

# 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)*  
Ten (10) Seagate Hard Drives that are stored at  
premises controlled by the FBI, as more fully  
described in Attachment A

Case No. MJ24-593

## 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)*:

Ten (10) Seagate Hard Drives that are stored at premises controlled by the FBI, as more fully described in Attachment A, incorporated herein by reference

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

See Attachment B, 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. § § 1343, 1349, and 1956(h)	Wire Fraud, Conspiracy to Commit Wire Fraud, and Conspiracy to Commit Money Laundering

The application is based on these facts:

- See Affidavit of FBI 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, FBI 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: 09/19/2024

*Judge's signature*

City and state: Seattle, Washington

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

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

3. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 1349

1 (Conspiracy to Commit Wire Fraud), 18 U.S.C. § 1343 (Wire Fraud), and 18 U.S.C.  
2 1956(h) (Conspiracy to Commit Money Laundering), have been committed by Estonian  
3 nationals Sergei Potapenko (“Potapenko”) and Ivan Turõgin, also known as Ivan  
4 Turygin, (“Turõgin”) (collectively, “the defendants”).

5 **PROCEDURAL AND OPERATIONAL HISTORY**

6 4. On October 27, 2022, a grand jury sitting in the Western District of  
7 Washington charged Potapenko and Turõgin in an eighteen-count indictment, charging  
8 each defendant with one count of Conspiracy to Commit Wire Fraud, in violation of 18  
9 U.S.C. § 1349; sixteen counts of Wire Fraud, in violation of 18 U.S.C. §§ 1343 and 2;  
10 and one count of Conspiracy to Commit Money Laundering, in violation of 18  
11 U.S.C. § 1956(h). The case is captioned *United States v. Potapenko, et. al.*, CR22-185  
12 RSL.

13 5. Following the indictment, the Department of Justice submitted to Estonian  
14 authorities a First Supplemental Request for Assistance, dated November 4, 2022, and a  
15 Second Supplemental Request for Assistance, dated November 8, 2022 (collectively, “the  
16 Estonian MLATs”), pursuant to the 1998 U.S.-Estonia Mutual Legal Assistance Treaty.

17 6. Among other things, the Estonian MLATs asked the relevant authorities in  
18 Estonia to conduct searches, in accordance with Estonian law, of the following locations  
19 for evidence relating to the defendants’ crimes:

- 20 a. Turõgin’s residence located at Kuusenõmme tee 19, Pirita linnaosa,  
21 Tallinn, Estonia;
- 22 b. Potapenko’s Residence located at Järvemetsa tee 5, Peetri, Estonia;
- 23 c. The residence of Tatjana Potapova, defendants’ CFO located at  
24 Rahu 18, Loksa, Estonia;

25 //

26 //

- d. The offices of various entities owned or affiliated with the defendants located at Tartu mnt 43, Tallinn, Estonia, and Tartu mnt 83, Tallinn, Estonia;
- e. Property leased by Burfa Media OÜ located at Varvi tn 5 (Laki tn 12), Tallinn, Estonia;
- f. Property leased by Burfa Tech OÜ located at Narva Technology Park, Elektrijsaama tee 59, Narva, Estonia; and
- g. Safe deposit box #912, belonging to Tatjana Potapova located at Swedbank in Tallinn, Estonia.

7. From November 20, 2022 through November 22, 2022, Estonian law enforcement conducted searches of the above-referenced locations (the “Estonian Searches”). At least one person representing the FBI was present at each location. Potapenko and Turõgin were also arrested on November 20, 2022, based on requests for provisional arrests that were transmitted by U.S. authorities to the Estonian authorities. Potapenko and Turõgin subsequently were released on bond pending the completion of extradition proceedings.

8. On May 28, 2024, after the Supreme Court of Estonia ruled that Potapenko and Turõgin could be extradited to the United States of America, they were arrested again in Estonia, and thereafter escorted by the FBI from Tallinn, Estonia, to Seattle, Washington on May 29, 2024.

9. Between January 2023 and September 2024, Estonian authorities transferred to custody of the FBI some of the material seized in response to the Estonian MLATs. The material provided included ten Seagate hard drives that included forensic copies, prepared by Estonian law enforcement, of 143 digital devices seized by Estonian authorities during the Estonian Searches of Potapenko’s, Turõgin’s, and Potapova’s residences, and three of the business locations, namely, Tartu mnt 83, Tallinn, Varvi tn 5

1 (Laki tn 12), Tallinn, and Narva Technology Park, Elektriijaama tee 59, Narva. An index  
2 listing the 143 devices the images of which are included on the ten Seagate hard drives is  
3 labelled Appendix 1 to Attachment A to this Affidavit, and is incorporated herein by  
4 reference.

#### 5 **PURPOSE OF AFFIDAVIT**

6 10. This Affidavit is being submitted pursuant to Federal Rule of Criminal  
7 Procedure 41 in support of an Application for a warrant authorizing the search of the  
8 contents of the ten Seagate hard drives, containing forensic copies of digital devices  
9 seized during the Estonian Searches that took place from November 20, 2022, through  
10 November 22, 2022, and which are now in the custody of the FBI in Seattle, Washington,  
11 further described in Attachment A to this Affidavit.

#### 12 **STATEMENT OF PROBABLE CAUSE**

13 11. The FBI investigation has revealed that, starting in 2013 and continuing  
14 through the present, Potapenko and Turõgin (together, the “defendants”), as well as  
15 various corporate entities they owned and/or controlled, and other co-conspirators,  
16 engaged in a multi-faceted fraud and money-laundering conspiracy. The defendants  
17 persuaded investors to invest hundreds of millions of dollars in defendants’  
18 cryptocurrency-related businesses by making false and fraudulent representations,  
19 pretenses and promises about those businesses. The defendants then used shell companies  
20 and other vehicles to funnel the fraud proceeds to themselves and other companies under  
21 their control. This conduct violated United States criminal laws, including Title 18,  
22 United States Code, Sections 1349 (Conspiracy to Commit Wire Fraud), 1343 (Wire  
23 Fraud), and 1956(h) (Conspiracy to Commit Money Laundering).

#### 24 **BACKGROUND REGARDING CRYPTOCURRENCY MINING**

25 12. I am familiar with matters related to cryptocurrency (also known as virtual  
26 currency) and cryptocurrency mining. Cryptocurrency is a type of digital asset. Unlike  
27

1 traditional currency (which is sometimes called “fiat currency”), cryptocurrency is not  
2 issued by any government or bank. Rather, users generate and exchange cryptocurrency  
3 using computers operating on decentralized, peer-to-peer networks. There are thousands  
4 of virtual currencies in use. Bitcoin is the most popular form of cryptocurrency.

5 13. Cryptocurrency mining is the process of using computers to generate new  
6 cryptocurrency for profit. Computers mine currency by performing operations that  
7 validate transactions and maintain the security of the cryptocurrency network. These  
8 verified transactions make up a decentralized, unchangeable ledger of cryptocurrency  
9 transactions called the “blockchain.” Cryptocurrency miners receive newly-created  
10 currency as a reward for using their computer power to complete the operations.

11 14. Cryptocurrency mining operations require substantial computer processing  
12 power. The greater a mining operation’s processing power, the more cryptocurrency it  
13 can be expected to produce. Processing power is measured by “hashrate,” which reflects  
14 the number of calculations that the computer can perform per second.

15 15. “Cloud mining” or “remote mining” is an economic arrangement in which  
16 participants can, in essence, rent a specified amount of hashrate from a mining operation  
17 for an agreed period of time (the contract period). During the contract period, the  
18 participant is entitled to receive a portion of the cryptocurrency generated by the mining  
19 operation. The participant’s share of the mining proceeds is based on the amount of  
20 hashrate purchased.

## 21 **EVIDENCE OF THE CHARGED OFFENSES**

### 22 **A. Summary of the Investigation**

23 16. As discussed below, my investigation has established that, from  
24 approximately 2013 through present day, Turõgin, Potapenko, and their co-conspirators  
25 deceived and defrauded others in relation to cryptocurrency and cryptocurrency-related  
26 ventures for their own personal gain. They further engaged in a series of financial  
27

1 transactions to obfuscate the true nature and location of the fraudulently obtained funds,  
2 and to enrich themselves.

3 17. This fraud scheme had four distinct stages, which together constitute a  
4 scheme or artifice to defraud:

5 ***a. Sale of Physical Cryptocurrency Mining Hardware and Equipment:***

6 Beginning in 2013, through their company “HashCoins,” Turōgin and Potapenko sold  
7 cryptocurrency mining hardware and equipment they did not have and could not  
8 reasonably expect to procure as promised. After selling equipment they could not deliver,  
9 Turōgin and Potapenko converted the customers’ orders into contractual rights to  
10 participate in a purported cloud mining operation called HashFlare, which Turōgin and  
11 Potapenko also owned and operated.

12 ***b. Sale of Cryptocurrency Mining Contracts:*** Between about 2015 and 2019,  
13 Turōgin, Potapenko, and other co-conspirators operated HashFlare as a fraud and Ponzi  
14 scheme. During this time, they fraudulently induced hundreds of thousands of individuals  
15 to invest in contracts that guaranteed the buyer a portion of HashFlare’s purported  
16 cryptocurrency mining power, and thus a portion of the mined cryptocurrency. Turōgin  
17 and Potapenko sold over \$575 million worth of mining contracts, but HashFlare did not  
18 have anywhere near the mining capacity needed to perform those contracts. When  
19 customers demanded that defendants distribute their portions of the mined currency,  
20 defendants paid the customers using cryptocurrency they had purchased on the open  
21 market rather than currency that had been mined by HashFlare as represented. In July  
22 2018, HashFlare canceled a majority of its contracts with investors.

