product Officer at HASHCOINS	Former Product Manager POLYBIUS

#### **D. TURYGIN and POTAPENKO's Use of Apple Services**

85. According to records obtained from Apple, POTAPENKO registered for an iCloud account on January 22, 2012. The Apple ID for this account was sergei.potapenko@gmail.com and the account is assigned DSID 624556209. The login alias for this account is sergei.potapenko@icloud.com. According to Apple, as of May 2020, POTAPENKO backed up his bookmarks, contacts, iOS Devices, iCloud Photos, Mail, Messages, and Notes using this account.<sup>8</sup> Between 2017 and 2020, POTAPENKO registered three MacBook Pros, and Apple TV, and an iPhone to this account.

86. According to records obtained from Apple, TURYGIN registered for an iCloud account on June 24, 2012. The Apple ID for this account was turygin@gmail.com and the account is assigned DSID 1931852295. According to Apple, as of May 2020, TURYGIN

<sup>8</sup> According to Apple, as of May 2020, for this account, there were no logs associated with FaceTime, iCloud, IDS Queries or Mail during the prior 25 days.

1 backed up his bookmarks, contacts, Find My Friends, iOS Devices, iCloud Drive, iCloud  
2 Photos, Notes, and Photo Stream using this account.<sup>9</sup> Between 2012 and 2018, TURYGIN  
3 registered two iPhones, two MacBook Pros, and one MacBook Air to this account.

4 87. I submit there is probable cause to search the **SUBJECT ACCOUNTS** for  
5 evidence of the HASHFLARE and HASHCOINS fraud. Specifically, there is probable  
6 cause to believe that the following types of records are maintained in these accounts.

7 88. **Stored Chat Communications:** Stored chats, including in Apple Messages,  
8 not only may contain communications related to the fraud perpetrated by HASHCOINS and  
9 HASHFLARE, but also help identify participants in those crimes, including HASHCOINS'  
10 and HASHFLARE's founders, employees, and investors. For example, HASHFLARE used  
11 group chat mechanisms, including Telegram, to recruit investors and to communicate  
12 amongst members. On December 22, 2017, HASHFLARE sent an email stating "Dear  
13 friends, . . . So how was this year with HashFlare? It was a year of exploding growth and  
14 related challenges . . . Thousands of HashFlare users already chat in our Telegram groups."  
15 HASHFLARE then provided links to English and Russian language Telegram groups.  
16 Based on my training and experience, along with information learned during the course of  
17 this investigation, I know that a user can elect to backup encrypted communications, like  
18 Telegram, onto their iCloud account. These communications may contain fraudulent  
19 statements, made to solicit investments in HASHFLARE, or may identify additional victims  
20 of HASHFLARE or HASHCOINS' fraud. Notably, POTAPENKO also had iMessages  
21 backed up to his account.

22 89. **Contacts:** Address books and contact lists may help identify both the owner  
23 of the account and locate co-conspirators, including other individuals who exercise control  
24 and influence over HASHFLARE or HASHCOINS. Additionally, these address books may  
25 identify HASHFLARE or HASHCOINS' employees, providing further evidence of these  
26 entities' internal structure. They may also identify the owners and representatives of Jeltan  
27

28 <sup>9</sup> According to Apple, as of May 2020, for this account, there were no logs associated with FaceTime, iCloud, IDS  
Queries or Mail during the prior 25 days.

1 Trading LP, Keleta UAB, and Dalmeron Projects, which would assist law enforcement in  
2 determining whether these companies are legitimate entities.

3 90. **Photos and Videos:** Similarly, HASHFLARE and HASHCOINS'  
4 representatives generated a number of videos and promotional materials. For example,  
5 HASHFLARE maintained a website, Twitter feed, YouTube account, and Facebook account,  
6 where representatives posted these photographs and videos. According to its Twitter feed,  
7 on April 19, 2018, HASHFLARE published a "trailer for a documentary about the  
8 construction of the new HashCoins computing centers in Iceland," linking to a video on  
9 YouTube. Similarly, on July 26, 2016, HASHFLARE posted the following photograph to its  
10 Twitter account, depicting a purported data center:



23 Accordingly, photographs and videos stored in the **SUBJECT ACCOUNTS** may be  
24 evidence of HASHFLARE and HASHCOINS' solicitation of investors and presentation of  
25 fraudulent statements. These photographs and videos may be stored in iCloud Photos or  
26 PhotoStream. Furthermore, cryptocurrency addresses, private keys, recovery seeds, PGP  
27 keys, and passwords are often comprised of long and complex character strings, and in my  
28 training and experience, I know that many cryptocurrency users write down or otherwise

1 record and store such items because they are too long to commit to memory. These items  
2 may be recorded in the user's photographs, in emails, in cloud document storage, in chat  
3 applications, or in other applications on electronic devices.

4       91.     **Documents:** Documents stored in the **SUBJECT ACCOUNTS** may identify  
5 the scope of HASHFLARE and HASHCOINS' criminal activity, including by recording lists  
6 of investors or identifying investment accounts. In my training and experience, I know that  
7 the commission of offenses in the manner set forth above necessarily requires the use of  
8 computers, smart phones, tablets, or other computer devices and storage media to access  
9 HASHFLARE's website, cryptocurrency exchanges and wallets, connect with and recruit  
10 investors, and engage in transfers of digital currency. I have learned, through training and  
11 experience, that individuals who engage in these types of offenses in this way also  
12 commonly use such electronic devices to keep track of investors and co-conspirators; keep  
13 records of transactions and criminal proceeds, including funds deposited at cryptocurrency  
14 exchanges; and store copies of online chats, emails, and other promotional data in cloud-  
15 based accounts. For example, documents were located in Google accounts belonging to  
16 TURYGIN and POTAPENKO, including invoices, contracts, bank statements, and other  
17 documents relevant to the fraudulent scheme under investigation. These documents may be  
18 stored in iCloud Drives or Notes.

19       92.     **Calendar Data:** Calendar data may reveal the timing and extent of criminal  
20 activity, including meetings attended by HASHFLARE and HASHCOINS' founders and  
21 travel to attend TCC promotional events. For example, according to information saved in  
22 TURYGIN and POTAPENKO's Google accounts, POTAPENKO and TURYGIN attended  
23 meetings regarding HASHFLARE, including a meeting held on November 20, 2019 to  
24 discuss HASHFLARE 2.0's Terms of Service.

25       93.     **Web History and Search Data:** Web history and search data may show when  
26 users accessed websites, HASHFLARE's social media sites, HASHFLARE's YouTube  
27 videos, or other online locations associated with HASHFLARE and HASHCOINS.  
28

1 | Additionally, web searching may identify the wallet providers used by each user to hold their  
2 | cryptocurrency.

3 |       **94. iCloud Storage and Backup:** I know that Apple’s iCloud services collect and  
4 | stores information about Apple devices registered to an iCloud account. If enabled, a user  
5 | may backup settings, app data, communications, documents, and other data stored on Apple  
6 | devices. If a device is backed up, encrypted communications, such as Telegram chats, may  
7 | be stored in an iCloud backup. For the reasons outlined above, each of these categories of  
8 | information are relevant to the crimes under investigation, and, therefore, iCloud data is also  
9 | requested. In addition, I know, based on training and experience that perpetrators maintain  
10 | copies of software programs and other applications, including, but not limited to,  
11 | cryptocurrency client and wallet files, digital signature software and related authentication  
12 | keys, as well as encryption software and related encryption keys. This data may also be  
13 | reflected in an iCloud backup. Based on my training and experience, and information gained  
14 | during the course of this investigation, I know that multiple backups, spanning a lengthy time  
15 | period, may be saved in a user’s iCloud account. Accordingly, although HASHFLARE and  
16 | HASHCOINS ceased selling mining contracts in 2018, information related to this time  
17 | period may still be stored on Apple’s servers. This is particularly true because electronic  
18 | devices, including computers and iPhones, purchased from 2012 until 2018 remain registered  
19 | to TURYGIN’s iCloud account. Additionally, electronic devices, including computers and  
20 | an iPhone, purchased from 2017 until 2018 remain registered to POTAPENKO’s iCloud  
21 | account. Additionally, more recent information may uncover the proceeds of HASHFLARE  
22 | and HASHCOINS’ fraud, the beneficial ownership of successor and associated corporations,  
23 | and efforts by POTAPENKO and TURYGIN to conceal their ownership in these entities—as  
24 | evidence by the December 31, 2020 article, referenced above.

25 |       **95.** In order to gather evidence of operations of HASHCOINS, HASHFLARE, and  
26 | other affiliated entities, including discussions of mining cryptocurrency and providing  
27 | returns to investors, the United States is seeking records from the identified Apple accounts  
28 | associated with POTAPENKO and TURYGIN.