23 ***c. Polybius Initial Coin Offering:*** In 2017, Turōgin and Potapenko launched  
24 an investment offering known as an Initial Coin Offering (“ICO”). Defendants  
25 represented that the proceeds of the ICO would be used to develop a digital bank, and  
26 further, that a portion of the bank’s proceeds would be distributed to investors.

1 Defendants raised over \$25 million in the ICO. However, defendants never formed a  
2 bank, never paid any distributions to investors, and instead transferred a large portion of  
3 the investment proceeds to shell companies, bank accounts, and cryptocurrency wallets  
4 they controlled.

5 **d. Laundering Proceeds:** To dissipate and conceal the fraud proceeds,  
6 defendants funneled the fraudulently obtained victim funds through a convoluted network  
7 of domestic and international shell companies, bank accounts, cryptocurrency exchanges,  
8 cryptocurrency wallets, and tangible property under their control. Turõgin and Potapenko  
9 used fraud proceeds to fund their lavish lifestyles, including travel on private jets, stays at  
10 luxurious international villas, and the purchase of real estate, designer jewelry, and  
11 luxury cars in Estonia. After shuttering HashFlare, Turõgin and Potapenko used fraud  
12 proceeds to purchase expensive cryptocurrency mining hardware, which they used to  
13 mine cryptocurrencies for personal gain.

## 14 **B. HashFlare & HashCoins**

### 15 **a. Incorporation and Ownership**

16 18. I have investigated the formation of numerous businesses controlled by the  
17 defendants. My investigation has revealed that the defendants owned or controlled the  
18 following business entities over the period charged in the Indictment: Burfa Media OÜ,  
19 Burfa Capital OÜ (aka Starfix OÜ), Burfa Tech OÜ (aka HashCoins OÜ), Dalmeron  
20 Projects LP, Polybius Foundation OÜ (aka Polybius Foundation SE, or Polybius  
21 Foundation AS), HashFlare LP (aka HashCoins LP, or Fast Consult LP), Advendor OÜ,  
22 Polybius Fintech MidCo OÜ, Polybius Tech OÜ, Apico OÜ, Felmaway OÜ, and  
23 Ecohouse Networks OÜ. My investigation has established that each of these entities was  
24 used to perpetrate the crimes charges in the indictment, or received proceeds derived  
25 from those crimes.

26 //



1 19. HashFlare maintained the website “hashflare.io.” HashCoins maintained  
2 the website “HashCoins.com.” According to HashCoins’ and HashFlare’s websites,  
3 Potapenko is a co-founder and CEO of the entities. According to public reporting,  
4 Turõgin was a co-founder and Business Development Chairman of HashCoins. Turõgin  
5 has also been identified as a co-founder of HashFlare in public reporting.

6 20. Three of defendants’ companies—Burfa Capital, Burfa Media, and Burfa  
7 Tech—are collectively referred to as the “Burfa Entities” in this Affidavit. Burfa Capital  
8 is a holding company for many of Turõgin’s and Potapenko’s other companies. Burfa  
9 Media purportedly provided mining capacity that was supposedly consumed by  
10 HashFlare. In May 2019, HashCoins was re-named “Burfa Tech” in the Estonian  
11 Business Registry.

12 **b. HashCoins Business Operations**

13 21. I have reviewed records showing that, beginning in 2014, HashCoins  
14 advertised the sale of what it characterized as proprietary cryptocurrency mining  
15 hardware. HashCoins’ website described HashCoins as a “manufacturer of bitcoin mining  
16 hardware.” HashCoins’ promotional material stated that the company had “produced  
17 thousands of devices” for cryptocurrency mining. However, I determined that HashCoins  
18 had no manufacturing capacity. I observed e-mail communications between the  
19 defendants and third parties, in which they attempted to purchase the main components  
20 that compose bitcoin mining rigs instead of manufacturing the components themselves.  
21 Instead, HashCoins purchased mining equipment from other manufacturers, placed  
22 HashCoins branding on the equipment, and resold it. HashCoins required up-front  
23 payment in full for all purchases of mining equipment. These facts were corroborated by  
24 a former employee during an interview with Estonian law enforcement, in which the  
25 employee said that HashCoins named mining equipment, but did not produce it.

26 //

1           22. Based on my investigation, by January 2015 at the latest, HashCoins had  
2 sold and continued to sell far more equipment than it had the capacity to acquire. An  
3 internal HashCoins business record reflects that, as of December 2014, HashCoins had  
4 delivered the promised equipment for only 14.5% of its orders. Emails obtained by the  
5 FBI show that, for most of 2015, HashCoins advised its customers of serial delays in the  
6 delivery of cryptocurrency mining equipment. Some customers who purchased thousands  
7 or tens of thousands of dollars' worth of mining equipment in 2014 still had not received  
8 their orders by late 2015 or early 2016. Yet, despite these unresolved and ongoing delays,  
9 for much of 2015 HashCoins continued to sell mining equipment it did not have and  
10 could not build or acquire.

11           **c. HashFlare Business Operations**

12           23. *HashFlare's Cloud Mining Service*: HashCoins' Terms of Service  
13 provided that, if HashCoins was unable to deliver physical equipment as promised, the  
14 company reserved the right to "offer the Customer compensation of equal or greater  
15 value in [the] form of virtual hardware and/or remote mining." By May 2015, Turõgin,  
16 Potapenko, and other co-conspirators invoked this provision to convert unfulfilled  
17 HashCoins contracts for the purchase and sale of physical cryptocurrency mining  
18 equipment into contractual rights to a share of HashCoins's virtual mining service, which  
19 defendants called "HashFlare."

20           24. By April 2015, defendants also began marketing HashFlare's purported  
21 cloud mining services to the general public. HashFlare advertised the following on its  
22 website: "Our service makes cryptocurrency mining available to every user. You no  
23 longer need to buy expensive equipment and spend your time setting up miners. Just  
24 select your desired capacity and earn income!" On another portion of its website,  
25 HashFlare advertised that "Cloud mining offers a unique option for mining with a low  
26 cost of entry as well as minimal risk and expense, which is opposite to traditional models  
27

1 of mining that involve procurement, maintenance and configuration of highly specialized  
2 software.”

3 25. HashFlare’s mining contracts purported to, in essence, rent out a portion of  
4 the computing power of HashFlare’s supposedly vast mining network. On its website,  
5 HashFlare explained that a user could “purchas[e] part of the mining power of hardware  
6 hosted and owned by a Cloud Mining services provider,” which “configur[es] the  
7 hardware, maintain[s] uptime and select[s] the most efficient and reliable [mining]  
8 pools.” The website stated that a customer’s “mining starts immediately after confirmed  
9 payment”; that the customer could “view all mining related information in real-time”; and  
10 that a customer could “instantly” withdraw mined currency. For example, on April 18,  
11 2015, for \$9.95, a user could buy one million hashrate (“one million hash per second” or  
12 “1 MH/s”) from HashFlare. For this rate, HashFlare advertised a “100% Scrypt Miner,”  
13 automatic accruals in Bitcoin, and a daily maintenance fee of \$0.01 per 1/MH/s.

14 26. HashFlare’s website also offered a dashboard that allowed investors to  
15 access their account information. The account information included, among other things,  
16 a balance ledger that showed the amount of cryptocurrency the user purportedly had  
17 generated through the user’s mining activity on HashFlare. The ledger also reflected  
18 deductions from the balance for “maintenance fees” incurred by the user. The user would  
19 then have the option to automatically reinvest the balance in additional mining activity or,  
20 alternatively, to withdraw the balance provided that it exceeded a minimum threshold,  
21 which generally fluctuated between 0.01 bitcoin to 0.05 bitcoin.

22 27. In addition to purportedly earning funds through cloud mining, HashFlare  
23 represented to users that they could earn funds by recruiting others to purchase HashFlare  
24 contracts. HashFlare advertised a referral program, informing users that “as a referrer,  
25 you are eligible to receive 10% referral commission bonus for every purchase made by  
26 any of your referrals, excluding reinvest and balance purchases.”  
27

1 28. *HashFlare's Sales of Hashrate*: I have reviewed internal HashFlare  
2 business records reflecting the company's sales and revenues. The records reflect that  
3 HashFlare collected over \$575 million from customers for the sale of hashrate between  
4 2015 and 2019.

5 29. I have also reviewed financial records obtained from banks and other  
6 financial institutions. While I have not yet received records for all HashFlare's accounts,  
7 the records I have reviewed are generally consistent with the internal HashFlare records  
8 referenced above. For example, according to financial records obtained from the United  
9 Kingdom, victims sent at least \$150 million to an account held by HashFlare at a  
10 financial institution known as Connectum. Examples of descriptions accompanying the  
11 transfer of money were: "HashFlare.io Invoice..."; "CLOUD MINING INVESTMENT";  
12 and "...Hashflare BTC Mining").

13 30. Similarly, bank records obtained from Latvia reflect those victims sent at  
14 least \$34 million to an account held by HashFlare at Latvijas Pasta Banka. These  
15 transfers were made in the names of various individuals, and often referenced the terms  
16 "Hashrate Purchase #."

17 31. The amounts deposited by victims into the accounts described in  
18 Paragraphs 29-30 are each within about 5% of the amounts shown as paid by victims into  
19 those accounts on the internal records.