1 96. Based on the above, there is probable cause to believe that information  
2 contained in the **SUBJECT ACCOUNTS** could reveal, among other things: (1) the plans  
3 and strategies formed by the users of the **SUBJECT ACCOUNTS** to defraud investors and  
4 customers, (2) the actions taken to execute those plans, (3) the operations and relationship  
5 between the various entities, including assets transferred between those entities; (4) the  
6 extent and capacity of mining operations at HASHCOINS and HASHFLARE; (5) the  
7 location of assets paid by investors to HASHCOINS and HASHFLARE; and (6) information  
8 on where HASHFLARE and HASHCOINS store their server data, including data on the  
9 identity and investment of each HASHFLARE subscriber. Therefore, the United States  
10 seeks records and information from Apple related to each of the **SUBJECT ACCOUNTS**.

#### 11 **BACKGROUND CONCERNING ONLINE ACCOUNTS**

12 97. As explained herein, information stored in connection with an online account  
13 may provide crucial evidence of the “who, what, why, when, where, and how” of the  
14 criminal conduct under investigation, thus enabling the United States to establish and prove  
15 each element or alternatively, to exclude the innocent from further suspicion.

16 98. In my training and experience, the information stored in connection with an  
17 online account can indicate who has used or controlled the account. This “user attribution”  
18 evidence is analogous to the search for “indicia of occupancy” while executing a search  
19 warrant at a residence. For example, communications, contacts lists, and images sent (and  
20 the data associated with the foregoing, such as date and time) may indicate who used or  
21 controlled the account at a relevant time.

22 99. Further, information maintained by the provider can show how and when the  
23 account was accessed or used. For example, as described below, providers typically log the  
24 Internet Protocol (IP) addresses from which users access the account, along with the time  
25 and date of that access. By determining the physical location associated with the logged IP  
26 addresses, investigators can understand the chronological and geographic context of the  
27 account access and use relating to the crime under investigation. This geographic and  
28 timeline information may tend to either inculcate or exculpate the account owner.

1 Additionally, information stored at the user's account may further indicate the geographic  
2 location of the account user at a particular time (e.g., location information integrated into an  
3 image or video).

4 100. Stored electronic data may provide relevant insight into the account owner's  
5 state of mind as it relates to the offense under investigation. For example, information in the  
6 account may indicate the owner's motive and intent to commit a crime (e.g., communications  
7 relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to  
8 conceal them from law enforcement).

### 9 1. Apple's Services

10 101. Apple is a United States company that produces the iPhone, iPad, and iPod  
11 Touch, all of which use the iOS operating system, and desktop and laptop computers based  
12 on the Mac OS operating system. Apple provides a variety of services that can be accessed  
13 from Apple devices or, in some cases, other devices via web browsers or mobile and desktop  
14 applications ("apps"). As described in further detail below, the services include email,  
15 instant messaging, and file storage:

16 102. Apple provides email service to its users through email addresses at the domain  
17 names mac.com, me.com, and icloud.com.

18 103. iMessage and FaceTime allow users of Apple devices to communicate in real-  
19 time. iMessage enables users of Apple devices to exchange instant messages ("iMessages")  
20 containing text, photos, videos, locations, and contacts, while FaceTime enables those users  
21 to conduct video calls.

22 104. iCloud is a file hosting, storage, and sharing service provided by Apple.  
23 iCloud can be utilized through numerous iCloud-connected services, and can also be used to  
24 store iOS device backups and data associated with third-party apps. ~~icloud~~ can be utilized to  
25 transfer data from an old device to a new device, including data derived from device backups  
26 and third-party applications.

27 105. iCloud-connected services allow users to create, store, access, share, and  
28 synchronize data on Apple devices or via icloud.com on any Internet-connected device. For



1 | example, iCloud Mail enables a user to access Apple-provided email accounts on multiple  
2 | Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used  
3 | to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing  
4 | allows the user to share those images and videos with other Apple subscribers. iCloud Drive  
5 | can be used to store presentations, spreadsheets, and other documents. iCloud Tabs enables  
6 | iCloud to be used to synchronize webpages opened in the Safari web browsers on all of the  
7 | user's Apple devices. iWorks Apps, a suite of productivity apps (Pages, Numbers, and  
8 | Keynote), enables iCloud to be used to create, store, and share documents, spreadsheets, and  
9 | presentations. iCloud Keychain enables a user to keep website username and passwords,  
10 | credit card information, and Wi-Fi network information synchronized across multiple Apple  
11 | devices.