20 **d. Termination of HashFlare's Operations**

21 32. Over the course of its lifespan, HashFlare changed its operations in ways  
22 that made it more difficult for customers to withdraw their balances. For example, in or  
23 around July 2018, HashFlare required all users to submit "Know Your Customer"  
24 identification before they could continue using services offered on the platform. In effect,  
25 these additional procedures reduced the ability of users to withdraw funds earned through  
26 mining. On online forums, users complained that, even after they submitted the necessary  
27

1 | documentation, HashFlare was taking weeks or months to verify their identities and pay  
2 | balances. Other users complained that they never received their requested balances.

3 |         33. On July 20, 2018, HashFlare announced that bitcoin mining had been  
4 | unprofitable for 28 days as of July 18, 2018, and that, per clause 5.5 of its Terms of  
5 | Service, all bitcoin mining contracts were suspended. According to its terms of service,  
6 | HashFlare informed investors that it would stop cryptocurrency mining “if the  
7 | Maintenance and Electricity Fees [are] larger than the Payout.” Specifically, according to  
8 | HashFlare’s terms, “If mining remains unprofitable for 21 consecutive days the Service is  
9 | permanently terminated . . . [and] Payouts and Fees will also be temporarily stopped.”

10 |         34. I have interviewed HashFlare investors who reported they were unable to  
11 | withdraw their balances after HashFlare suspended their bitcoin mining contracts. I later  
12 | learned that some victims received withdrawals after HashFlare shuttered its operations,  
13 | but it was sometimes a drawn out and difficult process.

14 |         35. After HashFlare suspended its contracts, investors, including those located  
15 | in the United States, began identifying red flags that led them to believe HashFlare was a  
16 | Ponzi scheme and not actually engaged in cryptocurrency mining as represented. Instead,  
17 | the investors believed that HashFlare was profiting on fluctuations in cryptocurrency  
18 | exchange rates, using those gains and new investment proceeds to repay earlier investors.  
19 | For example, investors reported that they visited HashFlare’s business address in Estonia,  
20 | and found that it did not appear to house a server farm or computing equipment  
21 | consistent with cryptocurrency mining. Additionally, according to these investors, the  
22 | rates charged by HashFlare for maintenance and electricity were above market average,  
23 | and pools that were used to mine did not produce the expected output.

24 |         36. HashFlare and HashCoins have stopped selling any mining contracts. As  
25 | described below, its founders and employees appear to have moved to successor  
26 | companies that continue to operate in the cryptocurrency space.

1 **e. Investigation of HashFlare’s and HashCoins’ Cloud Mining Equipment**

2 37. The FBI has investigated investors’ allegations that HashFlare was not  
3 actually engaged in cryptocurrency mining as represented to investors. As noted above,  
4 HashFlare’s business records reflect that it sold approximately \$575 million worth of  
5 hashrate to customers between 2015 and 2019. Based on HashFlare’s internal sales data,  
6 HashFlare agreed to provide customers with about 3,313.81 petahertz per second (PH/s)  
7 of bitcoin mining hashrate for the period March 2015 through about June 2019. Similarly,  
8 HashFlare’s internal records show that the company contracted to provide about 9,175  
9 gigahertz per second (GH/s) of hashrate for other types of cryptocurrencies such as ether,  
10 Litecoin, Dash, and Zcash. Part of the FBI’s investigation involved determining whether  
11 HashFlare’s mining equipment was sufficient to generate these amounts of hashrate.

12 38. As part of this analysis, I investigated what mining equipment was actually  
13 owned by HashFlare and its affiliates. During my review of HashFlare’s business records,  
14 I located an Excel file stored in a HashFlare employee’s Google Account. The Excel file  
15 contained a tab titled “Acquired Equipment,” which appeared to be an inventory of  
16 mining equipment acquired by Burfa Media and HashCoins, two companies owned by  
17 the defendants. The tab included data regarding the type of equipment purchased, the  
18 approximate time of its purchase, the amount of mining power it could generate, and the  
19 cost of the equipment. The time span of the equipment inventory was from 2015 through  
20 at least December of 2017.

21 39. In April 2023, I interviewed the former HashFlare employee who compiled  
22 the equipment list. The employee verified that the Acquired Equipment list was indeed an  
23 accurate and complete inventory of HashFlare’s mining equipment, and that he compiled  
24 the list using information given to him by the defendants. The former employee also  
25 confirmed that HashFlare did not have mining capacity sufficient to service the contracts  
26 it sold.

1 40. To further confirm that the Acquired Equipment tab was a complete list of  
2 mining equipment owned by defendants' companies, I compared the data in the Acquired  
3 Equipment tab with other business records, such as e-mail communications by and  
4 between HashFlare personnel and bank statements. For example, I searched these  
5 business records for invoices reflecting the purchase of mining equipment by defendants'  
6 companies. Based on this comparison, I found that the Acquired Equipment tab appeared  
7 to be a complete listing of the mining equipment owned by defendants' companies.

8 41. Using the inventory list, I then calculated the total amount of hashrate that  
9 could be generated by the equipment owned by defendants' companies, assuming that the  
10 equipment was run 24 hours per day, 365 days per year. I performed this analysis  
11 separately for Bitcoin mining contracts and mining contracts for alternative  
12 cryptocurrencies, which are known as "altcoins."

13 42. With respect to Bitcoin mining, I approximated that the Bitcoin mining  
14 equipment owned by the defendants could be expected to generate a total of 15.42 PH/s,  
15 or 0.5% of the 3,313.81 PH/s sold by HashFlare, for the period August 2017 through  
16 November 2019. In other words, and put simply, the defendants did not own enough  
17 equipment to service even 1% of their Bitcoin mining contracts.

18 43. With respect to altcoin mining, I approximated that, under the favorable  
19 assumptions set out above, defendants' mining equipment could be expected to generate  
20 237.80 gigahertz per second of hashrate for the period February 2015 through March  
21 2019. Over this period, HashFlare sold contracts to provide 8,938 gigahertz per second of  
22 hashrate. Based on this analysis, defendants owned mining equipment sufficient to  
23 service only about 2.5% of the hashrate that HashFlare sold.

24 **f. Sham Lease Agreements**

25 44. I learned that defendants appeared to have entered into contracts with other  
26 companies to provide mining capacity. However, on further investigation, I determined  
27

1 that many of the contracts were sham contracts with shell entities secretly controlled by  
2 defendants that did not involve the actual provision of any mining capacity, but instead  
3 served as vehicles to funnel fraud proceeds to the defendants. During interviews with law  
4 enforcement, Tatjana Potapova, CFO of the defendants' companies, admitted to assisting  
5 with the creation of sham lease agreements and corresponding sham invoices.

6 45. **Ecohouse:** Financial records show that, between July 24, 2015, and  
7 January 19, 2017, HashCoins transferred about €1,395,000 to the bank account of a  
8 company known as Ecohouse. The description of the payments on the bank statements  
9 consistently used the language "COMPUTATIONAL POWER LEASING  
10 AGREEMENT," an apparent reference to cloud mining.

11 46. Registration documents for Ecohouse show that the company's partners are  
12 two other shell companies, both domiciled in the Marshall Islands. An individual signing  
13 as an Ecohouse representative signed a document giving Turõgin a power of attorney.  
14 Turõgin opened at least eight bank accounts in the name of Ecohouse at European  
15 financial institutions. About €1,290,000 (88 percent of total outflows) was then  
16 transferred from Ecohouse into a Burfa Media bank account. An additional €59,500 (4  
17 percent of total outflows) was transferred from Ecohouse into Turõgin's personal bank  
18 account. Therefore, it appears that Ecohouse was a shell company controlled by the  
19 defendants.

20 47. I have obtained and reviewed some of Ecohouse's bank records. The  
21 records show no expenditures that would suggest Ecohouse was actually in the business  
22 of cloud mining or otherwise renting computational power.

23 48. **Dalmeron:** Financial records show that HashFlare transferred  
24 approximately \$109 million in victim funds to a company known as Dalmeron between  
25 May 2017 and December 2019. When financial institutions inquired about these  
26 transactions, defendants reported that the transfers were being made pursuant to a  
27



1 “Computational Power Rent Agreement” between HashCoins and Dalmeron. Defendants  
2 portrayed Dalmeron as a third-party entity unrelated to them or their businesses. For  
3 example, when one financial institution asked Potapenko for information about the  
4 location of Dalmeron’s equipment, Potapenko responded that Dalmeron’s management  
5 had refused to provide that information to him.

6 49. However, my investigation established that the defendants are the true  
7 beneficial owners of Dalmeron. First, on October 14, 2016, e-mail records show that  
8 Turõgin emailed an incorporation company requesting to purchase Dalmeron Projects,  
9 LP. Second, I have reviewed a document dated March 22, 2017 granting a Power of  
10 Attorney over Dalmeron in favor of Turõgin. Additionally, email records show that, on  
11 October 26, 2017, GoDaddy sent Potapenko an email receipt for the domain registration  
12 renewal of the website dalmeron.com. And, finally, Turõgin’s email account,  
13 turygin@gmail.com, is linked by cookies to dalmeronprojects@gmail.com. Accordingly,  
14 based on my training and experience, and information gained during the course of this  
15 investigation, I believe that DALMERON is controlled by Turõgin and Potapenko, and is  
16 not an independent party as represented by the defendants.

17 50. I reviewed Dalmeron’s bank records for evidence that the business was  
18 engaged in actual mining activity. Specifically, I looked for records showing that  
19 Dalmeron had purchased mining equipment or had paid maintenance or electricity costs,  
20 which tend to be very significant for any ongoing mining operation. The financial records  
21 show no evidence that Dalmeron engaged in any mining operations. Instead, the funds  
22 that HashFlare transferred to Dalmeron were simply funneled, through a series of  
23 transactions, to the Burfa Entities or other accounts under the defendants’ control.  
24 Between about May 2017 through July 2020, Dalmeron transferred approximately \$100  
25 million to companies owned and controlled by the defendants.

1 51. I participated in two interviews with Potapova (defendants' CFO) in which  
2 she explained that Dalmeron was a shell company controlled by the defendants to avoid  
3 paying Estonian taxes. Potapova further explained that she did not believe Dalmeron ever  
4 provided any actual service to HashFlare. Potapova also admitted to creating documents  
5 for banks involving transactions between Dalmeron and Burfa Media to help satisfy  
6 inquiries being made by banks. Potapova said the numbers on certain documents came  
7 from "out of the blue." Potapova stated that other employees also helped with Dalmeron-  
8 related matters, so she did not know all of the facts regarding Dalmeron.

9 **g. Review of Source of Payments to Investors**

10 52. In addition to investigating HashFlare's and HashCoins' cloud mining  
11 capabilities, the FBI also investigated the manner in which these entities paid the subset  
12 of investors who did receive some returns. Specifically, the FBI investigated whether  
13 defendants' entities were paying investors using currency mined by defendants' entities  
14 (which would be evidence of legitimate mining activity), or instead, whether they paid  
15 investors with cryptocurrency they had purchased (which would be evidence of a Ponzi  
16 scheme).

17 53. To perform this analysis, the FBI examined the blockchain to determine the  
18 source of the specific units of cryptocurrency used to pay investors. FBI investigators  
19 examined all of the deposits into the main wallet used by HashFlare to source investor  
20 withdrawal payments, and the analysis determined that only about 3% of the  
21 cryptocurrency paid to victims had been mined by HashFlare or HashFlare-affiliated  
22 companies. Over 90% of the currency used to pay investors had been purchased or  
23 received from virtual asset service providers on the open market. It was not possible to  
24 determine the origin of the remaining 7%. This was generally consistent with my  
25 conclusion, described above, that HashFlare only owned equipment sufficient to service  
26 between about 0.5% and 2.5% of the contracts it sold.  
27

1           54. The investigation found that the vast majority of payments made to  
2 customers were derived from a pool of victim deposits, which Turõgin, Potapenko, and  
3 others funneled through a series of hosted and private cryptocurrency wallets designed to  
4 make it appear as though victims who received payments were actually sharing in mining  
5 revenues, as opposed to simply receiving a portion of newer victims' deposits. Turõgin  
6 and Potapenko employed a "peel chain"—a technique that I know is sometimes used to  
7 launder cryptocurrency by, in essence, converting one large transaction into many smaller  
8 transactions that are unlikely to attract notice. In a peel chain, a small portion of the  
9 overall amount to be transferred "peels" off from the main address in a relatively low-  
10 value transfer. (In this case, Turõgin and Potapenko would, for instance, "peel" off  
11 chunks of 10 bitcoin for transfer into a larger cluster.) The remaining balance of the  
12 larger cryptocurrency amount transfers to a new address, and the process repeats itself  
13 until the desired larger transfer is complete.

14           55. Turõgin and Potapenko's use of a peel chain here appears to have been  
15 designed to prevent or disrupt victims from tracing payments they received from  
16 HashFlare back to the wallets that had received the initial victim deposits.

17           56. Estonian authorities independently analyzed HashFlare's cryptocurrency  
18 transactions, including 22,935 transfer chains related to HashFlare payout wallets, to  
19 determine if payouts to investors were coming from mining pools, which would be the  
20 expected source of payouts if HashFlare operated a legitimate mining operation. They  
21 reached similar conclusions as those reached by the FBI. Based on their analyses,  
22 Estonian authorities concluded that most of the payouts to victims came from the wallets  
23 where Bitcoin deposits were received, and only about 0.8% of payouts came from mining  
24 pools.

25           57. Based on the foregoing, my investigation established that HashFlare was  
26 not engaged in substantial cryptocurrency mining, as advertised. Instead, HashFlare  
27

1 appears to have operated as a Ponzi scheme by converting victims' deposits from fiat to  
2 cryptocurrency, or from one cryptocurrency to another, in order to pay back other victims  
3 and to conceal the true source of those payments.

#### 4 **C. Defendants' Fraudulent use of Polybius ICO Proceeds**

5 58. In addition to HashCoins, HashFlare, and the Burfa Entities, Turõgin and  
6 Potapenko also formed a second conglomerate, comprised of at least six entities—  
7 Polybius Foundation, Digital Ledger, Polybius Tech, Polybius Ventures, Polybius  
8 Fintech, and Polybius Fintech MidCo (collectively, referred to as "Polybius").

9 59. In approximately April 2017, the defendants began soliciting investments in  
10 an initial coin offering (ICO) to fund the Polybius Foundation. An email advertising the  
11 launch of the "Polybius project" indicated that the "HashCoins team would like to invite  
12 you to join our latest project Polybius for which we are launching crowdfunding on May  
13 31!" Other emails promoting Polybius were sent signed by the HashFlare team and/or by  
14 Turõgin.

15 60. In support of the ICO, the defendants created a prospectus explaining the  
16 terms of their offering and distributed it to HashFlare investors, through Twitter and other  
17 channels. The Prospectus described Polybius as "a team of financial, security, legal and  
18 technical experts." The Prospectus stated that Polybius Bank would be a "fully digital  
19 bank accessible everywhere at any time. It will have all the functions of a classical bank,  
20 but will not host any branches, nor any physical front-offices and will rely fully on the  
21 latest digital technologies." The front of the prospectus reads, in part: "Polybius  
22 POWERED BY HashCoins."

23 61. The prospectus explained that investors would receive Polybius "tokens."  
24 According to the prospectus, "a Polybius token represents the right to receive a part of the  
25 distributable profits of . . . Polybius Bank." The prospectus stated that the investment  
26 proceeds would be used "to support the establishment of the Polybius Bank," and that the  
27

1 “funds raised by the sale of tokens will be retained by the Polybius Foundation until they  
2 will be used.” In other words, the prospectus represented that funds raised in the ICO  
3 would be used only for Polybius business purposes, and a share of Polybius profits would  
4 be distributed to investors.

5 62. According to internal records maintained by representatives of Polybius,  
6 the ICO raised approximately \$25 million from outside investors during the summer of  
7 2017. On or around June 13, 2017, Turõgin, Potapenko, and others caused an article to be  
8 published on the PRNewswire with the subheading: “Polybius cryptobank ICO has raised  
9 over \$6 million in under three days, meeting the requirements to receive a European  
10 banking license.”

11 63. Following the completion of the ICO, Polybius announced that it would not  
12 be opening a bank, and that it would develop a mobile application instead. Polybius never  
13 formed a bank and never distributed any profits to tokenholders.

14 64. Contrary to their representations that ICO proceeds would be retained by  
15 the Polybius Foundation until used for its operations, defendants transferred a large  
16 portion of the ICO proceeds out of Polybius to be used for their own benefit. Based on a  
17 review of the blockchain and records provided by BlockFi, between around May 19,  
18 2021 and June 18, 2022, Polybius transferred 2,060 bitcoin that it initially received  
19 during its ICO—funds to be used to establish a digital bank—to Burfa Media’s BlockFi  
20 account. Burfa Media subsequently collateralized the Polybius ICO bitcoin to take out  
21 loans in order to buy at least \$13 million of mining equipment. Instead of being used to  
22 benefit former HashFlare investors or Polybius ICO participants, the mining equipment  
23 was used to personally benefit Turõgin and Potapenko.

24 **D. Use of Interstate Wires**

25 65. My investigation has established that the defendants used, and caused to be  
26 used, the interstate and foreign wires in various ways in furtherance of their scheme to  
27

1 defraud. For example, I have reviewed emails that HashFlare sent customers containing  
2 invoices for the purchase of hashrate to victims in the Western District of Washington via  
3 interstate and foreign wire transmissions. Similarly, I have reviewed bank records  
4 showing that investors funded their purchases of hashrate from HashFlare by means of  
5 interstate and foreign wire transmissions, including transmissions originating in the  
6 Western District of Washington and terminating outside of Washington.

7 **E. Role of Tatjana Potapova**

8 66. Potapova was hired as the CFO of the Burfa Entities in 2016, and she led an  
9 accounting department comprised of up to four people. I reviewed the contents of  
10 Potapova's e-mail account "tatjana@burfa.com," and observed many instances in which  
11 she provided invoices and contracts relating to HashFlare LP, HashCoins OÜ, Burfa  
12 Media OÜ, and Dalmeron, which she later confirmed contained false information during  
13 interviews with law enforcement.

14 **F. Estonian Searches**

15 67. I have reviewed reports written by the Estonian authorities documenting the  
16 Estonian Searches. Based on those reports, I understand that the Estonian authorities  
17 seized items that that they believed, and that in fact, constituted or contained evidence of  
18 the crimes being investigated at each of the locations at which they seized the devices  
19 imaged on the ten Seagate hard drives listed in Attachment A.

20 68. From my investigation, I also know that defendants and their employees  
21 used computers, cellular telephones, and other digital devices, throughout in their  
22 business activity, at both HashFlare and Polybius, including to send emails, interact with  
23 banks, conduct blockchain transactions, interact with employees, and monitor the  
24 operations of HashFlare.

25 69. At Turõgin's residence, located at Kuusenõmme tee 19, Pirita linnaosa,  
26 Tallinn, Estonia, Estonian authorities reported finding the following, among other things:  
27

- Agreements involving Dalmeron Projects, a shell company utilized by Turõgin to launder fraud proceeds, and agreements involving Burfa Media;
- Banking materials relating to Burfa Tech, Burfa Media, and Ivan Turõgin;
- Turõgin’s iPhone 13 Pro.<sup>1</sup> Evidence collected and reviewed throughout this investigation has shown that Turõgin utilized his iPhone to exchange text messages and e-mails about his business and financial dealings; and
- The other computing devices and external hard drives listed in Appendix 1 to Attachment A shown with the location “Turogin.”