12 |       106. Location Services allows apps and websites to use information from cellular,  
13 | Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's  
14 | approximate location.

15 |       107. App Store and iTunes Store are used to purchase and download digital content.  
16 | iOS apps can be purchased and downloaded through App Store on iOS devices, or through  
17 | iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac  
18 | OS. Additional digital content, including music, movies, and television shows, can be  
19 | purchased through iTunes Store on iOS devices and on desktop and laptop computers  
20 | running either Microsoft Windows or Mac OS.

21 |       108. Apple captures information associated with the creation and use of an Apple  
22 | ID. During the creation of an Apple ID, the user must provide basic personal information  
23 | including the user's full name, physical address, and telephone numbers. The user may also  
24 | provide means of payment for products offered by Apple. The subscriber information and  
25 | password associated with an Apple ID can be changed by the user through the "My Apple  
26 | ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which  
27 | the account was created, the length of service, records of log-in times and durations, the  
28 | types of service utilized, the status of the account (including whether the account is inactive

1 or closed), the methods used to connect to and utilize the account, the Internet Protocol  
2 address (“IP address”) used to register and access the account, and other log files that reflect  
3 usage of the account.

4 109. Additional information is captured by Apple in connection with the use of an  
5 Apple ID to access certain services. For example, Apple maintains connection logs with IP  
6 addresses that reflect a user’s sign-on activity for Apple services such as iTunes Store and  
7 App Store, iCloud, and the My Apple ID and iForgot pages on Apple’s website. Apple also  
8 maintains records reflecting a user’s app purchases from App Store and iTunes Store, “call  
9 invitation logs” for FaceTime calls, and “mail logs” for activity over an Apple-provided  
10 email account. Records relating to the use of the Find My iPhone service, including  
11 connection logs and requests to remotely lock or erase a device, are also maintained by  
12 Apple.

13 110. Apple also maintains information about the devices associated with an Apple  
14 ID. When a user activates or upgrades an iOS device, Apple captures and retains the user’s  
15 IP address and identifiers such as the Integrated Circuit Card ID number (“ICCID”), which is  
16 the serial number of the device’s SIM card. Similarly, the telephone number of a user’s  
17 iPhone is linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also  
18 may maintain records of other device identifiers, including the Media Access Control  
19 address (“MAC address”), the unique device identifier (“UDID”), and the serial number. In  
20 addition, information about a user’s computer is captured when iTunes is used on that  
21 computer to play content associated with an Apple ID, and information about a user’s web  
22 browser may be captured when used to access services through icloud.com and apple.com.  
23 Apple also retains records related to communications between users and Apple customer  
24 service, including communications regarding a particular Apple device or service, and the  
25 repair history for a device.

26 111. Apple provides users with five gigabytes of free electronic space on iCloud,  
27 and users can purchase additional storage space. That storage space, located on servers  
28 controlled by Apple, may contain data associated with the use of iCloud-connected services,

1 including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream,  
2 and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWorks  
3 and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs  
4 and iCloud Keychain). iCloud can also be used to store iOS device backups, which can  
5 contain a user's photos and videos, iMessages, Short Message Service ("SMS") and  
6 Multimedia Messaging Service ("MMS") messages, voicemail messages, call history,  
7 contacts, calendar events, reminders, notes, app data and settings, and other data. Records  
8 and data associated with third-party apps may also be stored on iCloud; for example, the iOS  
9 app for Telegram, an instant messaging service, can be configured to regularly back up a  
10 user's instant messages on iCloud. Some of this data is stored on Apple's servers in an  
11 encrypted form but can nonetheless be decrypted by Apple.