70. At Potapenko’s residence, located at Järvemetsa tee 5, Peetri, Estonia, the Estonian authorities reported finding the following, among other things:

- Virtual currency cold storage wallets;
- Potapenko’s iPhone 14 Pro<sup>2</sup> and iPhone 12 Mini. Evidence collected and reviewed throughout this investigation has shown that Potapenko utilized his iPhone to exchange text messages and e-mails about his business and financial dealings; and
- The other computing devices and external hard drives listed in Appendix 1 to Attachment A shown with the location “Potapenko.”

71. At Potapova’s residence, located at Rahu 18, Loksa, Estonia, the Estonian authorities reported finding the following, among other things:

---

<sup>1</sup> A search warrant was previously issued for this iPhone 13 Pro, but law enforcement has yet to access its contents due to its encryption settings.

<sup>2</sup> A search warrant was previously issued for this iPhone 14 Pro, but law enforcement has yet to access its contents due to technological issues related to its size.

- 1 • Business records relating to defendant’s businesses, including a contract
- 2 involving HashCoins;
- 3 • A Dell laptop, with the contents from the account tatjana@burfa.com on
- 4 it; and
- 5 • The other computing devices and external hard drives listed in
- 6 Appendix 1 to Attachment A shown with the location “Potapova;”

7 I know from my investigation that the use of computers was an integral part of  
8 Potapova’s role in the defendants’ businesses, and that Potapova used them for multiple  
9 purposes, including to send emails, interact with banks, create fraudulent invoices,  
10 interact with Potapenko and Turõgin, and record financial transactions.

11 72. I know from my investigation that the defendants have operated their  
12 businesses at several locations, evidence of which was available through public sources,  
13 bank statements, lease agreements, and mining equipment shipment information. Those  
14 locations were the same locations searched during the Estonian Searches list in Paragraph  
15 6.d - 6.f.

16 73. Since at least 2017, Tartu mnt 83, Tallinn, Estonia has been the publicly  
17 registered location of the defendants’ holding company, Burfa Capital, as well as most of  
18 its subsidiaries, including Burfa Tech, Burfa Media, and Burfa Real Estate. This was also  
19 an address used on invoices and bank statement applications for the defendants and their  
20 companies.

21 74. Although HashFlare and Dalmeron did not use Tartu mnt 83 as their  
22 address, because they existed as shell companies in other jurisdictions, since the  
23 defendants ultimately controlled both entities and utilized Tartu mnt 83 as the office  
24 space for their other companies, I have probable cause to believe that records for  
25 HashFlare and Dalmeron also were stored at that location.



1 75. At Tartu mnt 83, Tallinn, Estonia, the Estonian authorities reported finding  
2 the following, among other things:

- 3 • Numerous virtual currency cold storage wallets;
- 4 • Bank cards and records in the name of Burfa Media, Burfa Tech,  
5 Dalmeron Projects, Ivan Turõgin, and Sergei Potapenko;
- 6 • Folders with documents inside of them, relating to entities such as Burfa  
7 Media, Burfa Tech, HashCoins, Polybius Foundation, and Polybius  
8 Tech;
- 9 • USB device<sup>3</sup> with the name “Hash Flare” on it, determined during the  
10 inventory process to consist of about 1.26GB of data; and
- 11 • The other computing devices and external hard drives listed in  
12 Appendix 1 to Attachment A shown with the location “Tartu Mnt 83.”

13 76. At the property leased by Burfa Media OÜ at Varvi tn 5 (Laki tn 12),  
14 Tallinn, Estonia, the Estonian authorities reported finding the following, among other  
15 things:

- 16 • Virtual currency miners that match the brand and model of virtual  
17 currency miners that were purchased by the defendants using funds  
18 from the Polybius ICO;
- 19 • A virtual currency miner with the name “HashCoins” on it;
- 20 • Hard drives and multiple computers that may have been used to operate  
21 or store data relating to the virtual currency miners, including records  
22 regarding where the miners would deposit any virtual currencies that  
23 were mined; and

24  
25 \_\_\_\_\_  
26 <sup>3</sup> A search warrant was previously issued for this USB device, but law enforcement has yet to access its contents due  
27 to technological issues related to its formatting.

- The other computing devices and external hard drives listed in Appendix 1 to Attachment A shown with the location “Laki 12.”

77. At the property leased by Burfa Tech OÜ at Narva Technology Park, Elektriijaama tee 59, Narva, Estonia, the Estonian authorities reported finding the following, among other things:

- Virtual currency miners that match the brand and model of virtual currency miners that were purchased using funds from the Polybius ICO;
- Hard drives and multiple computers that may have been used to operate or store data relating to the virtual currency miners, including records regarding where the miners would deposit any virtual currencies that were mined; and
- The other computing devices and external hard drives listed in Appendix 1 to Attachment A shown with the location “Narva.”

78. As noted above, evidence developed throughout this investigation shows that the defendants used their digital devices to communicate about their fraudulent business activities, including the HashFlare and Polybius frauds and their money laundering conspiracy. Further, I know from my training and experience that criminals engaged in complex financial crimes frequently maintain evidence relating to those activities on their electronic devices. And, I know that information on one digital device can easily be copied to another digital device and that criminals frequently transfer and copy information between different digital devices.

79. Based on the above, I have probable cause to believe that the contents of the digital devices identified in Attachment A will contain evidence of the crimes being investigated.

1 **G. Forensic Evidence**

2 80. This application seeks permission to locate not only computer files that  
3 might serve as direct evidence of the crimes described on the warrant, but also for  
4 forensic electronic evidence that establishes how digital devices or other electronic  
5 storage media were used, the purpose of their use, who used them, and when.

6 81. Stored data can provide evidence of a file that was once on the digital  
7 device or other electronic storage media but has since been deleted or edited, or of a  
8 deleted portion of a file (such as a paragraph that has been deleted from a word  
9 processing file). Virtual memory paging systems can leave traces of information on the  
10 digital device or other electronic storage media that show what tasks and processes were  
11 recently active. Web browsers, e-mail programs, and chat programs store configuration  
12 information that can reveal information such as online nicknames and passwords.  
13 Operating systems can record additional information, such as the history of connections  
14 to other computers, the attachment of peripherals, the attachment of USB flash storage  
15 devices or other external storage media, and the times the digital device or other  
16 electronic storage media was in use. Computer file systems can record information about  
17 the dates files were created and the sequence in which they were created.

18 82. Information stored within a computer and other electronic storage media  
19 may provide crucial evidence of the “who, what, why, when, where, and how” of the  
20 criminal conduct under investigation, thus enabling the United States to establish and  
21 prove each element or alternatively, to exclude the innocent from further suspicion. In my  
22 training and experience, information stored within a computer or storage media (e.g.,  
23 registry information, communications, images and movies, transactional information,  
24 records of session times and durations, internet history, and anti-virus, spyware, and  
25 malware detection programs) can indicate who has used or controlled the computer or  
26 storage media. This “user attribution” evidence is analogous to the search for “indicia of  
27

1 occupancy” while executing a search warrant at a residence. The existence or absence of  
2 anti-virus, spyware, and malware detection programs may indicate whether the computer  
3 was remotely accessed, thus inculcating or exculpating the computer owner and/or others  
4 with direct physical access to the computer. Further, computer and storage media activity  
5 can indicate how and when the computer or storage media was accessed or used. For  
6 example, as described herein, computers typically contain information that log: computer  
7 user account session times and durations, computer activity associated with user  
8 accounts, electronic storage media that connected with the computer, and the IP addresses  
9 through which the computer accessed networks and the internet. Such information allows  
10 investigators to understand the chronological context of computer or electronic storage  
11 media access, use, and events relating to the crime under investigation. Additionally,  
12 some information stored within a computer or electronic storage media may provide  
13 crucial evidence relating to the physical location of other evidence and the suspect. For  
14 example, images stored on a computer may both show a particular location and have  
15 geolocation information incorporated into its file data. Such file data typically also  
16 contains information indicating when the file or image was created. The existence of such  
17 image files, along with external device connection logs, may also indicate the presence of  
18 additional electronic storage media (e.g., a digital camera or cellular phone with an  
19 incorporated camera). The geographic and timeline information described herein may  
20 either inculcate or exculpate the computer user. Last, information stored within a  
21 computer may provide relevant insight into the computer user’s state of mind as it relates  
22 to the offense under investigation. For example, information within the computer may  
23 indicate the owner’s motive and intent to commit a crime (e.g., internet searches  
24 indicating criminal planning), or consciousness of guilt (e.g., running a “wiping” program  
25 to destroy evidence on the computer or password protecting/encrypting such evidence in  
26 an effort to conceal it from law enforcement).

1 83. A person with appropriate familiarity with how a digital device or other  
2 electronic storage media works can, after examining this forensic evidence in its proper  
3 context, draw conclusions about how the digital device or other electronic storage media  
4 were used, the purpose of their use, who used them, and when

5 84. The process of identifying the exact files, blocks, registry entries, logs, or  
6 other forms of forensic evidence on a digital device or other electronic storage media that  
7 are necessary to draw an accurate conclusion is a dynamic process. While it is possible to  
8 specify in advance the records to be sought, digital evidence is not always data that can  
9 be merely reviewed by a review team and passed along to investigators. Whether data  
10 stored on a computer is evidence may depend on other information stored on the  
11 computer and the application of knowledge about how a computer behaves. Therefore,  
12 contextual information necessary to understand other evidence also falls within the scope  
13 of the warrant.

14 //

15 //

16 //

17

18

19

20

21

22

23

24

25

26


27

**CONCLUSION**

1  
2 85. Based on the foregoing, I respectfully request that the Court issue the  
3 proposed search warrant. Accordingly, by this Affidavit and Warrant, I seek authority for  
4 the government to search all of the devices specified in Attachment A (attached hereto  
5 and incorporated by reference herein) to the Warrant, and specifically to seize all of the  
6 data, documents, and records identified in Attachment B.

7  
8  
9   
10 ANDREW CROPCHO, AFFIANT  
11 Special Agent

12 The above-named agent provided a sworn statement attesting to the truth of the  
13 foregoing affidavit on September 19th, 2024.

14  
15   
16 THE HONORABLE BRIAN A. TSUCHIDA  
17 United States Magistrate Judge

**ATTACHMENT A**

Devices to be Searched

The government is authorized to search the following forensic copies of devices in the custody of the Federal Bureau of Investigation in Seattle, Washington, for the material identified in Attachment B:

1. Ten Seagate Hard Drives, which contain images of digital devices seized during searches in Estonian more specifically identified in Appendix 1 to this Attachment.

## APPENDIX 1

Device #	Name	Location	Type	Path
1	0280418_Dell	Laki 12	Dell	D:\_DIG-12235_Laki12_Varvi5\A134_ruum\0280418_Dell
2	1845052_SanDisk_USB	Laki 12	SanDisk USB	D:\_DIG-12235_Laki12_Varvi5\A134_ruum\1845052_SanDisk_USB
3	1845053_USB	Laki 12	USB	D:\_DIG-12235_Laki12_Varvi5\A134_ruum\1845053_USB
4	1845054_USB_AP8G	Laki 12	USB	D:\_DIG-12235_Laki12_Varvi5\A134_ruum\1845054_USB_AP8G
5	2186668_mac_mini	Laki 12	mac mini	D:\_DIG-12235_Laki12_Varvi5\A134_ruum\2186668_mac_mini
6	6242159_Asus	Laki 12	Asus	D:\_DIG-12235_Laki12_Varvi5\A134_ruum\6242159_Asus
7	J13-0366666_Cloudkey_GEN2	Laki 12	0366666_Cloudkey_GEN2	D:\_DIG-12235_Laki12_Varvi5\A134_ruum\J13-0366666_Cloudkey_GEN2
8	J13-0366666_Hikvision	Laki 12	Hikvision	D:\_DIG-12235_Laki12_Varvi5\A134_ruum\J13-0366666_Hikvision
9	J13-0366666_Hikvision	Laki 12	Hikvision	D:\_DIG-12235_Laki12_Varvi5\A134_ruum\J13-0366666_Hikvision
10	WD40PURZ-85TTDY0_Teine_ketas	Laki 12	Discs	D:\_DIG-12235_Laki12_Varvi5\A134_ruum\J13-0366666_Hikvision\WD40PURZ-85TTDY0_Teine_ketas
11	WD-WCC7K7DPSNT5_WD40PURZ-85TTDY0	Laki 12	Hikvision Drive	D:\_DIG-12235_Laki12_Varvi5\A134_ruum\J13-0366666_Hikvision\WD-WCC7K7DPSNT5_WD40PURZ-85TTDY0
12	J13-0366668_microSD_Kingston	Laki 12	microSD Kingston	D:\_DIG-12235_Laki12_Varvi5\A134_ruum\J13-0366668_microSD_Kingston
13	J13-0366669_HDD	Laki 12	Seagate HD	D:\_DIG-12235_Laki12_Varvi5\A134_ruum\J13-0366669_HDD
14	6241179_macbook	Narva	macbook	D:\_DIG-12243_Narva_Elektrijaama_tee_59D\6241179_macbook
15	668989_Kingston_USB	Narva	Kingston USB	D:\_DIG-12243_Narva_Elektrijaama_tee_59D\668989_Kingston_USB
16	669016_Kingston_USB	Narva	Kingston USB	D:\_DIG-12243_Narva_Elektrijaama_tee_59D\669016_Kingston_USB
17	669017_Kingston_USB	Narva	Kingston USB	D:\_DIG-12243_Narva_Elektrijaama_tee_59D\669017_Kingston_USB
18	669018_Kingston_USB	Narva	Kingston USB	D:\_DIG-12243_Narva_Elektrijaama_tee_59D\669018_Kingston_USB
19	669019_DataTraveler_3.0	Narva	Kingston USB	D:\_DIG-12243_Narva_Elektrijaama_tee_59D\669019_DataTraveler_3.0
20	669020_SanDisk_microSD	Narva	SanDisk Micro SD	D:\_DIG-12243_Narva_Elektrijaama_tee_59D\669020_SanDisk_microSD
21	669021_SanDisk_microSD	Narva	SanDisk Micro SD	D:\_DIG-12243_Narva_Elektrijaama_tee_59D\669021_SanDisk_microSD
22	669022_SanDisk_microSD	Narva	SanDisk Micro SD	D:\_DIG-12243_Narva_Elektrijaama_tee_59D\669022_SanDisk_microSD
23	669023_Sony_USB	Narva	Sony USB	D:\_DIG-12243_Narva_Elektrijaama_tee_59D\669023_Sony_USB
24	669024_Kingston_USB	Narva	Kingston USB	D:\_DIG-12243_Narva_Elektrijaama_tee_59D\669024_Kingston_USB
25	669025_Kingston_USB	Narva	Kingston USB	D:\_DIG-12243_Narva_Elektrijaama_tee_59D\669025_Kingston_USB
26	669026_USB_SP_DISK_3.0	Narva	USB SP DISK 3.0	D:\_DIG-12243_Narva_Elektrijaama_tee_59D\669026_USB_SP_DISK_3.0
27	669042_M2_SSD	Narva	M2 SSD	D:\_DIG-12243_Narva_Elektrijaama_tee_59D\669042_M2_SSD
28	669043_M2_SSD	Narva	M2 SSD	D:\_DIG-12243_Narva_Elektrijaama_tee_59D\669043_M2_SSD
29	669044_M2_SSD	Narva	M2 SSD	D:\_DIG-12243_Narva_Elektrijaama_tee_59D\669044_M2_SSD
30	669045_Kingston_USB	Narva	Kingston USB	D:\_DIG-12243_Narva_Elektrijaama_tee_59D\669045_Kingston_USB
31	Dell EMC PowerEdge T340	Narva	Dell EMC PowerEdge T340	D:\_DIG-12243_Narva_Elektrijaama_tee_59D\Dell EMC PowerEdge T340
32	Dell Server PowerEdge 630	Narva	Dell Server PowerEdge 630	D:\_DIG-12243_Narva_Elektrijaama_tee_59D\Dell Server PowerEdge 630
33	Dell Server PowerEdge R540	Narva	Dell Server PowerEdge R540	D:\_DIG-12243_Narva_Elektrijaama_tee_59D\Dell Server PowerEdge R540
34	DVR Hickvision	Narva	DVR Hickvision	D:\_DIG-12243_Narva_Elektrijaama_tee_59D\DVR Hickvision
35	Ruum_1_6240874_Lauaarvuti_Dell_SR00008	Narva	Lauaarvuti_Dell_SR00008	D:\_DIG-12243_Narva_Elektrijaama_tee_59D\Ruum_1_6240874_Lauaarvuti_Dell_SR00008
36	Ruum_5_2133332_Asus_SÇ4learvuti_RTL8821CE	Narva	Asus	D:\_DIG-12243_Narva_Elektrijaama_tee_59D\Ruum_5_2133332_Asus_SÇ4learvuti_RTL8821CE
37	Synology Server DS920	Narva	Synology Server DS920	D:\_DIG-12243_Narva_Elektrijaama_tee_59D\Synology Server DS920
38	Synology Server RS1619XS+_SR00005	Narva	Synology Server RS1619XS+	D:\_DIG-12243_Narva_Elektrijaama_tee_59D\Synology Server RS1619XS+_SR00005
39	Synology Server RS1619XS+_SR00006	Narva	Synology Server RS1619XS+	D:\_DIG-12243_Narva_Elektrijaama_tee_59D\Synology Server RS1619XS+_SR00006
40	s.potapenko_1520000_2TB	Potapenko	2TB	D:\_S.Potapenko\s.potapenko_1520000_2TB