12 112. In this case, I am investigating, among other things, TURYGIN and  
13 POTAPENKO's use of Apple accounts. In my training and experience, evidence of who  
14 was using an Apple ID and from where, and evidence related to criminal activity of the kind  
15 described above, may be found in the files and records described above. As previously  
16 described, stored emails, chats, and other files may not only contain communications relating  
17 to the crimes under investigation, but also help identify the participants in those crimes.  
18 Address books and contact lists may help identify others involved in HASHFLARE and  
19 HASHCOINS, including victim investors. Similarly, photographs and videos may help  
20 identify additional promotion materials created by HASHFLARE and HASHCOINS, or  
21 identify cryptocurrency wallet addresses. Documents may identify the scope of the criminal  
22 activity, including transactional information related to victims and the ultimate disposition of  
23 fraud proceeds. And calendar data may reveal the timing and extent of criminal activity and  
24 other information, including the formation of HASHFLARE and HASHCOINS and  
25 solicitation of investors. Search and browsing history may also constitute direct evidence of  
26 the crimes under investigation to the extent the browsing history or search history might  
27 include searches and browsing history related to HASHFLARE, HASHCOINS, or  
28 cryptocurrency mining, and other evidence of the crimes under investigation. In my training

1 and experience, as already described above, I also know that the commission of the  
2 violations in the manner set forth above necessarily requires the use of computers, smart  
3 phones, tablets, or other computer devices.

4 113. In addition, the user's account activity, logs, stored electronic communications,  
5 and other data retained by Apple can indicate who has used or controlled the account. For  
6 example, subscriber information, email and messaging logs, documents, and photos and  
7 videos (and the data associated with the foregoing, such as geo-location, date and time) may  
8 be evidence of who used or controlled the account at a relevant time. As an example,  
9 because every device has unique hardware and software identifiers, and because every  
10 device that connects to the Internet must use an IP address, IP address and device identifier  
11 information can help to identify which computers or other devices were used to access the  
12 account. Such information also allows investigators to understand the geographic and  
13 chronological context of access, use, and events relating to the crime under investigation.

14 114. Other information connected to an Apple ID may lead to the discovery of  
15 additional evidence. For example, the identification of apps downloaded from App Store  
16 and iTunes Store may reveal additional services used to communicate with the victims or  
17 deposit cryptocurrency. In addition, I know that encrypted applications, including Telegram,  
18 which was used by the founders and members of HASHFLARE and HASHCOINS, can be  
19 backed up in a user's iCloud data. Therefore, Apple's servers are likely to contain stored  
20 electronic communications and information concerning subscribers and their use of Apple's  
21 services. Additionally, a successor entity to HASHFLARE and HASHCOINS, POLYBIUS,  
22 advertised that it was creating an Apple application as part of its operations.

23 **INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

24 115. Pursuant to Title 18, United States Code, Section 2703(g), this application and  
25 affidavit for a search warrant seeks authorization to require Apple, and their agents and  
26 employees, to assist agents in the execution of this warrant. Once issued, the search warrant  
27 will be presented to Apple with direction that it identifies the accounts described in  
28

1 Attachment A to this affidavit, as well as other subscriber and log records associated with the  
2 accounts, as set forth in Section I of Attachment B to this affidavit.

3 116. The search warrant will direct Apple to create an exact copy of the specified  
4 account and records.

5 117. I, and/or other law enforcement personnel will thereafter review the copy of  
6 the electronically stored data and identify from among that content those items that come  
7 within the items identified in Section II to Attachment B for seizure.

8 118. Analyzing the data contained in the forensic copy may require special technical  
9 skills, equipment, and software. It could also be very time-consuming. Searching by  
10 keywords, for example, can yield thousands of “hits,” each of which must then be reviewed  
11 in context by the examiner to determine whether the data is within the scope of the warrant.  
12 Merely finding a relevant “hit” does not end the review process. Keywords used originally  
13 need to be modified continuously, based on interim results. Certain file formats, moreover,  
14 do not lend themselves to keyword searches, as keywords, search text, and many common  
15 email, database and spreadsheet applications do not store data as searchable text. The data  
16 may be saved, instead, in proprietary non-text format. And, as the volume of storage allotted  
17 by service providers increases, the time it takes to properly analyze recovered data increases,  
18 as well. Consistent with the foregoing, searching the recovered data for the information  
19 subject to seizure pursuant to this warrant may require a range of data analysis techniques  
20 and may take weeks or even months. All forensic analysis of the data will employ only those  
21 search protocols and methodologies reasonably designed to identify and seize the items  
22 identified in Section II of Attachment B to the warrant.