## APPENDIX 1

Device #	Name	Location	Type	Path
41	s.potapenko_1917232_USB	Potapenko	USB	D:\S.Potapenko\s.potapenko_1917232_USB
42	s.potapenko_1917233_2TB	Potapenko	2TB	D:\S.Potapenko\s.potapenko_1917233_2TB
43	s.potapenko_1917319_USB	Potapenko	USB	D:\S.Potapenko\s.potapenko_1917319_USB
44	s.potapenko_1917321-2xUSB	Potapenko	1917321-2xUSB	D:\S.Potapenko\s.potapenko_1917321-2xUSB
45	s.potapenko_1917322_1TB	Potapenko	1TB Drive	D:\S.Potapenko\s.potapenko_1917322_1TB
46	s.potapenko_5836152_macbookair	Potapenko	macbookair	D:\S.Potapenko\s.potapenko_5836152_macbookair
47	s.potapenko_6242215_macbookpro	Potapenko	macbookpro	D:\S.Potapenko\s.potapenko_6242215_macbookpro
48	S.Potapenko_G240616_iPad	Potapenko	iPad	D:\S.Potapenko\S.Potapenko_G240616_iPad
49	DELL	Potapova	DELL	D:\T.Potapova\T.Potapova LO PAPA\DELL
50	HP	Potapova	HP	D:\T.Potapova\T.Potapova LO PAPA\HP
51	LO fotod	Potapova	Photos	D:\T.Potapova\T.Potapova LO PAPA\LO fotod
52	T.Potapova_0322308_HP Probook	Potapova	HP Probook	D:\T.Potapova\T.Potapova_0322308_HP Probook
53	T.Potapova_1845057_Huawei	Potapova	Huawei	D:\T.Potapova\T.Potapova_1845057_Huawei
54	T.Potapova_1845061_iPhone 13 Pro Max	Potapova	iPhone 13 Pro Max	D:\T.Potapova\T.Potapova_1845061_iPhone 13 Pro Max
55	T.Potapova_6241854_Dell	Potapova	Dell	D:\T.Potapova\T.Potapova_6241854_Dell
56	T.Potapova-Cloud	Potapova	Cloud	D:\T.Potapova\T.Potapova-Cloud
57	1915619-hdd_2tb	Tartu Mnt 83	Toshiba hd	D:\_DIG-12166_Tartu-mnt\1915619-hdd_2tb
58	0001808251_Synology DS1517	Tartu Mnt 83	Synology DS1517	D:\_DIG-12166_Tartu-mnt\0001808251_Synology DS1517
59	0001808252_Dell Serverarvuti EMC PowereEdge	Tartu Mnt 83	Dell Serverarvuti EMC PowereEdge	D:\_DIG-12166_Tartu-mnt\0001808252_Dell Serverarvuti EMC PowereEdge
60	1915616-3xKetas	Tartu Mnt 83	3 Hard Drives	D:\_DIG-12166_Tartu-mnt\1915616-3xKetas
61	1915617_6USB	Tartu Mnt 83	6 USBs	D:\_DIG-12166_Tartu-mnt\1915617_6USB
62	1915618-1TB-HDD	Tartu Mnt 83	1TB HDD	D:\_DIG-12166_Tartu-mnt\1915618-1TB-HDD
63	1915620-4xketas	Tartu Mnt 83	4xdiscs	D:\_DIG-12166_Tartu-mnt\1915620-4xketas
64	1915621_2USB	Tartu Mnt 83	USB bitcoin miner	D:\_DIG-12166_Tartu-mnt\1915621_2USB
65	1915623_4USB	Tartu Mnt 83	USB	D:\_DIG-12166_Tartu-mnt\1915623_4USB
66	1917276_iPhone	Tartu Mnt 83	iPhone	D:\_DIG-12166_Tartu-mnt\1917276_iPhone
67	2133390_macbook_pro	Tartu Mnt 83	macbook pro	D:\_DIG-12166_Tartu-mnt\2133390_macbook_pro
68	2133391_macbook_pro_Potapenko	Tartu Mnt 83	macbook	D:\_DIG-12166_Tartu-mnt\2133391_macbook_pro_Potapenko
69	2133393_mac_mini	Tartu Mnt 83	mac mini	D:\_DIG-12166_Tartu-mnt\2133393_mac_mini
70	A463558_iMac	Tartu Mnt 83	iMac	D:\_DIG-12166_Tartu-mnt\A463558_iMac
71	G15-0436454_USB	Tartu Mnt 83	USB	D:\_DIG-12166_Tartu-mnt\G15-0436454_USB
72	G240578_iPhone14Pro	Tartu Mnt 83	iPhone14Pro	D:\_DIG-12166_Tartu-mnt\G240578_iPhone14Pro
73	G240584_Samsung_SSD_1TB	Tartu Mnt 83	Samsung SSD	D:\_DIG-12166_Tartu-mnt\G240584_Samsung_SSD_1TB
74	G240617_SamsungSSD_1TB	Tartu Mnt 83	SamsungSSD	D:\_DIG-12166_Tartu-mnt\G240617_SamsungSSD_1TB
75	G240618_500GB	Tartu Mnt 83	Toshiba HD	D:\_DIG-12166_Tartu-mnt\G240618_500GB
76	G240619_1TB	Tartu Mnt 83	Ledger?	D:\_DIG-12166_Tartu-mnt\G240619_1TB
77	G240620_4ese_ja_visiitkardid	Tartu Mnt 83	Chieftec External Storage	D:\_DIG-12166_Tartu-mnt\G240620_4ese_ja_visiitkardid
78	G240621_Ledger_ja_2xSD	Tartu Mnt 83	Ledger and USB	D:\_DIG-12166_Tartu-mnt\G240621_Ledger_ja_2xSD
79	G240622_2TB	Tartu Mnt 83	Western Digital 2TB	D:\_DIG-12166_Tartu-mnt\G240622_2TB
80	G240623_iPad	Tartu Mnt 83	iPad	D:\_DIG-12166_Tartu-mnt\G240623_iPad

## APPENDIX 1

Device #	Name	Location	Type	Path
81	G240624_SSD Samsung	Tartu Mnt 83	SSD Samsung	D:\_DIG-12166_Tartu-mnt\G240624_SSD Samsung
82	G240625_SamsungSSD_2TB	Tartu Mnt 83	SamsungSSD	D:\_DIG-12166_Tartu-mnt\G240625_SamsungSSD_2TB
83	G240628_iPhone14Pro	Tartu Mnt 83	iPhone14Pro	D:\_DIG-12166_Tartu-mnt\G240628_iPhone14Pro
84	014518_iMac	Tartu Mnt 83	iMac	D:\_DIG-12208_Felmaway\014518_iMac
85	014519_iMac	Tartu Mnt 83	iMac	D:\_DIG-12208_Felmaway\014519_iMac
86	014520_iMac Pro	Tartu Mnt 83	iMac Pro	D:\_DIG-12208_Felmaway\014520_iMac Pro
87	0322169-hp	Tartu Mnt 83	hp	D:\_DIG-12208_Felmaway\0322169-hp
88	1518630_USB	Tartu Mnt 83	USB	D:\_DIG-12208_Felmaway\1518630_USB
89	1915595_2xUSB	Tartu Mnt 83	2xUSB	D:\_DIG-12208_Felmaway\1915595_2xUSB
90	1915597_SonyXperia	Tartu Mnt 83	SonyXperia	D:\_DIG-12208_Felmaway\1915597_SonyXperia
91	1915600_iPhoneSE_punane	Tartu Mnt 83	iPhoneSE	D:\_DIG-12208_Felmaway\1915600_iPhoneSE_punane
92	1915601_Redmi	Tartu Mnt 83	Redmi	D:\_DIG-12208_Felmaway\1915601_Redmi
93	1915602_iPhoneSE	Tartu Mnt 83	iPhoneSE	D:\_DIG-12208_Felmaway\1915602_iPhoneSE
94	1915603_3xcards	Tartu Mnt 83	3xcards	D:\_DIG-12208_Felmaway\1915603_3xcards
95	1915605_USB_Intenso	Tartu Mnt 83	Intenso USB	D:\_DIG-12208_Felmaway\1915605_USB_Intenso
96	218683_HP Sylearvuti	Tartu Mnt 83	HP Sylearvuti	D:\_DIG-12208_Felmaway\218683_HP Sylearvuti
97	0001808441_LA	Tartu Mnt 83	Dreamline Tracer Asroc (PC)	D:\_DIG-13258_LO_Tartu-mnt_RUUMIST_503\0001808441_LA
98	1519993_myphone	Tartu Mnt 83	myphone	D:\_DIG-13258_LO_Tartu-mnt_RUUMIST_503\1519993_myphone
99	1833619_iPhone	Tartu Mnt 83	iPhone	D:\_DIG-13258_LO_Tartu-mnt_RUUMIST_503\1833619_iPhone
100	1844585_iPhone	Tartu Mnt 83	iPhone S	D:\_DIG-13258_LO_Tartu-mnt_RUUMIST_503\1844585_iPhone
101	1844620_iPhone	Tartu Mnt 83	iPhone	D:\_DIG-13258_LO_Tartu-mnt_RUUMIST_503\1844620_iPhone
102	218820_Lenovo	Tartu Mnt 83	Lenovo	D:\_DIG-13258_LO_Tartu-mnt_RUUMIST_503\218820_Lenovo
103	227002_macbook_pro	Tartu Mnt 83	macbook	D:\_DIG-13258_LO_Tartu-mnt_RUUMIST_503\227002_macbook_pro
104	227003_HP	Tartu Mnt 83	HP	D:\_DIG-13258_LO_Tartu-mnt_RUUMIST_503\227003_HP
105	227008_macbook_pro	Tartu Mnt 83	macbook	D:\_DIG-13258_LO_Tartu-mnt_RUUMIST_503\227008_macbook_pro
106	227009_macbook_pro	Tartu Mnt 83	macbook	D:\_DIG-13258_LO_Tartu-mnt_RUUMIST_503\227009_macbook_pro
107	227010_macbook_pro	Tartu Mnt 83	macbook	D:\_DIG-13258_LO_Tartu-mnt_RUUMIST_503\227010_macbook_pro
108	227011_macbook_pro	Tartu Mnt 83	macbook	D:\_DIG-13258_LO_Tartu-mnt_RUUMIST_503\227011_macbook_pro
109	227012_macbook_pro	Tartu Mnt 83	macbook	D:\_DIG-13258_LO_Tartu-mnt_RUUMIST_503\227012_macbook_pro
110	227044_mac-studio	Tartu Mnt 83	mac-studio	D:\_DIG-13258_LO_Tartu-mnt_RUUMIST_503\227044_mac-studio
111	227045_mac-studio	Tartu Mnt 83	mac-studio	D:\_DIG-13258_LO_Tartu-mnt_RUUMIST_503\227045_mac-studio
112	227046_macbook_pro	Tartu Mnt 83	macbook	D:\_DIG-13258_LO_Tartu-mnt_RUUMIST_503\227046_macbook_pro
113	227047_macbook_pro	Tartu Mnt 83	macbook	D:\_DIG-13258_LO_Tartu-mnt_RUUMIST_503\227047_macbook_pro
114	501-3.2-1_USB	Tartu Mnt 83	USB	D:\_DIG-13258_LO_Tartu-mnt_RUUMIST_503\501-3.2-1_USB
115	501-3.2-2_polybius.io_USB	Tartu Mnt 83	USB	D:\_DIG-13258_LO_Tartu-mnt_RUUMIST_503\501-3.2-2_polybius.io_USB
116	503-2.1_USB	Tartu Mnt 83	USB	D:\_DIG-13258_LO_Tartu-mnt_RUUMIST_503\503-2.1_USB
117	503-2.2_SanDisk_USB	Tartu Mnt 83	SanDisk USB	D:\_DIG-13258_LO_Tartu-mnt_RUUMIST_503\503-2.2_SanDisk_USB
118	C13-0072030_DELL	Tartu Mnt 83	DELL	D:\_DIG-13258_LO_Tartu-mnt_RUUMIST_503\C13-0072030_DELL
119	91R0A063F1QF	Tartu Mnt 83	DELL	D:\_DIG-13258_LO_Tartu-mnt_RUUMIST_503\C13-0072030_DELL\91R0A063F1QF
120	S455NA0N521972	Tartu Mnt 83	DELL	D:\_DIG-13258_LO_Tartu-mnt_RUUMIST_503\C13-0072030_DELL\S455NA0N521972