23 119. Based on my experience and training, and the experience and training of other  
24 agents with whom I have communicated, it is necessary to review and seize a variety of  
25 communications, chat logs and documents, that identify any users of the subject account and  
26 communications sent or received in temporal proximity to incriminating communications  
27 that provide context to the incriminating communications.  
28

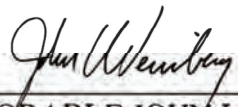
1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**CONCLUSION**

120. Based on the forgoing, I respectfully request that the Court issue the proposed search warrant. Accordingly, by this Affidavit and Warrant I seek authority for the government to search all of the items specified in Section I, Attachment B (attached hereto and incorporated by reference herein) to the Warrant, and specifically to seize all of the data, documents and records that are identified in Section II to that same Attachment.

  
\_\_\_\_\_  
Andrew Cropcho, Affiant  
Special Agent

The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit on the 11th day of March, 2021.

  
\_\_\_\_\_  
THE HONORABLE JOHN L. WEINBERG  
United States Magistrate Judge

**ATTACHMENT A**

**Apple Accounts to be Searched**

The electronically stored data, information and communications contained in, related to, and associated with, including all preserved data associated with Apple accounts:

a. Sergei.potapenko@gmail.com (DSID 624556209) (“**SUBJECT ACCOUNT 1**”); and

b. Turygin@gmail.com (DSID 1931852295) (“**SUBJECT ACCOUNT 2**”);

(collectively, the “Accounts”) that are stored at a premises controlled by Apple, Inc., a company that accepts service of legal process at One Apple Park Way, Cupertino, California 95014.

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**ATTACHMENT B**

**Particular Things to be Seized**

**I. Information to be disclosed by Apple, Inc.:**

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, Inc. (“Apple”), including any data, messages, records, files, logs, or information that has been deleted but is still available to Apple, or has been preserved pursuant to a request made under Title 18, United States Code, Section 2703(f), Apple is required to disclose the following information to the government for each Account or identifier listed in Attachment A, from Account inception to the present:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents of all emails associated with the account from April 2015 to the present, including stored or preserved copies of emails sent to and from the account



1 (including all draft emails and deleted emails), the source and destination addresses  
2 associated with each email, the date and time at which each email was sent, the size and  
3 length of each email, and the true and accurate header information including the actual IP  
4 addresses of the sender and the recipient of the emails, and all attachments;

5 d. The contents of all instant messages associated with the account from  
6 April 2015 to the present, including stored or preserved copies of instant messages (including  
7 iMessages, SMS messages, and MMS messages) sent to and from the account (including all  
8 draft and deleted messages), the source and destination account or phone number associated  
9 with each instant message, the date and time at which each instant message was sent, the size  
10 and length of each instant message, the actual IP addresses of the sender and the recipient of  
11 each instant message, and the media, if any, attached to each instant message;

12 e. The contents of all files and other records stored on iCloud, including all  
13 iOS device backups, all Apple and third-party app data, all files and other records related to  
14 iCloud Photo Library, Photo Stream, iCloud Drive, Safari Browsing History, and all address  
15 books, contact and buddy lists, notes, reminders, calendar entries, images, videos,  
16 voicemails, device settings, and bookmarks;

17 f. All activity, connection, and transactional logs for the account (with  
18 associated IP addresses including source port numbers), including FaceTime call invitation  
19 logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs,  
20 iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates  
21 of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple  
22 services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with  
23 web-based access of Apple services (including all associated identifiers), and logs associated  
24 with iOS device purchase, activation, and upgrades;

25 g. All records pertaining to the types of service used;

26 h. Records identifying the location of the subscriber.

27 i. All records pertaining to communications between Apple and any  
28 person regarding the account, including contacts with support services and records of actions

1 | taken; and

2 |           j.       All files, keys, or other information necessary to decrypt any data  
3 | produced in an encrypted form, when available to Apple (including, but not limited to, the  
4 | keybag.txt and fileinfolist.txt files).

5 |       Apple is hereby ordered to disclose the above information to the government within  
6 | **14 days** of service of this warrant.

7 |  
8 | **II.    Information to be seized by the government**

9 |       All information described above in Section I that constitutes fruits, contraband,  
10 | evidence, and instrumentalities of violations of Title 18, United States Code, Section 1343  
11 | (Wire Fraud), and occurring after April 2015, for each of the Accounts listed on Attachment  
12 | A, pertaining to the following matters:

13 |           a.       Items, records, or information related to the operation of a  
14 | cryptocurrency cloud mining Ponzi scheme;

15 |           b.       Items, records, or information related to cryptocurrency mining, the  
16 | advertisement, manufacture and sale of mining equipment, or the advertisement and sale of  
17 | cloud mining contracts;

18 |           c.       Items, records, or information related to the termination of mining  
19 | contracts and the profitability of cloud mining;

20 |           d.       Items, records, or information related to purchases of cloud mining  
21 | equipment, including communications with the companies Jeltan Trading, Dalmeron  
22 | Projects, Ecohouse Networks LP, Dalmeron Invest, Keleta UAB, Bitmain, Bitfury, and  
23 | Inno3d;

24 |           e.       Items, records, or information related to the transfer, purchase, sale, or  
25 | disposition of cryptocurrency;

26 |           f.       Items, records, or information related to communications with  
27 | HASHFLARE or HASHCOINS investors, including complaints by investors or requests for  
28 | return of funds;

1 g. Items, records, or information related to the advertisement of  
2 HASHFLARE or HASHCOINS' services;

3 h. Items, records, or information related to the owners, operators,  
4 employees, locations, assets, and business purpose of the companies HASHCOINS OU,  
5 HASHCOINS TRADE OU, HASHCOINS LP, HASHFLARE LP, Burfa Capital OU, Burfa  
6 Media OU, Burfa Real Estate OU, Burfa Tech OU, Burfa Trade OU, Burfa Invest OU,  
7 Polybius Foundation OU, Polybius Tech OU, Polybius Ventures OU, Polybius Fintech  
8 MidCo OU, Dalmeron Projects LP, Jeltan Trading, Dalmeron Invest, Ecohouse Networks  
9 LP, and Keleta UAB (collectively, the "SUBJECT ENTITIES");

10 i. Items, records, or information related to the use, creation, or operation  
11 of the "SUBJECT ENTITIES," including business plans and strategies, and the anticipated  
12 success, failure, or general validity thereof;

13 j. Items, records, or information related to the operation of hashflare.io,  
14 burfa.com, polybius.io, dalmeron.com, or hashcoins.com;

15 k. Items, records, or information concerning financial transactions  
16 associated with the operation of the SUBJECT ENTITIES, including bank accounts held by  
17 the SUBJECT ENTITIES, transfers of funds by the SUBJECT ENTITIES, expenditures of  
18 money or wealth, bank statements and other financial statements, and cryptocurrency  
19 holdings;

20 l. Items, records, or information related to cryptocurrency mining groups,  
21 cryptocurrency public keys or addresses, cryptocurrency private keys, representations of  
22 cryptocurrency wallets or their constitutive parts, to include "recovery seeds" and "root  
23 keys," which may be used to regenerate a wallet.

24 m. Items, records, or information related to the salaries or earnings of  
25 individuals employed by the SUBJECT ENTITIES.

26 n. Items, records, or information related to the payment or calculation of  
27 recruitment bonuses paid to HASHFLARE and HASHCOINS investors.  
28

1 o. Items, records, or information related to receipt of investor money,  
2 including the amount, purpose of the investment, and plans for spending that money.

3 p. Evidence indicating how and when the email account was accessed or  
4 used, to determine the geographic and chronological context of account access, use, and  
5 events relating to the crime under investigation and to the email account owner.

6 q. Evidence indicating the email account owner's state of mind as it relates  
7 to the crime under investigation.

8 r. The identity of the person(s) who created or used the user ID, including  
9 records that help reveal the whereabouts of such person(s).

10  
11 This warrant authorizes a review of electronically stored information, communications, other  
12 records and information disclosed pursuant to this warrant in order to locate evidence, fruits,  
13 and instrumentalities described in this warrant. The review of this electronic data may be  
14 conducted by any government personnel assisting in the investigation, who may include, in  
15 addition to law enforcement officers and agents, attorneys for the government, attorney  
16 support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete  
17 copy of the disclosed electronic data to the custody and control of attorneys for the  
18 government and their support staff for their independent review.  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC  
RECORDS PURSUANT TO FEDERAL RULES OF  
EVIDENCE 902(11) AND 902(13)**

I, \_\_\_\_\_, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by \_\_\_\_\_, and my title is \_\_\_\_\_. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of \_\_\_\_\_. The attached records consist of \_\_\_\_\_ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of \_\_\_\_\_, and they were made by \_\_\_\_\_ as a regular practice; and

b. such records were generated by \_\_\_\_\_'s electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of \_\_\_\_\_ in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by \_\_\_\_\_, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

\_\_\_\_\_  
Date

\_\_\_\_\_  
Signature