## APPENDIX 1

Device #	Name	Location	Type	Path
121	S455NA0N610317	Tartu Mnt 83	DELL	D:\_DIG-13258_LO_Tartu-mnt_RUUMIST_503\C13-0072030_DELL\S455NA0N610317
122	S455NA0N610322	Tartu Mnt 83	DELL	D:\_DIG-13258_LO_Tartu-mnt_RUUMIST_503\C13-0072030_DELL\S455NA0N610322
123	J13-0072029_Server Synology NAS	Tartu Mnt 83	Server Synology NAS	D:\_DIG-13258_LO_Tartu-mnt_RUUMIST_503\J13-0072029_Server Synology NAS
124	VRHU0EDK	Tartu Mnt 83	Server Synology NAS	D:\_DIG-13258_LO_Tartu-mnt_RUUMIST_503\J13-0072029_Server Synology NAS\VRHU0EDK
125	VRHUAXJK	Tartu Mnt 83	Server Synology NAS	D:\_DIG-13258_LO_Tartu-mnt_RUUMIST_503\J13-0072029_Server Synology NAS\VRHUAXJK
126	KT7900425_SSD	Tartu Mnt 83	SSD	D:\_DIG-13258_LO_Tartu-mnt_RUUMIST_503\KT7900425_SSD
127	KT7900427_iPhone	Tartu Mnt 83	iPhone	D:\_DIG-13258_LO_Tartu-mnt_RUUMIST_503\KT7900427_iPhone
128	KT7900429_Xiaomi	Tartu Mnt 83	Xiaomi	D:\_DIG-13258_LO_Tartu-mnt_RUUMIST_503\KT7900429_Xiaomi
129	KT7900430_Huawei LUA-L21	Tartu Mnt 83	Huawei LUA-L21	D:\_DIG-13258_LO_Tartu-mnt_RUUMIST_503\KT7900430_Huawei LUA-L21
130	KT7900431_iPhone_SE	Tartu Mnt 83	iPhone SE	D:\_DIG-13258_LO_Tartu-mnt_RUUMIST_503\KT7900431_iPhone_SE
131	KT7903736_Xiaomi_Redmi9A	Tartu Mnt 83	Xiaomi Redmi9A	D:\_DIG-13258_LO_Tartu-mnt_RUUMIST_503\KT7903736_Xiaomi_Redmi9A
132	D.Lazba-MacBook	Tartu Mnt 83	MacBook	D:\D.Lazba\D.Lazba-MacBook
133	I.Turogin-0647967-macbook	Turõgin	macbook	D:\I.Turogin\I.Turogin-0647967-macbook
134	I.Turogin-1520027-USB_32GB	Turõgin	USB 32GB	D:\I.Turogin\I.Turogin-1520027-USB_32GB
135	I.Turogin-1520029-USB_4GB	Turõgin	USB 4GB	D:\I.Turogin\I.Turogin-1520029-USB_4GB
136	I.Turogin-1520069-iPhone-WelcomeScreen	Turõgin	iPhone	D:\I.Turogin\I.Turogin-1520069-iPhone-WelcomeScreen
137	I.Turogin-1520070_iPhone-WelcomeScreen	Turõgin	iPhone-WelcomeScreen	D:\I.Turogin\I.Turogin-1520070_iPhone-WelcomeScreen
138	I.Turogin-1917215-WD	Turõgin	WD	D:\I.Turogin\I.Turogin-1917215-WD
139	I.Turogin-5836161-macbook_Pro	Turõgin	Macbook Pro	D:\I.Turogin\I.Turogin-5836161-macbook_Pro
140	I.Turogin-5836169-iPad	Turõgin	iPad	D:\I.Turogin\I.Turogin-5836169-iPad
141	i.turogin-5836171-macbookair	Turõgin	macbookair	D:\I.Turogin\i.turogin-5836171-macbookair
142	I.Turogin-5836172_iPad	Turõgin	iPad	D:\I.Turogin\I.Turogin-5836172_iPad
143	I.Turogin-665972_SSD	Turõgin	SSD	D:\I.Turogin\I.Turogin-665972_SSD

**ATTACHMENT B**

**Things to be Seized**

From the items listed in Attachment A of this warrant, the government is authorized to search for and seize the following items, which are evidence, instrumentalities, and/or fruits of violations of Title 18, United States Code, Sections, 1349, 1343, and 1956(h) from 2013 through 2022:

1. All material relating to any of the following business entities:
  - a. Burfa Media OÜ,
  - b. Burfa Capital OÜ (aka Starfix OÜ),
  - c. Burfa Tech OÜ (aka HashCoins OÜ),
  - d. Dalmeron Projects LP,
  - e. Polybius Foundation OÜ (aka Polybius Foundation SE, or Polybius Foundation AS),
  - f. HashFlare LP (aka HashCoins LP, or Fast Consult LP),
  - g. Advendor OÜ,
  - h. Polybius Fintech MidCo OÜ,
  - i. Polybius Tech OÜ,
  - j. Apico OÜ,
  - k. Felmaway OÜ; and
1. Ecohouse Networks OÜ, or any related entities;
2. All material relating to financial transactions involving Ivan Turõgin, Sergei Potapenko;
3. Financial documents, including, but not limited to, any evidence of the ownership, control or use of bank accounts or cryptocurrency wallets or accounts; wire transmissions and transfers of funds or assets, including cryptocurrency;
4. Cryptocurrency, cryptocurrency keys and wallets;

1 5. Any records or documentation related to the purchase, acquisition, or  
2 distribution of cryptocurrency, including keys, passwords, and recovery seed, or seed  
3 phrases;

4 6. Any records or documentation related to the purchase, sale acquisition, use,  
5 or lease of cryptocurrency mining equipment or capacity, including, but not limited to, the  
6 recipients or beneficiaries of any proceeds of any mining activity; and

7 7. Evidence sufficient to identify co-conspirators of Ivan Turōgin or Sergei  
8 Potapenko, including

9 a. Contact lists;

10 b. Telephone call history; and

11 c. Evidence of email or other online accounts, including passwords and  
12 account names.

13 8. The following digital forensic evidence associated with any devices  
14 identified in Appendix 1 to Attachment A:

15 a. Assigned phone number and identifying telephone serial number (ESN,  
16 MIN, IMSI, or IMEI);

17 b. Evidence of who used, owned, or controlled the digital device or other  
18 electronic storage media at the time the things described in this warrant  
19 were created, edited, or deleted, such as logs, registry entries, configuration  
20 files, saved usernames and passwords, documents, browsing history, user  
21 profiles, email, email contacts, “chat,” instant messaging logs, photographs,  
22 and correspondence;

23 c. Evidence of software that would allow others to control the digital device or  
24 other electronic storage media, such as viruses, Trojan horses, and other  
25 forms of malicious software, as well as evidence of the presence or absence  
26 of security software designed to detect malicious software;

27 d. Evidence of the lack of such malicious software;

- e. Evidence of the attachment to the digital device of other storage devices or similar containers for electronic evidence;
- f. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the digital device or other electronic storage media;
- g. Evidence of the times the digital device or other electronic storage media was used;
- h. Stored lists of recent received, sent, and missed calls;
- i. Stored contact information;
- j. Stored photographs, videos, addresses, calendar notes, notes, map history, or documents/files of or related to the misappropriation of assets from Majestic Glove, or any of its affiliated companies, including any embedded GPS data or other metadata associated with those photographs, videos, and other items;
- k. Stored web browsing history;
- l. Stored location data, including from any map applications.

**Persons Authorized to Review ESI**

This review of digital evidence may be conducted by any federal or local government personnel, sworn or non-sworn, assisting in the investigation, who may include, in addition to law enforcement officers and agents, federal and local contractors and support staff, attorneys for the government, attorney support staff, and technical experts. Pursuant to the requested warrant, the FBI may deliver a complete copy of the electronic data to the custody and control of attorneys for the government and their support staff for their independent review